RÉPUBLIQUE DU SÉNÉGAL
Un Peuple – Un But – Une Foi

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

UNIVERSITE CHEIKH ANTA DIOP DE DAKAR

FACULTE DES SCIENCES ET TECHNIQUES

DEPARTEMENT DE MATHEMATIQUES ET INFORMATIQUE
SECTION INFORMATIQUE

MÉMOIRE DE MASTER INFORMATIQUE

Spécialité : Réseaux et Télécommunications
Option : Réseaux, Systèmes et Services

Sujet : Les techniques d'authentification mutuelle basées sur la technologie blockchain

Présenté et soutenu publiquement par :

M. Ibrahima FALL

Encadré par Professeur **Cherif DIALLO**

Le : 03/Juin/2021

Pr. Karim KONATE	Professeur Titulaire, UCAD	Président
Dr. Ibrahima DIANE	Maître Assistant Titulaire, UCAD	Membre
Dr. Bassirou KASSE	Docteur Assistant vacataire, UCAD	Membre
Pr. Ibrahima NIANG	Professeur Titulaire, UCAD	Membre

Année universitaire 2019 – 2020

REMERCIEMENT

Au terme de ce modeste travail,

Tout d'abord, louange à notre seigneur « Allah » qui nous a guidé sur le droit chemin tout le long de cette expérience, nous a donné le courage et la volonté pour terminer ce travail et nous a inspiré les bons pas et les justes reflexes.

Par la suite, nous voudrions exprimer nos profondes gratitudes à notre encadreur Pr Cherif Diallo.

Nos vifs remerciements aux membres du jury d'avoir accepté d'examiner et d'évaluer notre travail. Un grand merci à tous les professeurs de la Section Informatique de l'université Cheikh Anta Diop de Dakar.

Enfin Nous tenons à remercier chaleureusement nos parents qui grâces à eux nous sommes arrivées là, à nos frères et sœurs qui avec leurs encouragements nous ont donné la volonté de travailler plus encore, et à nos amis qui étaient toujours présents à nos côtés dans les bons moments pour se réjouir avec nous et pour nous soulager dans les mauvais moments.

Dédicace

Je dédie ce modeste travail :

A mon exemple éternel, mon soutien moral et source de joie et de bonheur, celle qui s'est toujours sacrifiée pour me voir réussir, que dieu te garde dans son vaste paradis, à toi grande sœur **Alima FALL**.

A mon père, qui peut être fier de trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit. Merci pour les valeurs nobles, l'éducation et le soutien permanent venu de toi.

A ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçoit à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

A tous mes très chers frères Amadou, Moustapha, Meissa, Modou, Pape, Oumar, Ndiaga Matar, Mohamed, Youssou Diop et mes chères sœurs Aida, Sokhna, Mame Faly et ma cousine Fatou Kiné.

A tous mes amis Babacar, Amed Diop, Ibra, Dame….

A tous ceux que j'aime et qui m'aiment, mes tantes et mes oncles et ma famille.

A tous mes amis de l'université Cheikh Anta Diop de Dakar

Et à tous ceux qui sont proches de mon cœur et qui m'encouragent à donner le meilleur en moi.

Résumé

Une blockchain « ou chaîne de blocs » est un réseau permettant d'opérer des transactions en toute sécurité et sans l'intervention d'une partie tierce. Il s'agit d'un grand livre comptable public consignant les transactions de manière incontestable.

Les différents avantages que pourrait apporter la technologie Blockchain au secteur public, permettras la protection des données critiques, de pouvoir s'assurer de la propriété de biens, ou encore de créer un réseau puissant entre les différents services publics et surtout le stockage des données Ceci est fondamental pour plusieurs contextes au secteur publique.

Dans l'IoT, les objets traitent et échangent des données sans intervention humaine. Par conséquent, en raison de cette autonomie totale, ces entités doivent se reconnaître et s'authentifier mutuellement ainsi que garantir l'intégrité de leurs données échangées. Sinon, ils seront la cible d'utilisateurs malveillants et d'utilisation malveillante. En raison de la taille et des autres caractéristiques de l'IoT, il est presque impossible de créer un système d'authentification centralisé efficace.

Pour remédier à cette limite, dans cette étude, nous étudions un système des techniques d'authentification mutuelle basées sur la blockchain, ce qui garantit une identification et une authentification robustes des appareils. De plus, il protège l'intégrité et la disponibilité des données. Pour atteindre un tel objectif, les approches étudiées s'appuient sur les avantages de sécurité apportés par les blockchains, où les choses peuvent s'identifier et se faire confiance.

Mots clés : blockchain, transactions, IoT, authentification mutuelle,

Sommaire

Table des matières 5
Liste des figures 10
Liste des tableaux 11
Liste des abréviations 12

Chapitre 1: Présentation de la technologie Blockchain

1.1 Introduction.....15
1.2 Historique.....15
1.3 Définition.....16
1.4 Fonctionnement.....17
1.5 Les caractéristiques de la Blockchain.....19
1.5.1 Décentralisation.....22
1.5.2 Immuabilité.....22
1.5.3 Transparence 22
1.5.4 Efficacité.....22
1.5.5 Sécurité 23
1.5.6 Anonymat.....23
1.6 Les Composants de la Blockchain 23
1.6.1 Fonction de hachage cryptographique.....23
1.6.2 Nonce cryptographique.....24
1.6.3 Transactions.....24
1.6.4 Cryptographie des clés asymétrique.....24
1.6.5 Adressages et dérivations.....26
1.6.6 Stockage des clés privées.....26
1.7 Signature numérique.....28
1.8 Le mécanisme de consensus.....28

1.8.1 Proof of work (PoW)..... 30
1.8.2 Proof of stake (PoS)..... 31
1.8.3 Delegated Poof of Stake (DPos)..... 32
1.8.4 Pratical Byzantine Fault Tolerence..... 32
1.9 Evolution de la Blockchain..... 33
1.9.1 Blockchain 1.0..... 34
1.9.2 Blockchain 2.0..... 34
1.9.3 Blockchain 3.0..... 35
1.10 Types de Blockchain..... 36
1.10.1 Blockchain publique..... 37
1.10.2 Blockchain privée..... 40
1.10.3 Blockchain consortium..... 40
1.11 Application de la Blockchain..... 41
1.11.1 Banque..... 41
1.11.2 Soins de santé..... 42
1.11.3 Immobilier..... 42
1.11.4 IoT (internet of things)..... 44
1.11.5 Supply chain management..... 46
1.11.6 Gouvernement..... 46
1.11.7 Cybersécurité..... 47
1.11.8 Medias Sociaux..... 47
1.11.9 Intelligent Artificielle..... 47

1.12 Défis de la Blockchain..... 48
1.12.1 Défis techniques..... 48
1.12.1.1 Stockage..... 48
1.12.1.2 Sécurité..... 49
1.12.1.3 Confidentialité..... 49
1.13 Conclusion..... 51

Chapitre 2 :**Internet des objets et son intégration avec la Blockchain**

Chapitre 2

2.1 Introduction.....52
2.2 IoT.....52
2.3 Paradigme IoT.....53
2.4 Protocoles IoT.....58
2.5 Architecture IoT.....61
2.5.1 Architecture à trois couches.....61
2.5.2 Architecture à 5 couches.....61
2.5.3 Couche d'application.....62
2.6 Menaces et attaques dans l'IoT.....64
2.6.1 Botnet 66
2.6.2 Man In The Middle.....66
2.6.3 Injection par code 67
2.6.4 Déni de Service (DDoS) 67
2.7 Application de l'IoT.....68
2.7.1 Domotique.....69
2.7.2 Santé.....69
2.7.3 Agriculture intelligente.....70
2.7.4 Chaine d'approvisionnement.....70
2.7.5 Ville intelligente.....70
2.7.6 Réseau intelligent.....71
2.7.7 Voiture connectée.....71
2.7.8 Appareils portable.....72

2.8 Défis IoT.....72
2.8.1 Big data.....72
2.8.2 Réseau.....73
2.8.3 Hétérogénéité.....74
2.8.4 Interopérabilité.....74
2.8.5 Evolutivité.....74
2.8.6 Sécurisation et menaces de l'IoT.....74
2.9 Intégration avec Blockchain.....75
2.9.1 Besoin d'intégration de l'IoT et de la Blockchain.....75
2.9.2 Les défis de l'intégration.....76
2.9.3 Avantages de l'intégration.....77
2.10 Conclusion.....77

Chapitre 3 : Étude de solution d'authentification mutuelle existante basée sur la Blockchain

3.1 Introduction.....79
3.2 Présentation du projet 80
3.2.1 Problématique 80
3.2.2 Objectif 80
3.3 Utilisation de la blockchain pour la gestion de la confiance et de l'authentification dans l'IoT.....80
3.3.1 Utilisation de la blockchain pour contrôler les appareils IoT.....82
3.3.2 Comparaison.....83
3.3.3 Analyse 84
3.4 La solution Authenblue.....85
3.4.1 Phase de préparation.....86

3.4.2 Cryptage / Décryptage authentifié.....86
3.4.3 Personnalisation.....87
3.4.4 Association d'un appareil à un CPAN.....88
3.4.5 Chiffrement et déchiffrement authentifié.....90
3.5 Analyse.....91
3.6 conclusion.....91

Liste des figures.....

Figure 1.1 décrit l'histoire de la technologie blockchain de 1990 jusqu'à maintenant…....17

Figure 1.2 processus d'une transaction**.....18**

Figure 1.3 La structure d'une blockchain**.....19**

Figure 1.4 Exemple de fonctionnement Blockchain (Bitcoin) **.....20**

Figure 1.5 Chaîne de propriété de transaction**.....27**

Figure 1.6 Un exemple de code QR qui a encodé le texte «NISTIR 8202 - Présentation de la technologie Blockchain Exemple de code QR » **.....30**

Figure 1.7 signature numérique**.....32**

Figure 1.8 Blockchain publique**.....42**

Figure 1.9 Blockchain privée **.....43**

Figure 1.10 Blockchain consortium**.....43**

Figure 1.11 Les Applications de la Blockchain**.....45**

Figure 1.12 Défis de la blockchain**.....46**

Figure 2.1 Comparaison entre M2M et IoT**.....50**

Figure 2.2 Comparaison entre les objets connectés et la population mondiale**……..53**

Figure 2.3 Modèle de protocoles IoT**.....55**

Figure 2.4 Les trois couches de systèmes IoT : couche de perception, couche de réseau et couche d'application. Les couches se superposent et sont connectées aux couches adjacentes.

Figure 2.5 L'architecture à 3 couches à gauche et l'architecture à 5 couches à droite**…….59**

Figure 2.6 Attaque botnet**.....61**

Figure 2.7 Attaque Man In The Middle**.....63**

Figure 2.8 Attaque DDoS **.....66**

Figure 2.9 Défis de l'IoT**.....74**

Figure 3.1 : personnalisation**.....88**

Figure 3.2 : Élimination du mécanisme de liste noire lors de l'association d'un Appareil à un CPAN**.....90**

Figure 3.3 : Chiffrement et déchiffrement authentifiés**... .....91**

Liste des tableaux

Tableau 1.1 Exemples de texte d'entrée et de valeurs de résumé SHA-25 correspondantes**.....25**

Tableau 1.2 Champs dans une transaction **.....27**

Tableau 1.3 Comparaison entre Bitcoin et Ethereum**.....38**

Tableau 1.4 Comparaison entre contrats traditionnels et contrats intelligents **.....39**

Tableau 1.5 représente le tableau de comparaison des types de blockchain. **.....45**

Tableau 3.1 Comparaison entre les solutions proposées par les travaux connexes **.....84**

Tableau 3.2 phase de préparation dans le protocole Authenblue**.....87**

Tableau 3.3 Fonctions de cryptage / décryptage authentifiées**.....88**

Tableau 3.4 comparaison des solutions en termes de performance**.....86**

Tableau 3.5 Comparaison Authenblue avec d'autres solutions**.....92**

Liste des abréviations

EVM = Ethereum virtual machine
SHA256 = Secure hashing algorithm
PoW = Proof of work
PoS = Proof of stake
DPoS = Delagated Proof of Stake

DBFT = Delegated Byzantine Fault Tolerance

Dapp = decentralized Application

P2P = pair-to-pair

RFID = Radio frequency identification

IoT = Internet of Things

BCT = Blockchain technology

BATM = Blockchain Authentication and Trust Module

ECDSA = Elliptic Curve Digital Signature Algorithm

ETH = Ethereum

QR = Quick Response

RSA = Rivest-Shamir-Adleman

SHA = Secure Hash Algorithm

FIPS = Federal Information Processing Standard

WSN = Wireless Sensor Network

CPAN = Coordinators of Personal Area Network

LDAP = Light weight Directory Access Protocol

Introduction générale

La blockchain peut être utilisée car il s'agit d'un registre distribué, inviolable, non susceptible de corruption. Il a également la capacité de trouver les problèmes de sécurité critiques de l'IoT, principalement la fiabilité et l'intégrité des données. La blockchain donne accès à des logiciels pour envoyer et recevoir des transactions de données ou des événements de manière distribuée et fiable. De nos jours, la popularité de la blockchain augmente en raison de l'utilisation des affirmations numériques, contrats intelligents et stockage distributif.

Il y a eu un effort énorme ces dernières années pour tout adopter intelligemment à des fins personnelles, industrielles et sociales. Cela donne à l'Internet des objets (IoT) émergent plus d'impact, de potentiel et une large acceptation. Cependant, les problèmes de confidentialité et de sécurité entravent son adoption et son développement ultérieurs; ceci est principalement dû à sa dépendance à un cloud centralisé, à un brouillard, à des systèmes de détection d'intrusion, à un pare-feu et à un logiciel antivirus pour les données, le traitement des identités et la communication sécurisée. D'une part, les appareils IoT ont des failles d'authentification et d'autorisation dans le déploiement hétérogène et aussi relativement «vulnérables» face à des pirates malveillants en raison de contraintes de ressources. Si le seul appareil IoT est compromis, l'ensemble du réseau devient défectueux. Les défis des problèmes de sécurité sont de plus en plus nombreux par les autorités centrales ou des tiers comme le cloud, le brouillard, le pare-feu, etc. Pour fournir une technique cryptographique pour les problèmes d'authentification et de communication, pour éviter l'utilisation de l'autorité centrale, nous avons besoin d'une plate-forme décentralisée et cryptographiquement fort avec immuabilité.

La technologie émergente de la blockchain résout efficacement les problèmes et fournit des installations nouvelles supplémentaires telles que distribuées, visibles publiquement pour renforcer la sécurité.

Dans ce contexte et dans le cadre de notre projet de fin d’étude, on va organiser ce manuscrit de la façon suivant :

Dans le chapitre 1 introduit le concept du blockchain, ces caractéristiques, son fonctionnement, son évolution, ces composants et les champs d’application.

Dans le chapitre 2 nous allons analyser les concepts et les problèmes de sécurité de l’IoT et de son intégration avec la Blockchain.

Dans le chapitre 3 nous allons étudier les techniques d'authentification mutuelle utilisant la blockchain.

Contexte

La technologie Blockchain a le potentiel de sécuriser cet environnement grâce à la cryptographie, qui vise à ce que tous les consommateurs disposent d'une clé secrète unique permettant d'accéder à vos données.
Les protocoles ouverts basés sur Blockchain peuvent standardiser et automatiser les données en toute sécurité. De nombreux secteurs seraient les bénéficiaires de cette technologie, tels que la santé ou les secteurs du transport et de la logistique, qui pourraient également tirer de grands avantages de son utilisation pour intégrer les avantages de l'IoT.

Cette étude met l'accent sur la nécessité d'analyser toutes les informations à travers plusieurs études et recherches menées dans le domaine de l'IoT, de la Blockchain et de leur convergence, et présente les meilleures solutions d'authentification mutuelle basant sur la blockchain pour lutter contre les vulnérabilités des principales technologies faisant partie d'Internet des Objets.

1 Chapitre 1 : Étude de la technologie blockchain

1.1 Introduction

La protection des données sur Internet a toujours été un sujet qui a paniqué le Web: pas un jour ne se passe sans que les médias ne parlent de piratage de coordonnées bancaires ou de piratage de géants du e-commerce. C'est pourquoi les chercheurs se concentrent désormais sur le cryptage des données et les technologies de sécurité comme la blockchain.

Le 31 octobre 2008, un inconnu utilisant le pseudonyme «Satoshi Nakamoto [47]». A écrit dans une liste de diffusion pour les cypherpunks (un mouvement de personnes utilisant la cryptographie pour protéger la vie privée). : «Je travaille sur un nouveau système de monnaie électronique entièrement pair-à-pair, sans tiers de confiance». Ce texte est accompagné d'un lien vers Bitcoin.org et sur lequel est hébergé le livre blanc Bitcoin [46], rédigé dans un anglais clair, résumant le fonctionnement du nouveau protocole. Le premier concept Blockchain a été appliqué le 03 janvier 2009 dans le contexte du Bitcoin.

La technologie derrière Bitcoin et d'autres crypto-monnaies est une base de données de registre distribuée pour l'enregistrement des transactions, permettant aux utilisateurs de partager leur registre de transactions.

Dans ce chapitre, nous présentons et expliquons la technologie Blockchain avec ses fonctionnalités les plus importantes et les concepts associés.

1.2 Historique

Les prochaines années pour le bitcoin ont été tumultueuses, y compris l'effondrement de l'important échange de bitcoins, le mont. Gox et une réputation de plus en plus aigrie en tant que monnaie alimentant le bazar de drogue en ligne souterrain de la Route de la Soie. Mais de nombreuses entreprises ont vu une opportunité dans la technologie sous-jacente: la Blockchain, qui a rendu possible l'existence du bitcoin.

L'histoire de la technologie blockchain a ses racines dans les années 1980 et 1990 au 20ème siècle. Cependant, il est devenu largement reconnu en 2008 après la découverte de Bitcoin. Selon Marley Gray, directrice de la stratégie technologique pour les services financiers chez Microsoft, en 2008, une personne ou un groupe de personnes connu sous le nom de Satoshi Nakamoto a publié un article décrivant le bitcoin et comment il pourrait être utilisé pour la numérisation. Envoyez des paiements entre deux entités consentantes sans avoir recours à une institution financière tierce. Chaque transaction a été enregistrée dans le registre Blockchain, le bloc le plus récent étant lié à ceux précédant l'utilisation d'une signature numérique. Pour garantir la confiance dans le grand livre, les participants du réseau ont exécuté des algorithmes complexes pour vérifier ces signatures numériques et ajouter des transactions à la blockchain.

Selon Pilkington, la première notion de monnaie numérique a été inventée sur la base d'un serveur centralisé pour éviter les doubles dépenses, qui consiste à utiliser plus d'une fois les mêmes bitcoins. Cependant, cette perception n'a pas permis de résoudre les problèmes de double dépense, d'anonymat et de centralisation.

Le monde reste plusieurs années à utiliser l'architecture centralisée qui utilise un tiers pour contrôler et maintenir la confiance entre les parties de communication jusqu'à Szabo à la fin de 1990 a inventé une monnaie numérique décentralisée appelée bit gold. Après environ 10 ans, la crypto-monnaie Bitcoin a été présentée. La blockchain est devenue largement populaire après le papier légendaire de Nakamoto. Il a proposé de remplacer l'architecture centralisée classique par une nouvelle technique basée sur un mécanisme de consensus. Initialement, la technologie a été nommée blockchain comme deux mots «bloc» et «chaîne»; cependant, par 2016, deux mots sont combinés en un seul mot pour être ce que nous savons tous maintenant blockchain.

Pendant la période du 2011 à 2013, la blockchain est largement utilisée dans les crypto-monnaies, en particulier dans le transfert de devises et le paiement numérique. De nos jours, la technologie blockchain a émergé dans diverses applications et services pour utiliser les fonctionnalités de décentralisation et d'immuabilité [1].

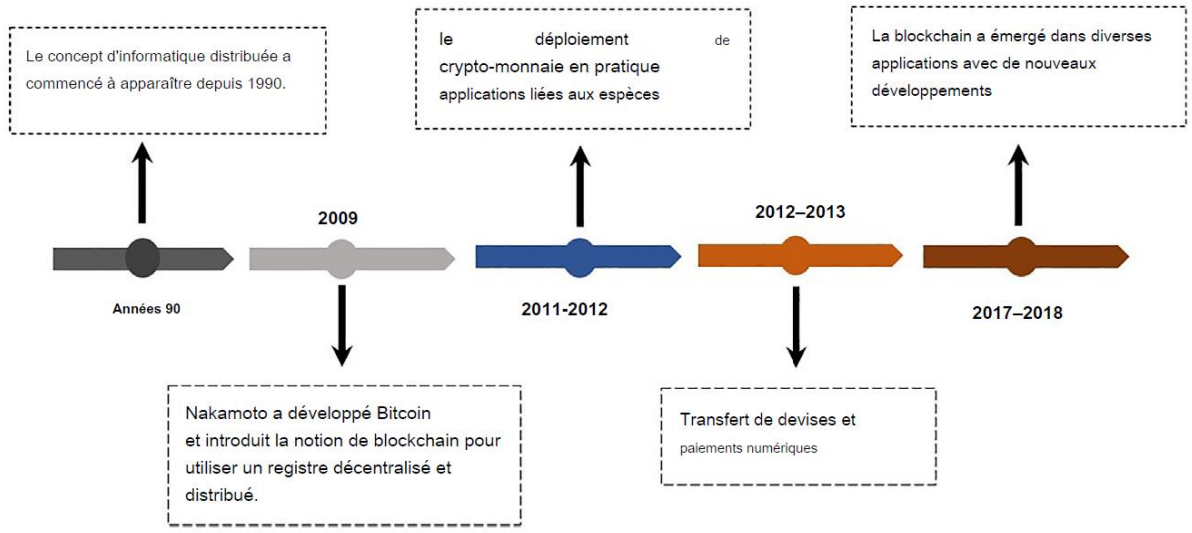


Fig.1.1 décrit l'histoire de la technologie blockchain de 1990 jusqu'à maintenant [1].

1.3 Définition de la blockchain

La blockchain fait référence à une chaîne de blocs sur laquelle sont stockées des informations de toutes sortes. La blockchain est généralement définie comme "une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe de contrôle central". La blockchain est une technologie de grand livre distribué, ou DLT (Distributed Ledger Technology), qui rassemble des systèmes numériques qui enregistrent les transactions d'actifs et leurs détails à plusieurs endroits à la fois. La blockchain est la technologie DLT la plus connue. [66]

Une blockchain est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs, depuis sa création. Pour la représenter, l'image du grand livre est fréquemment utilisée: la blockchain peut être comparée à un vaste registre public intégrant tous les échanges effectués par ses utilisateurs depuis sa création. L'une de ses principales caractéristiques est qu'elle ne peut pas être modifiée. Les blocs sont protégés par plusieurs méthodes cryptographiques innovantes qui rendent la modification a posteriori impossible5. C'est ce qui donne à cette technologie son caractère transparent : on peut uniquement ajouter des opérations, mais pas les modifier ni les supprimer, elles sont infalsifiables.

Cette technologie repose sur un système pair-à-pair décentralisé: les données ne sont pas hébergées par un seul serveur mais réparties entre les utilisateurs, sans intermédiaire. Certains utilisateurs détiennent des copies de la blockchain, qui est donc présente partout dans le monde. Ces centaines d'exemplaires sont constamment mis à jour simultanément. Contrairement aux bases de données traditionnelles, qui sont administrées par des opérateurs centralisés, la blockchain est administrée collectivement, par tous les nœuds du réseau. Ces nœuds obéissent tous au même protocole

informatique, qui définit les procédures à suivre, ainsi que les conditions à respecter pour mettre à jour la base de données. [68]

Concrètement, la technologie blockchain prend la forme d'un registre qui identifie des données, généralement des transactions, regroupées en blocs liés. Un bloc est simplement une collection d'informations réunies, et les blocs sont liés de manière irréversible (par des chaînes). Chaque bloc est validé par les nœuds du réseau, des utilisateurs-validateurs appelés «mineurs». Une fois validés, les blocs sont horodatés et intégrés dans la blockchain, accessible à tous les utilisateurs. La transaction est alors visible par le destinataire ainsi que par l'ensemble du réseau. Les mineurs sont payés via des jetons. La seule façon de modifier la blockchain est d'ajouter un bloc: il n'est pas possible de changer un bloc existant ou de modifier les chaînes.

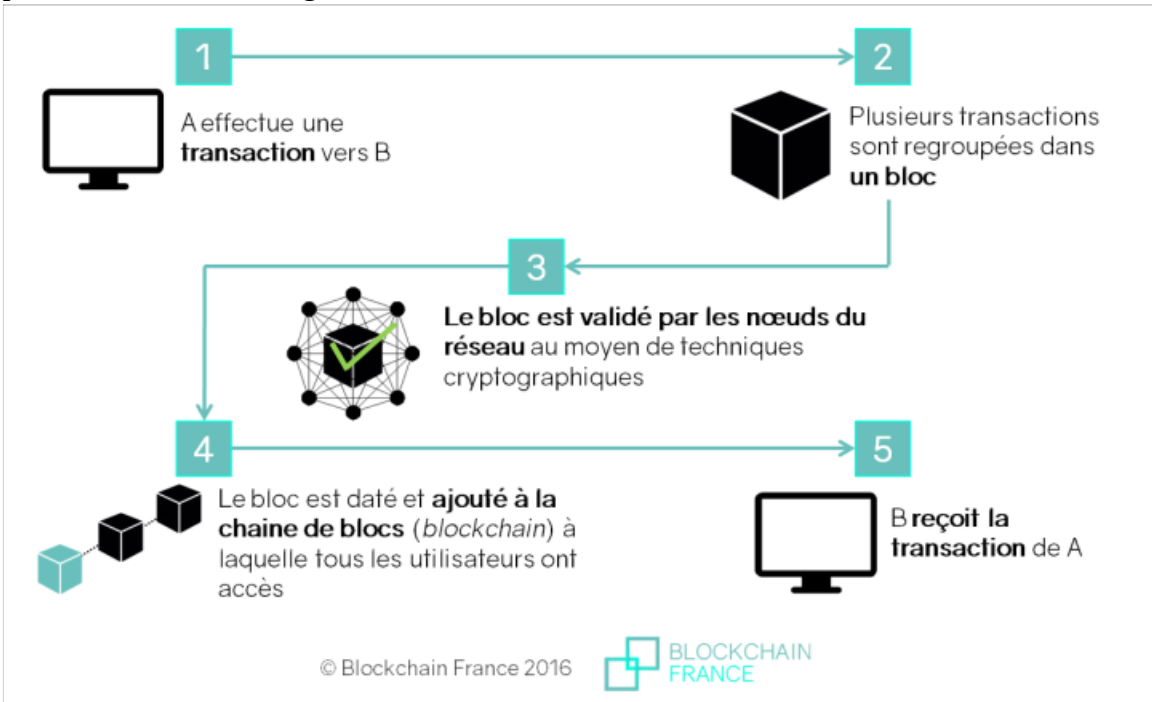


Fig.1.2 : processus d'une transaction

Source (Blockchain France)

Plusieurs caractéristiques sont associées à la blockchain: désintermédiation, traçabilité, transparence, consensus distribué, indélébile, structure distribuée, résilience, sécurité et confiance. Toutes ces caractéristiques constituent le potentiel innovant de la blockchain.

1.4 Fonctionnement de la Blockchain

Bitcoin repose sur un protocole sous-jacent appelé blockchain. On parle de blockchain car les transactions effectuées entre les utilisateurs du réseau sont regroupées par bloc «horodaté».

Une fois le bloc validé, en moyenne toutes les dix minutes, la transaction devient visible par tous les titulaires de registre, potentiellement tous les utilisateurs, qui l'ajouteront ensuite à leur blockchain. [1]

Chaque transaction utilise une cryptographie asymétrique, apparue avec le protocole Diffie-Hellman en 1976, qui fonctionne avec une paire de clés, l'une privée et l'autre publique, reliées entre elles par un algorithme de courbe elliptique (ECDSA). La clé publique peut être diffusée et permet de recevoir des transactions, la clé privée est gardée secrète. Protéger vos clés privées est le seul moyen de protéger vos bitcoins. Étant donné que toutes les transactions d'un propriétaire de clé publique peuvent être tracées, il s'agit davantage d'un pseudonyme que d'un système anonyme. La datation des blocs ainsi formés est appelée "horodatage".[1]

Chaque bloc, en plus des transactions et de l'horodatage, possède un identifiant (boîte noire du bloc 90 dans le schéma ci-dessous), qui se présente sous la forme d'un "hash" permettant de relier les blocs les uns aux autres. En informatique, le «hachage» convertit tout ensemble de données numériques en un hachage, c'est-à-dire en une courte séquence binaire qui lui est propre. L'algorithme de chiffrement utilisé à cet effet est appelé "fonction de hachage cryptographique". Le hachage d'un ensemble de données peut ainsi être comparé à une empreinte digitale, beaucoup moins complexe que l'individu dans son ensemble, mais l'identifiant de manière précise et unique. Une fonction de hachage est dite "unidirectionnelle": elle est conçue de telle sorte que le hachage produit, à savoir une image ou une empreinte de taille fixe créée à partir de données de taille variable, fournies en entrée, n'est pas possible. Celle utilisée pour le bitcoin est parmi les plus répandues: il s'agit de la fonction Secure Hash Algorithm-256 (SHA-256), ainsi appelée car elle produit des hachages d'une taille de 256 bits.[1]

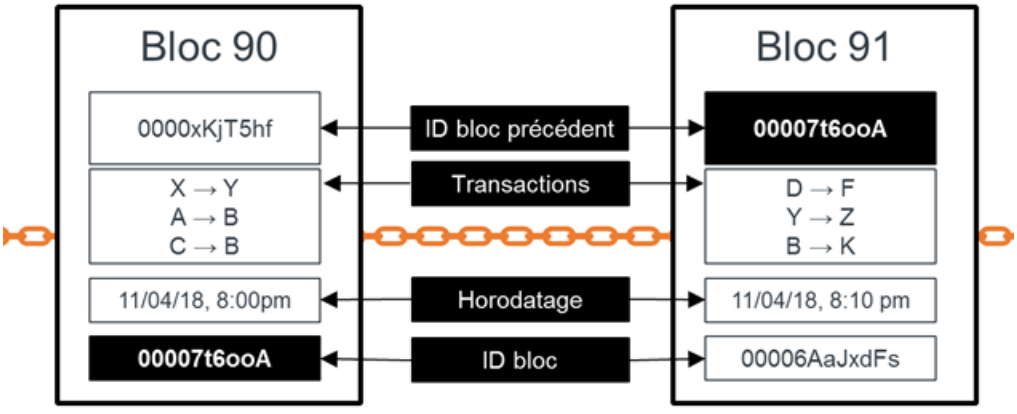


Figure1.3 : La structure d'une *blockchain*

Prenons le cas d'une opération réalisée sur la blockchain la plus ancienne et la plus courante, Bitcoin, qui a servi de modèle à toutes celles qui ont suivi. [66]

1) Osama veut envoyer 1 Bitcoin à Ilham sur le réseau Bitcoin, chacun a une adresse publique, appelée. «Clé publique» (l'équivalent. D'un RIB): une séquence d'environ 34 caractères contenant des chiffres et des lettres en minuscules ou majuscules (par exemple: 13o7TCoNWbaqYp9g89w1gHrZ7GvvKftRsd, pour l'un et 16Xgsii16x4icN7yjQg.XXl648d19 l'autre).

