

REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE ET DE l'INNOVATION

UNIVERSITE GASTON BERGER DE SAINT-LOUIS



U.F.R DE SCIENCES APPLIQUEES ET DE TECHNOLOGIE

DEPARTEMENT INFORMATIQUE

Mémoire de fin d'études pour l'obtention du diplôme de

Master Ingénierie en Réseaux et Systèmes Distribués(R2SD)

Sujet : Utilisation de la technologie Blockchain dans l'IoT pour la sécurisation des données

Présenté par :

M^me^ Fatou Diouf

Sous la direction de :

Dr. Chérif DIALLO

Année Académique : 2022-2023

REMERCIEMENTS

Louange à Dieu, le Tout-Puissant, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Je tiens à remercier toutes les personnes qui ont contribué au succès de la rédaction de ce mémoire.

Je voudrais, dans un premier temps, remercier mon directeur de mémoire, monsieur Chérif Diallo pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

J'adresse mes sincères remerciements à tous les professeurs de l'université Gaston Berger de Saint-Louis, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions et ont accepté de me rencontrer et de répondre à mes questions durant mes recherches.

Enfin, je voudrais exprimer ma reconnaissance envers mon très cher époux, ma famille, ma belle-famille, les amis et collègues qui m'ont apporté leur support moral et intellectuel tout au long de ma démarche.

DEDICACES

Je dédie ce mémoire à

Mon feu père, qui pourrait 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. Puisse Allah lui accorder un repos éternel.

Ma mère, qui a œuvré pour ma réussite, du fait de son amour, de son soutien, de tous les sacrifices consentis et de ses précieux conseils, de toute son assistance et de sa présence dans ma vie, reçoit à travers ce travail, aussi modeste soit-il,

L'expression de mes sentiments et de mon éternelle gratitude.

Mon cher époux, mes tontons, mes tantes, mes frères et sœurs pour avoir contribué à la réussite de ce travail d'une manière indirecte, d'y avoir apporté tant d'humeur et d'amour et pour tout le soutien moral prodigué dans les moments les plus difficiles.

Tous mes proches, grands et petits.

Mes ami(e)s avec lesquels j'ai partagé mes moments de joies et de bonheurs.

Tous mes enseignants.

RESUME

Le développement constant d'appareils informatiques interdépendants et l'émergence de nouvelles technologies de réseau ont entraîné une croissance spectaculaire du nombre d'appareils Internet des objets (IoT). Il a fourni une grande commodité à la vie des gens où ses applications ont été utilisées pour révolutionner les objets du quotidien connectés dans différents aspects de la vie tels que la maison intelligente, les soins de santé, les transports, l'environnement, l'agriculture et l'armée. Cette interconnectivité des objets IoT s'effectue via des réseaux sur une infrastructure cloud centralisée qui n'est pas limitée aux frontières nationales ou juridictionnelles. Il est crucial de maintenir la sécurité, la robustesse et l'authentification sans confiance pour garantir un échange sécurisé des données utilisateur critiques entre les objets IoT. Par conséquent, la technologie blockchain est récemment apparue comme une solution viable pour offrir des fonctionnalités aussi importantes. La décentralisation sécurisée de la blockchain peut surmonter les limites de sécurité, d'authentification et de maintenance de l'écosystème IoT actuel. Dans cet article, nous effectuons une analyse documentaire complète pour relever les défis récents en matière de sécurité et de confidentialité liés à l'IoT, où ils sont classés en fonction de l'architecture en couches de l'IoT : perception, réseau et couche d'application. De plus, nous étudions la technologie blockchain comme un pilier clé pour surmonter de nombreux problèmes de sécurité et de confidentialité de l'IoT. De plus, nous explorons la technologie blockchain et ses valeurs ajoutées lorsqu'elle est combinée avec d'autres nouvelles technologies comme l'apprentissage automatique, en particulier dans les systèmes de détection d'intrusion. De plus, nous soulignons les défis et les problèmes de confidentialité résultant de l'intégration de la blockchain dans les applications IoT. Enfin, nous proposons un cadre d'exigences de sécurité et de confidentialité IoT via la technologie blockchain. Notre principale contribution est d'épuiser la littérature pour mettre en évidence les problèmes récents de sécurité et de confidentialité de l'IoT et comment la blockchain peut être utilisée pour surmonter ces problèmes, néanmoins ; nous relevons les défis et les problèmes de sécurité ouverts que la blockchain peut imposer aux systèmes IoT actuels. Les résultats de la recherche formulent une base rigide sur laquelle une adoption efficace et sécurisée de l'IoT et de la blockchain est mise en évidence en conséquence.

ABSTRACT

The constant development of interrelated computing devices and the emergence of new network technologies have caused a dramatic growth in the number of Internet of Things (IoT) devices. It has brought great convenience to people's lives where its applications have been leveraged to revolutionize everyday objects connected in different life aspects such as smart home, healthcare, transportation, environment, agriculture, and military. This interconnectivity of IoT objects takes place through networks on centralized cloud infrastructure that is not constrained to national or jurisdictional boundaries. It is crucial to maintain security, robustness, and trustless authentication to guarantee secure exchange of critical user data among IoT objects. Consequently, blockchain technology has recently emerged as a tenable solution to offer such prominent features. Blockchain's secure decentralization can overcome security, authentication, and maintenance limitations of current IoT ecosystem. In this paper we conduct a comprehensive literature review to address recent security and privacy challenges related to IoT where they are categorized according to IoT layered architecture: perception, network, and application layer. Further, we investigate blockchain technology as a key pillar to overcome many of IoT security and privacy problems. Additionally, we explore the blockchain technology and its added values when combined with other new technologies as machine learning especially in intrusion detection systems. Moreover, we highlight challenges and privacy issues resulted due to integration of blockchain in IoT applications. Finally, we propose a framework of IoT security and privacy requirements via blockchain technology. Our main contribution is to exhaust the literature to highlight the recent IoT security and privacy issues and how blockchain can be utilized to overcome these issues, nevertheless; we address challenges and open security issues that blockchain may impose on the current IoT systems. Research findings formulate a rigid foundation upon which an efficient and secure adoption of IoT and blockchain is highlighted accordingly.