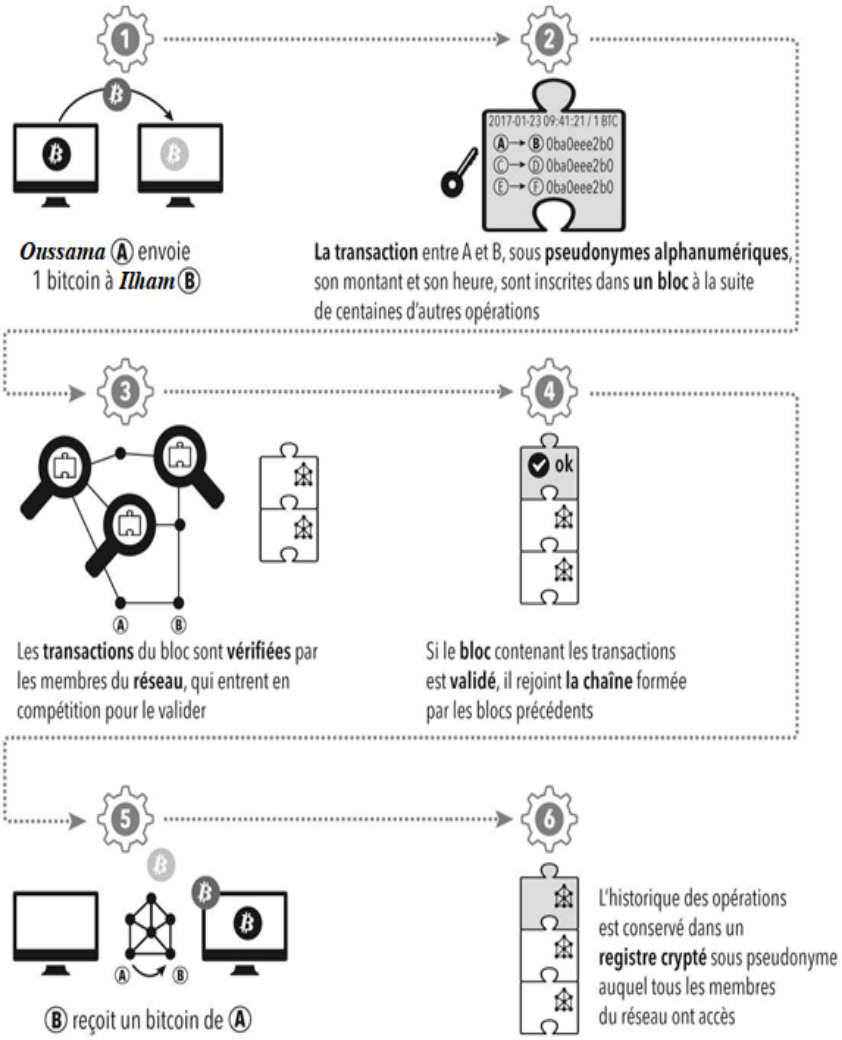


Figure 1.4 : Exemple de fonctionnement Blockchain (Bitcoin)

SOURCE : https://bitcoin.org

2) Oussama signer la transaction avec sa clé privée: une autre série de chiffres et de lettres, cette fois confidentielle (c'est. l'équivalent numérique de la clé de votre coffre-fort que vous ne donnez pas à perdre), qui Autorise les (points 1et 2 correspondant à l'étape 1 du schéma de la figure)

3) La transaction est ensuite écrite dans la blockchain. Il est entré, à la suite d'autres transactions, dans ce qu'on appelle un bloc (une grappe de. Plusieurs centaines, voire des milliers de transactions).
Pour chaque transaction, différentes informations apparaissent et peuvent donc être consultées par tous les membres du réseau:

- les clés publiques d'Oussama et d'Ilham: les transactions ne sont donc pas anonymes, mais effectuées sous les pseudonymes qui les constituent ces clés publiques;
- le nombre de Bitcoins transférés d'Oussama à Ilham: 1;
- l'heure précise, à la seconde près, et la date à laquelle l'opération a eu lieu (2019-07-12, 09:41:21).

4) Chaque bloc, en plus de toutes ces transactions, contient un résumé cryptographique du bloc précédent: un nombre, qui correspond à l'unique résultat possible qui est obtenu lors de la saisie des informations du bloc précédent dans une fonction appelée SHA256 (appelée le hachage ou le résultat d'un algorithme de hachage). Cela permet de noter l'ADN cryptographique du bloc précédent dans chaque bloc. Ainsi, si un hacker veut modifier a posteriori les informations d'un bloc, il devra corriger tous les blocs qui suivent, et ce sur chaque copie de la blockchain hébergée par chaque ordinateur du réseau (ce qui est Presque impossible) par ce système, les blocs sont donc enchaînés les uns aux autres (d'où le nom "Blockchain" - points 3 et 4 correspondant à Étape 2 du schéma de la figure)

5) Les membres du réseau qui le souhaitent concourront alors pour valider le blocage. Ils sont appelés «mineurs». Ils sont encouragés à le faire par. une récompense: celui qui a le privilège d'effectuer cette validation gagnera automatiquement 12,5 nouveaux Bitcoins, qui seront générés pour l'occasion par le système. Pour obtenir ce droit, tous les participants vérifieront la véracité des informations contenues dans toutes les transactions du bloc: Osama a-t-il réellement 1 Bitcoin au vu de toutes les transactions qu'il a déjà effectuées? N'utilise-t-il ce Bitcoin qu'une seule fois? Les autres transactions sont-elles justes? Mais, ils devront également résoudre un problème mathématique complexe, en utilisant les capacités de calcul de leur ordinateur (c'est le système de «preuve de travail»). Chaque ordinateur testera des solutions jusqu'à ce qu'il trouve la bonne. Le premier à réussir pourra valider le blocage et remporter la récompense. Le système a été conçu pour qu'une solution puisse être trouvée au bout de 10 minutes en moyenne (ce qui impose un léger retard dans la sécurisation de la transaction - point correspondant à l'étape 3 du schéma de la figure).
Le bloc est alors validé. Il est ajouté à la blockchain qui est mise à jour sur les ordinateurs de chaque participant (point correspondant à l’étape 4 du schéma de la figure).

6) Les participants n'acceptent ce nouveau bloc que si les transactions qu'il contient sont valides (si l'argent de chaque transaction n'est bien dépensé qu'une seule fois). Si le bloc est valide, ils expriment leur accord en travaillant sur le bloc suivant selon le même processus, et en entrant le hachage du bloc validé. C'est ce qu'on appelle un système de consensus.

7) Ilham a maintenant reçu le Bitcoin envoyé par Osama. En récompense du travail effectué, le mineur reçoit une certaine quantité de crypto-monnaie créée pour l'occasion (12,5 Bitcoins à ce jour, mais ce rendement diminue avec le temps).

1.5 Les caractéristiques de la Blockchain

1.5.1 Décentralisation

Dans un réseau centralisé traditionnel, les nœuds doivent être validés via un serveur centralisé de confiance. Cette approche pose un problème de retard de communication dans l'ensemble du système et augmente les coûts de calcul. La blockchain se compose de blocs pair-à-pair sans la participation d'un tiers. Cela signifie que la blockchain n'a pas besoin de s'appuyer sur un serveur centralisé pour stocker et mettre à jour plusieurs systèmes. Dans ce réseau distribué, tous les participants ou nœuds participent activement aux transactions avec un serveur décentralisé et slash le serveur [19].

1.5.2 Persistance

Toutes les transactions sont vérifiées dans la blockchain et les mineurs honnêtes stockent les données de transaction. Si les transactions sont incluses dans la liste, il est difficile de revenir en arrière ou d'effacer les transactions [19]. De plus, ces blocs sont également validés par d'autres mineurs, ils ne peuvent donc pas être manipulés.

1.5.3 Auditable

Toutes les transactions de la blockchain seront signées numériquement par l'expéditeur, enregistrant le bloc avec l'horodatage, ce qui permettra aux utilisateurs de suivre et de vérifier facilement les informations de transaction.

1.5.4 **Anonymat**

Dans la blockchain, les données sont sécurisées à l'aide de techniques de cryptage asymétrique. Pour authentifier le destinataire, tous les paiements sont signés numériquement. L'expéditeur interagit avec la blockchain pour prendre en charge un e-mail auto-généré et génère un ensemble d'adresses différent pour préserver son identité en tant que secret. Par conséquent, un propriétaire centralisé conservera les véritables identités de l'utilisateur; la divulgation de l'identité de l'expéditeur sera réduite au minimum [19].

1.5.5 **Autonome**

Comme il n'y a pas d'entité unique contrôlant le réseau blockchain, nous pouvons publier les nœuds signés et les examiner si d'autres nœuds les acceptent dans le réseau décentralisé. La base de consensus est venue en acceptant un nœud par tous les autres nœuds du réseau, garantissant que le transfert de données se fera en toute sécurité dans la blockchain [19].

1.5.6 **Immuabilité**

Les données de transaction sont validées avant d'être acceptées dans le bloc [20]. La blockchain enregistre en permanence les transactions. Les données des blocs ne peuvent pas être altérées. Si quelqu'un essaie de modifier les données, cela serait facilement attrapé car les données des blocs sont liées via la clé de hachage et la modification des données invaliderait les blocs suivants.

1.5.7 **Transparence**

La blockchain est une structure décentralisée où tous les participants peuvent publier leurs enregistrements et interroger les données des nœuds. Dans cette technologie blockchain, le système enregistre et maintient les informations de données de transaction dans un registre distribué ouvert [19]. Ces données sont ouvertes et fiables à tous les nœuds présents dans le même réseau pour accéder aux informations.

1.5.8 **Traçabilité**

Les données des blocs de la blockchain sont cryptées à l'aide d'algorithmes de hachage. Chaque bloc aura une clé de hachage. Chaque bloc du réseau contient la clé de hachage des blocs précédents

et est lié à travers eux [20]. Par conséquent, le traçage du bloc via la clé de hachage est confortable dans le réseau blockchain.

1.6 Les composants de la Blockchain

La technologie Blockchain peut sembler complexe; cependant, il peut être simplifié en examinant chaque composant individuellement. À un niveau élevé, la technologie de la Blockchain utilise des mécanismes informatiques bien connus et des primitives cryptographiques (fonctions de hachage cryptographique, signatures numériques, cryptographie à clé asymétrique) mélangées à des concepts de tenue de registres (tels que l'ajout de registres uniquement). Cette section traite de chaque composant principal individuel: fonctions de hachage cryptographique, transactions, cryptographie à clé asymétrique, adresses, registres, blocs et comment les blocs sont enchaînés.

1.6.1 Fonctions de hachage cryptographique

Un élément important de la technologie blockchain est l'utilisation de fonctions de hachage cryptographique pour de nombreuses opérations. Hashing est une méthode d'application d'une fonction de hachage cryptographique aux données, qui calcule une sortie relativement unique (appelée résumé de message, ou juste digérer) pour une entrée de presque n'importe quelle taille (par exemple, un fichier, un texte ou une image). Il permet aux individus de prendre indépendamment les données d'entrée, de hacher ces données et de dériver le même résultat - prouvant qu'il n'y a eu aucun changement dans les données. Même le plus petit changement à l'entrée (par exemple, changer un seul bit) entraînera un résumé de sortie complètement différent. [65]

Les fonctions de hachage cryptographique ont ces propriétés de sécurité importantes:

1) Ils sont résistants à la préimage. Cela signifie qu'ils sont à sens unique, donc il est mathématiquement impossible de calculer la valeur d'entrée correcte étant donné une valeur de sortie (par exemple trouver X tel que hash(X) =digérer)

2) Elles sont préimage résistant. Cela signifie que l'on ne peut pas trouver une entrée hachée sur une sortie spécifique. Plus spécifiquement, les fonctions de hachage cryptographiques sont conçues de telle sorte que, étant donné une entrée spécifique, il est impossible de trouver une deuxième entrée qui produit la même sortie (par exemple, étant donné X, trouver y tel que hash (x) = hacher(y)). La seule approche disponible est de rechercher de

manière exhaustive l'espace d'entrée, mais cela est impossible d'un point de vue informatique avec toute chance de succès. [5]

3) Elles sont résistantes aux collisions. Cela signifie que l'on ne peut pas trouver deux entrées qui hachent vers la même sortie. Plus spécifiquement, il est impossible de trouver deux entrées qui produisent le même condensé (par exemple, trouver un X et y quel hachage (x) = hacher(y)).

Une fonction de hachage cryptographique spécifique utilisée dans de nombreuses implémentations de blockchain est l'algorithme de hachage sécurisé (SHA) avec une taille de sortie de 256 bits (SHA-256). De nombreux ordinateurs prennent en charge cet algorithme dans le matériel, ce qui le rend rapide à calculer. SHA-256 a une sortie de 32 octets (1 octet = 8 bits, 32 octets = 256 bits), généralement affichée sous la forme d'une chaîne hexadécimale de 64 caractères (voir le tableau 1 ci-dessous).

Cela signifie qu'il y a $2^{256} \approx 10^{77}$ ou 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 valeurs de résumé possible. L'algorithme pour SHA-256, ainsi que d'autres, est spécifié dans la norme FIPS (Federal Information Processing Standard) 180-4 [5]. Le site Web NIST Secure Hashing [6] contient des spécifications FIPS pour tous les algorithmes de hachage approuvés par le NIST.

Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Tableau 1.1: Exemples de texte d'entrée et de valeurs de résumé SHA-25 correspondantes

Puisqu'il existe un nombre infini de valeurs d'entrée possibles et un nombre fini de valeurs de résumé de sortie possibles, il est possible, mais hautement improbable, d'avoir une collision où hash (x) = hacher(y) (c'est-à-dire que le hachage de deux entrées différentes produit le même condensé). SHA-256 est dit résistant aux collisions, car pour trouver une collision dans SHA-256, il faudrait exécuter l'algorithme, en moyenne, environ 2^{128} fois (ce qui fait 340 indécillions, ou plus précisément 340,282,366,920,938,463,463,374,607,431,768,211,456; ou 3.402×10^{38}).

Au sein d'un réseau blockchain, les fonctions de hachage cryptographique sont utilisées pour de nombreuses tâches, telles que:

1) Déviation d'adresse
2) Identifiant unique
3) Sécurisation des données de bloc (un nœud de publication hachera les données de bloc, créant un condensé qui sera stocké dans l'en-tête de bloc).
4) Sécurisation de l'en-tête de bloc

Il existe de nombreuses familles de fonctions de hachage cryptographiques utilisées dans la technologie blockchain (SHA-256 n'est pas le seul), comme Keccak (qui a été sélectionné par le NIST comme le gagnant d'un concours pour créer le standard de hachage SHA-3) comme RIPEMD-160. [6]

1.6.2 Nonce cryptographique

Un nonce cryptographique est un nombre arbitraire qui n'est utilisé qu'une seule fois. Un nonce cryptographique peut être combiné avec des données pour produire différents condensés de hachage par nonce:

Hash (data + nonce) = condensé

Seule la modification de la valeur nonce fournit un mécanisme pour obtenir différentes valeurs de résumé tout en conservant les mêmes données. Cette technique est utilisée dans le modèle de consensus de preuve de travail.

1.6.3 Transactions

Les transactions sont stockées dans les fichiers appelés blocs. Ils sont cryptés et sont généralement liés à des transactions précédentes, formant ainsi une chaîne. Un propriétaire d'une valeur (devise numérique dans BC Bitcoin) signe numériquement la transaction précédente avec sa clé publique et crée un hachage. Le propriétaire de la transaction précédente signe alors le hachage avec sa clé privée. [65]

La figure 1.5 illustre une version simplifiée de la chaîne de propriété. Dans des cas plus complexes, le nombre d'entrées et des sorties peuvent être multiples. Une transaction contient un certain nombre de champs, comme indiqué dans le tableau 1.2.

Tableau 1.2: Champs dans une transaction

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1-9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1-9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

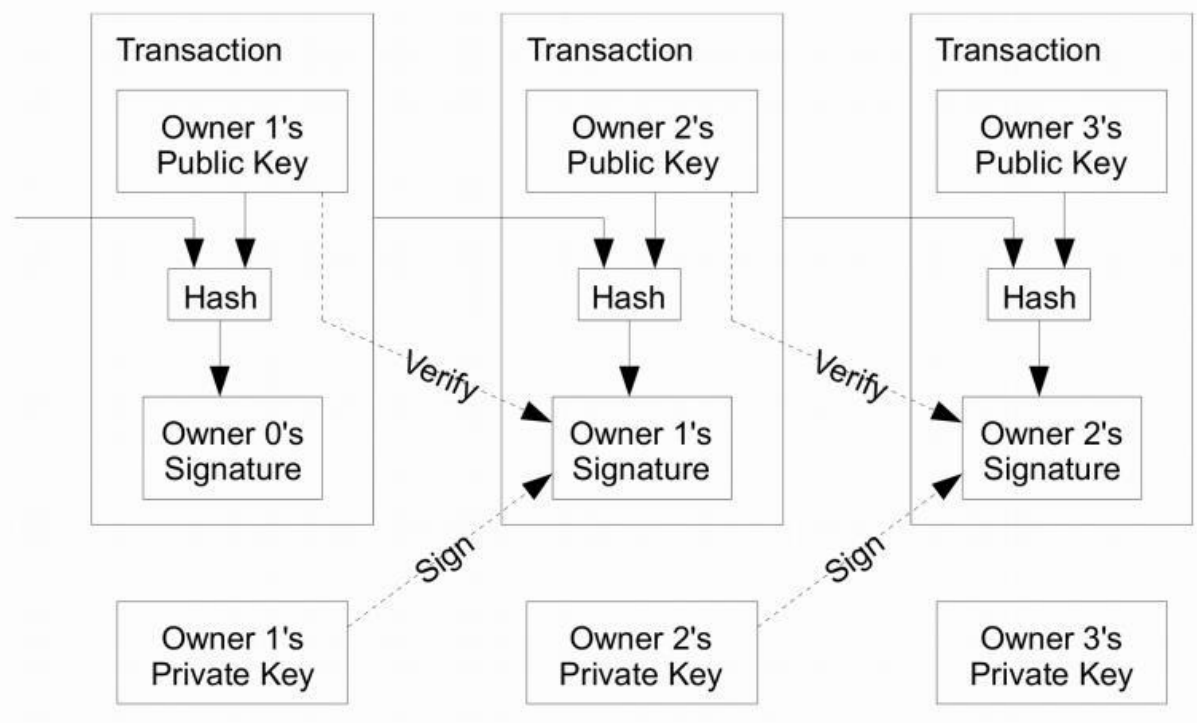


Figure 1.5 : Chaîne de propriété de transaction

Dans Blockchain Bitcoin la transaction est un transfert de valeur Bitcoin qui diffuse sur le réseau et est collecté en blocs. Les transactions ne sont pas cryptées. Il est donc possible d'afficher chaque transaction collectée dans un bloc. Elles sont regroupées en blocs et exécutées sur tous les nœuds participants.

1.6.4 Cryptographie à clé asymétrique

La technologie blockchain utilise la cryptographie à clé asymétrique (également appelée cryptographie à clé publique). La cryptographie à clé asymétrique utilise une paire de clés: une clé publique et une clé privée qui sont mathématiquement liées l'une à l'autre. La clé publique est rendue publique sans réduire la sécurité du processus, mais la clé privée doit rester secrète si les données doivent conserver leur protection cryptographique. Même s'il existe une relation entre les deux clés, la clé privée ne peut pas être déterminée efficacement en fonction de la connaissance de la clé publique. On peut crypter avec une clé privée puis décrypter avec la clé publique. Alternativement, on peut crypter avec une clé publique puis décrypter avec une clé privée. [10]

La cryptographie à clé asymétrique permet une relation de confiance entre des utilisateurs qui ne se connaissent pas ou ne se font pas confiance, en fournissant un mécanisme pour vérifier l'intégrité et l'authenticité des transactions tout en permettant aux transactions de rester publiques. Pour ce faire, les transactions sont «signées numériquement». Cela signifie qu'une clé privée est utilisée pour crypter une transaction afin que toute personne disposant de la clé publique puisse la décrypter. La clé publique étant librement disponible, le chiffrement de la transaction avec la clé privée prouve que le signataire de la transaction a accès à la clé privée. Alternativement, on peut chiffrer les données avec la clé publique d'un utilisateur de sorte que seuls les utilisateurs ayant accès à la clé privée puissent la déchiffrer. Un inconvénient est que la cryptographie à clé asymétrique est souvent lente à calculer. [11]

Cela contraste avec la cryptographie à clé symétrique dans laquelle une seule clé secrète est utilisée à la fois pour crypter et décrypter. Avec la cryptographie à clé symétrique, les utilisateurs doivent déjà avoir une relation de confiance établie les uns avec les autres pour échanger la clé pré-partagée. Dans un système symétrique, toute donnée chiffrée qui peut être déchiffrée avec la clé pré-partagée confirme qu'elle a été envoyée par un autre utilisateur ayant accès à la clé pré-partagée; aucun utilisateur sans accès à la clé pré-partagée ne pourra voir les données décryptées. Comparée à la cryptographie à clé asymétrique, la cryptographie à clé symétrique est très rapide à calculer. Pour cette raison, quand on prétend crypter quelque chose en utilisant la cryptographie à clé asymétrique, souvent les données sont cryptées avec une cryptographie à clé symétrique, puis la clé symétrique est cryptée à l'aide de la cryptographie à clé asymétrique. [10]

Voici un résumé de l'utilisation de la cryptographie à clé asymétrique dans de nombreux réseaux blockchain:

1) Les clés privées sont utilisées pour signer numériquement les transactions.
2) Les clés publiques sont utilisées pour dériver des adresses.
3) Les clés publiques sont utilisées pour vérifier les signatures générées avec des clés privées.
4) La cryptographie à clé asymétrique permet de vérifier que l'utilisateur transférant la valeur à un autre utilisateur est en possession de la clé privée capable de signer la transaction.

Certains réseaux de blockchain autorisés peuvent tirer parti de l'infrastructure de clé publique existante d'une entreprise pour la cryptographie à clé asymétrique afin de fournir les informations d'identification de l'utilisateur - plutôt que de laisser chaque utilisateur du réseau de blockchain gérer ses propres clés asymétriques. Cela se fait en utilisant les services d'annuaire existants et en utilisant ces informations dans le réseau blockchain. Les réseaux blockchain qui utilisent un service d'annuaire existant peuvent y accéder via des protocoles existants, tels que le protocole LDAP (Light weight Directory Access Protocol) [10], et utiliser les informations de l'annuaire de manière native, ou les importer dans une autorité de certification interne au sein du réseau blockchain.

1.6.5 Adressages et dérivation d'adresses

Certains réseaux blockchain utilisent un adresse, qui est une courte chaîne alphanumérique de caractères dérivés de la clé publique de l'utilisateur du réseau blockchain à l'aide d'une fonction de hachage cryptographique, ainsi que des données supplémentaires (par exemple, numéro de version, sommes de contrôle). La plupart des implémentations de blockchain utilisent des adresses comme points de terminaison «à» et «de» dans une transaction. Les adresses sont plus courtes que les clés publiques et ne sont pas secrètes. [69]Une méthode pour générer une adresse consiste à créer une clé publique, à lui appliquer une fonction de hachage cryptographique et à convertir le hachage en texte:

Clé publique ⟶ fonction de hachage cryptographique ⟶ adresse

Chaque implémentation de blockchain peut implémenter une méthode différente pour dériver une adresse. Pour les réseaux blockchain sans autorisation, qui permettent la création de compte anonyme, un utilisateur de réseau blockchain peut générer autant de paires de clés asymétriques, et donc d'adresses, qu'il le souhaite, permettant un degré variable de pseudo-anonymat. Les adresses peuvent servir d'identifiant public dans un réseau blockchain pour un utilisateur, et souvent

une adresse sera convertie en un code QR (Quick Response Code, un code à barres bidimensionnel qui peut contenir des données arbitraires) pour une utilisation plus facile avec le mobile dispositif.



Figure 1.6 - Un exemple de code QR qui a encodé le texte «NISTIR 8202 - présentation de la technologie Blockchain Exemple de code QR »

Les utilisateurs du réseau blockchain peuvent ne pas être la seule source d'adresses au sein des réseaux blockchain. Il est nécessaire de fournir une méthode d'accès à un contrat intelligent une fois qu'il a été déployé dans un réseau blockchain. Pour Ethereum, les contrats intelligents sont accessibles via une adresse spéciale appelée compte contractuel. Cette adresse de compte est créée lors du déploiement d'un contrat intelligent (l'adresse d'un compte de contrat est calculée de manière déterministe à partir de l'adresse du créateur du contrat intelligent **[11]**). Ce compte de contrat permet au contrat d'être exécuté chaque fois qu'il reçoit une transaction, ainsi que de créer des contrats intelligents supplémentaires à son tour.

1.6.6 Stockage des clés privées

Avec certains réseaux blockchain (en particulier avec les réseaux blockchain sans autorisation), les utilisateurs doivent gérer et stocker en toute sécurité leurs propres clés privées. Au lieu de les enregistrer manuellement, ils utilisent souvent un logiciel pour les stocker en toute sécurité. Ce logiciel est souvent appelé portefeuille. Le portefeuille peut stocker des clés privées, des clés publiques et des adresses associées. Il peut également exécuter d'autres fonctions, telles que le calcul du nombre total d'actifs numériques qu'un utilisateur peut posséder [41].

Si un utilisateur perd une clé privée, tout actif numérique associé à cette clé est perdu, car il est impossible, d'un point de vue informatique, de régénérer la même clé privée. Si une clé privée est volée, l'attaquant aura un accès complet à tous les actifs numériques contrôlés par cette clé privée. La sécurité des clés privées est si importante que de nombreux utilisateurs utilisent un matériel sécurisé spécial pour les stocker; alternativement, les utilisateurs peuvent profiter d'une industrie émergente de services de séquestre de clés privées. Ces services de séquestre clés peuvent également satisfaire les lois KYC en plus de stocker des clés privées, car les utilisateurs doivent fournir une preuve de leur identité lors de la création d'un compte.[41]

Le stockage des clés privées est un aspect extrêmement important de la technologie blockchain. Quand il est rapporté dans les nouvelles que «la crypto-monnaie XYZ a été volée à…», cela signifie presque certainement que certaines clés privées ont été trouvées et utilisées pour signer une transaction envoyant de l'argent vers un nouveau compte, et non que le réseau de la blockchain lui-même a été compromis. Notez que, comme les données de la blockchain ne peuvent généralement pas être modifiées, une fois qu'un criminel vole une clé privée et transfère publiquement les fonds associés à un autre compte, cette transaction ne peut généralement pas être annulée.

1.7 La signature numérique

Une signature numérique (DS) [41] fait référence à une approche cryptographique pour authentifier le contenu numérique et garantir son intégrité. DS utilise un système de cryptographie à clé publique (PKI). La cryptographie à clé publique (PKI) consiste en une clé publique et une clé privée qui sont appariées mais asymétriques (non identiques). La clé publique de la paire est généralement partagée avec les entités autorisées et le propriétaire de cette paire de clés ne divulgue pas la clé privée. L'une ou l'autre des clés peut être appliquée pour crypter un message; la clé opposée qui n'est pas utilisée pour crypter le message à partir des paires est utilisée pour décrypter le message. La figure 6 (a) montre qu'un message est chiffré avec une clé publique, une clé privée est utilisée pour déchiffrer le message. Alternativement, la figure 6 (b) montre que le texte chiffré du message est généré en utilisant la clé privée et le texte en clair est produit en utilisant la clé publique.

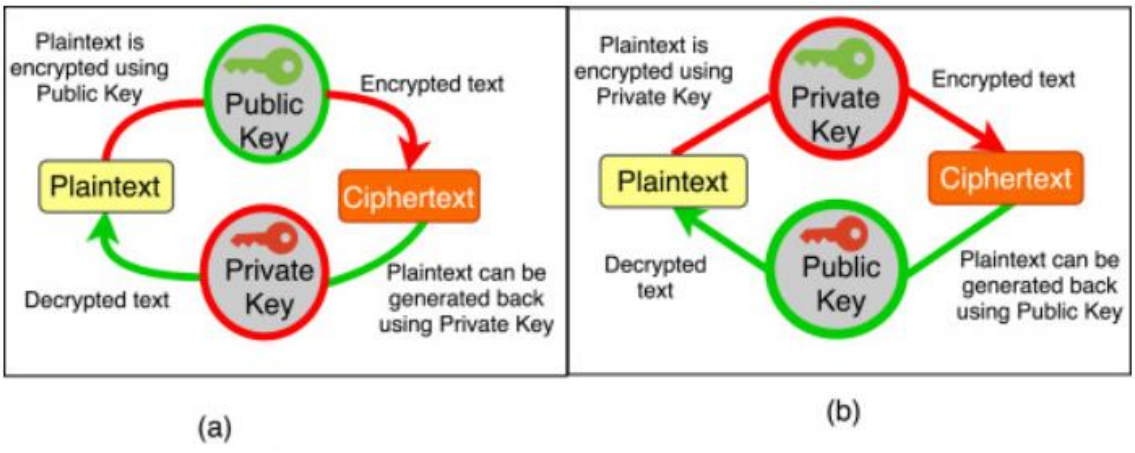


Fig.1.7 signature numérique

1.8 Les mécanismes de consensus

Le protocole de consensus c'est la technique par lequel le réseau d'une *Blockchain* assuré le consensus sur le contenu de la blockchain et sur la manière de la création et la validation des nouveaux blocs. Donc le consensus est une technique de coordination de travail dans la *Blockchain*.

Les 3 caractéristiques d'un modèle de consensus :

1) **La sécurité :** un modèle de consensus est réputé sécurisé si tous les nœuds génèrent le même output est cette output respect les règles de protocole.
2) **Tolérance aux pannes :** la Blockchain et capable de fonctionner malgré la défaillance d'un nombre des nœuds.
3) **Vivacité :** les nœuds qui fonctionnent de manière conforme aux règles sont compensés par le système pour continuer leur fonctionnement.