TABLE DES MATIERES

REMERCIEMENTS I
DEDICACES II
RESUME III
ABSTRACT IV
LISTE DES FIGURES VIII
LISTE DES TABLEAUX IX
LISTE DES ACRONYMES X
Introduction générale ..... - 1 -
CHAPITRE 1 : Concepts fondamentaux de l'internet des objets ..... - 4 -
1.1. Introduction ..... - 4 -
1.2. Définition ..... - 4 -
1.3. Fonctionnement de l'internet des objets ..... - 5 -
1.3.1. Technologies de l'IoT ..... - 5 -
1.3.2. Composants de l'IoT ..... - 6 -
1.4. Architecture et Ecosystème de l'internet des objets ..... - 8 -
1.4.1. Architecture de l'IoT ..... - 8 -
1.4.2. Ecosystème de l'IoT ..... - 10 -
1.5. Protocoles ..... - 14 -
1.6. Historique de l'internet des objets ..... - 16 -
1.7. Domaines d'applications ..... - 17 -
1.8. Les avantages et les inconvénients de l'IoT ..... - 21 -
1.8.1. Les avantages ..... - 21 -
1.8.2. Les inconvénients ..... - 21 -
1.9. Les défis ..... - 22 -
1.10. Conclusion ..... - 24 -
Chapitre 2 : Sécurité de l'IoT ..... - 25 -
2.1. Introduction ..... - 25 -
2.2. La différence entre vulnérabilité, menace et risque ..... - 25 -
2.2.1. Vulnérabilité ..... - 25 -
2.2.2. Menace ..... - 25 -
2.2.3. Risque ..... - 25 -
2.3. Les propriétés de sécurité ..... - 25 -
2.4. Les vulnérabilités de l'internet des objets ..... - 27 -
2.5. Les attaques visant l'IdO ..... - 29 -
1) Les attaques actives ..... - 29 -

2) Une attaque passive ..... - 30 -
2.6. L'Authentification dans l'IoT ..... - 32 -
2.6.1. Les différentes techniques d'authentification ..... - 32 -
2.6.2. Les risques liés aux techniques d'authentification ..... - 33 -
2.6.3. Les solutions pour la sécurisation des appareils IoT ..... - 33 -
2.7. Conclusion ..... - 34 -
Chapitre 3 : La technologie blockchain ..... - 35 -
3.1. Introduction ..... - 35 -
3.2. Définition de la blockchain ..... - 35 -
3.3. Historique de la blockchain ..... - 35 -
3.4. Le système blockchain ..... - 36 -
3.5. Les types de réseaux de blockchain ..... - 37 -
3.6. Les composants d'une blockchain ..... - 38 -
3.7. Fonctionnement de la blockchain ..... - 39 -
3.8. Structure d'une chaine de blocs ..... - 40 -
3.9. Écosystème blockchain ..... - 42 -
3.10. Les caractéristiques essentielles d'une blockchain ..... - 43 -
3.11. Les mécanismes de validation des blocs ..... - 44 -
a) Preuve de travail ou Proof of work (pow) ..... - 44 -
b) Preuve d'enjeu ou Proof of stake(pos) ..... - 45 -
c) Preuve d'enjeu Délégué (Delegated Proof of stake) ..... - 46 -
d) La preuve d'autorité (PoA) ..... - 46 -
3.12. Plateformes de la blockchain ..... - 48 -
1) Bitcoin ..... - 48 -
2) Ethereum ..... - 48 -
3) Hyperledger Fabric ..... - 49 -
4) Litecoin ..... - 49 -
5) Binance Coin ..... - 49 -
6) IOTA ..... - 49 -
7) Tendermint ..... - 49 -
3.13. Domaines d'applications de la blockchain ..... - 49 -
3.14. Avantages, inconvénients et défis de la blockchain ..... - 50 -
3.14.1. Avantages ..... - 51 -
3.14.2. Les inconvénients ..... - 52 -
3.14.3. Les défis ..... - 53 -
3.15. Conclusion ..... - 54 -

Chapitre 4 : Méthodes d'authentification basées sur la blockchain pour sécuriser l'IoT ..... - 55 -
4.1. Introduction ..... - 55 -
4.2. Pourquoi l'IoT a-t-il besoin de la blockchain ? ..... - 55 -
4.3. Le contrôle d'accès dans l'IoT ..... - 55 -
4.3.1. L'authentification mutuelle ..... - 56 -
4.3.2. La cryptographie ..... - 56 -
4.3.3. Protocoles d'authentification ..... - 62 -
4.4. Authentification sécurisée basée sur la blockchain avec des performances améliorées pour le Fog Computing ..... - 72 -
4.4.1. Méthodologie proposée ..... - 72 -
4.4.2. Architecture du système ..... - 73 -
4.4.3. Fonctionnement du système proposé ..... - 74 -
4.5. Étude d'un nouveau protocole d'authentification basé sur la blockchain dans l'IoT ..... - 76 -
4.5.1. Schéma d'authentification basé sur la technologie blockchain dans l'IoT ..... - 76 -
4.5.2. Notre solution pour sécuriser la communication des objets connectés contre les attaques à répétition ..... - 83 -
4.6. Conclusion et perspective ..... - 84 -
Conclusion générale ..... - 85 -
BIBLIOGRAPHIE et REFERENCE ..... - 86 -

LISTE DES FIGURES

Figure 1:Une nouvelle dimension pour l'Ido [2] ..... - 5 -
Figure 2: Fonctionnement de l'internet des objets ..... - 7 -
Figure 3: Architecture de l'IoT (A : trois couches) (B : cinq couches) [35] ..... - 9 -
Figure 4: Architecture à quatre couches de l'IoT ..... - 10 -
Figure 5: L'écosystème de l'internet des Objets (IoT) ..... - 10 -
Figure 6: Collecte de données [17] ..... - 11 -
Figure 7: Mode d'opération des IoT [17] ..... - 12 -
Figure 8: Connection des objets à internet ..... - 14 -
Figure 9: Principaux protocoles IoT -modèle TCP/IP ..... - 16 -
Figure 10: Evolution du nombre d'objets connectés de l'IoT ..... - 17 -
Figure 11: Domaines d'application de l'IoT ..... - 21 -
Figure 12: les propriétés de sécurité ..... - 26 -
Figure 13: Les 10 vulnérabilités de l'IOT selon OWASP ..... - 29 -
Figure 14: schéma de différents types d'authentification ..... - 32 -
Figure 15: Schéma de la blockchain ..... - 35 -
Figure 16: Historique de la technologie blockchain Source : blockchain 101.com ..... - 36 -
Figure 17: Le réseau des nœuds [18] ..... - 37 -
Figure 18: Schéma des différents types de blockchain ..... - 38 -
Figure 19: Fonctionnement de la blockchain ..... - 39 -
Figure 20: schéma récapitulatif expliquant le fonctionnement d'une blockchain publique lors d'une transaction ..... - 40 -
Figure 21: Structure de base de la chaine de blocs ..... - 42 -
Figure 22: Ecosystème de blockchain ..... - 43 -
Figure 23: Architecture des caractéristiques d'une blockchain ..... - 44 -
Figure 24 : Classification des algorithmes de consensus Blockchain par mécanisme ..... - 47 -
Figure 25: domaines d'application de la blockchain ..... - 50 -
Figure 26: Avantages de la blockchain, Source : « Blockchain, catalyseur de nouvelles approches en assurance », PwC, mars 2017 ..... - 52 -
Figure 27: Les fonctionnalités de la cryptographie ..... - 57 -
Figure 28: Chiffrement à clé publique ..... - 59 -
Figure 29: Schéma d'un chiffrement par bloc ..... - 60 -
Figure 30: Schéma d'un chiffrement à flot ..... - 61 -
Figure 31: Classification des protocoles étudiés pour l'établissement de clé ..... - 63 -
Figure 32: Un système d'authentification et d'accord clé basé sur une carte à puce et un nœud de passerelle pour l'Ido ..... - 66 -
Figure 33 : Les étapes de protocole de hachage ..... - 69 -
Figure 34: Mutual Authentication Key Establishment Phase ..... - 70 -
Figure 35 Organigramme de l'architecture globale du système proposé ..... - 73 -
Figure 36: Système d'authentification basé sur la blockchain Neo et le Fog computing ..... - 73 -
Figure 37 : Diagramme de flux pour l'enregistrement des utilisateurs ..... - 75 -
Figure 38 : Diagramme de flux pour l'authentification de l'utilisateur ..... - 76 -
Figure 39: Modèle du système ..... - 77 -
Figure 40: Diagramme de séquence de l'initialisation ..... - 79 -
Figure 41: Diagramme de séquence de l'enregistrement ..... - 80 -
Figure 42 : Diagramme de séquence de l'authentification ..... - 82 -