Étant donné que les systèmes de blockchain sont de nature décentralisée, ils ne nécessitent pas d'autorité centralisée de confiance. Des méthodologies de consensus décentralisées sont mises en œuvre par blockchain afin de fournir la fiabilité et l'uniformité des données ainsi que des transactions sécurisées. Actuellement, quatre grands mécanismes de consensus sont utilisés dans la technologie blockchain: la preuve de travail (PoW), la tolérance aux pannes byzantine pratique (PBFT), la preuve d'enjeu (PoS) et la preuve d'enjeu déléguée (DPoS) (Zheng et coll., 2016). Certaines autres méthodologies de consensus qui ont été mises en œuvre dans quelques-unes des technologies de la blockchain sont la preuve de bande passante (PoB) (Ghosh et coll., 2014)

1.8.1 Proof of Work (PoW)

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

Une PoW est exigée pour la validation de chaque bloc. D'une part, elle a l'avantage de protéger l'intégrité des transactions et des blocs, car afin qu'un attaquant puisse modifier un bloc, il doit modifier tous les blocs qui le succèdent et fournir une nouvelle PoW pour chacun de ces blocs, ainsi que la mise à jour de tous les objets par la nouvelle version de la chaîne (falsifiée). Ce qui nécessite une énorme puissance de calcul et d'énergie. D'autre part, la PoW souffre de certaines lacunes qui peuvent avoir des mauvaises conséquences. Sans parler du fait que la PoW consomme une grande quantité d'énergie lors de la résolution du défie mathématique, ce mécanisme peut mener à une potentielle tragédie des ressources d'usage commun (tragedy of commons) [18]. En effet, au fil du temps, les récompenses diminueront, ce qui entraînera une diminution du nombre de mineurs, car les seuls frais qui seront gagnés viendront des transactions. Ces frais de transactions vont également diminuer due à la concurrence d'autres systèmes similaires. La diminution du nombre de mineurs rend l'écosystème blockchain vulnérable à l'attaque du 51%. Cette dernière se produit lorsqu'un mineur malicieux (ou un pool de mineurs malicieux) contrôlent 51%, ou plus, de la puissance de calcul du réseau. Ainsi, il peut créer des blocs de transactions frauduleux pour lui-même, ou pour une autre entité, tout en invalidant les transactions des autres utilisateurs dans le réseau. Enfin, dans certains mécanismes de consensus, tel que celui de la chaîne la plus longue (longest chain) appliqué dans Bitcoin, de nombreux mineurs qui valident des blocs et réalisent la PoW ne sont pas récompensés, car ils n'ont pas assez de puissance pour construire la chaîne la plus longue, ce qui leur cause beaucoup de pertes. La PoW représente la méthode de validation de bloc la plus adoptée par les systèmes blockchain. [65]

Le concept du l'algorithme le plus utilisé dans la Blockchain existait bien avant sa naissance. Il a été publié à l'origine par Cynthia Dwork et Moni Naor en 1993, mais le terme «preuve de travail» a été inventé par Markus Jakobsson et Ari Juels dans un document publié en 1999 (Blockgeeks, 2017). Dans le cas de Bitcoin, la preuve de travail suppose que tous les membres du réseau votent en utilisant leur puissance de calcul en résolvant le PoW et la construction et la validation du bloc. La preuve de travail peut être considérée comme le principal composant afin de définir un calcul informatique coûteux, également appelé extraction qui doit être effectuée afin de générer un nouveau bloc. [65]

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

1.8.2 **Proof of Stake (PoS)**

Afin de résoudre les lacunes de la PoW (Preuve de Travail), la PoS (Preuve d'Enjeu) a été proposée. Dans ce mécanisme il n'y a pas de minage où on consomme beaucoup de ressources. Les mineurs sont appelés forgeurs. Un forgeur peut valider des blocs en fonction de la quantité d'argent qu'il possède. Ce qui signifie que plus il possède de monnaies, plus il augmente sa chance de validation. Si on compare la PoS à un jeu de pari, où chaque forgeur parie sur un bloc. On peut dire qu'une fois que les blocs honnêtes (ne contiennent aucune transaction frauduleuse) sont ajoutés à la chaîne, chaque forgeur touche une récompense relative à son pari. Et contrairement à la PoW où les mineurs malicieux sont pardonnés, dans la PoS un forgeur dont le bloc s'avère malhonnête est pénalisé et le montant du pari qu'il a mis est débité de son solde. Le point faible de la PoS est que

les forgeurs qui possèdent beaucoup de monnaies sont ceux qui bénéficient le plus. Il existe plusieurs systèmes blockchain qui utilisent la PoS, et d'autres qui replacent la PoW par la PoS.[65]

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

1.8.3 **Delagated Proof of Stake (DPoS)**

La principale différence entre les PoS et les DPoS réside dans le fait que les PoS sont un processus démocratique direct, tandis que le DPoS est démocratiquement représentatif - les parties prenantes élisent des délégués pour générer et valider un bloc. Avec beaucoup moins de noeuds pour valider le bloc, le bloc peut être confirmé rapidement, ce qui signifie que la transaction peut être confirmée rapidement (Zheng, 2016) et (Kikitamara, 2017)

1.8.4 **Practical Byzantine Fault Tolerante(PBFT)**

La tolérance aux pannes byzantine pratique (PBFT) est un algorithme de consensus utilisé lorsqu'il existe une confiance partielle entre les nœuds. C'est un algorithme de réplication pour endurer les fautes byzantines [22]. La tolérance aux pannes byzantine (BFT) est le composant d'un réseau pour parvenir à un accord nonobstant lorsqu'une partie des nœuds du système néglige de réagir ou réagit avec de fausses données. L'objectif d'un composant BFT est de se protéger contre les défaillances du cadre en utilisant une prise de décision globale, à la fois des nœuds corrects et défectueux, qui vise à réduire l'impact des nœuds cassés.[23]

Le problème du général byzantin peut être expliqué comme suit. Imaginez qu'en dehors d'une ville adverse, peu de divisions de la force armée byzantine restent à l'extérieur, et chaque division est instruite par son propre général. Les généraux peuvent se parler uniquement par émissaire. Après avoir observé l'ennemi, ils doivent choisir un plan de match typique. Dans tous les cas, une partie des généraux pourrait être des escrocs, essayant d'empêcher les généraux fidèles de s'entendre. Les généraux doivent décider quand attaquer la ville; cependant, ils ont besoin d'une partie dominante solide de leurs forces armées pour attaquer simultanément. Les généraux doivent avoir un calcul pour s'assurer que chaque général inébranlable adopte un plan de match similaire, et peu de filous ne peuvent pas faire en sorte que les généraux fiables reçoivent un arrangement horrible. Les généraux dévoués feront tous ce que le calcul dit qu'ils devraient, mais les escrocs peuvent faire tout ce qu'ils veulent. Le calcul doit garantir une condition peu attentive à ce que font les escrocs.

Les généraux fiables doivent parvenir à la compréhension mais doivent s'entendre sur un arrangement raisonnable [23].
Hyperledger fabric utilise le PBFT comme algorithme de consensus, puisque PBFT pourrait traiter jusqu'à un tiers des copies byzantines vindicatives. Un autre bloc est résolu en un tour. Dans chaque cycle, un élément essentiel serait choisi par certaines lignes directrices. De plus, il est en charge de demander la transaction. La procédure entière pourrait être isolée en trois étapes: pré-arrangée, arrangée et soumise. À chaque étape, un hub entrerait dans l'étape suivante au cas où il aurait pu voter à partir de plus des deux tiers de tous les éléments considérés. Ainsi, PBFT nécessite que chaque concentrateur soit connu du réseau. Comme PBFT, Stellar Consensus Protocol (SCP) [21] est également une convention de compréhension byzantine. Dans PBFT, chaque hub doit interroger différents hubs, tandis que SCP donne aux membres le privilège de choisir quel ensemble de membres différents accepter.

1.9 Evolution de la blockchain

En 2009, l'évolution de la blockchain a commencé avec le concept en développement de « l'économie entre homologues » sur Internet, connu sous le nom de Bitcoin [11]. Le bitcoin est fourni et pris en charge, pas par une autorité centrale, par ex. Banque ou entreprise comme PayPal, mais par consentement automatique entre utilisateurs du réseau. Son caractère unique repose toutefois sur le fait que les utilisateurs ne devaient pas se faire confiance [11, 12]. Grâce à l'autocontrôle algorithmique, toute tentative malveillante de tromper le système est interdite. Techniquement, le bitcoin est une monnaie numérique qui est traitée via Internet dans un système décentralisé sans confiance utilisant un registre public appelé blockchain. Il combine le partage de fichiers pair-à-pair entre Bit Torrent et la cryptographie à clé publique [11]. Les avantages de la blockchain ne se limitent pas à l'économie entre pairs. Ils s'étendent aux domaines politique, environnemental, médical, etc. Par exemple :

- Pour lutter contre les systèmes politiques oppressifs, la technologie blockchain peut être utilisée pour intégrer dans un cloud décentralisé des fonctions qui, auparavant, nécessitaient une administration par des organisations juridiquement responsables.

- La coordination, la tenue des registres et l'irrévocabilité des transactions utilisant la technologie de la blockchain sont des caractéristiques qui pourraient être aussi essentielles au progrès de la

société que la Magna Carta ou la Rosetta Stone. Dans ce cas, la blockchain peut servir de référentiel d'archives publiques pour des sociétés entières, y compris le registre de tous les documents, événements, identités et actifs. Dans ce système, toute propriété pourrait devenir une propriété intelligente ; c'est la notion d'encoder chaque actif dans la blockchain avec un identifiant unique permettant de suivre, contrôler et échanger (acheter ou vendre) l'actif sur la blockchain. Cela signifie que toutes sortes d'actifs corporels (maisons, voitures) et numériques peuvent être enregistrés et traités sur la blockchain.
Les avantages susmentionnés de la blockchain peuvent être classés en trois catégories : Blockchain 1.0, 2.0 et 3.0 [12]. Les sous-sections suivantes décrivent brièvement chacune des catégories.

1.9.1 **Blockchain 1.0**

Bitcoin est une monnaie numérique. Il a été créé en 2009 par une entité anonyme utilisant le nom Satoshi Nakamoto [47]. Les paiements utilisant les bitcoins sont enregistrés dans un grand livre public stocké sur des ordinateurs connectés au réseau bitcoin. Le grand livre peut être consulté à tout moment sur Internet. Bitcoin est la première et la plus grande crypto-monnaie décentralisée, tandis que les autres monnaies numériques incluent : Altcoin, Litecoin et Dogecoin [13]. Les utilisateurs peuvent envoyer et recevoir des Bitcoins par voie électronique moyennant des frais de transaction optionnels (ou très minimes) à l'aide d'un portefeuille (un logiciel sur un ordinateur personnel, une application mobile ou une application Web). En réponse à ces transactions, de nouveaux bitcoins sont créés en guise de récompense pour le traitement informatique (appelé extraction), qui est utilisé pour vérifier et enregistrer les transactions en bitcoins dans le grand livre [11].

Il a été introduit pour la première fois sur une liste de diffusion cryptographique le 31 octobre 2008 et a été publié en tant que logiciel à code source ouvert en 2009. L'idée de construire cette monnaie numérique ou virtuelle est de construire un système décentralisé qui permettrait à la monnaie de pouvoir être transférée électroniquement avec des frais de transaction négligeables ou nuls. Il s'agit du premier réseau pair-à-pair qui permet à ses utilisateurs de ne disposer d'aucune autorité centrale ni de banques. Ces bitcoins sont construits à partir d'un protocole bitcoin. Selon ce protocole, il y aurait un nombre défini de bitcoins pouvant être produits (extraits), soit 21 millions. Cependant, chaque bitcoin peut être divisé en parties plus petites pouvant aller jusqu'à un centième de bitcoin. Cette plus petite division du bitcoin est appelée "Satoshi".

Bitcoin a des utilisateurs qui sont répandus à travers le monde et il n'est pas contrôlé par une seule personne. Du point de vue de l'utilisateur, bitcoin est une application qui fournit un portefeuille et permet aux utilisateurs d'effectuer des transactions entre eux. Pour effectuer des transactions, les utilisateurs sont libres d'utiliser le logiciel de leur choix, à condition que le logiciel soit compatible et respecte les règles du protocole Bitcoin. Ce système de paiement électronique repose sur une preuve cryptographique plutôt que sur la confiance, raison pour laquelle le besoin d'un tiers est éliminé. Les transactions effectuées sont pratiquement impossibles à inverser ou à détruire. Le réseau bitcoin partage un grand livre public appelé blockchain.

1.9.2 **Blockchain 2.0 (contrats intelligents)**

Dans la blockchain, les contrats intelligents vont au-delà de simples transactions de bitcoins et comportent des instructions plus détaillées (traitement) intégrées [14]. Formellement, un contrat intelligent est une méthode d'utilisation de la blockchain (ou transactions bitcoin) pour former des accords entre agents. En général, un contrat (discuté dans la section 2.2.2), c'est une promesse faite à deux agents ou plus de travailler (ou de ne pas faire) de travail en échange de quelque chose d'autre [15]. Chaque agent doit faire confiance à l'autre agent pour remplir sa part de l'engagement. Le contrat intelligent comporte le même type de règlement pour agir ou ne pas agir, mais il élimine la nécessité pour un agent de faire confiance aux autres agents [14]. En effet, un contrat intelligent est un code logiciel exécuté sur une blockchain sans aucune discrétion. En fait, deux éléments des contrats intelligents qui les distinguent sont l'auto-applicabilité et la décentralisation [14]. L'auto-applicabilité signifie qu'après son lancement, les agents engagés dans le contrat intelligent n'ont plus besoin d'être en contact. Décentralisé signifie que les contrats intelligents ne subsistent pas sur un seul serveur centralisé ; ils sont distribués et s'exécutent automatiquement sur le réseau de chaînes de blocs [17]. L'illustration classique des contrats intelligents dans la vie quotidienne est un distributeur automatique. Contrairement à une personne, le distributeur automatique se comporte de manière algorithmique ; le même jeu d'instructions sera exécuté à chaque fois dans tous les cas [14].

Un exemple de contrat intelligent de base, avec des instructions plus détaillées par rapport aux bitcoins, est *un cadeau d'héritage disponible dès le dix-huitième anniversaire* [17]. Vous pouvez créer une transaction qui repose sur la chaîne de blocs et reste non initiée jusqu'à ce que les deux conditions suivantes soient déclenchées.

1) . Le programme définit la date (18ème anniversaire) à laquelle lancer la transaction, ce qui inclut la vérification si la transaction a déjà été exécutée.
2) . Le programme analyse une base de données de registre de décès en ligne pour certifier que l'entité héréditaire (parent ou grand-parent) est décédée. Lorsque le contrat intelligent confirme le décès, il peut automatiquement transférer l'héritage (par exemple, des fonds).

1.9.3 **Ethereum**

Ethereum est un projet open source construit par les développeurs du monde entier, semblable au protocole Bitcoin, mais beaucoup plus adaptable et flexible, car il permet aux utilisateurs de créer et d'utiliser les applications décentralisées exécutées sur la technologie de blockchain sous-jacente. Généralement, il existe deux approches pour créer une application blockchain: démarrer un réseau indépendant ou établir un protocole sur Bitcoin. Ethereum a introduit une blockchain avec un langage de programmation intégré complet de Turing qui permet à quiconque d'écrire des contrats intelligents et des applications décentralisées avec des règles et des paramètres personnalisés.[70]

Contrairement aux états dans Bitcoin, Ethereum a des comptes. Les deux types de comptes sont les suivants: (1) comptes contrôlés de manière externe (ou) comptes d'utilisateur, et (2) contrats, c.-à-d. Extraits de code. Les transactions peuvent être initiées à partir des deux types de comptes, mais les contrats ne peuvent démarrer une transaction qu'à la suite d'autres transactions qu'ils ont reçues. Les contrats sont écrits dans un langage de programmation de haut niveau (Solidity, par exemple), qui est ensuite converti en bytecode Ethereum Virtual Machine (EVM). La devise intégrée pour le

réseau Ethereum, Ether, peut être utilisée pour échanger des actifs numériques et fournit également un mécanisme pour payer les frais de transaction. La plus petite dénomination d'Ether est Wei (1018 Wei = Ether). Dans Ethereum, il n'y a pas de limite de taille de bloc comme dans Bitcoin, mais il existe un concept appelé «Gas». Dans Ethereum, tous les calculs programmables, y compris la création de contacts, l'exécution d'opérations et la réalisation d'appels de messages, ont un coût convenu universellement, mesuré en termes de gaz. Au lieu d'une limite de taille de bloc, il existe une limite de gaz (définie par l'expéditeur de la transaction) pour chaque transaction, ce qui signifie que la validation de cette transaction ne doit pas utiliser plus de gaz que la limite mentionnée. Le gaz restant non utilisé à la fin de la transaction est remboursé sur le compte de l'expéditeur. De plus, le temps d'exploitation de blocs dans Ethereum est considérablement réduit à 15 secondes en moyenne par rapport aux 10 minutes de Bitcoin. Cela se fait par la mise en œuvre du protocole GHOST, qui est une politique de sélection de la chaîne principale dans l'arborescence de blocs. Toutefois, ce temps peut être réduit davantage en fonction de la taille des transactions et de la difficulté de calcul liée à la validation d'un bloc.[70]

Tableau 1.3 : Comparaison entre Bitcoin et Ethereum

Les sujets	Bitcoin	Ethereum
Concept	Monnaie numérique	Contrats intelligents
Fondateur	Satoshi Nakamoto	Vitalik Buterin
Méthode de libération	Genesis Block Mined	Prévente
Crypto-monnaie utilisée	Bitcoin (Satoshi)	Éther
Algorithme	SHA-256	Ethash
Minage des Blocs	10 minutes	12-14 secondes
Évolutif	Pas encore	Oui

1.9.3.1 **Hyperledger Fabric**

Hyperledger Fabric est une blockchain open-source privée, créée par la Linux Foundation, plus précisément par IBM. Contrairement à Bitcoin et Ethereum, Hyperledger Fabric ne fournit pas une monnaie virtuelle. Selon la nature des informations stockées, les transactions peuvent être publiques ou confidentielles. Hyperledger utilise le Practical Byzantine Fault Tolerant (PBFT) comme mécanisme de consensus. Comme expliqué dans [20], PBFT est un mécanisme utilisé dans

les réseaux distribués, et qui tolère un certain taux de fautes afin de permettre la continuité des opérations du système. Tous les objets participants se connaissent et sont de confiances, et les objets validateurs sont choisis aléatoirement. Hyperledger Fabric permet également le développement des smart contracts appelé chaine de codes. [67]

1.9.3.2 **Contrats Intelligents**

L'idée à la base du « contrat intelligent » est de changer le comportement de quelque chose, en fonction de l'entrée (données), lorsque certaines conditions sont remplies. Dans le contexte d'un système de grand livre distribué, un contrat intelligent est un morceau de code qui est stocké à une adresse particulière de la blockchain. L'adresse de stockage est déterminée lors de la création d'un contrat intelligent. Lorsqu'une transaction est envoyée à cette adresse, le code du contrat intelligent est exécuté, ce qui peut entraîner la lecture / l'écriture de données dans le grand livre distribué sur lequel elle est présente. Un contrat intelligent peut prendre des décisions, lire des données et exécuter d'autres contrats.

Tableau 1.4 : Comparaison entre contrats traditionnels et contrats intelligents

Traditional contracts	Smart contracts
1-3 days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not necessary
Expensive	Fraction of the cost
Physical presence	Virtual presence
Lawyers necessary	Lawyers may not necessary

Source : https://www.linkedin.com/pulse/smart-contracts-its-applications-sudip-nair

Le tableau 5 montre les avantages des contrats intelligents par rapport aux contrats traditionnels. Les contrats intelligents peuvent être exécutés très rapidement et il n'existe aucune exigence de présence physique. [17]

Lorsque nous traitons avec des appareils IoT, nous souhaitons essentiellement effectuer certaines actions en fonction des données reçues. Par exemple, imaginez un capteur de lux qui envoie des données à un système toutes les minutes. Sur la base de ces données, ce système devra allumer / éteindre les lumières entourant ce capteur. Si tous les périphériques sont connectés, cela pourrait être possible dans des conditions normales. Toutefois, pour que cela fonctionne avec une application basée sur la technologie de la blockchain, des contrats intelligents sont nécessaires car ils fournissent la logique des opérations tout ou rien. Malheureusement, la mise en œuvre de contrats intelligents par Ethereum est totalement déterministe et isolée, c'est-à-dire qu'un contrat intelligent n'a pas accès aux données extérieures à la blockchain. Cela ne peut fonctionner qu'avec

des données sur la chaîne. Après avoir codé un contrat intelligent dans un langage de haut niveau tel que Solidity ou Snake, le code sera compilé dans du bytecode EVM (Ethereum Virtual Machine) et sera stocké à une adresse de la blockchain. Il est appelé lorsqu'une transaction est envoyée à cette adresse. [65]

1.9.4 **Blockchain 3.0 (innovations basées sur les Smarts Contracts)**

Outre le fait que la blockchain réinvente la quasi-totalité des catégories de services ou de transactions financiers, elle pourrait également offrir des possibilités de reconfiguration similaires à toutes les industries et, plus largement, à presque tous les domaines de l'activité humaine [16]. Par exemple, Northern Trust et IBM utilisent les contrats intelligents pour aider à transformer l'administration du capital investissement [17].

D'autres projets comme ADEPT d'IBM, Slock.it, Trans Active Grid et Filament [18] ; utilisent avec succès des contrats intelligents comme technologie sous-jacente pour la commercialisation d'innovations. Cependant, à l'instar des contrats traditionnels, les contrats intelligents ont également donné lieu à des contestations judiciaires dans le domaine du droit des contrats, qui pourraient nuire à la réputation des innovations conçues.

1.10 Types de Blockchain

La blockchain peut être ”avec permission” (privée) ou ”sans permission” (publique). La première catégorie impose des restrictions aux contributeurs du consensus. Seul ceux de confiances et choisis qui ont le droit de valider des transactions. Elle ne nécessite pas beaucoup de calcul pour atteindre un consensus, ainsi, elle est économique en termes de temps d’exécution et en énergie. Généralement les transactions sont privées et ne sont accessibles que par les objets autorisés. La deuxième catégorie (blockchain publique) utilise un nombre illimité d’objets anonymes. En se basant sur la cryptographie, chaque acteur peut communiquer d’une manière sécurisée. Chaque objet est représenté par une paire de clés (publique/privée), et a le droit de lire, d’écrire et de valider des transactions dans la blockchain. La blockchain est sûre si 51% des objets (ou plus) sont honnêtes et lorsque le consensus du réseau est atteint. Généralement, les blockchains sans permission consomment beaucoup d’énergie et de temps, car elles exigent un montant de calcul pour renforcer la sécurité du système (ex. en utilisant la PoW).

Il existe trois types de Blockchain, selon leur mode de fonctionnement :

1.10.1 **Blockchain publique** :

Tout le monde peut lire ou écrire des données et la seule condition est de disposer d'un ordinateur et d'une connexion Internet. Une partie de ce type de réseau restreint l'accès uniquement en lecture ou en écriture. Ethreum et Bitcoin sont des exemples qui utilisent une approche où tout le monde peut écrire. Un réseau public de blockchain est totalement ouvert et n'importe qui peut participer au réseau en le rejoignant. Le réseau dispose normalement d'un système de récompense pour inciter davantage de membres à rejoindre le réseau [24]. Tout le monde peut vérifier la transaction et la confirmer et peut également participer à l'obtention d'un consensus. La **Fig. 1.11** démontre la blockchain publique.

Les avantages des blockchains publiques sont :

1) **Confiance :** L'objectif des blockchains publiques depuis le début était d'éliminer les médiateurs de toute structure, et de manière plus critique, elle cherche à évacuer les fiducies qui leur sont accordés. À vrai dire, les membres du réseau ne devraient pas avoir à se confier pour le réseau pendant les transactions sont à traitées et à vérifiées. Les blockchains publiques sont sans confiance, car tout le monde est encouragé à prendre la meilleure décision pour l'amélioration du réseau [25].

2) **Transparent et ouvert :** Toutes les informations internes des transactions sont ouvertes au public pour vérification. La simplicité d'une blockchain publique est peut-être un élément remarquable qui attire un large éventail de cas d'utilisation, du vote aux transactions financières. De plus, la légitimité des transactions et des informations peut être confirmée par n'importe qui dans le réseau [25].

3) **Sécurise** : La blockchain sera plus sécurisée avec l'augmentation du nombre de participants actifs et une plus grande décentralisation. Avec plus de nœuds dans le réseau, il sera beaucoup plus difficile pour tout pirate informatique d'attaquer l'environnement. Dans un réseau public de blockchain, n'importe qui peut devenir un nœud ou un mineur complet et ajouter à la sécurité du Framework. Il est à toute fin utile inimaginable pour les pirates informatiques de conspirer et de travailler ensemble pour superviser le réseau d'accord. [25].

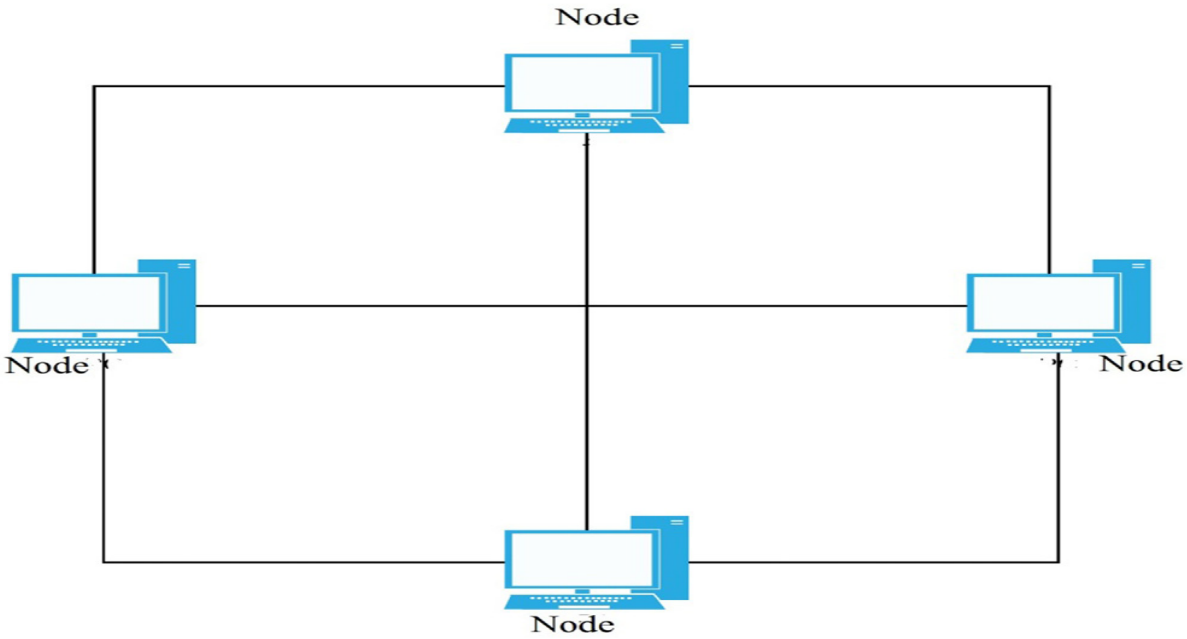


Figure 1.8 Blockchain publique

1.10.2 **Blockchain privée** :

Un réseau blockchain privé nécessite une demande et doit être approuvé soit par l'expéditeur du réseau, soit par les règles établies par l'expéditeur du réseau [17].]Les organisations qui mettent en place une blockchain privée disposeront d'un réseau autorisé. Cela limite les personnes autorisées à participer au réseau et certaines transactions spécifiques. Les membres doivent obtenir une invitation ou une autorisation pour se joindre. Le système de contrôle d'entrée pourrait fluctuer: les membres existants pourraient choisir les futurs participants; un expert administratif pourrait délivrer des licences avec intérêt; ou un consortium pourrait décider des choix. Lorsqu'un nœud a rejoint le réseau, il maintiendra la blockchain de manière décentralisée. Tous les nœuds participeront au transfert de données, mais seuls quelques nœuds auront une autorisation spéciale et un accès spécial tel que l'écriture sur la blockchain. Ceci est très utile lorsque la Blockchain est utilisée entre entreprises appartenant à la même branche. Parmi les plus célèbres, citons Hyperledger (de Linux Fondation) et Ripple (protocole permettant les transferts internationaux). Fig. 1.12 démontre la blockchain privée. [17]

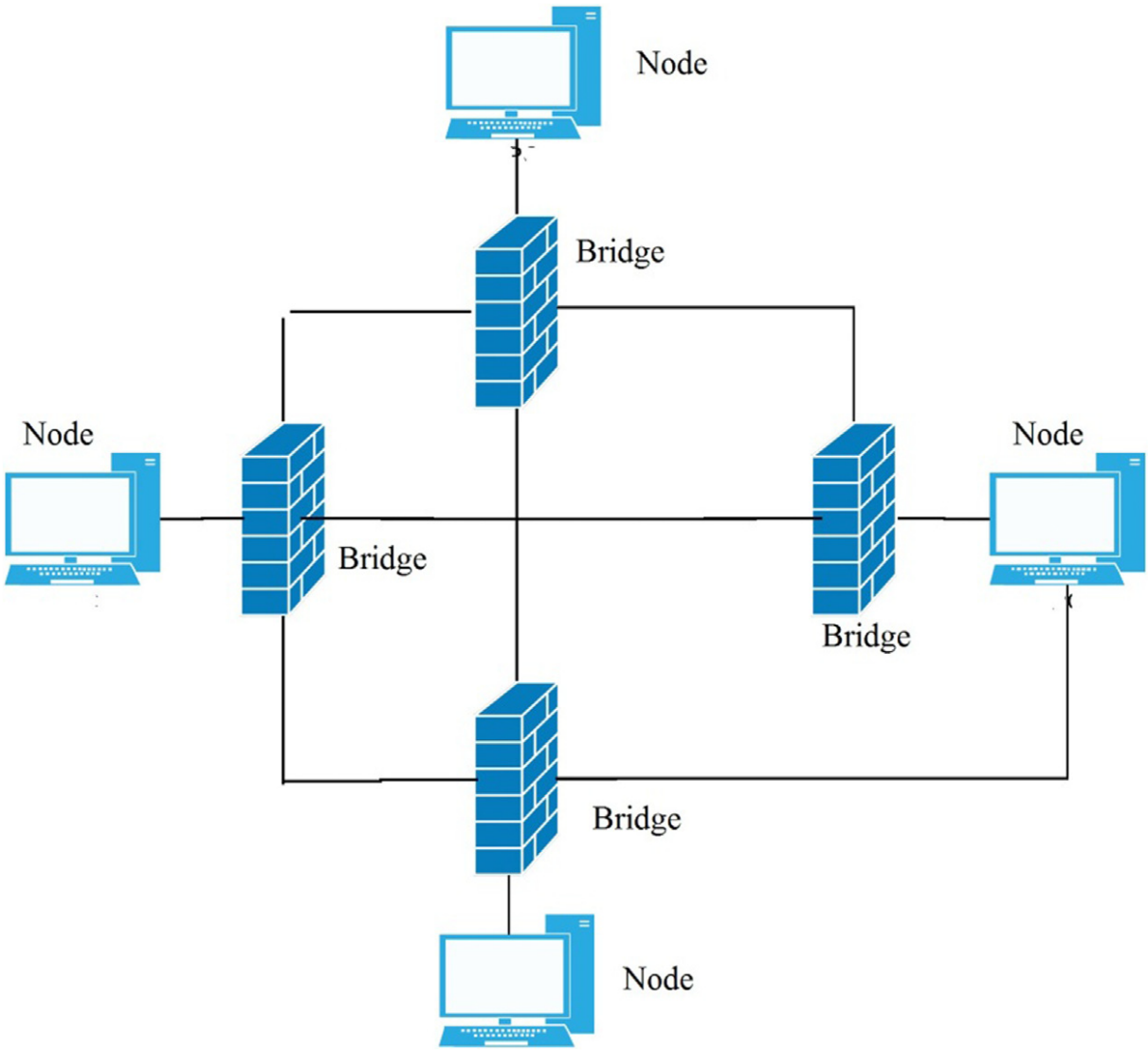


Fig1.9 Blockchain privée

Les avantages de la blockchain privée sont :

4) Plus rapide: Les blockchains privées traitent des transactions plus élevées par seconde (TPS) par rapport aux blockchains publiques, car la présence d'un nombre limité de membres approuvés entraîne essentiellement moins d'occasions d'obtenir un accord pour le réseau. Cela permet de traiter plus de transactions pour chaque bloc; les blockchains privées peuvent traiter des milliers, voire un grand nombre de TPS, contrairement aux sept TPS de Bitcoin [25].
5) Evolutif : Étant donné que seuls quelques nœuds sont approuvés et soucieux de traiter les informations, le réseau peut prendre en charge et traiter un grand nombre de transactions plus élevées. Pas du tout comme un cadre décentralisé où la réalisation d'un accord pourrait exiger un certain investissement, le processus de leadership de base dans un réseau privé

est progressivement intégré et donc beaucoup plus rapide. Une similitude est que cela nécessite un investissement pour 100 instructeurs pour vérifier votre papier de test (et convenir qu'il est vrai / faux) par rapport à un éducateur solitaire qui le tamponne. [25].

Les avantages des blockchains privées sont :

1) L'algorithme de consensus est codé en dur dans le système et la validation de la transaction utilise un modèle basé sur la confiance. Cela limite l'évolutivité du réseau après le déploiement, et comme la validation des transactions utilise la confiance entre les nœuds, cela crée la possibilité d'attaques internes au sein du réseau.

2) L'utilisation de langages de programmation non standard pour la rédaction de contrats intelligents rend leur adoption difficile. Cela crée de la confusion et des erreurs parmi les programmeurs. La communauté open source travaillant sur Hyperledger est encore peu documentée et insuffisante par rapport à d'autres homologues, ce qui rend le déploiement plus difficile.

3) Seules les transactions déterministes sont prises en charge par Hyperledger, ce qui rend difficile l'adoption à grande échelle de la technologie dans l'IoT. Les appareils IoT génèrent une large gamme de données, et chaque appareil génère des données différentes des autres appareils en raison des différentes normes et protocoles suivis par les fabricants et les programmeurs.

Quel que soit le type de blockchain, les deux ont un avantage. Parfois, nous avons besoin d'une blockchain publique en raison de son hébergement; Cependant, nous avons parfois besoin d'un contrôle privé comme des blockchains de consortium ou une blockchain privée, en fonction de l'administration que nous proposons ou de l'endroit où nous l'utilisons.

1.10.3 **Blockchain consortium** :

Les blockchains de consortium contrastent avec leur partenaire public en ce qu'elles sont autorisées, et de cette manière, toute personne disposant d'une association Web pourrait accéder à une blockchain de consortium. Ces types de blockchains pourraient également être décrits comme semi-décentralisés. Le contrôle d'une blockchain de consortium n'est pas concédé à une substance solitaire mais plutôt à un rassemblement de personnes affirmées. Avec une blockchain de consortium, la procédure d'accord va probablement varier à celle d'une blockchain publique. Plutôt que quiconque ait la possibilité de partager la méthodologie, les membres de l'accord d'une blockchain de consortium vont probablement être un rassemblement de nœuds pré-approuvés sur le réseau. De cette manière, les blockchains de consortium ont les inclusions de sécurité qui sont inaliénables dans les blockchains publiques, [26]. Le droit de lecture peut être public ou limité aux participants. Les Blockchains du consortium préservent la confidentialité des données, comme les Blockchains privés. Cela implique que le nœud qui avait un spécialiste peut être choisi à l'avance, pour la plupart a des organisations telles que business to business, et les données dans une blockchain peuvent être ouvertes ou privées et peuvent être considérées comme partiellement décentralisées. Hyperledger, Corda [27], et R3CEV sont des blockchains de consortium.

La **Fig. 1.10** démontre les blockchains de consortium.

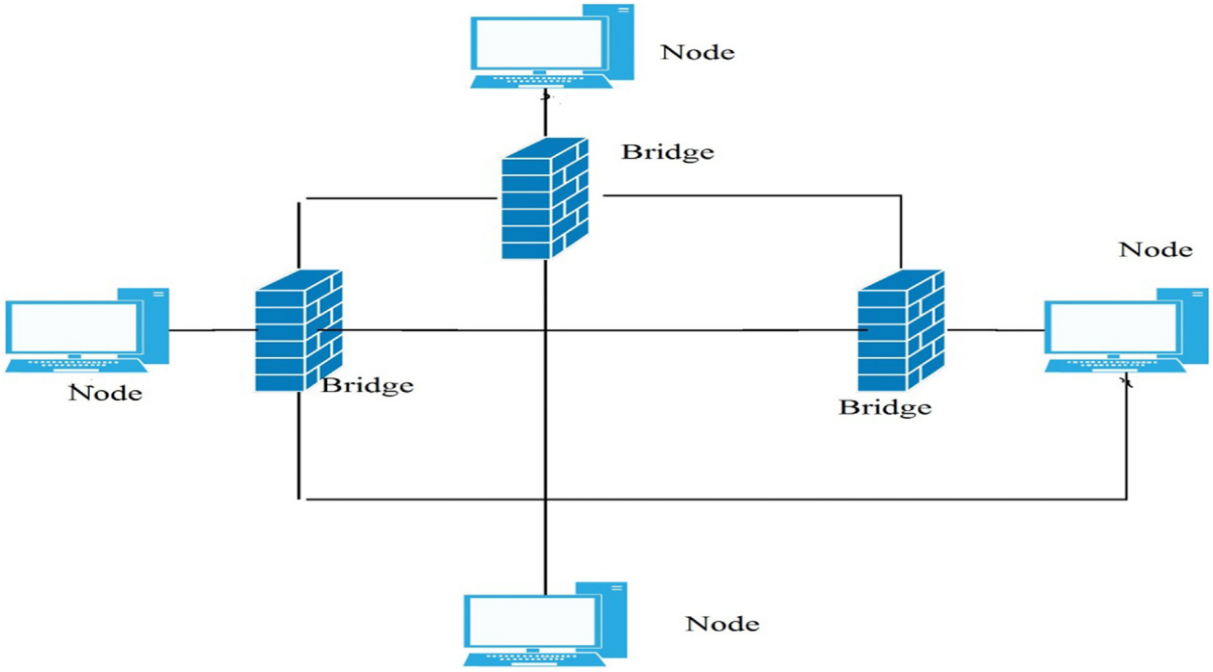


Fig1.10 Blockchain de consortium

Tableau 1.5 représente le tableau de comparaison des types de blockchains.

Propriété	**BC Publique**	**BC Privée**	**BC Consortium**
Détermination du consensus	Tous les mineurs	Une organisation	Ensemble de nœuds sélectionné
Autorisation	Publique	Publique ou restreinte	Publique ou restreinte
Immutabilité	Presque impossible de falsifier	Pourrait être possible	Pourrait être possible
Efficacité	Faible	Haute	Haute
Centralisé	Oui	Oui	Partiel
Processus de consensus	Sans permission	Autorisé	Autorisé

1.11 Les Applications de la Blockchain

Cette section explique les applications de la blockchain dans différents secteurs tels que la banque, la santé, l'immobilier, la chaîne d'approvisionnement, le gouvernement, la cybersécurité, les médias sociaux et l'intelligence artificielle (IA), comme indiqué dans Fig.1.11. [16]

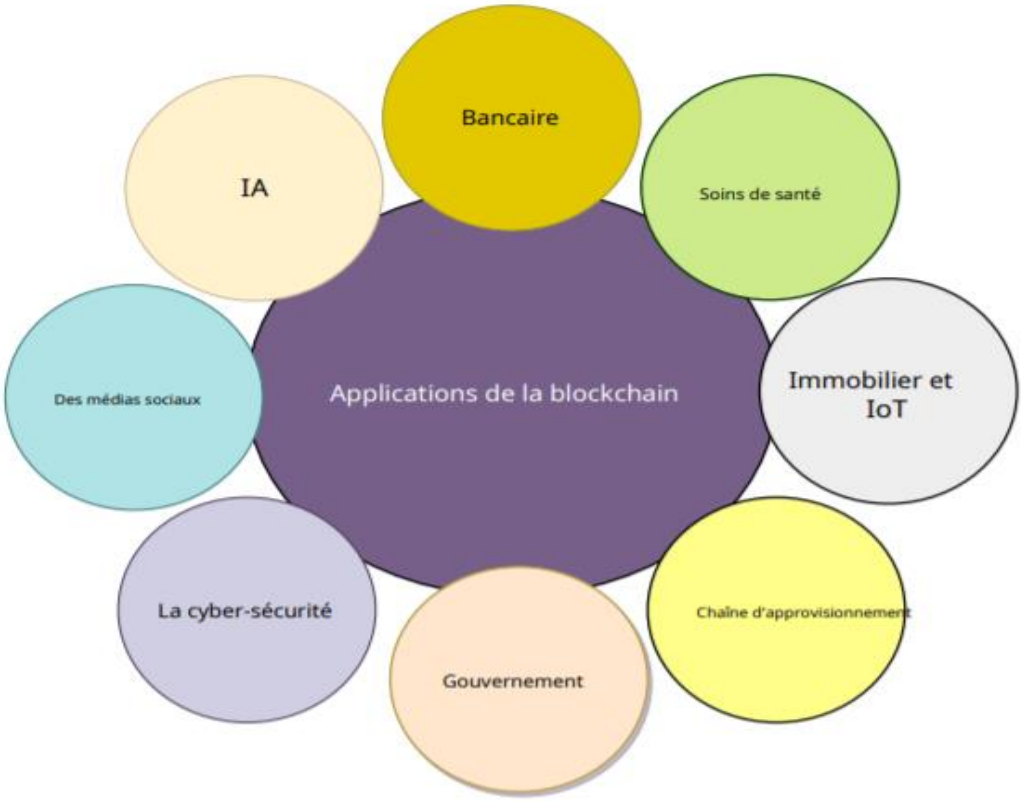


Figure 1.11 Les Applications de la Blockchain

1.11.1 Banque

Le succès de Bitcoin nous a amenés à nous attendre à ce que la blockchain remplace de nombreuses fonctions essentielles du système bancaire. En raison de son architecture décentralisée, la technologie blockchain devrait fournir des services bancaires de base tels que le paiement avec des frais minimes ou sans frais avec un transfert rapide et sécurisé entre les clients. Cependant, pour que la blockchain soit adoptée par les institutions financières, les développeurs de blockchain doivent gagner la confiance des clients et des institutions financières. Les principaux défis à relever sont d'assurer la sécurité par rapport aux exigences du secteur financier. Le temps n'est pas loin lorsque la technologie blockchain sera adoptée dans les institutions financières pour tirer parti des contrats intelligents et de la monnaie unifiée.

1.11.2 Soins de Santé

Considérons la vie d'un patient et ses conditions de santé comme différents états d'un réseau, alors tout le monde peut parfaitement cartographier la santé et l'état d'un patient à différents moments avec l'architecture blockchain. Par sa définition, la blockchain enregistre les différentes transactions sur le réseau avec une politique de zéro altération par quiconque dans les données de transaction une fois qu'elle est validée. Des efforts doivent être déployés pour améliorer le fonctionnement des soins de santé. Ce problème est plus répandu dans les pays en développement ou les pays pauvres où pratiquement aucune tentative n'est faite par le secteur des soins de santé pour enregistrer les données sur la vie des patients de manière organisée. Il incombe en grande partie aux patients de ces pays de conserver un registre des données sur les patients. Les patients aussi, la plupart du temps en raison de l'inconscience, ne conservez pas les dossiers de leur état de santé sur une période de temps. C'est ici que la blockchain peut renforcer le patient tout en lui offrant la possibilité de contrôler ses propres dossiers médicaux. Cela aidera également les médecins et autres membres du personnel médical à récupérer le dossier médical antérieur d'un patient. Un tel accès facile et intégré aux données des patients entre les différentes parties prenantes du système de soins de santé comme les médecins, les pharmaciens et d'autres étudiants et chercheurs en médecine mènera à un système de soins de santé plus efficace.[70]

1.11.3 Immobilier

Avec l'augmentation des applications informatiques et l'introduction de régulateurs, tels que l'autorité de régulation immobilière (RERA) en Inde, le marché immobilier a montré un certain engagement à accroître la confiance dans la vente et l'achat de terrains. Selon Paul Clitheroe, "Avant de commencer à essayer de déterminer dans quelle direction le marché immobilier se dirige, vous devez être conscient qu'il existe des marchés au sein des marchés" [14]. La déclaration ci-dessus précise que les choses ne sont pas aussi simples et transparentes dans les secteurs de l'immobilier. Il n'y a pas si longtemps, c'était une pratique courante adoptée par les vendeurs avides de vendre un lopin de terre un nombre infini de fois. Pour ce faire, la plupart du temps, ils ont pu modifier la chaîne des registres de propriété. La blockchain apporte une clarification à cette situation problématique en donnant un mécanisme dans lequel il est difficile de transférer les registres de propriété existants.

La technologie blockchain tire parti de son architecture décentralisée et augmente la résistance à la fraude. Il est également censé fournir un processus rationalisé qui non seulement réduit le temps nécessaire à la vérification des dossiers, mais réduit également la main-d'œuvre impliquée pour ce faire. L'objectif principal est de supprimer les intermédiaires en stockant, en vérifiant le transfert d'enregistrement de bande à l'aide de la technologie blockchain. Il peut également aider un utilisateur à rechercher la propriété souhaitée. La plupart des sites Web de propriété commerciale en Inde comme les briques magiques et 99 acres ne garantissent pas l'exactitude des données sur la propriété, car n'importe qui peut répertorier sa propriété sur les plates-formes ci-dessus. Tous les problèmes ci-dessus peuvent être résolus lorsque les enregistrements de propriété seront répertoriés sur une seule base de données décentralisée basée sur la blockchain. Il peut fournir aux acheteurs

potentiels des données fiables authentifiées par la technologie blockchain. Il peut également aider dans les contrats de location intelligents signés numériquement entre le locataire et le propriétaire.

1.11.4 **IoT** (internet of Things)

Pour l'IoT, une architecture légère privée peut être développée sur une technologie qui supprime la surcharge de la blockchain tout en préservant ses avantages en matière de confidentialité et de secret. L'IoT peut grandement bénéficier de la nature décentralisée de la blockchain pour rendre le stockage de données et la connectivité des appareils dignes de confiance via des nœuds, sans l'implication d'une autorité centralisée.

1.11.5 **Supply chain management** (SCM):

SCM concerne l'industrie du transport et de la logistique; moyen de transport pour transférer des marchandises d'un endroit à un autre. De bonnes compétences managériales sont donc nécessaires pour que la SCM soit efficace et maintienne le fonctionnement de la chaîne. Les termes tels que décentralisé processus, distribué et grand livre public sont les attributs de la technologie blockchain qui a le pouvoir de modifier la technique liée à : comment les affaires sont-elles menées dans SCM?

Dans SCM, la blockchain a une chaîne de commandes intégrée en tant qu'enregistrements d'une chaîne qui ne peut pratiquement pas être effacée complètement et on peut vérifier la chaîne d'enregistrements, grâce à la nature distribuée du registre blockchain.

1.11.6 **Gouvernement**

Le gouvernement, dans ses plusieurs programmes de protection sociale, bénéficie de l'adoption de la technologie blockchain. Il peut améliorer ses services de livraison, éliminer les intermédiaires et prévenir les cas de fraude fiscale. La plupart des fonctions gouvernementales et de la technologie blockchain sont essentiellement les mêmes. Le gouvernement lance des programmes de protection sociale qui peuvent être considérés comme un réseau impliquant plusieurs parties prenantes ». De même, la blockchain maintient un registre distribué.

1.11.7 **La cybersécurité**

Le gouvernement se concentre également sur la cybersécurité à travers plusieurs frontières du monde numérique. De nombreux efforts ont déjà été déployés pour renforcer la cybersécurité. La beauté de la blockchain est que les données sont très difficiles à modifier car chaque modification des données peut être facilement suivie. On peut facilement vérifier ses données en regardant les versions précédentes d'un bloc. Cela signifie que pour falsifier le réseau, il faut détruire tout le réseau. Ainsi, avec la taille accrue du réseau basé sur la blockchain, les chances de pénétrer dans un réseau diminuent. Les clés de vérification par distribution de données à tous les autres nœuds

peuvent être supprimées. Tout changement dans n'importe quel nœud de données est reflété sur tous les nœuds.

1.11.8 Médias Sociaux

Il n'y a pas si longtemps, les médias sociaux n'étaient pas considérés comme un endroit sérieux. Ses principales fonctions étaient le divertissement et la connectivité sociale. Mais avec le temps, la popularité et la taille des médias sociaux ont considérablement augmenté. De nos jours, il partage une quantité égale d'espace avec les principaux médias tels que les informations et la presse écrite. Les problèmes dans les médias sociaux propagent de fausses nouvelles et provoquent des informations menant à des émeutes communautaires. Le système de grand livre distribué par blockchain peut empêcher les fausses informations et nouvelles. La technologie Blockchain ne peut pas facilement authentifier le contenu des données sur le réseau social, mais peut facilement identifier et vérifier la source des données. Le besoin est de développer de nouveaux modèles commerciaux basés sur la blockchain pour les médias sociaux.

1.11.9 Intelligence Artificielle

Bien que la technologie de la blockchain ait une décennie, peu de tentatives ont été faites pour créer des applications du monde réel qui peuvent utiliser les concepts de blockchain et d'IA. Mais le scénario change très vite; de nos jours, il existe des tentatives considérables et significatives pour combiner la blockchain avec l'IA. Traditionnellement, le fonctionnement de Bitcoin est basé sur un algorithme de hachage basé sur l'approche de la force brute. Il examine chaque candidat pour la solution. L'algorithme d'IA peut s'attaquer à la situation de manière plus intelligente et plus efficace. Un grand réseau de blockchain peut transmettre une grande quantité de données sur lesquelles l'algorithme d'IA peut travailler. L'intégration de l'apprentissage automatique et de l'IA améliorera l'architecture sous-jacente de la blockchain.

1.12 Défis de la blockchain

Dans cette section nous allons donner un aperçu sur les défis liés aux aspects techniques, à la mise en œuvre et à l'acceptabilité de la blockchain.

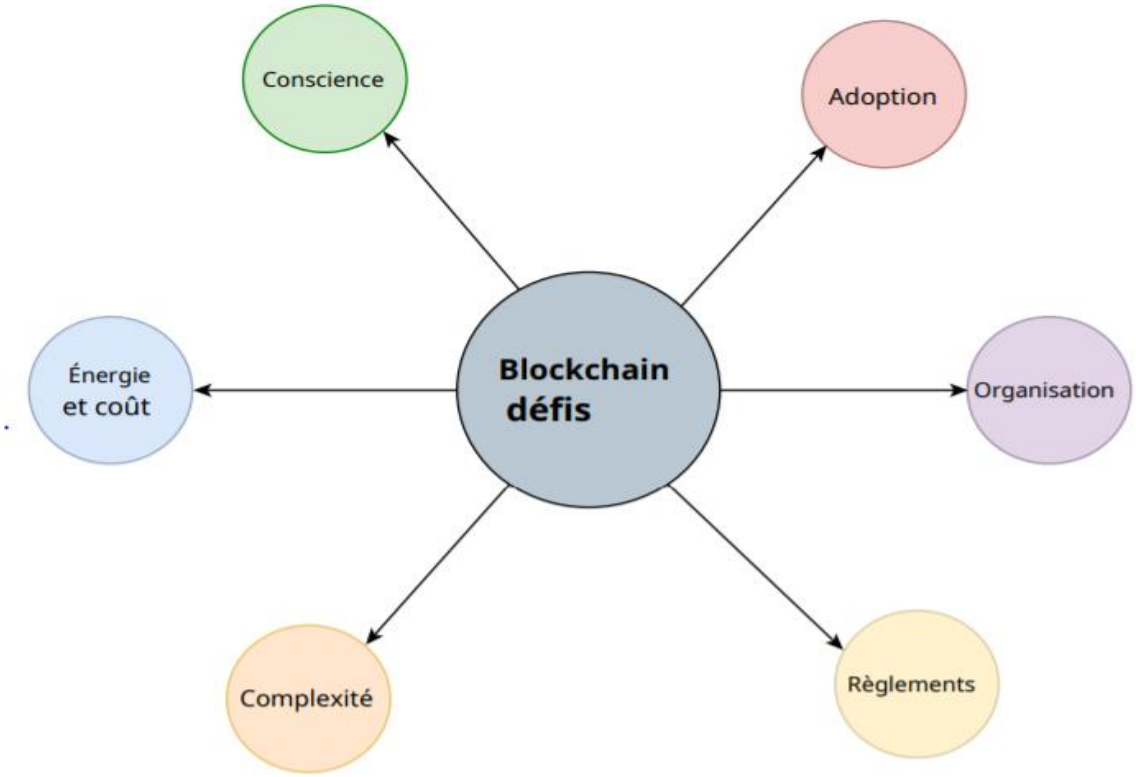


Fig 1.12 Défis de la blockchain

Dans la Fig. 1.12, les cercles extérieurs dans le plan concentrique représentent différents défis relatifs à la technicité, à la mise en œuvre et à l'acceptabilité. Il représente les différents défis rencontrés lors de l'utilisation de la technologie blockchain.

1.12.1 Défis techniques

1.12.1.1 Stockage

L'un des défis majeurs auxquels la blockchain est confrontée est le manque d'espace. La chaîne garde de plus en plus et nécessite donc de plus en plus de ressources et affecte négativement les performances. En raison de millions de transactions nécessitant une attention particulière, la blockchain devient lourde. Il est nécessaire de stocker toutes les transactions précédentes pour valider les nouvelles, ce qui augmente le besoin d'une plus grande capacité. Cela crée un autre problème: les mineurs préfèrent les transactions dont le coût est plus élevé, ce qui retarde les petites transactions.

Quelques-unes des solutions proposées sont les suivantes :

1) L'optimisation du stockage peut être effectuée en supprimant les données plus anciennes, ce qui libère les nœuds de toutes les transactions précédentes.

2) La blockchain pourrait être repensée où le bloc est divisé en deux sections, une à tenir les transactions et l'autre pour que les mineurs se disputent pour devenir le leader qui génère les micros blocs.

1.12.1.2 **Sécurité**

Plusieurs vulnérabilités ont été découvertes dans le protocole.

1) L'égoïsme des mineurs: La majorité (51%) des mineurs pourraient affecter la blockchain et même modifier les transactions qui ont eu lieu. Cela constitue une menace sérieuse pour la sécurité des utilisateurs et de la blockchain. Des chercheurs récents ont découvert que même sans la majorité, les mineurs pourraient sérieusement affecter la blockchain.

2) Attaque double dépense: Puisqu'il nécessite une transaction d'une certaine profondeur avant de pouvoir être confirmé, ce qui peut prendre 20 40 minutes en moyenne, il est possible que des utilisateurs malveillants dépensent à nouveau la même pièce. Cela pourrait également être fait avec l'aide d'un mineur. Ainsi, cela pose un risque sérieux sur les transactions

1.12.1.3 **Confidentialité**

Une caractéristique majeure de toutes les crypto-monnaies est que toutes les transactions sont transparentes. Comme l'information est accessible au public, il a été constaté qu'elle pourrait être utilisée pour atteindre les utilisateurs impliqués dans la transaction. Chaque utilisateur peut être identifié grâce aux nœuds auxquels il se connecte et ces informations peuvent être utilisées pour trouver le début d'une transaction. Cela viole la vie privée de l'utilisateur qui a été assurée par l'anonymat de l'utilisateur. Il existe une méthode permettant de lier le pseudonyme de l'utilisateur à son adresse IP même s'il utilise des pare-feu. Il s'agit d'une violation de la vie privée de l'utilisateur.

1.13 Conclusion

La blockchain est une structure de données permettant de créer et de partager un registre distribué de transactions entre un réseau d'ordinateurs. Il permet aux utilisateurs d'effectuer et de vérifier immédiatement des transactions sans autorité centrale. Blockchain est une base de données de transactions qui contient des informations sur toutes les transactions jamais exécutées dans le passé et fonctionne sur le protocole Bitcoin. Les technologies blockchain contiennent de la cryptographie, des mathématiques, un algorithme et un modèle économique, combinant des réseaux pair-à-pair et utilisant un algorithme de consensus distribué pour résoudre le problème de synchronisation des bases de données distribuées traditionnelles, c'est une construction d'infrastructure multi-domaines intégrée. Les technologies Blockchain composées de six éléments clés. - Décentralisé, Transparent, Open Source, Autonomie, Immuable, Anonymat. Les technologies blockchain peuvent être divisées en trois types. Blockchain publique, Blockchain du consortium, Blockchain privée. Avantages de la technologie Blockchain - Désintermédiation, utilisateurs responsabilisés, données de haute qualité, durabilité, fiabilité et longévité, intégrité des processus, transparence et immuabilité, simplification de l'écosystème, efficacité, audibilité, traçabilité, transparence, transactions plus rapides, coûts de transaction réduits.

2 Chapitre 2: Internet des objets et son intégration avec Blockchain

2.1 Introduction

Le terme *« Internet of Things »* (Internet des objets) désigne la connexion quotidienne d'éléments à l'Internet afin de tirer parti des possibilités offertes par la communication presque immédiate entre différents éléments et systèmes. Cela est possible, surtout grâce à l'amélioration des réseaux de communication et des systèmes de stockage et de traitement, ainsi qu'à l'énorme évolution de la technologie qui permet de fournir la connectivité nécessaire à tout appareil.

Dans ce chapitre, nous présentons le paradigme IoT avec ses principaux protocoles et architectures, en introduisant les technologies les plus importantes pour l'IoT.

2.2 IoT

Le concept d'IoT a été créé par Kevin Ashton en 1999, pionnier britannique de la technologie, qui a fondé l'Auto-ID Center, Massachusetts [1] au MIT (Massachusetts Institute of Technology), université privée de Cambridge, souvent classée parmi les universités les plus prestigieuses du monde.
L'Internet des objets apporte des défis et des opportunités prometteuses. La recherche sur l'IoT a une valeur économique et sociale importante pour le développement de la prochaine génération de technologies de l'information, des réseaux et de la communication.

Les objets connectés

Ce concept qui consiste à coupler un objet à un réseau numérique s'est largement répandu, et a été adapté en fonction des besoins de ses utilisateurs potentiels. On le retrouve dans tous les domaines d'activité, aussi bien le commerce, le transport, l'éducation que la santé.
Actuellement il n'existe pas de définition officielle pour les OC, mais on peut essayer de les qualifier comme tout matériel électronique capable de communiquer avec un ordinateur, un smartphone ou une tablette via une liaison sans fil (Wi-Fi, Bluetooth, etc.) qui le relie à Internet ou à un réseau local.

2.3 Paradigme IoT

Il n'y a pas de définition universellement acceptée de l'Internet des objets, car ce paradigme décrit non seulement un nouveau type d'architecture technique, mais également un nouveau concept qui définit la manière dont nous interagissons avec le monde physique. On expose ici deux définitions du concept celui de l'IEEE (Institut des ingénieurs électriciens et électroniciens) et celui de l'UIT (Union internationale des télécommunications) [2] :

1) IEEE définit l'IoT comme "un réseau d'éléments (chacun intégré avec des capteurs) qui sont connectés à Internet ". (Rapport spécial sur l'internet des objets en mars 2014).
2) UIT définit l'IoT comme "un réseau omniprésent dans lequel le concept d'omniprésent est fondé sur le concept global de réseau et des périphériques réseau". (Rapport 2005 sur l'IoT, série UIT Y, 20).

Si on devait définir l'Internet des objets avec nos propres mots, On dirait que c'est la connexion de toutes sortes d'objets les uns avec les autres via Internet pour créer un environnement communicable numériquement.
Un concept important lié à l'Internet des objets est le M2M (Machine-to-Machine) qui représente un ensemble de technologies permettant aux machines de communiquer entre elles et conduire l'action. M2M utilise des réseaux sans fil pour connecter Internet et des périphériques les uns aux autres avec une intervention humaine directe minimale, pour fournir des services répondant aux besoins d'un large éventail d'industries. D'autre part, l'IoT représente la coordination des périphériques, des appareils, des machines connectées à Internet via plusieurs réseaux, l'interaction humaine est un facteur clé.

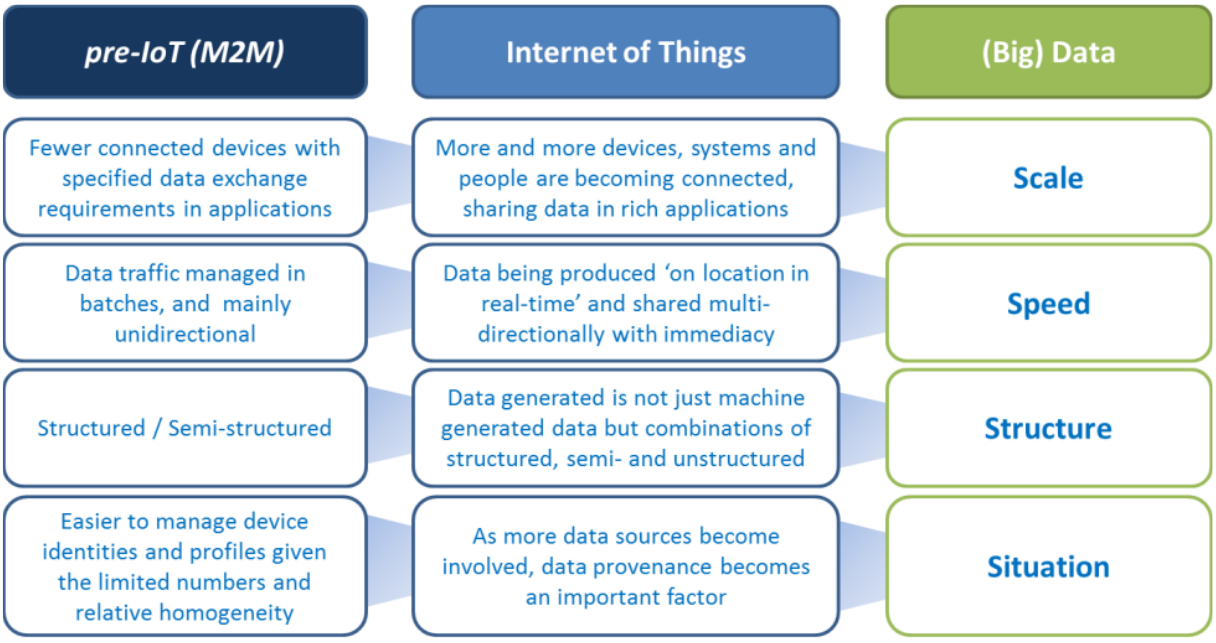


Figure 2.1: Comparaison entre M2M et IoT

Source: Machina Research report "Why NoSQL Databases are needed for the IoT"

La figure 4 illustre différents aspects liés au M2M et à l'IoT. Généralement, les deux concepts sont similaires. Les principales différences sont l'évolutivité, la structure et la vitesse.

L'IoT a plus d'appareils connectés que le M2M et il est plus utilisé dans le secteur grand public alors que le M2M a une connotation industrielle plus forte.

Le concept de M2M a été utilisé pendant la Seconde Guerre mondiale pour identifier un ami ou un ennemi afin d'empêcher les pilotes de frapper des cibles alliées. Aujourd'hui, il est utilisé dans plusieurs applications telles que la maintenance des machines, la mesure, la sécurité, la fourniture de chaînes, le suivi des actifs ou la surveillance à distance [2]-[4].

Différentes organisations travaillant dans le processus de normalisation IoT et M2M se concentrent sur les différents aspects, protocoles et autres éléments importants de l'Internet des objets.

Au niveau international, l'UIT-T travaille sur l'IoT, notamment sur les aspects réseau de l'identification d'objets et sur le réseau de capteurs omniprésent.

En Amérique du Nord, de nombreuses organisations de normalisation travaillent à la promotion des normes IoT :

1) IEEE fonctionne dans les applications M2M. Il étudie des moyens efficaces de prendre en charge une consommation d'énergie moindre du périphérique, un nombre important de périphériques au niveau des stations de base, des transmissions en rafales réduites et une authentification améliorée du périphérique.

2) ATIS (Alliance pour les solutions pour l'industrie des télécommunications) vise à définir une couche de service commune pour plusieurs applications M2M et les interfaces correspondantes entre la couche d'application et les couches de transport.

3) TIA (Telecommunications Industry Association*)* est intéressée par la spécification de protocoles omniprésents pour la communication avec des périphériques intelligents utilisés dans les industries et la publication de sa norme d'architecture de référence pour les communications de périphériques intelligents (TIA-4940).

4) OMA *(*Open Mobile Alliance*)* est intéressée par l'extension du protocole de gestion des appareils pour les communications M2M et fonctionne sur les services de localisation pour les applications M2M mobiles.