LISTE DES TABLEAUX

Tableau 1:Les principaux systèmes technologiques nécessaires au fonctionnent de l'IdO ..... - 7 -

Tableau 2: Principaux moyens de communication selon la portée et l'autonomie (CRE)..... - 13 -

Tableau 3: la relation entre les services et les mécanismes de sécurité ..... - 27 -

Tableau 4: Les différentes types d'attaque dans l'IdO..... - 31 -

Tableau 5: Avantages et inconvénients de la preuve de travail (POW), de la preuve d'enjeu (POS) et d'une forme hybride des deux modes de preuve (OPECST, d'après Giang-Truong Nguyen and Kyungbaek Kim23(*))..... - 47 -

Tableau 6: Comparaison entre cryptographie symétrique et cryptographie asymétrique (Source : 10 /01/2015, Pr BELKHIR Abdel Kader)..... - 61 -

Tableau 7: Tableau comparatif entre les protocoles de gestions de clé ..... - 71 -

LISTE DES ACRONYMES

AC : Autorité de Certification

AMQP : Constrained Application Protocol

BS : Station de base

BCN : Réseau Blockchain

CN : Noeud de cluster

CBC MAC : Cipher Bloc Chaining Message Authentication Code

COAP : Constrained Application Protocol

CCE : Cryptographie à courbe elliptique

DoS: Deni of Service

DDS: Data Distribution Service

DPOS: Delegated Proof of stake

DDoS: Déni de service distribué

ECDSA : Algorithme de signature numérique à courbe elliptique

GS1 : normes mondiales 1

IoT : Internet of Things

IdO : Internet des Objects

IP : Internet Protocol

Ipv6 : Internet Protocol version 6

IDENTIFIANT : Identité

IHM : interfaces Homme-machine

LAN : Local Area Network

LPWAN : Liaison sans fil à faible consommation énergétique

6LoWPAN: IPv6 over Low Power Wireless Area Networks

LoRaWAN: Low Range Wide Area Network

MITM: Le concept de Man-in-the-Middle

MQTT: Message Queue Telemetry Transport

M2M: Machine to Machine

MAC : Contrôle d'accès au support

NFC : Near Field Communication

NIC: The National Intelligence Council

OMAC: One-Key CBC MAC

OSI: Open Systems Interconnection

OWASP: Open Worldwide Application Security Project

PBK: Clé Publique

PVK: Clé Privée

PoW: Proof of Work

PoS: Proof of Stake

PoA: Proof of Authority

PoAh: Proof of Authentication

PIN: Personal Identity Number

PSK: Pre-Shared Key

PKI: Public Key Infrastructure

RFID : Radio Frequency Identification

RCSFs : réseaux de capteurs sans fil

RPoW: Reusable Proof of Work

RSA: Rivest Shamir Adleman

SN : Nœud de capteur

TIC : Technologie d'**i**nformation et de la **c**ommunication

TCP/IP : Transmission Control Protocol / Internet Protocol

TCP : Transmission Control Protocol

TTP : Tiers de confiance

Tu : Utilisateur

UDP : User Datagram Protocol

UMAC : fonction de hachage universelle

WSN/WSNS : Wireless Sensor Networks

Introduction générale

Internet a changé notre mode de vie au cours de ces dernières années et continue de le faire, notamment avec le nombre croissant d'objets/appareils nous appartenons ou nous entourons capables de se connecter à internet. Aujourd'hui, l'internet des Objets (IdO), ou Internet of Things (IoT) en anglais, est une base pour connecter des objets, des capteurs, des actionneurs et d'autres technologies intelligentes, ajoutant ainsi une nouvelle dimension au monde de technologie d'information et de la communication (TIC).

L'internet des objets (IdO) est un concept dans lequel le monde virtuel des technologies de l'information s'intègre parfaitement au monde réel des objets. Il permet de relever certains défis technologiques auxquels la communauté fait face dans la vie de tous les jours. Ce nouveau concept est une solution innovante pour réaliser une analyse quantitative de tous les objets qui nous entourent. Une condition préalable requise pour l'IdO est l'identification des objets. Si tous les objets et les personnes de la vie réelle étaient équipés d'identifiants (physiques ou logiques : adresse IP, adresse MAC, Tag RFID, ou tout autre type d'identifiant), ils pourraient être gérés et inventoriés par des ordinateurs. L'un des éléments importants dans le paradigme IoT est les réseaux de capteurs sans fil (RCSFs). Ces RCSFs ont obtenu une popularité élevée en raison de leur large éventail d'applications. Ces réseaux ont motivé beaucoup de travaux de recherches en raison de leurs caractéristiques uniques qui les différencient des réseaux câblés/sans-fil traditionnels. Les technologies de communication sans fil sont sujettes à différents types de menaces de sécurité et d'attaques, rendant ainsi les objets et les services IoT, reposant majoritairement sur ces technologies, une cible privilégiée des attaquants. En effet, le déploiement des objets formant l'IdO dans un environnement souvent sans surveillance, ainsi que les limites en protection physique ainsi qu'en ressources (stockage, calcul, mémoire, énergie) de ces objets, rendent l'IdO vulnérable (objets, réseaux, applications) à une variété d'attaques potentielles, pour lesquels les solutions de sécurité conventionnelles sont mal adaptées.

La sécurité est parmi les principaux défis de l'internet des Objets (IdO). Cependant, aujourd'hui, les chercheurs dans ce domaine tentent de trouver des solutions pour assurer la sécurité des objets connectés, des réseaux et garantir la confidentialité et la sécurité de la vie privée des utilisateurs, tout en prenant en considération les limites des dispositifs de l'IdO (énergie, mémoire, puissance de calcul, etc.), mais en gardant les performances du réseau.