Au niveau européen, le *CEN* se concentre sur les technologies d'identification, les protocoles de collecte de données et les protocoles de communication. L'*ETSI* est d'avantage axé sur les activités de normalisation M2M.

En Asie, la normalisation IoT est effectuée par différentes organisations. En Chine, par le comité technique 10 du CCLAT, qui travaille principalement dans le domaine de la surveillance de la santé

en ligne et des systèmes de communication des véhicules. En Corée, TTA a fondé M2M PG (PG708) sur les exigences de service, la structure de données et le schéma d'identification, tandis qu'au Japon, la normalisation est réalisée via l'*ARIB*, qui est centré sur le réseau intelligent, les villes intelligentes et les maisons intelligentes [4]. Pour comprendre plus en détail le fonctionnement de l'IoT, il est important de connaître d'autres concepts clés ; Capteurs, connectivité, middleware, adressage et évolutivité, stockage et visualisation des données :

Les capteurs convertissent une entrée non électrique en un signal électrique pouvant être envoyé à un circuit électronique. Ils sont chargés de créer des informations pour le réseau IoT via la collecte de données de l'environnement à des fins différentes. Ils doivent être petits, polyvalents et économes en énergie. Toutes les applications IoT comportent un ou plusieurs capteurs, qui sont peu onéreuses et consomment moins d'énergie [5].

La connectivité permet aux appareils de communiquer entre eux et également avec des services et des applications fonctionnant dans le nuage. *La conception de réseau* est très importante dans le paradigme de l'IoT en raison du volume énorme d'éléments interconnectés et de l'impact que la conception peut avoir sur les performances globales du système.

Le middleware interconnecte et intègre tous les éléments qui rendent l'internet des objets possibles. Il fait partie de l'architecture permettant la connectivité pour un grand nombre de tâches en fournissant une couche de connectivité pour les capteurs ainsi que pour les couches d'application fournissant des services assurant des communications efficaces entre logiciels [2],[6].
Il agit comme une interface permettant aux diverses applications sur des systèmes hétérogènes de communiquer facilement les unes avec les autres.

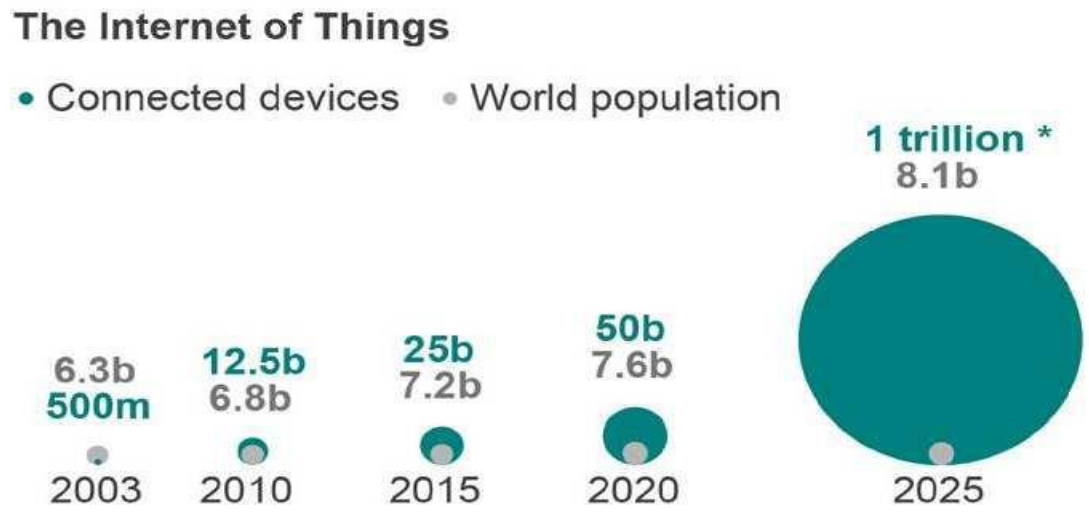


Figure 2.2: Comparaison entre les objets connectés et la population mondiale

Source : Cisco IBSG

La figure 2.2 illustre la comparaison entre les périphériques connectés et la population mondiale par années et leur évolution attendue.

Nous pouvons observer l'énorme potentiel de croissance des appareils connectés. Alors qu'en 2003, la population mondiale s'élevait à 6,3 milliards d'habitants et à 500 millions d'appareils connectés, on s'attend à ce qu'environ 1 billion d'objets soient connectées contre 8,1 milliards d'habitants dans le monde en 2025.

L'adressage et l'évolutivité sont très importants, car tous les objets inclus dans le réseau IoT doivent avoir un identifiant unique. L'IoT englobe un très grand nombre de périphériques. Par conséquent, les schémas d'adressage sont essentiels pour distinguer tous les éléments, leurs fonctionnalités, leur emplacement et également pour contrôler ces éléments via Internet. Comme nous le savons, une adresse IP est semblable à un numéro de téléphone ou à une adresse postale. Lorsqu'on se connecte à Internet, chaque appareil est attribué à une adresse IP, ainsi que chaque site possède une adresse IP. Tout ce qui est connecté et les autres éléments qui vont être connectés doivent être identifiés par leur identificateur, emplacements et fonctionnalités. Les caractéristiques à prendre en compte pour créer une adresse unique sont les suivantes : fiabilité, unicité, persistance et évolutivité.

L'IoT a besoin d'une architecture permettant l'évolutivité, c'est-à-dire la capacité de connecter un jour, cent appareils et le lendemain, un million.

Le système d'adressage utilisé depuis la naissance d'Internet s'appelle IPv4 et le nouveau système d'adressage s'appelle IPv6.

La raison pour laquelle le système IPv4 doit être remplacé par IPv6 est qu'Internet manque d'espace adresse IPv4, et IPv6 fournit un nombre exponentiel d'adresses IP, L'IPv6 est utilisé pour l'IoT car IPv4 est incapable de répondre à la croissance rapide des besoins en espace. Il a introduit des schémas d'adressage pris en charge et évolutifs pour fournir un accès sécurisé aux ressources de manière unique et à distance [3].

Stockage et analyse de données La très grande quantité de données contenues dans l'IoT doit être intelligemment collectée, analysée, traitée et stockée pour une surveillance, une activation et une prise de décision plus efficace et plus intelligente. Développer des algorithmes intelligents est une nécessité pour donner un sens à une gestion efficace des données.

Le cloud computing : le stockage basé sur le cloud et les analyses basées sur le cloud constituent une excellente solution pour gérer, stocker et traiter en temps réel les données d'un nombre imprévisible de périphériques. À travers différents appareils IoT, les données sont collectées et peuvent être partagées avec d'autres données via des services basés sur un nuage. Ces services fournissent des informations précieuses aux utilisateurs. En outre, il peut être utilisé pour un meilleur actionnement automatique et une commande à distance [3].

La visualisation est l'aspect le plus important de la conception globale de l'IoT, car toutes les choses et tous les appareils nécessitent une interaction avec les utilisateurs. En cette ère de technologie et de communication, les téléphones intelligents et les tablettes sont devenus très populaires à cause de leur facilité d'utilisation et de leur capacité à accéder rapidement aux informations.
Les écrans 2D et 3D ont fourni aux utilisateurs une grande quantité d'informations utiles de plusieurs manières. L'utilisation de tablettes et de téléphones intelligents est devenue très importante pour permettre cette interaction.

Les systèmes sont capables de modéliser les données obtenues, de déterminer comment détecter les événements et de fournir différentes manières de visualiser les données, mais en essayant toujours de montrer la représentation des informations en fonction des besoins des consommateurs [7,8].

L'IoT fonctionne sur le modèle de réseau TCP/IP et utilise 4 couches et connecte tous les périphériques via Internet. Ces niveaux sont les suivants : niveau de la liaison de données, niveau de la mise en réseau, niveau de transport et niveau d'application [9].

Niveau de liaison de données Sur cette couche, on connecte les périphériques situés à proximité et ceux plus éloignés avec des réseaux appropriés.

Niveau de mise en réseau Le protocole qui est configuré pour dominer au niveau de la mise en réseau est IPv6.

Niveau de transport À ce niveau, TCP (Transmission Control Protocol) a dominé, le protocole est utilisé par HTTP et de nombreux autres protocoles tels que SMTP, POP3 et IMAP4. TCP est un protocole de couche de transport utilisé par les applications nécessitant une livraison garantie. UDP (User Datagram Protocol) est l'un des membres principaux de la suite de protocoles Internet. TCP et UDP sont les protocoles les plus utilisés sur le protocole IP [10].

Le niveau d'application est responsable de la présentation des données. HTTP est probablement le protocole le mieux connu à ce niveau pour faire fonctionner le Web, mais ne convient pas dans les environnements à ressources limitées, car il nécessite des en-têtes complexes comportant au moins neuf paquets TCP. De plus, HTTP ne garantit pas la livraison des messages. L'environnement IoT nécessite de très petites interactions avec de petits appareils et une très faible consommation d'énergie [9].

2.4 Protocoles IoT

De nombreux protocoles ont été développés spécifiquement pour les environnements IoT, Les principaux protocoles sont CoAP, MQTT, AMQP, XMPP et REST [6],[11]-[16].

En raison des nombreuses exigences des périphériques connectés, il est peu probable qu'un seul protocole l'emporte. On explique ici quelques protocoles plus courants utilisés aujourd'hui :
CoAP (Constrained Application Protocol) a été conçu par IETF Constrained RESTful Environment. Il s'agit d'un protocole de transfert Web spécialisé créé pour la connectivité des appareils sous contrainte dans l'IoT et pour les applications M2M telles que l'énergie intelligente et l'automatisation des bâtiments. Il fonctionne uniquement avec UDP et il est très rapide dans la communication entre périphériques. L'architecture CoAP est divisée en deux sous-couches principales :

La messagerie et la demande/réponse. La sous-couche de messagerie est responsable de la fiabilité et de la duplication des messages, tandis que la demande/réponse est responsable de la communication. CoAP comprend quatre types de messages : non confirmable, confirmable, réinitialisation et accusé de réception.

Pour une transmission fiable sur UDP, des messages confirmables sont utilisés. En outre, il utilise le format de données Efficient XML Interchange, qui est un format de données binaire et est plus efficace en termes d'espace par rapport au format HTML / XML en texte brut. Comme UDP autorise la diffusion et la multidiffusion, on peut transmettre à plusieurs hôtes en utilisant moins de bande passante. Cela convient parfaitement aux environnements de réseau local où les périphériques doivent se parler rapidement, ce qui est traditionnel pour certains paramètres M2M.

Il est destiné à être utilisé dans des réseaux à faible puissance et à contrainte, tels que 6LoWPAN et LLN / IoT, nécessitant une surveillance et une manipulation à distance [13], [16].

MQTT (Message Queue Telemetry Transport) est un protocole de publication exécuté sur TCP. Il a été développé par IBM en tant que protocole client / serveur pour répondre aux exigences de messagerie entre périphériques. C'est un protocole qui le rend adapté aux applications IoT. Du fait qu'il fonctionne sur TCP, il ne peut pas être utilisé avec tous les types d'applications IoT. Prend en charge les principaux modèles de messages IoT : publication / abonnement et demande / réponse. Ce protocole implémente la QoS et la communication sécurisée.

MQTT-SN (Message Queue Telemetry Transport-Sensor Network) est une extension de MQTT conçue pour les appareils à faible consommation et à faible coût. Il est basé sur MQTT mais a quelques optimisations pour WSN. Certains protocoles sans fil sont pris en charge par MQTT-SN tels que Bluetooth, ZigBee et UDP [13], [14].

REST (Representational State Transfer) est utilisé comme protocole IoT pour échanger des données entre applications et pour intégrer des applications appartenant à différents domaines. En outre, il utilise HTTP comme protocole basé et utilise le paradigme client / serveur [12].

XMPP Le **protocole de** messagerie et de présence extensible utilise TCP et a été initialement conçu pour la messagerie instantanée [15].

AMQP Le protocole avancé de Message Queuing utilise TCP et est conçu pour connecter des serveurs ensemble [15].

DDS Data Distribution Service utilise TCP et est conçu pour connecter des périphériques à d'autres périphériques.
La **suite de protocoles IoT** inclut les protocoles sans fil suivants :

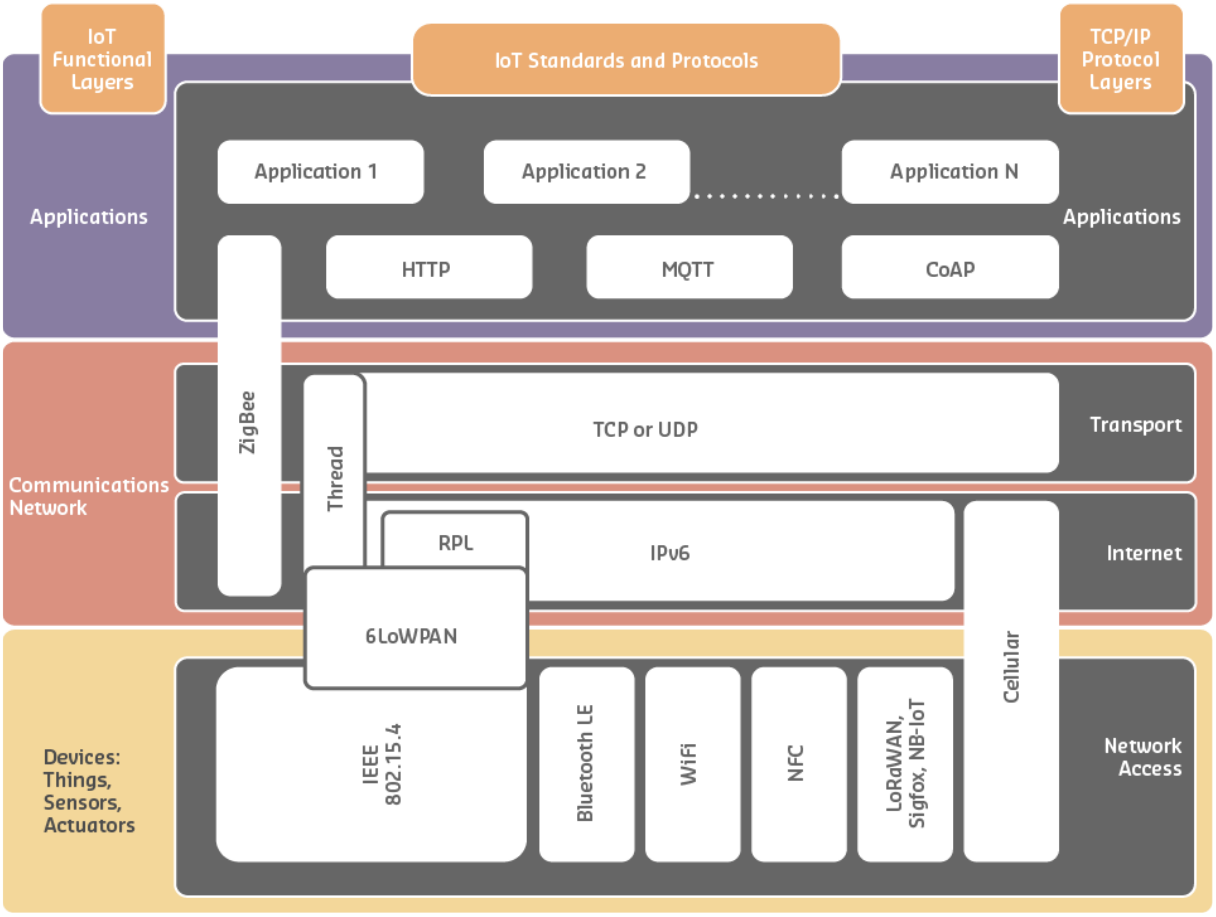


Figure 2.3: Modèle de protocoles IoT

Source : Cisco Netacademy - Principes de base de l'IoT : Sécurité de l'IoT

Le protocole IEEE 802.15.4 est conçu pour les réseaux locaux sans fil à faible débit (LR-WPAN) destinés à être utilisés par des périphériques peu coûteux et à faible vitesse. ZigBee, Thread et 6LoWPAN sont basés sur cette norme.

Zigbee est un groupe simple et peu coûteux de protocoles de communication sans fil de niveau supérieur qui implémentent de petits PANs de faible puissance. Il est largement implémenté dans

la domotique et la collecte de données de dispositifs médicaux. Thread est un protocole maillé sans fil spécialement conçu pour les réseaux domestiques IoT.

Bluetooth Low Energy (BLE) est un réseau personnel sans fil à faible consommation d'énergie (WPAN) fonctionnant sur une fréquence radio de 2,4 GHz avec la même couverture que Bluetooth.

Le Wi-Fi est le protocole de réseau local sans fil (WLAN) le plus courant basé sur les normes IEEE 802.11 qui utilise des fréquences radio de 2,4 GHz et 5 GHz.

La communication en champ proche (NFC) est un ensemble de protocoles pour la communication entre appareils dans une plage de 4 cm.
Cellular est un réseau qui divise la zone de couverture en cellules avec une station de base dans chaque cellule. Il couvre une vaste zone géographique et couvre les technologies mobiles, notamment : 2G (GSM), 3G (UMTS), 4G (LTE / WiMax) et la dernière 5G.

Les protocoles LPWAN (Low-Power WAN) permettent aux périphériques contraints de transmettre de petites quantités de données sur une longue plage allant jusqu'à 10 km. LoRaWAN, SigFox, NB-IoT sont quelques exemples de LPWAN qui fonctionnent généralement sur des bandes RF sans licence.
- Dans l'IoT, il existe quatre types de connexion différents par lesquels les données se déplacent [12], [18] :

-**Device to device** désigne la connexion entre deux périphériques ou plus. Différents types de réseaux peuvent les communiquer et les principaux protocoles utilisés sont Bluetooth, Z-Wave et ZigBee. Ce modèle est utilisé dans différents scénarios, par exemple dans les environnements de maison intelligente où il nécessite un faible débit de données. Il peut également être utilisé dans des environnements de voitures connectées pour partager des informations afin d'améliorer de nombreux problèmes tels que la sécurité et la fluidité du trafic.

-**Device to cloud** représente un périphérique se connectant à un service cloud Internet afin d'échanger des données et de contrôler le trafic des messages. Dans ce modèle, Ethernet ou Wi-Fi peut être utilisé.
- L'appareil à passerelle implique un logiciel d'application fonctionnant sur un périphérique de passerelle local servant d'intermédiaire entre un appareil IoT et un service cloud. Cette passerelle pourrait fournir des fonctionnalités de sécurité et autres telles que la traduction de données ou de protocoles.

-**Partage de données Back-End** Avec ce modèle, les utilisateurs peuvent exporter et analyser des données d'objets intelligents à partir d'un service cloud en combinaison avec des données provenant d'autres sources, puis les envoyer à d'autres services à des fins d'analyse.

2.5 Architecture IoT

L'Internet des objets peut être capable d'interconnecter divers objets hétérogènes via Internet. Il est donc nécessaire de disposer d'une architecture en couches flexible. IoT représente une vaste gamme de technologies et pour cette raison, il est impossible de considérer une seule architecture IoT comme modèle de référence pouvant être utilisé pour toutes les opérations IoT. Il n'y a pas d'architecture standard pour l'IoT et, en fonction du contexte, ces architectures sont utilisées en fonction des besoins souhaités. Les principaux facteurs à prendre en compte lors du développement d'une nouvelle architecture sont la sécurité, la fiabilité, la confidentialité, la qualité de service et l'interopérabilité. Les architectures les plus utilisées sont l'architecture à 3 couches et l'architecture à 5 couches. 20]-[28]

2.5.1 **Architecture à trois couches** a été la première architecture IoT proposée. Elle est composée de la couche de perception, de la couche réseau et de la couche application.

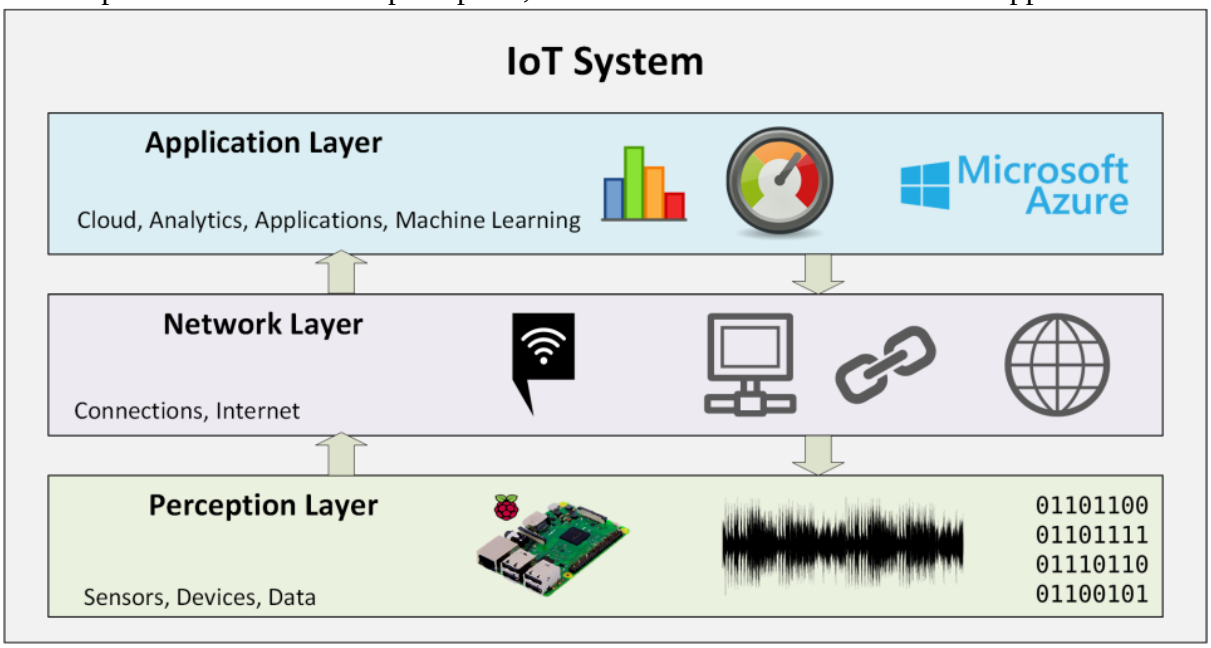


Figure 2.4: Les trois couches de systèmes IoT : couche de perception, couche de réseau et couche d'application.
Source: Mikko Nykyri data analytics for predictive maintenance in a pulp mill

Couche de perception l'objectif de cette couche est d'acquérir les données de l'environnement à travers des capteurs et des actionneurs, qui assurent plusieurs fonctionnalités telles que la localisation, l'humidité, l'accélération, la température, les vibrations, le poids, etc.

Le bon fonctionnement d'un système IoT dépendra des capacités dans la gestion des données et l'utilisation intelligente qui en est faite. Pour cette raison, le système doit pouvoir collecter des informations à partir de ces capteurs, puis les stocker et les analyser. Plusieurs types de capteurs sont utilisés dans les différentes applications disponibles. Cette couche est divisée en deux parties : le nœud de perception (contrôleurs, capteurs, etc.) responsable de l'acquisition de données et le

réseau de perception qui communique avec le réseau de transport et envoie les données collectées à la passerelle ou aux instructions de contrôle du contrôleur. Le capteur bien connu aujourd'hui est le Smartphone. Il est armé avec différents types de capteurs intégrés ; lumière, mouvement, proximité, caméra et microphone. Il existe d'autres capteurs utilisés dans différents secteurs et avec d'autres objectifs. Ils peuvent être des ordinateurs portables, des appareils mobiles, des puces intégrées, des navires, des véhicules et tous les appareils. Chacun de ces objets est considéré comme une source de données pour le réseau IoT. Avant la transmission, les données sont prétraitées par les unités de la couche de perception, puis filtrées et envoyées au réseau. Ces unités ont normalement peu de place pour le stockage temporaire, une petite unité de traitement et des fonctions de sécurité. RFID, NFC et WSN sont des technologies utilisées dans cette couche.

Couche réseau est la couche la plus importante, le cœur de l'IoT, et transmet les informations recueillies par la couche de perception. Cette couche comprend un réseau de convergence, un traitement intelligent, une gestion de réseau et des centres d'information. IPv6 est considéré comme le protocole clé pour cette couche et les technologies 3G, Wi-Fi, FTTX, Bluetooth Low Energy, ZigBee sont certaines des technologies utilisées sur cette couche.

Couche application permet la convergence entre les besoins sociaux de l'IoT et la technologie industrielle. L'objectif de cette couche est de fournir un service d'information composé de trois parties : module client de l'internet des objets, stockage de données et interrogation de données. Cela implique le Cloud Computing, l'informatique omniprésente, le traitement intelligent et les méga bases de données. Quelques exemples d'applications IoT sont l'authentification d'identité, la gestion logistique, le transport intelligent. En raison du développement de l'IoT, l'architecture à trois couches ne suffisait pas pour couvrir toutes les exigences du paradigme de l'IoT. Pour cette raison, d'autres architectures ont été proposées [28].

2.5.2 **Architecture à 5 couches** contient la couche de perception, la couche de transport, la couche de traitement, la couche d'application et la couche de gestion (couche métier).

Couche de perception correspond à la couche de perception de l'architecture à 3 couches et la couche de transport correspond à la couche réseau de l'architecture à 3 couches. Dans la couche de traitement, toutes les données transmises depuis la couche de transport sont stockées, traitées et analysées. Les éléments clés de cette couche sont le cloud computing, l'informatique omniprésente, la base de données et le traitement intelligent.

Couche application crée les applications IoT distinctes et fournit des applications pour une utilisation industrielle. L'acquisition, le stockage, l'analyse et le traitement des données reçues de la couche de transport sont effectués à travers cette couche.

Couche métier est responsable de tout ce qui concerne les applications IoT et la confidentialité des utilisateurs [17], 28].

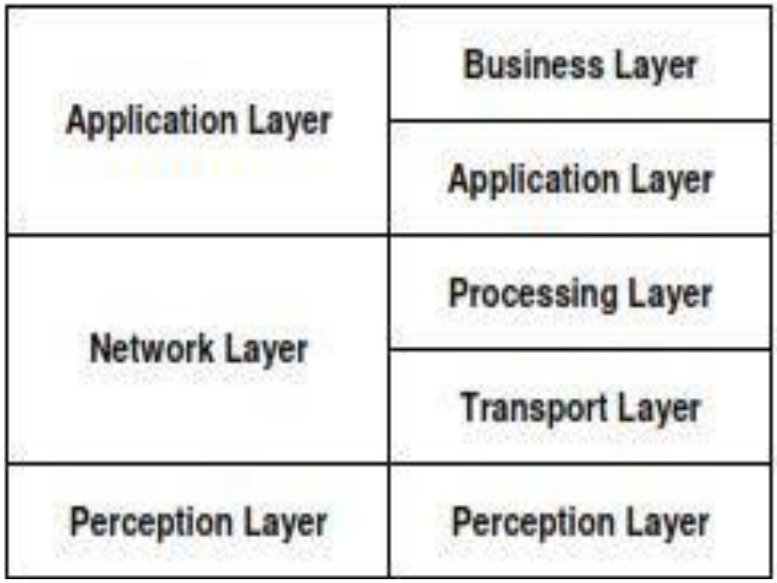


Fig.2.5 L'architecture à 3 couches à gauche et l'architecture à 5 couches à droite

La Fig.2.5 présente les architectures à 3 et 5 couches. À gauche, architecture à 3 couches composée de la couche de perception, de la couche réseau et de la couche application. A droite, architecture à 5 couches composée de la couche de perception, de la couche de transport, de la couche de traitement, de la couche application et de la couche métier.
Il existe d'autres modèles d'architecture utilisés à des fins particulières, mais ils ne peuvent pas être traités comme des architectures standards. Ces architectures sont [22] :

-IoT-A est une architecture orientée métier qui génère différentes architectures de référence en fonction des exigences spécifiques du domaine.

-BeTaaS est une architecture permettant la communication entre machines. Dans BeTaaS, il y a quatre couches ; couche physique, couche d'adaptation, couche TaaS et couche de service.

-OpenIoT est une architecture construite à partir du modèle de référence défini dans l'IoT-A. L'objectif principal est de fournir l'infrastructure qui est un middleware basé sur le cloud.

-IoT @ work est un projet de la Commission européenne. L'objectif principal de ce modèle d'architecture est de créer le domaine de l'automatisation industrielle. Les couches de cette architecture dépendent de sa zone de déploiement.

Vasilomanolakis et al. [22] étudient ces quatre architectures IoT. Ils ont élaboré une liste afin d'établir un ensemble standard d'exigences de sécurité pour les technologies IoT. Ces exigences sont la sécurité du réseau, la gestion des identités, la confidentialité, la confiance et la résilience.

2.5.3 Couche Application

La couche application fournit des services à un programme d'application pour garantir qu'une communication efficace avec un autre programme d'application sur un réseau est possible. Le cloud computing est une technologie de l'information, qui fonctionne dans cette couche

Le cloud computing consiste à fournir des services informatiques tels que des serveurs, du stockage, des bases de données, des réseaux, des analyses et bien plus encore via Internet. Il répartit la tâche de calcul dans un pool de ressources composé d'un grand nombre de ressources informatiques et permet aux utilisateurs d'obtenir un espace de stockage et un service d'informations.

Il existe une grande quantité de ressources informatiques virtuelles capables de se maintenir et de se gérer dans le système. L'intégration de l'IoT et du Cloud Computing peut permettre la création d'environnements intelligents. Dans le développement de l'Internet mobile, les services d'informatique en nuage basés sur des appareils mobiles tels que tablettes, téléphones portables, etc. ont vu le jour et ont été utilisés pour des environnements de partage d'informations [45].

Le cloud computing peut être utilisé dans plusieurs contextes et il existe trois classes fondamentales:

-SaaS (logiciel en tant que service). Dans ce modèle, une entreprise sert le maintenance, support et fonctionnement que les clients utiliseront pendant la période où ils ont souscrit le service. Salesforce est un exemple de SaaS.

-IaaS (infrastructure en tant que service). Dans ce modèle de distribution, le service est fourni via une plateforme de virtualisation. Au lieu d'acquérir des serveurs, des équipements réseau ou de l'espace dans le centre de données, les clients achètent toutes ces ressources à un fournisseur de services externe. La fourniture de ces services se fait via le Web. Amazon Web Services EC2 en est un exemple.

-PaaS (plate-forme en tant que service*)*. PaaS propose plusieurs services fournis en tant que solution intégrale sur le Web. Google App Engine est un exemple de ce modèle.

Le Paradigme Cloud Computing

Lorsque les données sont échangées entre différentes entités telles que des bases de données et des applications, elles sont exposées à plusieurs types d'attaques avant qu'elles ne parviennent aux utilisateurs des menaces pour la sécurité des informations peuvent provenir de la couche par le biais principalement d'accès non autorisés, de vol de données, de fourniture de données. Fausses données, vers et virus, où la couche réseau en modifiant la destination des données et les informations source [20], [21].

La question de la sécurité est le principal aspect concerné par les calculs dans le cloud. Le Cloud Computing implique certaines informations clés des entreprises et devient la cible des pirates. En raison de problèmes de sécurité, il n'est pas recommandé aux sociétés sensibles aux données telles que les sociétés financières et médicales d'adopter la technologie de cloud computing.
Les problèmes de sécurité dans le Cloud Computing incluent :

-**Attaque de Wrapping.** Cette attaque consiste en une duplication du compte utilisateur et du mot de passe lors de la phase de connexion. Les messages SOAP échangés lors de la phase de configuration entre le navigateur Web et le serveur sont donc affectés par les attaquants.

-**Attaque de Flooding.** Ces attaques se produisent lorsqu'un attaquant génère de fausses données, qui pourraient constituer un type de code à exécuter dans l'application d'un utilisateur légitime.

-**Problème de vol de données.** Dans cette attaque, le compte d'utilisateur et le mot de passe sont volés. En conséquence, l'intégrité du stockage et la sécurité dans le cloud peuvent être attaquées.

Pour éviter une attaque de wrapping, Zunnurhain et al.[22] proposent d'augmenter la sécurité lors du passage du message du serveur Web à un navigateur Web à l'aide du message SOAP


SOAP est une spécification de protocole permettant l'échange d'informations structurées lors de la mise en œuvre de services Web dans des réseaux informatiques. Son but est d'induire l'extensibilité, la neutralité et l'indépendance. https://en.wikipedia.org/wiki/SOAP.

La solution consiste à ajouter un bit redondant avec l'en-tête SOAP qui sera déclenché lorsque le message est perturbé par une tierce partie pendant le transfert. Ce bit sera vérifié et s'il est trouvé déclenché, une nouvelle valeur de signature sera générée. Pour atténuer les attaques par inondation, tous les serveurs du nuage pourraient être organisés en un groupe de serveurs. Chaque groupe peut être désigné pour un travail spécifique. Lorsqu'un serveur est surchargé, un nouveau serveur sera déployé dans le groupe.

Pour remédier au vol de données, le client peut, à la fin de chaque session, envoyer un courrier électronique sur l'utilisation et la durée avec un numéro spécial à utiliser pour accéder au système à la prochaine fois.

Stergiou et al. [23] analysent les problèmes de sécurité liés aux technologies IoT et Cloud Computing et à leur combinaison. Pour protéger les données, ils proposent la combinaison des algorithmes AES et RSA dans l'intégration des technologies IoT et Cloud.


AES est un algorithme de chiffrement par blocs à clés symétriques et une norme gouvernementale américaine pour le chiffrement et le déchiffrement des données classifiées et sécurisées. L'AES dispose de trois chiffreurs de blocs fixes de 128 bits avec des tailles de clés cryptographiques de 128, 192 et 256 bits. La taille de la clé est illimitée, alors que la taille maximale

du bloc est de 256 bits. https://www.techopedia.com/definition/1763/advanced-encryption-standard-aes

RSA est un algorithme utilisé par les ordinateurs modernes pour chiffrer et déchiffrer des messages. C'est un algorithme cryptographique asymétrique.

2.6 Menaces et attaques dans l'IoT

Les cyberattaques les plus courantes dans un environnement IoT sont les attaques par botnet, par l'usurpation d'identité, l'usurpation de données et d'identité, l'injection de code et les attaques DDOS.

2.6.1 **Botnet**

Un botnet est un ensemble de périphériques Internet, tels que des ordinateurs, des smartphones ou des équipements IoT, connectés entre eux pour effectuer des tâches particulières. Les botnets ont été développés à l'origine pour optimiser l'efficacité des tâches répétitives nécessaires au bon fonctionnement des sites Web. Par exemple, ils sont utilisés avec Internet Relay Chats pour maintenir une expérience utilisateur cohérente. [27]

Malheureusement, les botnets sont maintenant couramment formés par un attaquant prenant le contrôle des périphériques, sans le consentement préalable de ceux qui en sont propriétaires. Cela se fait par l'utilisation de téléchargements en profondeur, de programmes malveillants et de chevaux de Troie. Il est courant d'utiliser des réseaux de zombies lors d'attaques DDOS, de détourner des données et de mener des campagnes de spam par courrier électronique.

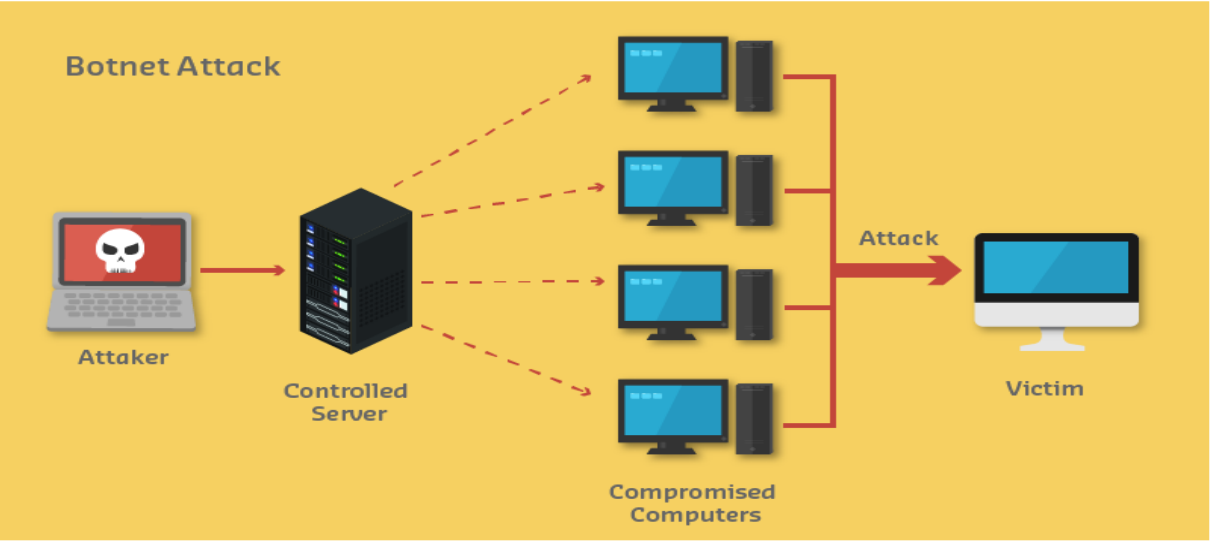


Figure 2.6 attaque botnet

Source : https://courses.edx.org/courses/course-v1:CurtinX+IOT5x+3T2018/course/

2.6.2 **Man In The Middle(MitM)**

Il s'agit d'un type d'attaque d'usurpation d'identité qui intercepte les communications entre les nœuds pour voler des informations telles que les informations d'authentification. Lors de cette attaque, un pirate informatique capture une partie de la communication, généralement des identifiants de connexion, et le rejoue à nouveau pour contourner la phase d'authentification et accéder au système. Les pirates peuvent également manipuler des messages et relayer de fausses informations. [27]

Un scénario de MitM au sein de l'IoT est la transmission de fausses données de capteurs pour interrompre les opérations commerciales et endommager les actifs physiques. Par exemple, de fausses informations sur l'humidité du sol peuvent provoquer des arrosages excessifs et des inondations dans la zone, endommageant les cultures. De fausses lectures à basse température peuvent endommager des périphériques physiques en surchauffant.

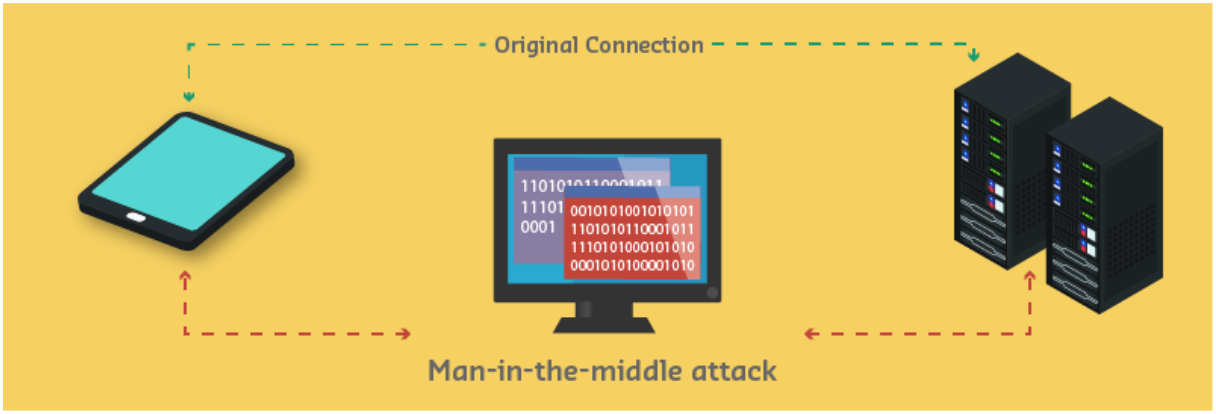


Figure 2.7: Attaque man in the middle

Source : https://courses.edx.org/courses/course-v1:CurtinX+IOT5x+3T2018/course/

L'identité et les données des personnes peuvent être capturées à l'aide de nombreuses ressources avec des mesures de sécurité faibles. De nombreux appareils IoT, tels que les tablettes, les téléphones mobiles et les appareils portables, sont configurés avec des mesures de sécurité faibles, ce qui permet aux pirates informatiques de collecter facilement les informations personnelles et les données d'identité de l'utilisateur.

Pour effectuer le vol d'identité, les pirates collectent le plus de données personnelles possible et les analysent pour découvrir l'identité de la personne ciblée.

2.6.3 **Injection de code**

Dans les attaques par injection de code, un code malveillant est injecté dans un programme informatique, ce qui modifie son déroulement. Les pirates peuvent usurper une identité, modifier ou détruire des données existantes, ou même acquérir l'administration d'un serveur de base de données.

Une méthode de stockage des données d'applications IoT consiste à utiliser des bases de données créées à l'aide du langage SQL (Structured Query Language) ou du langage XML (Extensible

Markup Language). Cependant, ces bases de données peuvent être sujettes aux attaques par injection de code.

- Injection XML : Au cours d'une injection XML, un attaquant tente d'injecter différentes balises XML dans le code dans l'intention de modifier la structure XML. Une attaque réussie aboutit à l'exécution d'une opération restreinte, telle que la modification des données de paiement ou la connexion d'un administrateur non autorisé. WS-Attacks.org fournit des exemples d'attaques et de contre-mesures.

- Injection SQL : Technique d'injection de code qui consiste à placer du code malveillant dans des instructions SQL via des zones de saisie sur des pages Web. Le site w3schools décrit les dangers potentiels de l'utilisation des entrées utilisateur dans les instructions SQL.

2.6.4 **Déni de service (DDoS)**

Le déni de service est un type d'attaque réseau dans lequel des services sont interrompus ou deviennent indisponibles pour les utilisateurs, les appareils ou les applications.

Les deux principaux types d'attaques DoS sont :

- Volume de trafic écrasant : Lors de cette attaque, la cible est submergée par une quantité énorme de données envoyées par l'attaquant à un débit que ne peuvent pas gérer les périphériques, le réseau ou les applications cibler. Cette grande quantité de trafic ralentit éventuellement le service ou peut même provoquer un crash complet du système.

- Paquets formatés de manière malveillante : Lors de cette attaque, le destinataire ne peut pas gérer les paquets formatés de manière malveillante envoyés par l'attaquant. Cela se traduit éventuellement par des performances ralenties ou par un crash complet du système.
Par rapport à d'autres types d'attaques, le déni de service ne dérobe généralement pas d'informations personnelles et ne crée pas de faille de sécurité, mais refuse l'accès aux utilisateurs autorisés des appareils ou des services. Cela peut à son tour entraîner une perte de réputation de l'organisation et avoir généralement un coût élevé pour réparer les dommages.
Si l'attaque DoS provient de plusieurs sources, elle s'appelle attaque DDoS (Distributed Denial of Service).

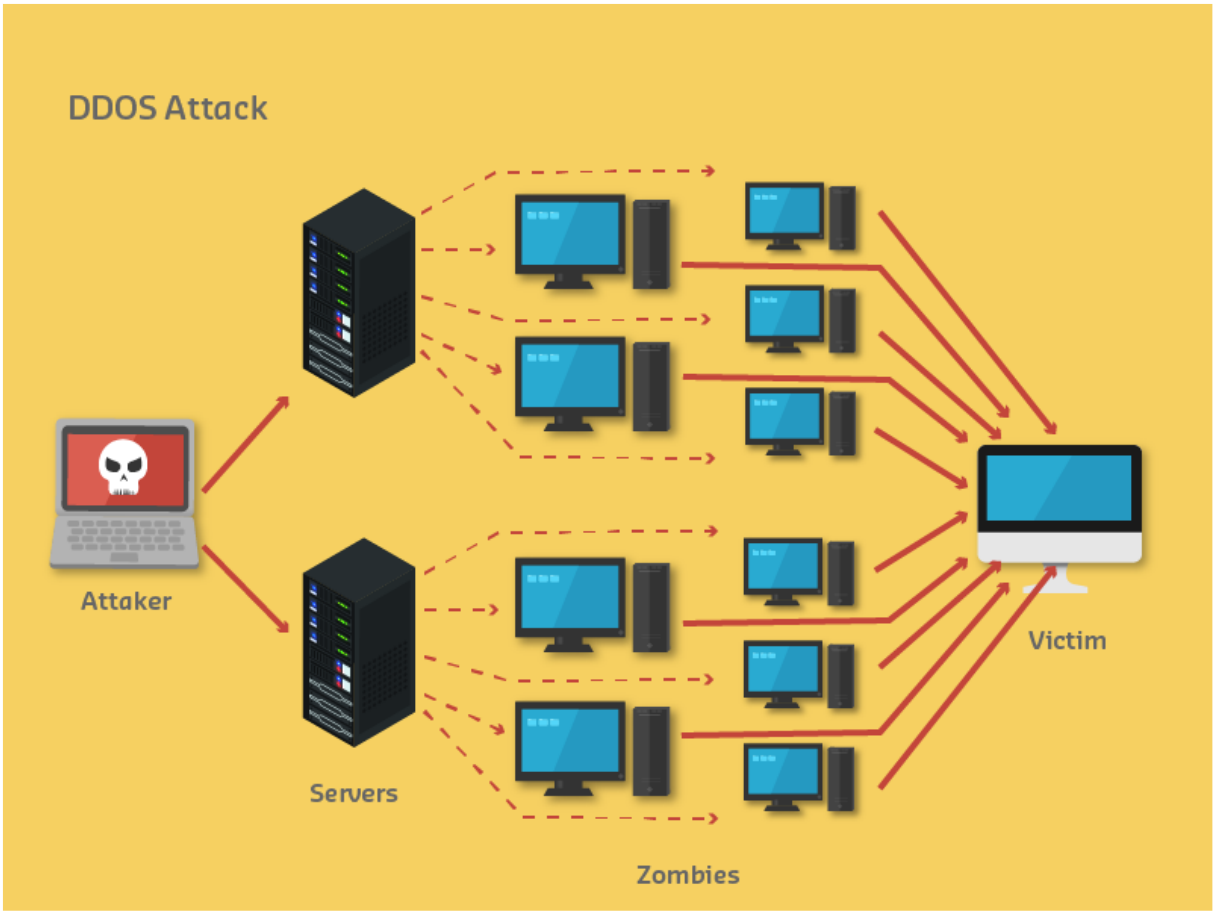


Figure 2.8 : Attaque DDoS

Source : https://courses.edx.org/courses/course-v1:CurtinX+IOT5x+3T2018/course/

2.7 Applications de l'IoT

Le système IoT peut interconnecter presque tous les objets physiques et virtuels de notre environnement qui génèrent de nouveaux services et applications. Ces applications peuvent être adoptées dans différents domaines pour augmenter notre qualité de vie. Cette section fournit une discussion sur les applications IoT courantes.

2.7.1 Domotique

La maison intelligente est l'une des applications les plus populaires du système IoT. Grâce aux technologies de détection et d'actionnement ainsi qu'aux WSN, les gens peuvent connecter une variété d'appareils intelligents à l'intérieur de leurs maisons pour résoudre leurs intérêts. Dans une maison intelligente, il existe plusieurs capteurs pour activer des services intelligents et automatisés qui fonctionnent avec un minimum d'efforts humains. En outre, les capteurs sont utilisés pour maintenir la sécurité et la sûreté [25].

Bien que les avantages pris en charge par la maison intelligente soient innombrables, cela pose certains problèmes de sécurité et de confidentialité, car toutes les actions et tous les événements survenus dans la maison sont enregistrés. Si un attaquant a réussi à enfreindre le système, il peut le faire agir de manière malveillante. Ainsi, la maison intelligente doit être protégée de manière à permettre aux appareils intelligents d'informer le propriétaire de toute action anormale. En outre, la fiabilité est un autre défi car aucun administrateur n'existe pour observer le comportement du système [26].

2.7.2 **Santé**

L'IoT a prouvé qu'il peut offrir plusieurs avantages pour le domaine de la santé en créant de nouvelles applications et services qui aident les patients et maintiennent l'innovation dans le domaine. Il existe plusieurs appareils portables développés pour surveiller et suivre l'état de santé des patients. Ces appareils permettent aux patients plus âgés de vivre de manière autonome sans crainte. En outre, ces dispositifs peuvent être utilisés pour observer et stocker en permanence l'état de santé des patients et envoyer des messages d'avertissement dans des situations anormales. Si la situation est mineure, l'appareil lui-même peut recommander un traitement pour le patient. S'il s'agit d'une situation majeure, l'appareil peut envoyer des messages urgents à l'hôpital ou aux ambulances pour être immédiatement expédiés [27].

2.7.3 **Agriculture intelligente**

Avec l'existence de plusieurs capteurs dans l'environnement IoT, les agriculteurs peuvent utiliser les données collectées pour produire un meilleur retour sur investissement. Les paramètres du sol tels que l'humidité, le niveau de sel et la température peuvent être collectés et mesurés à l'aide des capteurs disponibles pour augmenter la production agricole. De plus, avec l'existence de plusieurs technologies sans fil telles que le système d'information géographique et la télédétection, il existe de nombreuses chances de collecter rapidement et efficacement des informations pertinentes sur le sol, ce qui peut aider à remplacer l'effort humain par des machines automatiques pour augmenter la production agricole. [29].

Il y a une croissance significative de l'adoption des appareils IoT dans le domaine agricole. On prévoit que le nombre d'appareils IoT dans l'agriculture atteindra environ 75 millions d'ici la fin de 2020 [30]. L'intégration de solutions IoT dans l'agriculture présente plusieurs avantages. Par exemple, des capteurs peuvent être utilisés pour surveiller la qualité du sol, la progression de la croissance des cultures et les conditions météorologiques outre les performances du personnel et l'efficacité des équipements. En outre, le système IoT peut aider à automatiser diverses opérations tout au long du cycle de vie des cultures, à améliorer la gestion de la méthode de production et à garantir des normes avancées de qualité des cultures. [31].

2.7.4 **Chaine d'approvisionnement et logistique**

Le système IoT tente de faciliter les opérations du monde réel dans les systèmes d'entreprise et d'information. En utilisant des technologies de capteurs telles que la RFID et la communication en champ proche (NFC), les produits peuvent être suivis du fabricant au lieu de distribution. Les étiquettes RFID attachées aux produits sont utilisées pour identifier de manière unique chaque produit et collecter automatiquement les informations pertinentes pour les transmettre en temps réel avec les informations de localisation. Ces balises sont utilisées pour transmettre des messages

indiquant exactement quels produits, tailles et variations de style, ainsi que la température et l'humidité des produits. De plus, la capture automatisée des données donne une visibilité en temps réel du stock et évite le comptage manuel et les erreurs humaines. En termes simples, l'IoT est sur le point de révolutionner la chaîne d'approvisionnement avec à la fois des efficiences opérationnelles et des opportunités de revenus [32].

2.7.5 **Ville intelligente**

La notion de ville intelligente fait référence à l'adoption d'appareils IoT tels que des capteurs, des compteurs, des lumières, etc., pour surveiller et collecter des informations sur la ville environnante. Ces informations sont utilisées pour améliorer les services publics et les infrastructures de la ville. Les solutions IoT sont impliquées dans de nombreux domaines des villes intelligentes tels que l'éclairage public intelligent, la gestion des déchets, le stationnement intelligent et la gestion du trafic. [33].

Pour le trafic intelligent, les informations collectées par les capteurs sur le trafic peuvent être envoyées aux téléphones des citoyens pour surveiller le trafic en temps réel et permettre aux conducteurs de choisir la meilleure route pour économiser du temps et des efforts de conduite. En outre, les conducteurs peuvent être avertis en cas d'accident pour s'éloigner de la congestion. Pour la gestion des déchets, des capteurs IoT sont déployés dans les poubelles pour envoyer des messages à des autorités spécifiques pour signaler que les poubelles doivent être vidées. En outre, ces capteurs peuvent être utilisés pour optimiser les camions à ordures afin de réduire l'utilisation d'émergence [34].

2.7.6 **Réseau intelligent**

Utiliser efficacement l'énergie et finalement économiser plus d'argent peut être obtenu grâce à l'utilisation de capteurs IoT pour collecter des informations pertinentes sur la consommation d'énergie à la maison, par exemple, en suggérant de meilleures façons d'économiser de l'énergie. En outre, les informations des capteurs IoT peuvent être utilisées pour fournir aux consommateurs toutes les informations pertinentes sur divers fournisseurs d'énergie de manière automatisée pour choisir le meilleur pour les consommateurs.

Le concept de réseaux intelligents ajoute de l'intelligence au cycle de flux d'énergie du fournisseur au consommateur. Ce type d'intelligence peut être utilisé pour aider les consommateurs à être conscients de la consommation d'énergie et de la tarification dynamique [35]. En outre, l'une des principales applications du réseau intelligent est un compteur intelligent qui collecte, enregistre et analyse la consommation d'énergie à différents moments de la journée. Ces informations peuvent être utilisées par les consommateurs pour ajuster leur consommation d'énergie et modifier leur mode de vie afin de réduire les coûts.

2.7.7 **Voiture connectée**

La voiture intelligente ou ce qu'elle appelait la voiture connectée a commencé à être déployée dans notre communauté. Ce type de voiture peut accéder à Internet et partager ses données avec d'autres appareils. Le nombre de voitures équipées de cette installation augmente chaque jour, ce qui va permettre l'apparition de plusieurs applications pour les voitures connectées dans un futur proche [36]. La voiture connectée offre plusieurs avantages par rapport à la voiture normale. Il peut réduire les accidents de voiture et diminuer les erreurs des conducteurs de voiture en permettant au conducteur de conduire la voiture à distance. Ces voitures sans conducteur peuvent également gagner du temps et réduire le stress au volant. Plusieurs constructeurs automobiles tels que BMW, Ford et Volvo ont confirmé qu'il y aura des voitures entièrement autonomes d'ici la fin de 2021 [31].

2.7.8 **Appareils portables**

Les Wearables ont un énorme intérêt sur les marchés du monde entier. De nombreuses entreprises ont commencé à produire ces appareils avec d'énormes quantités pour satisfaire des demandes croissantes telles que Google et Samsung. Selon Statista, le nombre d'appareils portables connectés devrait atteindre 830 millions à la fin de 2020. Les appareils portables sont équipés de capteurs et ont la possibilité de se connecter à Internet pour le partage de données. Ces capteurs collectent des données sur l'utilisateur qui sont ensuite traitées pour extraire des informations significatives. Les appareils portables les plus courants concernent le fitness, la santé et le divertissement [37].

2.8 Défis de l'IoT

Bien que les solutions IoT offrent d'innombrables avantages, elles soulèvent de nombreux défis qui doivent être résolus. Les problèmes les plus courants du système IoT, notamment le Big Data, la mise en réseau, l'évolutivité, l'hétérogénéité, l'interopérabilité et la sécurité et la confidentialité, sont abordés dans cette section. Ils ont également résumé dans Fig.2.9.

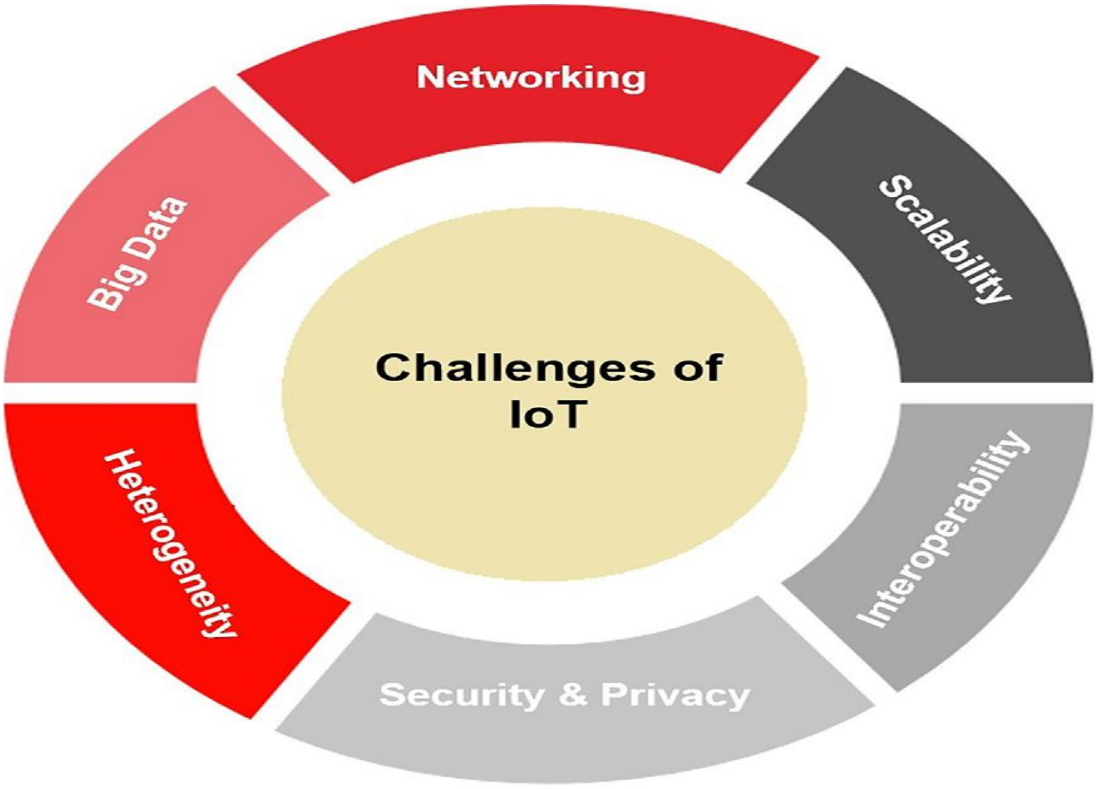


Fig.2.9 Défis de l'IoT

Source : Cisco Netacademy - Principes de base de l'IoT : Sécurité de l'IoT

2.8.1 Big Data

Le Big Data est une expression assez nouvelle qui indique la quantité massive de données, qu'elles soient structurées ou non, ce qui est difficile à traiter avec les méthodes classiques de base de données et les techniques logicielles. Il se caractérise par ce que l'on appelle les 5V, le volume, la variété, la variabilité, la valeur et la vitesse. Le Big Data suscite un énorme intérêt de la part de plusieurs organisations en tant que nouveau domaine industriel tel que les réseaux sociaux en ligne (Twitter, Facebook et Instagram) car il existe une énorme quantité de données collectées via les réseaux sociaux. Par exemple, dans 2010, Twitter a produit en moyenne environ 10 téraoctets de données par jour [38].

Avec des milliards d'appareils et d'objets, l'IoT est l'une des principales sources de Big Data. Bien que le cloud computing puisse être utilisé pour stocker des données de manière permanente, le traitement de cette énorme quantité de données est un problème considérable, en particulier la performance de diverses applications IoT est basée sur le service de gestion de données. En outre, cette énorme quantité de données soulève des problèmes de sécurité et de confidentialité, car garantir l'intégrité des données sera une tâche très difficile à réaliser. [39].

2.8.2 **Réseau**

Le principal moteur du système IoT est de connecter tous les objets / périphériques pour partager leurs informations. Ces dispositifs sont de forme et de structure différente qui fait utiliser différents protocoles de réseau de communication [40]. La mise en œuvre d'un protocole de mise en réseau pour l'IoT doit être conçue en tenant compte des performances et de la convivialité du système. En effet, le protocole réseau a un impact majeur sur le comportement du réseau. Ainsi, le choix du protocole de mise en réseau approprié est un problème qui doit être résolu. En outre, la sélection de la topologie de réseau appropriée pour le protocole est un autre défi [59].

2.8.3 **Hétérogénéité**

L'IoT est l'un des exemples populaires qui décrit le problème de l'hétérogénéité car il implique des milliards d'appareils différents dans leur nature. L'objectif principal du système IoT est de construire une méthode commune pour abstraire l'hétérogénéité de ces appareils et réaliser la meilleure exploitation de leurs fonctionnalités [41].

Étant donné que le système IoT se développe considérablement, la recherche d'applications capables de s'adapter à différents matériels et logiciels des appareils IoT continuera à atteindre l'efficacité maximale du système IoT. Les fournisseurs de services doivent prendre en compte la grande diversité des options de connectivité réseau, des protocoles et des méthodes de communication lors de la mise en œuvre d'un service pour le système IoT.

2.8.4 **Interopérabilité**

L'interopérabilité fait référence à la capacité des composants du système à coopérer les uns avec les autres de manière efficace quelles que soient leurs spécifications techniques. Bien que l'interconnexion d'appareils hétérogènes IoT permette de partager leurs informations, ce qui se traduit par la création de nouveaux services, elle a un prix. Au fur et à mesure que l'acceptation du système IoT augmentait et que le nombre d'objets connectés et de réseaux augmentait, l'interopérabilité devient une priorité fondamentale pour interconnecter efficacement divers éléments. [42]

Malgré la présence de plusieurs résultats proposés pour résoudre le problème d'interopérabilité comme les frameworks open source, la technologie data over-sound et la création d'une couche de services IoT commune, l'interopérabilité reste un défi majeur à relever. [43].

2.8.5 **Evolutivité**

L'évolutivité est l'un des défis majeurs du système IoT qui doit être géré pour contenir l'augmentation massive des appareils connectés. L'évolutivité signifie la capacité du système à faire face à la croissance potentielle du système de manière efficace sans affecter les performances du système. Être évolutif est une opération obligatoire pour que le système IoT réponde aux différentes exigences, car l'intérêt des personnes varie avec le temps et les situations environnementales. [44]. Par conséquent, le problème de l'évolutivité nécessite plus de recherche pour tester les potentiels du système IoT lors de l'augmentation du nombre d'appareils connectés.

2.9 Intégration IoT avec Blockchain

Cette section se concentrera sur la collaboration entre l'IoT et la blockchain, appelée IoT basé sur la blockchain (BIoT). L'intégration de ces deux technologies mentionnées ci-dessus sera une approche décentralisée qui résoudra de nombreux problèmes. En adoptant une communication P2P cohérent, l'utilisateur peut traiter des centaines et des milliards de transactions entre les appareils, ce qui réduira apparemment le coût. La blockchain alliée aux réseaux IoT allouera les besoins de calcul et de stockage sur de nombreux appareils. Cela empêchera donc tout le réseau de tomber en panne. Lors de l'établissement de la communication P2P, un certain nombre de défis tels que la sécurité, l'évolutivité, la confidentialité, etc., entrent en jeu. Lorsque les deux technologies se combinent, une solution qui respectera la confidentialité ainsi que la sauvegarde dans des réseaux gigantesques peut être proposée. Cette combinaison ne compromettra aucune forme de validation et d'accord pour les transactions afin que les activités telles que l'usurpation d'identité et le vol puissent être facilement évitées. Pour accomplir les utilitaires liés aux solutions IoT habituelles sans tactique décentralisée, il sera difficile de gérer les transactions. [47] Donc, il doit garder trois fonctions fondamentales:

- Messagerie d'égal à égal
- Partage de fichiers diffusé
- Harmonisation des appareils autonomes

La sauvegarde doit être construite comme la base des structures IoT, avec des autorisations de légitimité sévères, une justification et une authentification des données. Après cela, les données doivent être mieux encodées pour améliorer le système de sécurité [43]. Au niveau de la sollicitation, développement logiciel les administrations ont besoin de meilleures compétences en codage qui sont non seulement stables, mais également robustes et fiables, avec des normes améliorées d'amélioration du code, une étude des menaces et une analyse. Lorsque les systèmes interagissent avec chaque appareil, il est vraiment crucial d'avoir une norme d'interopérabilité approuvée, ce qui est inoffensif et légal. Sans avoir une structure inférieure en béton, il peut créer plus d'intimidations avec tous les appareils connectés au réseau IoT. Notre objectif est de sécuriser et de protéger les appareils IoT. Cela peut être fait à l'aide de la blockchain car elle prend en charge les clés cryptographiques et le réseau décentralisé.