Problématique

L'internet des objets et son intégration dans tous les domaines présentent des problèmes plus complexes en termes de protection des données et des réseaux en communications, la gestion d'identité et le contrôle d'accès. De plus, toute organisation qui utilise une infrastructure liée à l'internet des objets va générer une grande quantité de flux d'informations (ressources humaines, procédés de production …). De telles informations doivent rester confidentielles, contrôlées par l'organisation et seulement accessibles quand cela est nécessaire et uniquement par les personnels autorisés. La protection des composants objets internet doit être prise en compte à l'aide de mécanismes de sécurité adéquats et adaptés à l'environnement, à l'activité de l'entreprise. Cela implique l'utilisation de stratégies et de protocoles de sécurité tant au niveau du réseau qu'aux interactions entre les objets et les services fournis. Parmi les solutions,

on a le système de détection d'intrusion collaborative qui détecte les intrusions en temps réel et ses attaques sont partagées entre ses systèmes de détection grâce à la blockchain La technologie blockchain dans le domaine de l'IoT permet le stockage des données en garantissant la sécurité dans le transfert des données et la traçabilité des données.

Ainsi l'authentification est un aspect essentiel pour garantir une bonne sécurité dans les environnements IoT. Les objets traitent et échangent des données sans intervention humaine. Par conséquent, en raison de cette autonomie totale il est primordial de mettre des mécanismes d'authentification pour éviter d'éventuelles menaces. De nombreux chercheurs ont proposé plusieurs types de mécanismes d'authentification d'objets connectés adaptés à l'environnement IoT. La plupart de ces recherches sont basées sur une authentification centralisée selon laquelle tous les dispositifs doivent contacter une certaine entité ce qui crée un inconvénient majeur. Lorsque l'entité centrale est compromise, le modèle d'authentification est invalide. De tels inconvénients dans la conception de l'IdO peuvent être surmontés en utilisant la technologie blockchain. La blockchain est connue comme la technologie sous-jacente du bitcoin. Elle peut être définie comme un grand livre distribué. Elle permet de remplacer le tiers de confiance par un bloc transparent et non falsifié d'enregistrements disponibles via une forme distribuée, de sorte que la confiance est déplacée d'une entité unique vers des nœuds de blockchain décentralisés. L'objet de notre étude va donc porter sur les méthodes d'authentification basées sur la blockchain pour l'IoT mais aussi de proposer un protocole d'authentification des objets IoT en se basant sur les aspects de la blockchain.

C'est ainsi dans ce mémoire que nous allons étudier de nouveaux mécanismes légers et robustes doivent être développés pour contrer les menaces et les attaques auxquelles les infrastructures de l'IdO sont exposées. Une première ligne de défense est d'utiliser des mécanismes d'authentification adaptés aux capacités et aux contraintes des objets et des technologies de communication afin d'assurer les services d'authentification des objets et de mettre en œuvre des canaux sécurisés permettant la protection des données.

- **Motivations**
  La sécurité de l'internet des objets (IoT) est très importante, car cette technologie est présente dans tous les domaines et elle est à l'origine de plusieurs cyberattaques. La sécurité de l'IoT est primordiale, chaque « nœud » doit être protégé contre les logiciels espions et malveillants, les chevaux de Troie, et toutes les intrusions menaçant la vie privée. L'internet des objets présente de nouveaux défis en termes de protection des données. Cependant, il ne suffit pas d'empêcher ou d'autoriser les accès pour garantir la sécurité. Il faut surveiller qui accède à quelle ressource et surtout quand. Afin d'éviter des failles de sécurité dramatiques (l'usurpation d'identité, le vol d'information et la modification des données), l'union de la blockchain et du temps réel présente une solution optimale.
- **Objectifs**
  L'objectif du mémoire consiste à proposer des mécanismes d'authentification des objets IoT basés sur la technologie blockchain.
  Contenu du mémoire :
  Afin de répondre à nos objectifs, notre travail est structuré en quatre chapitres :

- **Chapitre 1 :** dans ce chapitre, nous avons évoqué l'internet des objets, la définition de ses concepts de base, son fonctionnement, son écosystème, son historique, ses domaines d'application, mentionné ses avantages et ses inconvénients et enfin les défis de l'IoT.
- **Chapitre 2 :** nous avons présenté dans ce chapitre la sécurité de l'IoT : les vulnérabilités et les attaques rencontrées dans l'internet des objets, les types d'authentifications ainsi que la sécurisation de l'IoT.
  Chapitre 3 : dans ce chapitre, nous allons étudier la technologie blockchain.
- **Chapitre 4 :** méthodes d'authentification basées sur la blockchain pour sécuriser l'IoT.

CHAPITRE 1 : Concepts fondamentaux de l'internet des objets

1.1. Introduction

L'internet des objets (l'IoT) repose sur l'idée que tous les objets peuvent être connectés à internet et sont donc capables d'émettre de l'information et éventuellement de recevoir des commandes. Il n'existe pas de définition standard, unifiée et partagée de l'internet des objets. Certaines techniques de l'IoT, tandis que d'autres se concentrent plutôt sur les usages et les fonctionnalités. Il faut réussir à exprimer ce que représente l'internet des objets tout en restant accessible aux non experts, et suffisamment concerté pour représenter son impact dans la vie quotidienne. L'IoT désigne une information qui se fond dans notre quotidien pour nous simplifier la vie.

Dans ce chapitre, nous définissons de manière générale l'internet des objets.

1.2. Définition

L'internet des objets (IoT ou encore IdO) représente l'extension d'internet à des choses et à des lieux du monde physique. Cela a permis à toute l'humanité de plonger dans les profondeurs de l'internet et de rechercher ses mystères pour devenir l'un des outils indispensables dans notre vie quotidienne. Ainsi, son utilisation a touché tous les aspects de la vie quotidienne [1].

L'internet des objets est défini par l'union internationale des télécommunications comme une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution et cela veut dire que l'internet des objets est apparu dans le cadre d'une direction issue de la mécanisation et standardisation, appliquée à l'automatisation du traitement du document et de l'information sur support matériel puis numérique.

Il représente les échanges d'informations et de données provenant de dispositifs présents dans le monde réel vers le réseau internet. Aussi l'internet des objets représente les échanges d'informations et de données provenant de dispositifs présents dans la réalité vers le réseau internet. Il est considéré comme la troisième évolution de l'internet, baptisée web 3.0 qui fait suite à l'ère du web social [1]. Surtout avec l'ajout d'une connexion internet qu'a donné une valeur supplémentaire en termes de fonctionnalité, d'information, d'interaction avec l'environnement ou d'usage.

L'internet des objets responsable d'un accroissement exponentiel du volume de donnée généré sur le réseau à l'origine du big data. Alors l'IdO est considéré comme un concept ayant des répercussions sur les technologies et la société [2].

Il est considéré comme le réseau de réseaux qui permet via des systèmes d'identification électronique, et des dispositifs mobiles sans fil, d'identifier des entités numériques et des objets, physiques, et du récupérée, stocker, transférer et traiter entre les mondes physiques et virtuels. Il est le système des systèmes et pas juste le réseau des réseaux. Parfois l'objet deviendra un acteur autonome de l'internet, capable de percevoir, analyser et d'agir selon les contextes engagés, et cela vu dire que l'avènement de l'internet des objets liées à celui des

technologies ou méthodes logicielle liées à l'intelligence artificielle, et des sciences de la complexité [2].