Les appareils IoT génèrent beaucoup de données. Le besoin de l'heure actuel est d'assurer la sécurité et la fiabilité des données pour le contenu généré par des millions d'appareils IoT hétérogènes. La technologie blockchain peut aider à augmenter la sécurité des données. La nature décentralisée de la technologie blockchain élimine les inconvénients associés à un système basé sur une architecture centralisée. Par exemple, les téléphones mobiles et les smartphones; les utilisateurs veulent que la taille de l'appareil soit réduite sans aucune compensation avec la sécurité de l'appareil ou la fonction de calcul. De même, dans le cas de l'IoT, les gens préfèrent les appareils de petite taille qui peuvent suivre leur santé ou leurs données financières sans compromettre aucun type de perte en raison de la grande vulnérabilité aux menaces de sécurité.

2.9.1 Besoin d'intégration de l'IoT et de la Blockchain

L'IoT génère un vaste réseau gigantesque à l'aide d'interactions de machine à machine. Les capteurs numériques, les appareils photo ou les smartphones sont tous des machines. Nos défis sont d'augmenter la confiance dans un tel environnement où chaque machine a accès aux données et ils vérifieront s'il y a une falsification par un appareil ou un nœud. L'intégration BIoT peut augmenter le partage de données et les parties prenantes d'une gestion de la chaîne d'approvisionnement. Les villes intelligentes et les véhicules intelligents doivent partager des données qui doivent être fiables. Des données fiables apportent plus de nœuds dans le système et augmenteront en fin de compte les performances. [47]

La technologie blockchain apporte de l'autonomie en créant un environnement pour BIoT où les appareils ou les machines peuvent interagir. BIoT permettra à l'IoT pour les paiements numériques avec ses fonctionnalités de traçabilité. Bien que la faible vitesse de calcul des nœuds de la blockchain soit un problème grave et qu'elle réduit également les performances de l'IoT. Cependant, BIoT fournira également des calculs rapides. Cette augmentation de la puissance de calcul est en fait le résultat du BIoT. [47]

Une telle intégration de la technologie blockchain et de l'IoT permet en fait aux utilisateurs de profiter des avantages des deux technologies de manière plus efficace et plus puissante. Cependant, la mise en œuvre de l'intégration de la blockchain et de l'IoT présente de nombreux problèmes et défis qui seront abordés dans la sous-section suivante. Certains des avantages de BIoT sont les suivants. [47]

- Augmentation de la vitesse de calcul
- Augmentation de la confiance
- Sécurité des données
- Augmentation de la capacité de génération de données des nœuds IoT
- Résolution des problèmes d'évolutivité des nœuds de blockchain de manière transparente.
- Augmentation de la traçabilité de toutes les transactions
- Résolution des problèmes d'adressage
- Rendre les machines intelligentes
- Collection des données à partir de la source et du traitement

2.9.2 Les défis de l'intégration

BIoT tire le meilleur parti de la technologie blockchain et de l'IoT. Mais il y a quelques défis à relever :

- Actuellement, les protocoles basés sur le consensus choisissent le mineur avec un certain degré de hasard. Mais en l'absence de consensus du réseau, ils peuvent devenir victimes des

fourchettes de la blockchain. Par conséquent, il est nécessaire de développer des protocoles de consensus axés sur l'IoT pour le système BIoT. De tels protocoles peuvent gérer la complexité de communication toujours croissante.

- L'évolutivité de la blockchain est également l'un des problèmes importants.

- La sécurité des appareils et des protocoles IoT contre les menaces réseau telles que les logiciels malveillants doit également être abordée. La blockchain isolée est capable de contrer de telles attaques de manière très efficace, mais cela devient un problème avec les appareils IoT.
- La confidentialité des données dans les nœuds de la blockchain est un problème très critique qui doit être traité de manière très efficace. Par exemple, les dossiers médicaux d'un patient ou les devis intelligents pour les contrats intelligents sont des cas d'utilisation de BIoT qui exigent la confidentialité.
- Les données générées à partir d'un grand réseau IoT en temps réel apportent une limitation sérieuse pour BIoT.

2.9.3 **Avantages de l'intégration**

En intégrant la technologie blockchain à l'IoT, nous espérons bénéficier des avantages suivants:

- L'architecture décentralisée de la blockchain augmente la sécurité des dispositifs hautement vulnérable de l'IoT. Hacker peut modifier ou altérer uniquement la blockchain locale car il est très difficile d'apporter des modifications dans chaque bloc de blockchain.
- Sécurité renforcée de la blockchain grâce au cryptage et aux algorithmes cryptographiques de la blockchain.
- Les contrats intelligents sont stockés dans un réseau blockchain qui non seulement réduit le temps de traitement d'une transaction, mais aide à plusieurs types de détection de fraude.
- La combinaison BIoT a le potentiel d'éliminer le besoin d'intermédiaires.

- La combinaison BIoT conduit au cadre dans lequel les algorithmes d'apprentissage automatique peuvent être appliqués aux données en temps réel générées à partir d'appareils IoT basés sur la blockchain et peuvent permettre le renforcement de la gestion de la chaîne d'approvisionnement.

2.10 Conclusion

La technologie blockchain était initialement censée être l'architecture derrière la crypto-monnaie, mais elle est maintenant utilisée dans de nombreux domaines divers. Les efforts doivent tirer des leçons de l'expérience de son utilisation dans la monnaie Crypto et s'orienter vers ses applications dans divers domaines tels que les soins de santé, l'économie et les régimes de protection sociale du gouvernement… Une prise de conscience pour accroître les connaissances sur la technologie

blockchain dans les organisations est nécessaire. Il faut identifier les domaines dans lesquels la technologie blockchain peut résoudre le problème de l'intermédiation. L'IoT, bien que de plus en plus populaire, souffre de vulnérabilités en matière de sécurité et de confidentialité [48]. Les méthodes traditionnelles de sécurité et de confidentialité sont inappropriées pour l'IoT en raison de la topologie décentralisée. Le problème devient plus grave car dans l'IoT, de nombreux appareils ont des contraintes de ressources. Des millions d'appareils qui forment l'épine dorsale de tout réseau IoT sont également susceptibles d'être attaqués par des pirates informatiques menant au vol de données. Des efforts sont nécessaires pour rechercher une intégration transparente pour établir la relation entre les objets et leurs environnements.

L'IoT peut en outre être appliqué dans plusieurs industries, ce qui conduit au terme IIoT. La combinaison de la blockchain et de l'IoT doit être utilisée afin de surmonter les limites de la blockchain. Une telle combinaison est capable de réduire les algorithmes d'extraction coûteux en calcul de la technologie blockchain. Ainsi, avec cette combinaison, on peut opter pour une architecture IoT légère. Pour maximiser les avantages de la combinaison blockchain et IoT, de nouveaux modèles devraient être créés pour prendre en charge différentes applications IoT distribuées. Pour une combinaison réussie de blockchain, l'IoT doit résoudre des problèmes tels que l'évolutivité et la réduction du trafic aérien indésirable. Les concepteurs de bases de données doivent travailler pour améliorer le débit des transactions des bases de données blockchain. Avec l'augmentation rapide du nombre de transactions, la convolution de l'algorithme de minage augmente, la blockchain est analogue à Internet; Internet qui est connu aujourd'hui n'a rien à voir avec ce qu'il était à l'époque, il en va de même pour la blockchain. La blockchain, lorsqu'elle fusionne avec l'IoT, peut ajouter un tout nouvel aspect à Internet, ce qui introduira non seulement de nouvelles normes de transparence des données, mais entraînera également une meilleure communication P2P.

3 Chapitre 3 : Etude de solution existante d'authentification mutuelle basés sur la Blockchain

3.1 Introduction

L'Internet des objets (IoT) est l'endroit où presque tout peut être contrôlé et géré à distance. L'évolution de l'IoT a permis de rendre la vie beaucoup plus facile, d'améliorer les fonctionnalités et les fonctionnalités des appareils [51]. Les appareils IoT sont constitués de composants physiques, L'Internet des objets (IoT) est l'endroit où presque tout peut être contrôlé et géré à distance. L'évolution de l'IoT a permis de rendre la vie beaucoup plus facile, d'améliorer les fonctionnalités et les fonctionnalités des appareils. Par exemple, pendant un jour de pluie, une personne peut fermer les fenêtres de la maison et allumer les radiateurs à distance depuis son bureau. Les appareils IoT sont constitués de composants physiques, tels que les microcontrôleurs, les émetteurs-récepteurs et la mémoire. En plus de cela, ils sont intégrés à un ensemble de protocoles simples, qui établissent la communication entre les appareils IoT et leurs utilisateurs, et des codes écrits pour gérer et contrôler les appareils IoT [52]. L'IoT contribue à rendre Internet universel et immersif en permettant des communications simples et larges avec de nombreux appareils, tels que les appareils domestiques, les automobiles, les caméras de surveillance et les capteurs. En outre, l'IoT aide au développement de nombreuses applications qui utilisent la quantité excessive de données générées par ces appareils pour offrir de nouveaux services aux personnes, aux gouvernements et aux organisations. En outre, il est à noter que de nombreuses industries ont commencé à fabriquer des appareils IoT où il existe de nombreux produits IoT à utiliser pour les maisons intelligentes, l'assistance médicale, les fabricants de véhicules et dans une variété d'autres domaines [53]. Indépendamment des fonctionnalités avancées de l'IoT, les appareils IoT eux-mêmes ne sont pas sécurisés. L'absence de systèmes de gestion de clés robustes, une authentification d'identité efficace, une faible tolérance aux pannes et de nombreux autres problèmes conduisent les appareils IoT à être facilement ciblés par les attaquants [55].

Pour surmonter ces problèmes fondamentaux, de nombreux travaux de recherche ont exhorté à utiliser la technologie Blockchain, car ses fonctionnalités peuvent fournir des solutions prometteuses pour une variété de problèmes de sécurité IoT. La blockchain possède de nombreuses fonctionnalités avancées qui la distinguent de toute autre technologie [56]. Initialement, la blockchain était liée au bitcoin, qui est principalement connu pour ses mécanismes de preuve de travail et basés sur le hachage. De nos jours, la blockchain est connue pour fournir des garanties de sécurité et fonctionnelles. La blockchain peut être utilisée par de nombreuses industries dans différentes applications pour améliorer à la fois la fonctionnalité et la sécurité [60]. Les systèmes d'authentification robustes utilisés dans la crypto-monnaie pour authentifier les transactions ont rendu le champ de la crypto-monnaie protégé contre diverses attaques [61]. La sécurité de l'IIoT a besoin d'un solide système de gestion de l'authentification des identités qui authentifie les appareils. De plus, la prise en compte des capacités limitées des dispositifs IIoT en réduisant autant que possible la consommation de ressources est cruciale pour la durabilité du domaine IIoT.

Ce travail vise à répondre aux questions suivantes:

3.2 Présentation du projet

3.2.1 Problématique

Actuellement, les systèmes de gestion de l'authentification d'identité appliqués dans l'IIoT ont deux défis principaux qui les empêchent d'être largement adoptés. Ces défis sont la faible vitesse et le stockage de ses appareils.

Le développement d'un protocole d'authentification basée sur la blockchain léger et solide pour authentifier mutuellement les identités des dispositifs IIoT et des coordinateurs ainsi que leurs messages est le principal problème à résoudre dans ce chapitre. Avoir un tel protocole protège contre divers types d'attaques, telles que l'attaque de l'homme du milieu(MitM), la modification et la fabrication de messages.

3.2.2 Objectif

- Proposé un protocole d'authentification mutuelle efficace pour authentifier les identités et les messages IIoT tout en étant suffisamment léger pour s'adapter aux capacités limitées de l'IIoT

- Montré comment ce protocole peut-il améliorer la sécurité IIoT et le protéger contre de nombreuses attaques.

3.3 Utilisation de la blockchain pour la gestion de la confiance et l'authentification dans l'IoT

Dans 2017, le document intitulé «Blockchain Based Trust & Authentication for Decentralized Sensor Networks» a posé un modèle de sécurité qui utilise la structure de données blockchain pour enregistrer les capteurs d'authentification décentralisée et les données de confiance pour atteindre l'intégrité et la validité, pour avoir des données cryptographiques authentifiées, et la confiance dans un réseau pair-à-pair de capteurs sans fil homologues, largement utilisé dans l'environnement IoT [54]. De plus, la gestion de la sécurité et de la confidentialité dans WSN pose des problèmes tels que la faiblesse des ressources de calcul, les contraintes de consommation d'énergie et la fonctionnalité matérielle. En outre, le document s'est concentré sur deux sujets, la sécurité et la confidentialité des données, l'authentification des nœuds et la gestion de la confiance. Premièrement, l'authentification et la gestion de la confiance; WSN a des contraintes de sécurité sur l'authentification des nœuds pour confirmer la validité et la confidentialité des données. Deuxièmement, la gestion de la confiance, qui est prise en compte dans le mécanisme d'authentification pour reconnaître le fiduciaire et le fiduciaire. En outre, ce chapitre a brièvement mentionné la blockchain et son utilisation dans les transactions financières, où elle utilise des blocs de hachages cryptographiques dans un ordre linéaire qui ont le hachage de bloc précédant et suivant pour assurer la continuité [54]. Le cadre est une

architecture orientée service qui gère les données dans un réseau décentralisé, qui se compose de nœuds à ressources limitées qui utilisent un système intégré en eux. Le module proposé est le module d'authentification et de confiance Blockchain (BATM), où il utilise une infrastructure à clé publique pour assurer la confidentialité par le cryptage, l'authentification par signature numérique et la confiance par la validation d'identité de Peer. L'authentification BATM utilise une clé principale pour générer des clés secondaires pour le cryptage et la signature numérique, de sorte que la gestion des clés a une grande importance dans le module. L'exploration de blocs BATM, où la charge utile de données contient les informations sur l'état du nœud de réseau (NN) et les données cryptographiques. Dans le cas de l'authentification, le nœud donne ses informations d'identification, y compris la clé principale, les clés secondaires. En outre, pour réduire le nombre d'attaques, le renouvellement de la clé est effectué en ayant des délais de validité de clé, où la clé est renouvelée lorsque le temporisateur expire [54]. De plus, la confidentialité de la sécurité du réseau dépend des données de la blockchain, donc BATM empêche l'ajout d'un nouveau bloc à moins qu'il ne provienne d'un nœud authentifié qui n'a créé aucune charge utile dans le bloc, où le choix de la charge utile à inclure dans le bloc se fait par le mineur. De plus, pour avoir un bloc valide, il doit résoudre un problème et inclure la charge utile valide approuvée du mineur (y compris la signature numérique de valeur aléatoire du bloc authentifié précédent), que les deux sont créés par le mineur. Comme démontré dans l'algorithme ci-dessous [54].

Algorithm 1: Block Validity Check

Require: currentblock, previousblock **Ensure:** block validity

```
1:  if not (HashCurrentBlock resolves problem) then
2:  return false
3:  end if
4:  if not (MinerApproval payload valid) then
5:  return false
6:  end if
7:  if CurrentBlock has event payload for miner NN then
8:  return false
9:  end if
10:  if not (all payloads in block valid) then
11:  return false
12:  end if
13:  return true
```

Gestion de la confiance BATM, qui est accomplie en maintenant le niveau de réputation des nœuds, où la réputation est constituée d'une surveillance mutuelle de tous les nœuds du réseau, qui peut être connue à partir de la charge utile du nœud où il contient le comportement du nœud provenant de son actions, et il est collecté au fil du temps pour assurer sa crédibilité. En outre, le niveau de confiance est calculé à partir du nombre de nœuds authentifiés sur le nœud. Cette façon de gérer la confiance a rendu impossible pour les attaquants de surcharger le réseau de nœuds validés en ayant, des minuteries, des délais de validité des clés et la réputation des événements [54]. En conclusion, ce chapitre présente un nouveau module qui utilise la

blockchain dans les réseaux de capteurs décentralisés; qui est l'un des principaux composants de l'IoT, qui assure la gestion de la confiance et l'authentification, la sécurité et la confidentialité des données dans le but d'une meilleure gestion des informations des utilisateurs. Un autre mécanisme qui traite de l'authentification des appareils IoT a été proposé dans 2018 nommé BCTrust [57]. BCTrust a été proposé par Hammi et al. [57]. Il est basé sur la technologie blockchain et il cible le domaine de l'IoT car il ne surcharge pas ses appareils. Le mécanisme a été mis en œuvre via la plate-forme Ethereum, avec une couche supplémentaire pour rendre le réseau blockchain privé. De plus, certains nœuds ont reçu des privilèges élevés, comme indiqué dans le contrat intelligent. Ces nœuds sont nommés coordinateur du réseau personnel (CPAN). Les nœuds CPAN sont les seuls à pouvoir effectuer des transactions, et pour assurer cette sécurisation, chaque nœud possède sa propre paire de clés.

Chaque nœud CPAN gère un ensemble de nœuds sous lui. Dans le mécanisme BCTrust, le principe «L'ami de mon ami est mon ami» est ce sur quoi repose le mécanisme. Par cela, si un nœud nommé n est géré par le CPAN du nom N, alors N authentifie initialement n. Une fois n authentifié, une transaction est envoyée à la blockchain pour être validée par les CPAN. Cette transaction montre que N authentifie et gère n, et par conséquent, N a les clés symétriques partagées de n à utiliser pour échanger des données en toute sécurité. Tout ce processus se fait en échangeant quatre messages. Si n veut changer son CPAN, pour être dans un ensemble différent de nœuds, il suffit d'échanger deux messages pour ce processus. Tout d'abord, le nouveau CPAN vérifie la transaction susmentionnée dans la blockchain. Deuxièmement, si ce nouveau CPAN trouve que n est déjà authentifié par N, il demande la clé de n via un canal sécurisé qui utilise une clé et un vecteur d'initialisation. Maintenant que le nouveau CPAN a la clé de n, n est officiellement considéré comme géré par ce CPAN, qui doit donc envoyer une transaction exactement comme la précédente. Le travail en [57] ont montré comment leur mécanisme a moins de temps et de consommation d'énergie par rapport aux mécanismes précédents. La raison principale en serait la réduction des messages nécessaires à échanger lors de l'association d'un nœud à un nouveau CPAN.

3.3.1 Utilisation de la blockchain pour contrôler les appareils IoT

Cette section traite de deux travaux connexes sur l'utilisation de la technologie blockchain pour contrôler les appareils IoT en termes de consommation de ressources.

Huh et coll. [59] ont proposé une nouvelle approche pour gérer les appareils IoT et les sécuriser. Ce qui différencie leur approche des autres, c'est leur adoption de la technologie blockchain. Néanmoins, l'approche a pris en compte les limites des capacités de l'IoT et propose un mode d'économie d'énergie. La plate-forme blockchain adoptée ici est Ethereum, et le cryptosystème utilisé est RSA. Les clés publiques sont stockées via Ethereum, tandis que les clés privées sont conservées sur les appareils eux-mêmes. Ethereum utilise des contrats intelligents. Dans cette approche, les contrats sont utilisés pour inclure des codes de contrôle des appareils IoT.

Javid et coll. [54] ont proposé une intégration de la blockchain avec l'IoT en utilisant une plateforme décentralisée basée sur la blockchain. Leur travail visait à empêcher l'accès non autorisé au réseau en utilisant la fonctionnalité de contrat intelligent d'Ethereum. Ils ont également proposé une méthode d'allocation de ressources permettant de résoudre le problème de la transformation des appareils IoT en zombies pour effectuer des attaques DDoS. La

solution proposée d'intégration d'Ethereum à l'architecture de communication appareil-serveur IoT a trois propriétés de sécurité et d'architecture, un cadre basé sur la blockchain pour détecter et prévenir les attaques IoT DDoS; un cadre distribué pour contrôler et permettre des opérations IoT sans confiance; et l'intégration des anciens appareils IoT avec de faibles capacités de calcul.

Comme [53] a mentionné les problèmes de point de défaillance unique que le serveur centralisé IoT introduit; le cadre IoT-Ethereum proposé dans [53] utilise la fonctionnalité de contrat intelligent pour éviter de tels problèmes, ainsi que d'autres problèmes liés à l'authentification et à la confiance. Le point de défaillance unique peut être éliminé en répartissant le contrôle et la confiance entre plusieurs nœuds participants; où les exigences de calcul pour exécuter la blockchain sont réparties entre les nœuds, et la confiance est établie par un protocole de consensus au lieu d'un tiers; le cadre peut être considéré comme décentralisé par les méthodes précédentes.

3.3.2 Comparaison

Pour analyser les solutions actuelles de renforcement de la sécurité IoT, et pour décider de la contribution éventuelle à proposer, six des travaux de recherche précités, des solutions proposées sont utilisées comme références. Comme représenté sur le **tableau.3.1**, les solutions sont BATM [54], BCTrust [57], Li et coll. [63], Ting et coll. [62], Huh et coll. [59] et IoT-Ethereum Framework [53]. La comparaison est faite en fonction des aspects de sécurité qu'ils ciblent, ces aspects sont la confidentialité, l'intégrité, la disponibilité, l'authentification, l'autorisation, la non-répudiation et une gestion des clés. Outre les aspects de sécurité, d'autres facteurs sont choisis, à savoir l'utilisation de la blockchain (BC), si la solution utilise la blockchain ou non, et la consommation de ressources, si la solution proposée tient fortement compte des faibles capacités des appareils IoT et utilise leurs ressources. Efficacement avec une consommation relativement faible ou non.

Tableau 3.1 : Comparaison entre les solutions proposées par les travaux connexes

Facteur	Solutions					
	BATM	BCTrust	LX	TTW	HCK	IoT-Ethereum framework
confidentialité	√	√	√	√	√	×
intégrité	√	√	√	√	√	×
disponibilité	×	√	×	×	×	√
authentification	√	√	√	√	√	√
autorisation	×	√	×	×	×	√
non-répudiation	√	√	√	√	√	√
consommation de ressources	√	√	×	√		×
gestion des clés	√	×	×	×	√	×

3.3.3 Analyse

Cette section fournit une analyse des solutions comparées dans **tableau3.1**. Il analyse chaque solution sur la base des facteurs abordés. Dans le modèle BATM, il utilise la blockchain pour

garantir deux des principaux composants du modèle de sécurité de l'information, à savoir la confidentialité et l'intégrité via le cryptage. De plus, il fournit une authentification en utilisant une infrastructure à clé publique et une signature numérique tout en garantissant la non-répudiation en utilisant la signature numérique. De plus, il consomme moins d'énergie et prend moins de temps selon le modèle RESTful [58], en outre, il consomme moins de ressources car il y a peu de gaspillage de ressources en référence à l'architecture orientée services, sur laquelle BATM est basé [64].

Pour la seconde solution, le mécanisme BCTrust, tous les aspects de sécurité sont pris en compte. Il utilise une plate-forme Ethereum privée personnalisée, ce qui lui permet de satisfaire à la fois les aspects de sécurité appliqués dans Ethereum. De plus, l'utilisation de clés symétriques et asymétriques et la procédure qu'elle suit pour authentifier les appareils IoT satisfont aux aspects de confidentialité, d'intégrité et d'authentification. En ce qui concerne la consommation de ressources, BCTrust consomme moins d'énergie que les mécanismes précédents. La principale raison derrière cela serait la réduction des messages nécessaires à échanger lors de l'association d'un nœud à un nouveau CPAN, comme expliqué précédemment.

Pour les schémas LX et TTW, les deux prennent en compte les mêmes aspects de sécurité, à savoir la confidentialité, l'intégrité, l'authentification et la non-répudiation. Ils ne considèrent pas l'aspect autorisation comme dans le BATM. De plus, ces systèmes n'utilisent pas la technologie de la blockchain. LX et TTW varient dans les gammes de consommation de leurs ressources. Le schéma TTW consomme moins de mémoire et d'énergie que LX [63]. Néanmoins, le schéma TTW a une meilleure utilisation pour les microcontrôleurs dans lesquels il l'a rendu plus rapide que LX d'environ 30%. Contrairement au schéma LX qui consomme fortement les microcontrôleurs pendant l'une de ses phases, qui est la phase unsigncrypt.

Quant à l'approche HCK, elle adopte la technologie blockchain, contrairement à LX et TTW. Quant aux aspects de sécurité considérés, ils couvrent les mêmes que les schémas LX et TTW. Pour la consommation des ressources, HCK dispose d'un mode d'économie d'énergie [59]. Cela aide à économiser l'énergie des appareils IoT. En ce qui concerne la consommation de mémoire, HCK nécessite un support de stockage élevé, ce qui n'est pas applicable dans les appareils IoT. Par conséquent, une solution à cette faiblesse doit être abordée dans les travaux futurs.

Enfin, quant au framework IoT-Ethereum, il cible et prend en compte les aspects de sécurité de disponibilité, d'authentification, d'autorisation et de non-répudiation. De plus, il utilise la technologie blockchain, car il utilise Ethereum, une variante de blockchain. De plus, les transactions et l'échange de données sont vérifiés dans ce cadre en utilisant des capacités de calcul et de traitement élevées [53].

Après avoir comparé et analysé les solutions proposées dans les travaux associés, il s'avère que BCTrust est la seule solution qui a pris en compte les six aspects de sécurité spécifiés. En plus de cela, le mécanisme BCTrust a eu le moins de frais généraux sur les appareils IoT où il n'épuise pas leurs capacités limitées. Sur cette base, travailler sur d'autres améliorations de ce mécanisme peut conduire à disposer d'un mécanisme puissant d'authentification et de gestion des appareils IoT.

Tableau 3.4 : comparaison des solutions en termes de performance

Solutions / **Critères**	BATM	BCTrust	LX	TTW	HCK	IoT-Ethereum framework
Capacité de calcul	Elevée	Elevée	Faible	Faible	Elevée	Elevée
Temps de traitement	Faible	Faible	Moyenne	Faible	Faible	Faible
Consommation d'énergie	Moyenne	Très faible	Elevée	Moyenne	Faible	Faible
Capacité de mémoire requise	Faible	Faible	Elevée	Moyenne	Elevée	Moyenne

3.4 La solution Authenblue

Le protocole Authenblue vise à améliorer le mécanisme d'authentification dans le protocole BCTruct. BCTrust dispose d'un mécanisme d'authentification pour authentifier les appareils IIoT et les CPAN dans les réseaux OCARI. En outre, il utilise la technologie blockchain pour améliorer la fonction d'association. Quant à Authenblue, il doit être appliqué dans un environnement WSN basé sur Zigbee. L'accent est mis sur la personnalisation, l'association, l'authentification et les fonctions de cryptage / décryptage. Authenblue authentifie les identités et les messages IIoT d'une meilleure manière. De plus, il a une meilleure gestion des clés que celle de BCTrust. Authenblue vise à fournir une authentification élevée des identités et des paquets des appareils IIoT, ainsi qu'un bon cryptage et une bonne intégrité. Pendant ce temps, assurer sa légèreté et sa compatibilité avec les capacités limitées des environnements IIoT. Authenblue fournit une authentification mutuelle légère et une méthode de gestion des clés pour les périphériques IIoT et leurs CPAN dans le WSN. Dans un WSN, il existe différents clusters. Chaque cluster possède des périphériques IIoT et est coordonné par un CPAN. Tous les CPAN et nœuds doivent avoir leurs propres clés uniques. Ces clés et autres identificateurs uniques (UI) sont définis par une autorité de confiance du réseau, appelée fournisseur. Avec ces valeurs uniques, les appareils IIoT et les CPAN lancent des procédures d'association et d'authentification. Lorsque l'association et l'authentification sont effectuées avec succès, des canaux sécurisés entre les nœuds IIoT et leurs CPAN sont établis. Grâce à ces canaux, les CPAN et les nœuds IIoT peuvent échanger des paquets en toute sécurité. Toutes ces fonctions sont abordées ci-dessous en phases suivies de leurs exigences fonctionnelles.

3.4.1 Phase de préparation

Au départ, les CPAN et les périphériques IIoT doivent être configurés pour avoir des clés et des valeurs uniques. Les valeurs générées en phase de préparation confèrent à chaque appareil une identité distinctive, le **tableau3.2** illustre cette phase.

Tableau 3.2 phase de préparation dans le protocole Authenblue

Acteur	**Fournisseur et administrateur**
Description	Les CPAN doivent avoir des clés initiales et les appareils IIoT doivent avoir des identifiants uniques avec les clés des appareils. Le fournisseur doit générer ces valeurs, et l'administrateur doit les définir sur les CPAN et les appareils IIoT. Ce processus a le choix à faire une fois qu'un nouvel appareil CPAN / IIoT est introduit. Après cela, l'administrateur de renouveler ces valeurs par exemple tous les ans ou tous les cinq ans.
Priorité	Une fonction phase doit être dans un premier temps. Sans cette phase de préparation, Authenblue ne peut pas fonctionner
Processus	**Génération de clés CPAN :** • L'administrateur entre les adresses MAC des CPAN au fournisseur. • Le fournisseur génère une clé secrète pour chaque CPAN. • L'administrateur a défini chaque clé dans son CPAN.
	Génération de clés d'appareil IIoT : • L'administrateur entre les adresses MAC de l'appareil dans le fournisseur. • L'administrateur spécifie un CPAN qui coordonnerait ce périphérique IIoT. • Le fournisseur génère un identifiant unique pour l'appareil IIoT. • Le fournisseur génère une clé de périphérique dérivée de l'interface utilisateur et de la clé initiale du CPAN.

3.4.2 Cryptage/Décryptage authentifié

Les nœuds IIoT associés à leurs CPAN peuvent communiquer via un canal sécurisé résultant des phases d'association et d'authentification. Les CPAN doivent avoir des clés initiales et les appareils IIoT doivent avoir des identifiants uniques ainsi que des clés d'appareils. Le fournisseur doit générer ces valeurs et l'administrateur doit les définir sur les CPAN et les appareils IIoT. Ce processus doit être effectué une fois qu'un nouveau dispositif CPAN / IIoT est introduit. Les paquets envoyés par les CPAN et les nœuds IIoT peuvent être authentifiés en les chiffrant et en les envoyant avec une balise. A travers cela, la confidentialité, l'intégrité et l'authentification des deux, l'identité et le message sont accomplies. Le **Tableau3.3** illustre cette phase.

Tableau 3.3: Fonctions de cryptage / décryptage authentifiées

Acteur	**Appareils IIoT et CPAN**
Description	Les paquets envoyés par les CPAN et les nœuds IIoT peuvent être authentifiés par cryptage et les envoyer avec une étiquette. Grâce à cela, la confidentialité, l'intégrité et l'authentification des deux, l'identité et le message, est accomplie.
Priorité	Le cryptage / décryptage authentifié peut être effectué après une association réussie avec un CPAN
Processus	**Cryptage authentifié** • L'expéditeur crypte les données à envoyer à l'aide du cryptage authentifié fonction dans AES-GCM. • L'expéditeur génère une balise pour les données chiffrées.
	Décryptage authentifié • Le récepteur vérifie l'étiquette reçue, si elle s'avère incorrecte, il laisse tomber le paquet, sinon, il passe à l'étape suivante. • Le récepteur déchiffre le texte chiffré en fonction du déchiffrement authentifié fonction dans AES-GCM.