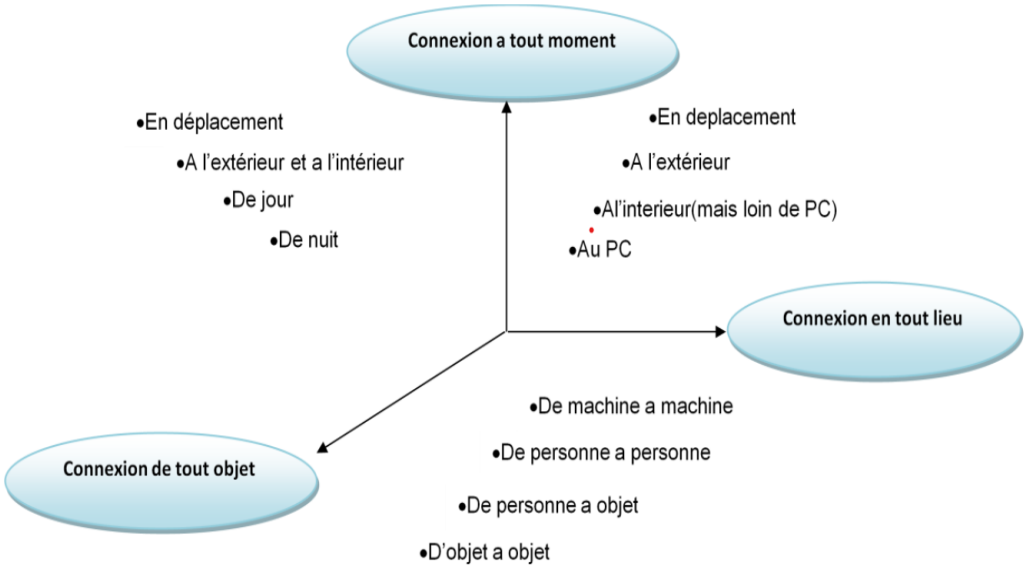


Figure 1:Une nouvelle dimension pour l'Ido [2]

1.3. Fonctionnement de l'internet des objets

Le fonctionnement de l'IoT s'explique par ses technologies et composantes.

1.3.1. Technologies de l'IoT

L'internet of Things (IoT) permet l'interconnexion des différents objets intelligents via l'internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. Citons quelques exemples de ces technologies.

« L'IoT désigne diverses solutions techniques (RFID, TCP/IP, technologies mobiles, etc.) qui permettent d'identifier des objets, de capter, stocker, traiter et transférer des données dans les environnements physiques, mais aussi entre des contextes physiques et des univers virtuels. » [2]. En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur ce point, quelques-unes qui sont, selon Han et Zhanghang, les technologies clés de l'IoT. Ces technologies sont les suivantes : RFID, WSN et M2M, et sont définies ci-dessous.

• RFID (Radio Frequency Identification) : le terme RFID englobe toutes les technologies qui utilisent les ondes radio pour identifier automatiquement des objets ou des personnes. C'est une technologie qui permet de mémoriser et de récupérer des informations à distance grâce à une étiquette qui émet des ondes radio [3]. Il s'agit d'une méthode utilisée pour transférer les données des étiquettes à des objets ou pour identifier les objets à distance. L'étiquette contient des informations stockées électroniquement pouvant être lues à distance [4].

• WSN (Wireless Sensor Network) : c'est un ensemble de nœuds qui communiquent sans fil et qui sont organisés en un réseau coopératif. Chaque nœud possède une capacité de traitement et peut contenir différents types de mémoires, un émetteur-récepteur RF et une source d'alimentation, comme il peut aussi tenir compte des divers capteurs et des actionneurs [5]. Comme son nom l'indique, le WSN constitue alors un réseau de capteurs sans fil qui peut être une technologie nécessaire au fonctionnement de l'IoT.

• M2M (Machine to Machine) : c'est « l'association des technologies de l'information et de la communication avec des objets intelligents dans le but de donner à ces derniers les moyens d'interagir sans intervention humaine avec le système d'information d'une organisation ou d'une entreprise » [6].

1.3.2. Composants de l'IoT

Un système IoT réunit de nombreux acteurs et composants technologiques qui assurent le bon fonctionnement d'un système IoT. Une solution d'IoT s'articule autour de cinq composants essentiels que sont [4] : les objets (capteurs), le réseau (connectivité), les données, les informations et les applications d'exploitation.

• Les objets : pour capter des données de valeur. Ce sont les équipements actifs ou passifs pouvant générer de la donnée exploitable et créatrice de valeur pour les utilisateurs. Les objets sont composés d'éléments passifs : les capteurs, et pour certains d'éléments actifs les rendant capables de traitements d'enrichissement de données et de transmission de celle-ci. Les données sont aussi diverses que les métiers. Nous pouvons aussi bien avoir des données de température, d'humidité, de positionnement, de temps de fonctionnement, de niveau, d'alerte… [4]

• Le réseau : pour transmettre les données. Les réseaux sont le maillon prépondérant d'un projet d'IoT, ils doivent répondre à un critère d'usage : La couverture de la zone d'usage des objets : Sur un campus, Sur une ville, à l'ensemble de la planète.[4]

• Les données : dans un projet d'IoT, les données sont nos diamants bruts. Il s'agit surtout des éléments bruts que nous récoltons depuis les objets ou les outils de processus industriels pour l'IoT. Afin de créer de la valeur pour les utilisateurs de ces données, il est absolument nécessaire de les stocker, archiver et sauvegarder dans des bases de données et de correctement structurer cette dernière. En effet, une base de données correctement structurée améliorera la performance des services IoT d'exploitation [4].

• Les informations : les informations sont les résultats des données traitées, corrélées et analysées. Ces informations doivent, elles aussi, être stockées, archivées et sauvegardées dans des bases de données [4].

• Les applications d'exploitation : les applications d'exploitation sont en principe les interfaces homme-machine (IHM) dans lesquelles nous pouvons visualiser les données sous forme de tableau de bord [4].

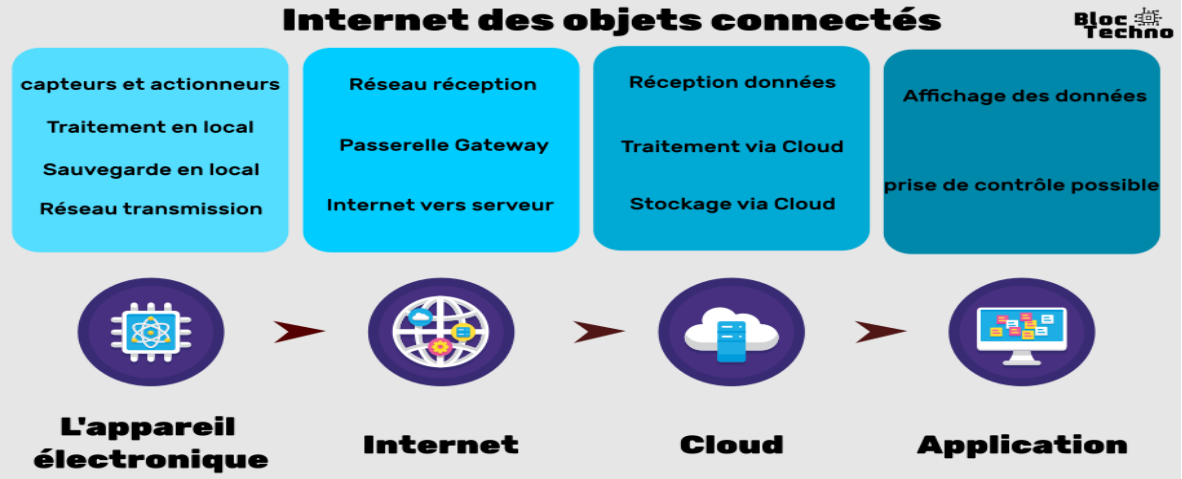


Figure 2: Fonctionnement de l'internet des objets

Tableau 1:Les principaux systèmes technologiques nécessaires au fonctionnent de l'IdO

Type de Système	**Identification (y compris lecteur)**	**Capteurs**	**Connexion**	**Intégration**	**Traitement de données**	**Réseaux**
Enjeux	Reconnaitre chaque objet de façon unique et recueillir les données stockées au niveau de l'objet	Recueillir des informations présentes dans l'environnement pour enrichir les fonctionnalités du dispositif.	Connecter les systèmes entre eux.	Intégrer les systèmes pour que les données soient transmises d'une couche à l'autre.	Stocker et analyser les données pour lancer des actions ou pour aider à la prise de décision.	Transférer les données dans les mondes physiques et virtuels
Technologies anciennes (exemple)	Codes barre, Solutions RFID simples	Thermomètre, Hydromètre ……	Câble, Bluetooth, Infrarouge, Wifi, satellites…	Middlewares…	Excel, ERP, CRM…	Internet, Ethernet…

Technologies récentes (exemple)	Solutions RFID complexes, Surface Acoustic Waves, puces Optiques, ADN	Capteurs miniaturisés Nanotechnologies	Bluetooth, Near Field Communication (NFC), Wifi	Middlewares évolués		Réseau EPC Global…

1.4. Architecture et Ecosystème de l'internet des objets

1.4.1. Architecture de l'IoT

Une architecture technique est un cadre créé pour permettre aux concepteurs et aux développeurs de considérer le système dans son ensemble et de le décomposer en sections. Selon les normes mondiales 1 (GS1), « une architecture de référence est une fondation pour permettre l'intégration des diverses technologies dans les applications IoT » [34].

Il existe de nombreuses propositions d'architectures pour l'IoT. Parmi les architectures qui ont été proposées, il y a l'architecture à cinq couches proposée par Wu et al et à trois couches proposée par IEEE (voir figure 3). En ce moment, il n'y a pas une architecture universellement acceptée.

A. Architecture à trois couches

Cette architecture se compose de :

La couche application (application layer) est chargée de fournir des services spécifiques à l'application à l'utilisateur. Il définit diverses applications dans lesquelles l'internet des objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente.[35]

La couche réseau (abstract layer) est responsable de la connexion à d'autres objets intelligents, périphériques réseau et serveurs. Ces fonctionnalités sont également utilisées pour la transmission et le traitement des données des capteurs.[35]

La couche perception (things layer) est la couche physique, qui possède des capteurs pour détecter et recueillir des informations sur l'environnement. Il détecte certains paramètres physiques ou identifie d'autres objets intelligents dans l'environnement.[35]

B. Architecture à cinq couches

Cette architecture à cinq couches se compose de :

La couches de perception et d'application : leur rôle est le même que celui de l'architecture à trois couches.

La couche de transport (transport layer) transfère les données du capteur de la couche de perception à la couche de traitement et vice versa via des réseaux tels que sans fil, 3G, LAN, Bluetooth, RFID et NFC.[35]

La couche de traitement (processing layer) est également appelée couche middleware. Il stocke, analyse et traite d'énormes quantités de données provenant de la couche transport. Il peut gérer et fournir un ensemble diversifié de services aux couches inférieures. Il utilise de nombreuses technologies telles que les bases de données, le cloud computing et les modules de traitement des mégadonnées.[35]

La couche métier (business layer) gère l'ensemble du système IoT, y compris les applications, les modèles commerciaux et de profit et la confidentialité des utilisateurs.[35]

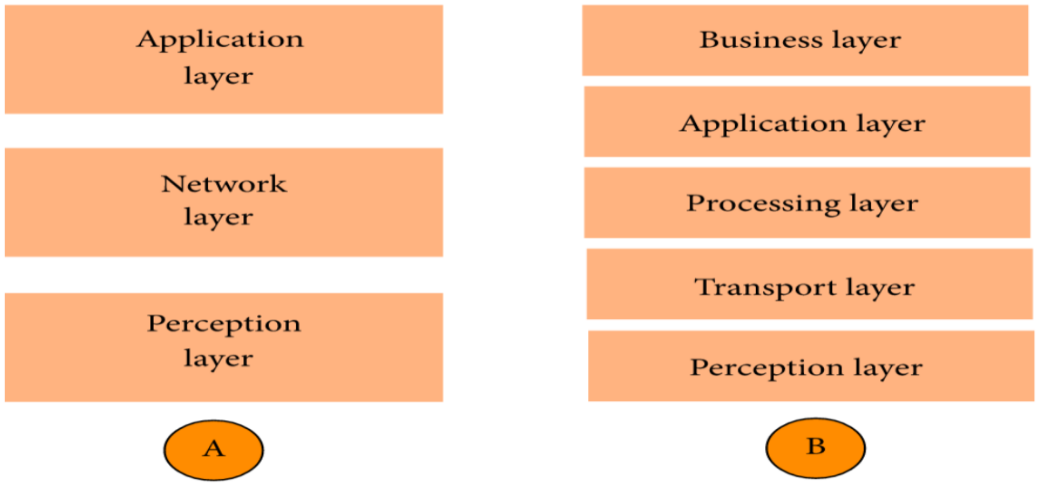


Figure 3: Architecture de l'IoT (A : trois couches) (B : cinq couches) [35]

C. Architecture à quatre couches

L'architecture à trois couches précédente, qui est la plus basique en raison du développement continu de l'IoT, ne peut pas répondre à certaines exigences de l'IoT, notamment sur la question de la sécurité. En effet les risques de menaces augmentent dans l'architecture à trois couches du fait que les informations sont envoyées directement dans la couche réseau. C'est ainsi qu'une autre architecture a été proposée. Cette architecture comporte quatre couches, dont les trois sont comme celles de l'architecture à trois couches et ont les mêmes fonctionnalités. La couche supplémentaire au niveau de cette nouvelle architecture est la couche support. Elle permet de mettre en place une plateforme fiable pour la couche application. Les plateformes de support comportent des machines de calcul intelligentes qui sont organisées par le biais du cloud computing et de la grille de réseau. Cette couche agit comme un pont entre la couche application et la couche réseau.