3.4.3 **Personnalisation**

La **Fig.3.1** illustre comment la clé initiale Ki est générée pour le CPAN. Dans un premier temps, l'administrateur doit saisir manuellement l'adresse MAC et le nom du CPAN dans le fournisseur, qui à son tour génère la clé [Ki = HMAC (MAC, aléatoire)] et la stocke dans la base de données locale. La clé générée sera reçue et insérée manuellement dans le CPAN par l'administrateur.

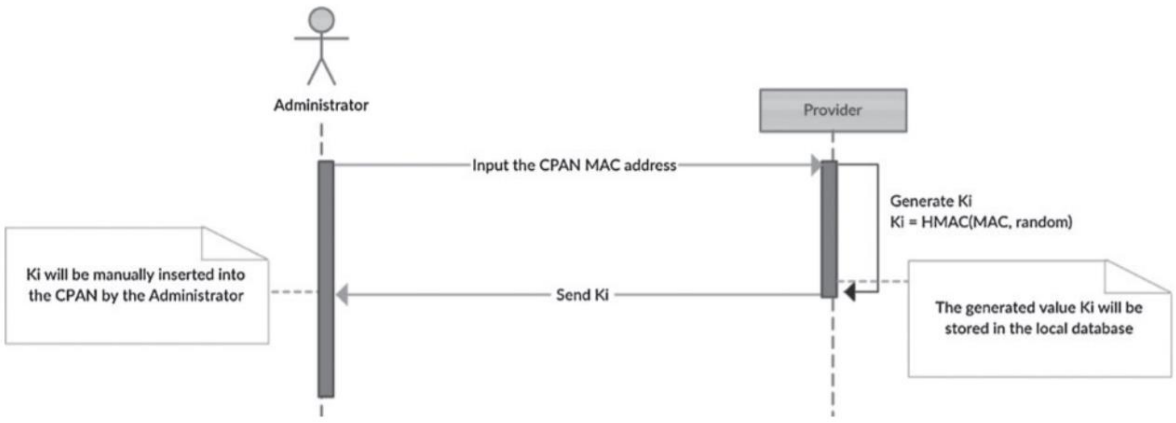


Figure 3.1 personnalisation

3.4.4 **Association d'un appareil à un CPAN**

Processus d'association d'un appareil à un CPAN dans le protocole d'authentification mutuelle BCTrust [57] est illustré dans le diagramme ci-dessous. Dans un premier temps, l'appareil envoie une demande d'association contenant son interface utilisateur au CPAN, qui à son tour génère un défi (un nombre aléatoire) et l'envoie à l'appareil en tant que demande d'authentification. Le dispositif calcule ensuite otp1 en utilisant sa clé dérivée Kd et le défi reçu [otp1 = HOTP (Kd, défi)], puis envoie l'otp1 calculé au CPAN en tant que réponse d'authentification. Le CPAN calcule Kd de l'appareil via la fonction de personnalisation, où il insère sa clé initiale Ki et l'interface utilisateur de l'appareil [Kd = HMAC (Ki, UI)], puis génère otp1 'en utilisant le Kd de l'appareil et le défi [otp1' = HOTP (Kd, défi)]. Le CPAN compare ensuite entre l'otp1 reçu et l'otp1 'calculé; s'ils diffèrent, l'authentification de l'appareil échoue et son association_req_count (compteur de demandes d'association ayant échoué) sera comparé à association_req_max (nombre maximum de tentatives de demandes d'association ayant échoué), s'ils sont égaux, l'interface utilisateur de l'appareil sera mise sur liste noire et l'opération d'association s'arrêtera si ils sont différents, l'association_req_count du périphérique sera incrémentée et l'opération d'association s'arrête. Sinon, si l'otp1 'calculé est égal à l'otp1 reçu, l'appareil est authentifié avec succès et le CPAN génère une clé symétrique Ku (mode unicast), signature, hiddenKeyBroadcast et otp2 [Ku = PRF (Kd, challenge), signature = HMAC (Ku, otp1), hiddenKeyBroadcast = signature $\oplus$ Kb, otp2 = HOTP (Ku, hiddenKeyBroadcast)]. Le CPAN envoie au périphérique une réponse d'association qui contient otp2 et hiddenKeyBroadcast. L'appareil calcule à son tour Ku, signature, Kb et otp2 '[Ku = PRF (Kd, challenge), signature = HMAC (Ku, otp1), Kb = ignature $\oplus$ hiddenKeyBroadcast, otp2 '= HOTP (Ku, hiddenKeyBroadcast)]. Si l'otp2' calculé est égal à l'otp2 reçu, le CPAN est authentifié avec succès, **une authentification mutuelle** est réussie et un canal sécurisé est créé. Sinon, l'authentification CPAN échoue et l'opération d'association s'arrête. Fig.3.1 démontre également comment un attaquant peut tirer parti du mécanisme de liste noire pour mettre sur liste noire l'interface utilisateur d'appareils légitimes innocents; où un attaquant envoie au CPAN une demande d'association qui contient l'interface utilisateur usurpée du périphérique a2, puis reçoit une demande d'authentification du CPAN qui contient un défi. En calculant otp1 en utilisant un Kd incorrect [otp1 = HOTP (Kd, challenge)] et en l'envoyant au CPAN comme réponse d'authentification, le CPAN le compare à l'otp1 'calculé, qui deviendra différent, provoquant un échec d'authentification de l'appareil. Le CPAN mettra alors sur liste noire l'interface utilisateur du périphérique a2 si son association_req_count est égal à association_req_max, ou incrémentera l'association_req_count du périphérique, puis l'opération d'association s'arrête. Ce mécanisme de liste noire basé sur l'interface utilisateur est une faiblesse de BCTrust, contrairement à ce qui est illustré dans la **Figure 3.1**, où le mécanisme de liste noire basé sur L'interface utilisateur des appareils sur liste noire peut être exploité par des attaquants pour entraîner la mise sur liste noire d'appareils légitimes, l'élimination de ce mécanisme du protocole empêcherait la survenue de telles attaques**. Fig.3.2** illustre comment le protocole fonctionnerait après l'élimination du mécanisme de liste noire.

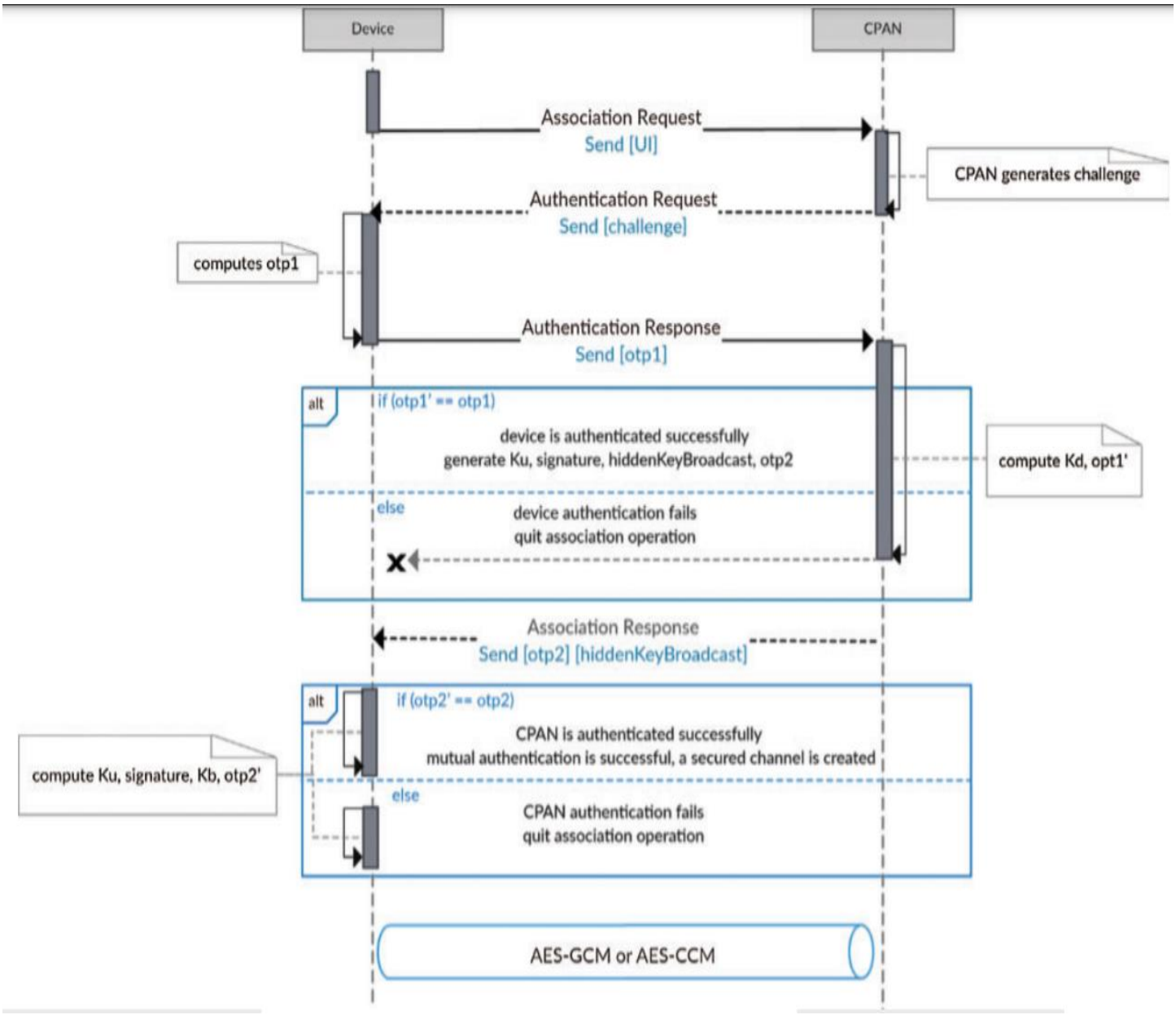


Figure 3.2: Élimination du mécanisme de liste noire lors de l'association d'un Appareil à un CPAN

3.4.5 **Chiffrement et déchiffrement authentifiés**

Maintenant que les périphériques IIoT sont associés aux CPAN et que chaque nœud IIoT a le Ku et le Kb, les nœuds IIoT et les CPAN peuvent crypter et décrypter leurs paquets. Les fonctions de cryptage et de décryptage sont les fonctions de cryptage / décryptage authentifiées dans AES-GCM,

qui sont adoptées dans BCTrust [63]. **Fig.3.3** montre un diagramme de séquence qui illustre comment un appareil IIoT peut crypter des données (P) et les envoyer au CPAN sous forme de n blocs de texte chiffré (C) concaténés avec une étiquette (T). Tout d'abord, l'appareil génère un IV basé sur sa clé (K), Ku si le paquet doit être envoyé au CPAN et un Kb si le paquet doit être envoyé à tous les nœuds du cluster, et un compteur. Après cela, l'appareil utilise des données authentifiées supplémentaires (A) qui sont préconfigurées et connues des deux côtés. Le dispositif calcule ensuite H en chiffrant 128 zéros avec le K. Après cela, il définit un compteur (Y) qui est initialisé à la valeur du IV concaténé avec 31 zéros et a1. Le compteur continue d'incrémenter jusqu'à ce qu'il atteigne (n), le nombre de blocs de texte en clair à chiffrer. La balise est calculée comme suit: T = MSBt (GHASH (H, A, C, len (A), len (C)) ⊕ E (K, Y0)), où MSBt fait référence à la prise des t bits de gauche du résultat.

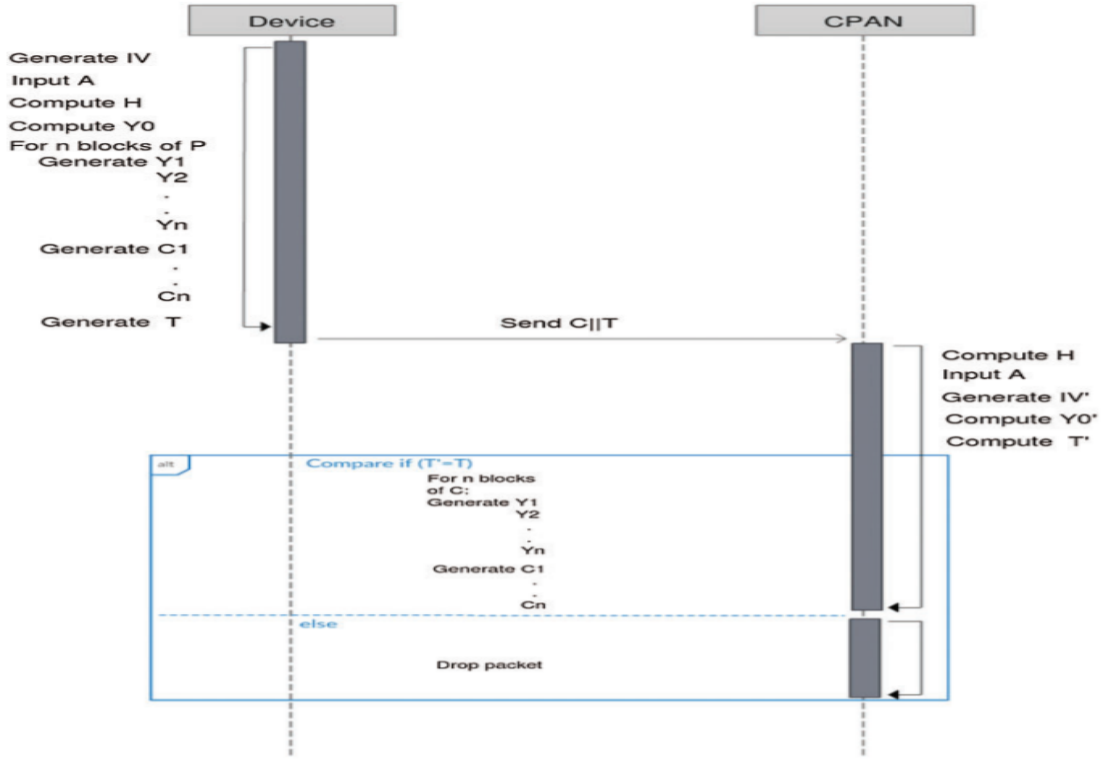


Figure 3.3: Chiffrement et déchiffrement authentifiés

Le même processus doit être effectué du côté CPAN, cependant, l'ordre est différent lorsque le CPAN doit calculer l'étiquette et la comparer avec celle reçue, si elles correspondent, puis il déchiffre le paquet en calculant le OU exclusif de leurs valeurs ainsi que le compteur Y après avoir été chiffré par K. Sinon, il supprime les paquets reçus.

3.5 Analyse

Cette section le compare aux solutions évoquées précédemment dans la revue de la littérature, tableau3.5 montre cette comparaison. Les deux principaux aspects qui différencient Authenblue des autres solutions sont sa gestion des clés.

Tableau 3 .5 Comparaison Authenblue avec d'autres solutions

Facteur	Solutions						
	BATM	BCTrust	LX	TTW	HCK	IoT-Ethereum framework	Authenblue
confidentialité	√	√	√	√	√	×	√
intégrité	√	√	√	√	√	×	√
disponibilité	×	√	×	×	×	√	√
Authentification mutuelle	√	√	√	√	√	√	√
autorisation	×	√	×	×	×	√	√
non-répudiation	√	√	√	√	√	√	√
consommation de ressources	√	√	×	√		×	√
gestion des clés	√	×	×	×	√	×	√

3.6 Conclusion

Ce chapitre a couvert les solutions basées sur la blockchain sur la sécurité IoT, en particulier la sécurité dans les communications IoT, l'utilisation de la blockchain pour la gestion de la confiance et l'**authentification** dans le domaine de l'IoT, et l'utilisation de la blockchain pour contrôler les appareils IoT. De plus, plusieurs solutions concernant la sécurité IoT ont été comparées et analysées, avec la conclusion que travailler sur les améliorations du mécanisme BCTrust conduirait à disposer d'un puissant système d'authentification d'identité basé sur la blockchain pour la gestion. Nous avons étudié un nouveau protocole d'authentification nommé Authenblue qui aide au processus d'authentification des capteurs, des nœuds IIoT et des coordinateurs dans un environnement IIoT. Il s'agit d'une solution de sécurité qui vise à améliorer le processus d'authentification dans l'environnement IIoT, en aidant à atténuer l'apparition de certaines cyber-

attaques. Authenblue améliore le protocole d'authentification sur lequel BCTrust et d'autres modèles s'appuient en améliorant la manière de générer les interfaces utilisateur. Les valeurs d'identificateurs uniques (UI) sont passées de valeurs statiques, adresses MAC des capteurs, à des valeurs générées lors de la phase de démarrage. Une telle modification est cruciale pour le processus de gestion clé. Cela rend le processus de renouvellement des clés de capteur plus efficace en renouvelant leurs valeurs d'interface utilisateur au lieu de changer la clé secrète du CPAN.

Le résultat de la simulation montre qu'Authenblue dispose d'un mécanisme de gestion des clés efficace. Cela est dû à la manière de générer l'interface utilisateur des capteurs. Dans Authenblue, les interfaces utilisateur sont générées sur la base d'un générateur aléatoire pour produire une longueur de 128 bits. Contrairement à la valeur statique présentée dans la solution BCTrust. Cela facilite le renouvellement des identifiants et des clés secrètes des capteurs eux-mêmes. Cela rend le processus de renouvellement des clés de capteur plus efficace en renouvelant leurs valeurs d'interface utilisateur au lieu de changer la clé secrète du CPAN.

Conclusion générale

On utilise la blockchain pour créer la confiance sur deux dimensions : l'origine de l'information et son inaltérabilité (son intégrité dans le temps).

Il est utile de comprendre les blockchains dans le contexte de bitcoin, mais surtout ne pas supposer que tous les écosystèmes blockchain ont besoin de mécanismes bitcoin tels que preuve de travail, règle de chaîne la plus longue. D'un autre côté, des registres distribués privés et des blockchains peuvent être déployés pour résoudre d'autres problèmes. Comme toujours, il existe des avantages et des inconvénients pour chaque solution, et on doit les considérer individuellement pour chaque cas d'utilisation.

L'intégration d'une blockchain dans IoT permettrait à l'utilisateur de mieux protéger sa vie privée en contrôlant l'accès à ses données qui sont les seuls à pouvoir accéder à la chaîne informatique sur laquelle les objets connectés communiquent.

La technologie blockchain pourrait fournir un moyen de suivre l'historique unique de chaque périphérique, en enregistrant un registre des échanges de données entre celui-ci et d'autres périphériques, services Web et utilisateurs humains.

Cette étude propose une nouvelle application pour la blockchain en tant que stockage décentralisé sécurisé pour les clés cryptographiques ainsi que des informations de confiance dans le cadre de l'autonomie Réseaux de capteurs sans fil. L'authentification Blockchain et le module de confiance et ses connaissances à caractère humain. Les modèles proposés montrent comment utiliser l'immuabilité du blockchain pour apporter des solutions aux problématiques élevées dans le domaine des réseaux décentralisés. Plus précisément, nous montrer comment il est possible de construire une solution complète fournissant des mécanismes d'authentification ainsi qu'une évaluation de la confiance dans un réseau auto-organisé et évolutif.

Références

[1] : Source : Blockchain France, 2016, « La Blockchain décryptée : Les clefs d'une révolution », https://blockchainfrance.net/decouvrir-la-blockchain/la-blockchain-decryptee-les-clefs-dune-revolution/

[2] : https://blog.hubspot.com/sales/real-estate-quotes

[3] J. Han, M. Ha, D. Kim, Practical security analysis for the constrained node networks: Focusing on the dtls protocol, dans: 2015 5e Conférence internationale sur l'Internet des objets (IOT), IEEE, 2015.

[4] C. Simko, Attaques de l'homme au milieu dans l'IoT. Globalsign, 2016.

[5] A. Botta, et al. Intégration du cloud computing et de l'Internet des objets: une enquête, Future Gener. Com. Sy. 56 (2016) 684 700.

[6] S. Chakrabarty, DW Engels, S. Thathapudi, Black SDN for the Internet of Things, dans: 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, IEEE, 2015.

[7] H. Suo, et al, Security in the Internet of Things: a review, in: 2012 Conférence internationale sur l'informatique et l'ingénierie électronique, IEEE, 2012.

[8] K. Zhao, L. Ge, Une enquête sur la sécurité de l'Internet des objets, dans: 2013 Neuvième conférence internationale sur l'intelligence et la sécurité informatiques, IEEE, 2013.

[11] Joy Patra Amitranjan Gantait and Ayan Mukherjee. Implementing blockchain for cognitive iot applications, part 1: Integrate device data with smart contracts in ibm blockchain. Available at: https://www.ibm.com/developerworks/cloud/library/ cl-blockchain-for-cognitive-iot-apps-trs/,

[12] Auto logger for trygg kjoreadferd. Available at: https://www. autologger.no/, 2018.

[13] Chain of things. Case study 1: Chain of security. Available at: https: //www.chainofthings.com/cs1chainofsecurity/, 2018.

[14] Internet des objets médicaux, prévisions jusqu'en 2021, Frost & Sullivan store.frost.com/industries/healthcare/internet-of-medical-things-IoHT-market research/internet-of-medical-things- previsions jusqu'à 2021 .html.

[15]www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_busines

[16] Sooh yung Kim Se young Huh, SangraeCho. Managingiotdevicesusingblockchain platform. Available at: http://ieeexplore.ieee.org/stamp/stamp. jsp?tp=&arnumber=7890132, 2017.

[17] Forcast: "Medtech and the Internet of Medical Things", July 2018, Deloitte Centre for Health Solutions

[18] J. J. P. C. Rodrigues, D. B. D. R. Segundo, H. A. Junqueira, M. H. Sabino, R. M. Prince, J. Al-Muhtadi, V. H. C. D. Albuquerque, "Enabling Technologies for the Internet of Health Thing", IEEE Access, Volume 6, 2018.

[19]:K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing Blockchains: Characteristics & Applications," arXiv preprint. arXiv:1806.03693.

[20]: M. Castro, B. Liskov, Tolérance aux pannes byzantine pratique et récupération proactive, ACM Trans. Comp. Syst. 20 (4) (2002) 398 461.
[21] : D. Mazieres, Le protocole de consensus stellaire: un modèle fédéré pour le consensus au niveau Internet, Stellar Develop. Trouvé. (2015) 32.
[22] Miguel Castro, Barbara Liskov, et al. Practical Byzantine fault tolerance. In OSDI, volume99, pages173–186,1999

[**23]** : L. Lamport, R. Shostak, M. Pease, Le problème des généraux byzantins, ACM Trans. Programme. Lang. Syst. 4 (3) (1982) 382 401.
[24] P. Jayachandran, La différence entre la blockchain publique et privée, Blog IBM Blockchain, 2017, p. 31.

[25] Aziz, Blockchain publique vs privée Quelle est la différence, Blog Masterthecrypto, 2018.

[26] B. Asolo, Consortium Blockchain Explained, blog Mycryptopedia, 2018.

[27] RG Brown et al, Corda: une introduction. R3 CEV, 2016, vol. 1, p. 15.

[28] I. Chatzigiannakis, et al., True self-configuration for the loT, dans: 9th IEEE International Conference Computing: Networking, Applications andWorksharing, 2012, pp. 545 - 551.

[29] II P ă tru, M. Caraba ș, M. B ă rbulescu, L. Gheorghe, Smart home IoT system, dans: Netw. Educ. Res. RoEduNet Int. Conf. 15e éd. RoEduNet 2016 — Proc., 2016, pp. 365 - 370.

[**30]** BL Risteska Stojkoska, KV Trivodaliev, Un examen de l'Internet des objets pour la maison intelligente: défis et solutions, J. Clean. Prod. 140, pp (2017) 1454 - 1464.

[31] KL Krishna, O. Silver, WF Malende, K. Anuradha, application Internet des objets pour la mise en oeuvre d'un système d'agriculture intelligente, dans: Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), vol. 25 (15) ou 2017, p. 54 - 59.

[32] MA Akka ș, R. Sokullu, Un système de surveillance des serres basé sur l'IoT avec Micaz motes, dans: International Workshop on IoT, M2M and Healthcare (IMH 2017), vol. 113, 2017, pp. 603 - 608.

[33] L. Da Xu, W. He, S. Li, Internet des objets dans les industries: une enquête, IEEE Trans. Ind. Inf. dix (4) (2014) 2233 – 2243

[34] Z. Guo, Z. Zhang, W. Li, Création d'une plate-forme de gestion d'identification intelligente dans le système de logistique ferroviaire au moyen de l'Internet des objets, Procedia Eng. 29 (2012) 726 - 730.

[35] une. Zanella, N. Bui, a. Castellani, L. Vangelista, M. Zorzi, Internet des objets pour les villes intelligentes, IEEE Internet Things J. 1 (1) (2014) 22 - 32.

[36] R. Khatoun, S. Zeadally, Solutions de cybersécurité et de confidentialité dans les villes intelligentes, IEEE Commun. Mag. 55 (3) (2017) 51 - 59.

[37] HF Atlam, MO Alassafi, A. Alenezi, RJ Walters, GB Wills, XACML for building access control policies in Internet of Things, in: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), 2018.

[38] M. Kalmeshwar, N. Prasad, Internet des objets: architecture, problèmes et applications, Int. J. Eng. Res. Appl. 07 (06) (2017) 85 - 88.

[39] S. Cirani, M. Picone, Wearable Computing for the Internet of Things, IEEE Computer Society, 2015, pp. 35 - 41.

[40] J. Lin, C. Chen, C. Lin, Intégration de la prise en compte de la qualité de service avec la virtualisation dans les systèmes de cloud computing pour les applications sensibles aux retards, Futur. Gener. Comput. Syst. (2013) 478 - 487.

[41] C. Liu, C. Yang, X. Zhang, J. Chen, Vérification de l'intégrité externe pour les Big Data externalisées dans le cloud et l'IoT: une vue d'ensemble, Futur. Gener. Comput. Syst. 49 (2015) 58 - 67.

[42] M. Chen, J. Wan, F. Li, Communications de machine à machine: architectures, normes et applications, KSII Trans. Internet Inf. Syst. 6 (2) (2012) 480 - 497.

[43] A. Alenezi, NHN Zulkipli, HF Atlam, RJ Walters, GB Wills, The impact of cloud forensic readiness on security, in: Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017), 2017, pp. 511 - 517.

[44] HF Atlam, A. Alenezi, RK Hussein, GB Wills, Validation d'un modèle de contrôle d'accès adaptatif basé sur les risques pour l'Internet des objets, Int. J. Comput. Netw. Inf. Secur. (2018) 26 - 35.

[45] D. Bubley, Technologie des données sur le son: communications et couplage d'appareil à appareil sans réseaux radio sans fil, Int. J. Comp. Intell. Res. (2017).

[46] A. Gupta, R. Christie, PR Manjula, Évolutivité dans l'Internet des objets: caractéristiques,

[47] K. Rose, S. Eldridge, L. Chapin, The Internet of Things: An Overview, Understanding the Issues and Challenges of a More Connected World, Livre blanc publié par Internet Society, 15 octobre 2015.

[48] A. Dorri, SS Kanhere, R. Jurdak, Blockchain dans l'Internet des objets: défis et solutions, 2016, préimpression arXiv arXiv: 1608.05187.

[49] Tarak Nandy, Norjihan Abdul Ghani et Sananda Bhattacharya, "Revue sur Security of Internet of Things Authentication Mechanism », publié dans IEEE Access, Vol. 7, Page No. 151054-151089,2019.

[50] Mardianabinti Mohamad Noor, Wan Haslina Hassan, " Recherches en cours sur Internet of Things (IoT) security: A survey », publié dans ELSEVEIR Computer Networks, page No. 283-294, 2019.

[51] B. Marsh et P. Piscioneri, «L'Internet des objets postaux», dans Proc. Int. Conf. sur les technologies et systèmes de collaboration, Atlanta, États-Unis, p. 3-4, 2015.

[52] R. Alhajri, R. Zagrouba et F. Alhaidari, «Enquête pour la détection d'anomalies des botnets IoT à l'aide de la machine 2242, 2019. apprentissage des encodeurs automatiques, " Journal international de recherche en génie appliqué, vol. 14, non. 10, pp. 2417

[53] U. Javaid, AK Siang, MN Aman et B. Sikdar, «Mitigating IoT device based DDoS attack using blockchain, "dans Proc. 1er atelier sur les crypto-monnaies et les blockchains pour les systèmes distribués, Munich,Allemagne, p. 71–76, 2018.

[54] A. Moinet, B. Darties et JL Baril, «La confiance et l'authentification basées sur la blockchain pour les réseaux de capteurs décentralisés», vol. 1, pp. 1–6, 2017.

[55] F. Alhaidari, A. Rahman et R. Zagrouba, «Nuage de choses: architecture, applications et défis , " Journal of Ambient Intelligence and Humanized Computing, vol. 3, non. 6, p. 1099, 2020

[56] H. Atlam, A. Alenezi, M. Alassafi et G. Wills, «Blockchain with Internet of Things: Benefits défis et orientations futures » Journal international des systèmes et applications intelligents, vol. dix 6, p. 40–48, 2018

[57] MT Hammi, P. Bellot et A. Serhrouchni, «BCTrust: Une blockchain d'authentification décentralisée mécanisme basé, ”dans Proc. Communications et réseau sans fil IEEE Conf., Barcelone, 2018.

[58] LH Nunes, LHV Nakamura, HF Vieira, RMO Libardi, EM Olivera et al., «Évaluation des performances et de l'énergie des services Web RESTful dans Raspberry Pi», dans Proc. IEEE 33e Int. Performance Informatique et communications Conf., Austin, Texas, p. 1–9, 2014.

[59] S. Huh, S. Cho et S. Kim, «Managing IoT devices using blockchain platform», dans Proc. 19e Int. Conf sur les technologies de communication avancées, Bongpyeong, p. 464–467, 2017

[60] M. Maqsood, A. Rahman, L. Malrey et JY Choi, «Chiffrement d’image basé sur l’évolution à l’aide de la table de vérité des codons d’ARN», Optique et technologie laser, vol. 121, p. 105818, 2020

[61] FH Al-Naji et R. Zagrouba, «Une enquête sur les méthodes d'authentification continue dans l'environnement de l'Internet des objets», Journal des communications informatiques, vol. 163, pp. 109-133, 2020.

[62] PY Ting, JL Tsai et TS Wu, «Méthode de chiffrement de signes adaptée aux appareils IoT à faible consommation dans un réseau de capteurs sans fil», Journal des systèmes IEEE, vol. 12, non. 3, pp. 2385-2394, 2018.

[63] F. Li et P. Xiong, «Communication sécurisée pratique pour l'intégration de réseaux de capteurs sans fil dans l'Internet des objets», Journal des capteurs IEEE, vol. 13, non. 10, pp. 3677–3684, 2013.

[64] HA Moniem et HH Ammar, «Prédiction des performances de l'architecture orientée services, une enquête», International Journal of Computer Applications Technology and Research, vol. 3, non. 12, pp. 831–835, 2014.

[65] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: Proceedings of the 2017 IEEE BigData Congress, Honolulu, HI, 2017, pp. 557_564.

[66] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf

[67] https://blogdigital.beijaflore.com/blockchain-consensus/

[68] https://hyperledger-fabric.readthedocs.io/en/release-1.4/network/network.html

[69] https://blogdigital.beijaflore.com/blockchain-utilisation/

[70] "Comment l'adresse d'un contrat Ethereum est-elle calculée?" Ethereum Stack Exchange, 29 janvier 2016, 22:14 https://ethereum.stackexchange.com/questions/760/how-is-the-address-of-an-ethereum-contract-computed.