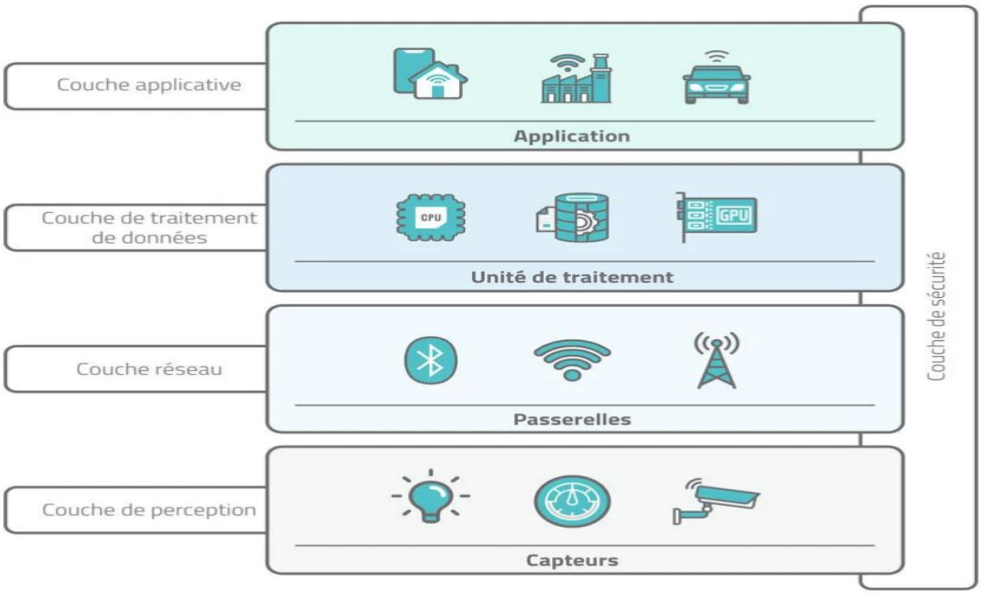


Figure 4: Architecture à quatre couches de l'IoT

1.4.2. Ecosystème de l'IoT

Un écosystème IoT est composé d'objets compatibles avec le Web ou utilisant des systèmes informatiques embarqués.

Un objet connecté à l'IoT est capable de collecter des données sur son environnement via des capteurs. Il exploite ensuite ces dernières via des processeurs avant de les envoyer à un ou plusieurs destinataires à l'aide de son matériel de communication intégré.

Il partage les données collectées par le biais d'une passerelle IoT. Il s'agit d'une solution permettant la communication entre appareils ou entre ceux-ci et le cloud. Les informations sont donc transférées directement vers le cloud à des fins d'analyse et d'exploitation ou à un autre appareil IoT pour une analyse locale.



Figure 5: L'écosystème de l'internet des Objets (IoT)

1.4.2.1. Domaines des objets connectés

- **Un objet** est, avant toute chose, une entité physique ; par exemple, un livre, une voiture, une machine à café électrique ou un téléphone mobile. Dans le contexte précis de l'internet des objets, cet objet possède au minimum un identifiant unique attaché à une identité exprimant d'une part ses propriétés immuables (type, couleur, poids, etc.) et son état, c'est-à-dire l'ensemble de ses caractéristiques pouvant évoluer au cours du temps (position, niveau de batterie, etc.) [2].
- **Un objet connecté,** c'est un dispositif permettant de collecter, stocker, transmettre et traiter des données issues du monde physique [17]. Un objet connecté doit être adopté à un usage, il a une certaine forme d'intelligence [18]. Identifiés et identifiables de façon unique et ayant un lien direct ou indirect via un concentrateur « Gateway » avec internet [17].

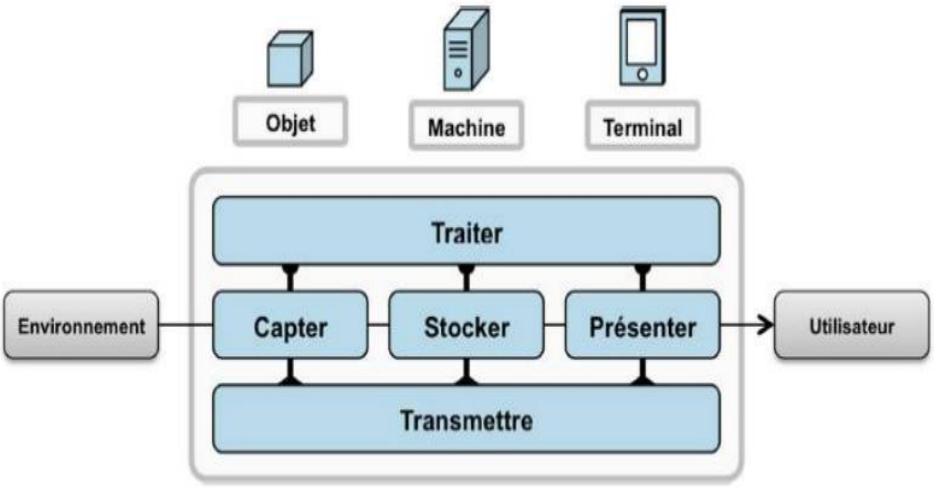


Figure 6: Collecte de données [17]

Un objet connecté peut interagir avec le monde physique de manière indépendante sans intervention humaine.

Nous distinguons deux types d'objets :

Les objets passifs : ils utilisent généralement un tag (puce RFID, code-barre 2D). Ils embarquent une faible capacité de stockage (de l'ordre du kilo-octet) leur permettant d'assurer un rôle d'identification. Ils peuvent parfois, dans le cas d'une puce RFID, embarquer un capteur (température, humidité) et être réinscriptibles [17].

Les objets actifs : ils peuvent être équipés de plusieurs capteurs, d'une plus grande capacité de stockage et être dotés d'une capacité de traitement ou encore être en mesure de communiquer sur un réseau [17].

Précisons le rôle des différents processus présentés sur cette figure 7 :

Capter : désigne l'action de transformer une grandeur physique analogique en un signal numérique.

Concentrer : permet d'interfacer un réseau spécialisé d'objets à un réseau IP standard (ex. Wi-Fi) ou des dispositifs larges publics.

Stocker : qualifie le fait d'agréger des données brutes, produites en temps réel, méta, taguées, arrivant de façon non prédictible.

Présenter : indique la capacité de restituer les informations de manière compréhensible par l'homme, tout en lui offrant un moyen d'agir et/ou d'interagir [17].

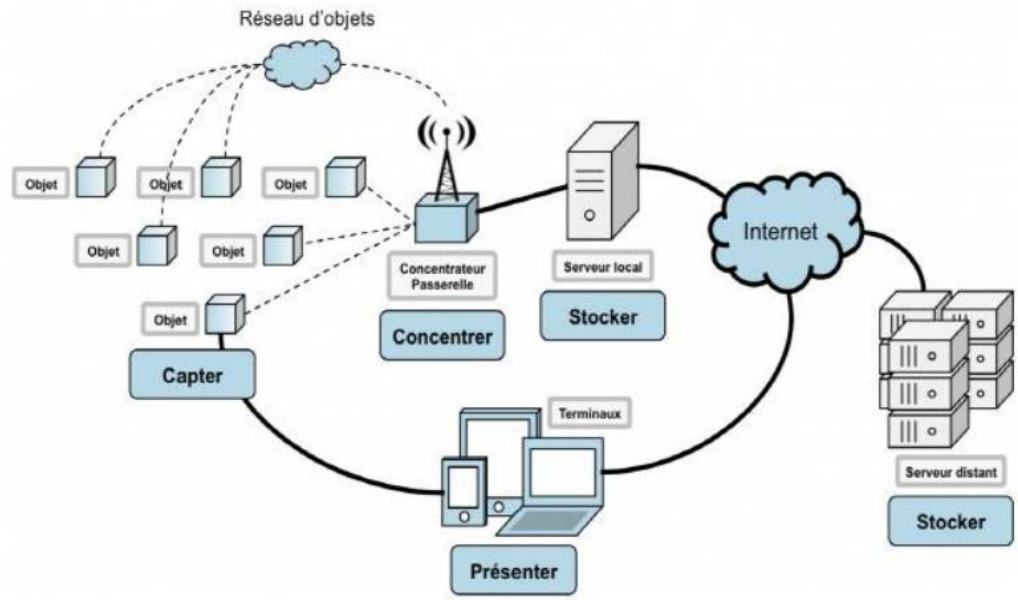


Figure 7: Mode d'opération des IoT [17]

La valeur ajoutée des objets connectés réside dans leurs capacités à communiquer. Ils utilisent pour cela des moyens de communication sans fil.

1.4.2.2. La famille de réseaux IoT

Il existe trois grandes familles de réseaux.

- Réseaux LAN

Les réseaux LAN (Local Area Network) sont des réseaux de **courte à moyenne portée** (entre 1 m et 100 m).

Les plus connus sont le Bluetooth et le Wi-Fi, lequel permet des connexions à haut débit, mais est très énergivore. Le wifi ne convient donc que pour les appareils branchés sur secteur ou dont l'alimentation électrique peut être aisée et fréquente.

Il existe d'autres standards que le Bluetooth et le Wi-Fi, comme le NFC ou encore la RFID.

- Réseaux cellulaires

Les réseaux cellulaires sont des réseaux **longue portée** (jusqu'à 30 km).

Ils sont basés sur la technologie GSM comme la 4G par exemple, et permettent de transférer une quantité importante de données (images, vidéos, etc.) avec un **très haut débit**.

Ils nécessitent l'installation d'une carte SIM dans l'appareil à connecter, afin d'identifier celui-ci sur le réseau de communication.

- Réseaux LPWAN

Les réseaux LPWAN (Low Power Wide Area Network) sont des réseaux **longue portée** (de l'ordre de plusieurs kilomètres) et **à faible consommation énergétique**.

À l'image des réseaux Sigfox et LoRa, ces réseaux ont été spécifiquement conçus pour transporter les données IoT à faible coût.

Tableau 2: Principaux moyens de communication selon la portée et l'autonomie (CRE)

	Courte portée			Moyenne portée			Longue portée	
Technologie	NFC	Bluetooth	Zigbee	Z-Wave	Wifi	BLE	Sigfox	LoRa
Portée moyenne (en intérieur)	<10cm	10m	10m	50m	50m	50m	>2km	>2km
Débit (en Mbits/s)	1*10^-3	1*10^-3	1*10^-2	1*10^-2	1*10^-2	1*10^-3	1*10^-3	1*10^-3
Autonomie	Mois	Jours	Années	Années	Jours	Mois	Années	Années
Fréquence	2,4 GHz	2,4 GHz	2,4 GHz 868 MHz	868 MHz	2,4 GHz 5 GHz	2,4 GHz	868 MHz	868 MHz
Usage	Téléphonie cartes de paiement	Périphériques informatique et Multimédia	Domotique		Navigation internet Transferts importants de données	Périphériques informatique et multimédia	Prévention d'incidents Collecte de données Gestion de réseaux	

Les passerelles :

La plupart des objets connectés ne sont pas pourvus de connections directe au réseau internet. Ils s'y connectent à travers une passerelle (gateway). Ces passerelles jouent le rôle d'intermédiaire pour connecter l'objet à internet et envoyer ses données. C'est le cas par exemple de nos box, ou de nos smartphones.

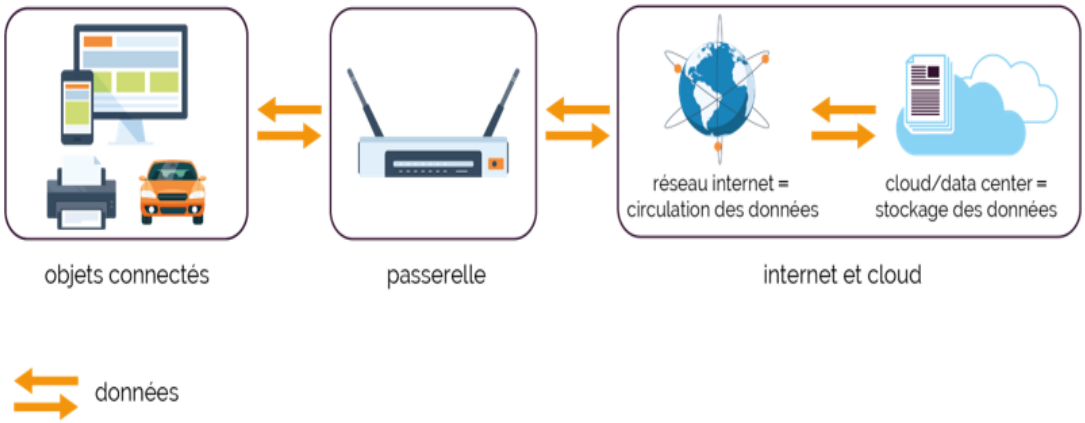


Figure 8: Connection des objets à internet

Ces passerelles fournissent tout ce qui est nécessaire en termes de connectivité, de sécurité et de management des appareils pour rendre les données disponibles sur internet.

1.5. Protocoles

Les appareils IoT communiquent à l'aide des protocoles IoT. Le protocole IP (Internet Protocol) est un ensemble de règles qui détermine la façon dont les données sont envoyées à internet. Les protocoles IoT garantissent que les informations d'un appareil ou d'un capteur seront lisibles et compréhensibles par un autre appareil, une passerelle, un service.

Différents protocoles IoT ont été conçus et optimisés pour différents scénarios et utilisations. Compte tenu de la diversité des appareils IoT disponibles, il est important d'utiliser le bon protocole dans le bon contexte.

Le type de protocole IoT dont nous aurons besoin dépend de la couche d'architecture du système dans laquelle les données voyageront.

Le modèle OSI (Open Systems Interconnection) fournit une carte des différentes couches qui envoient et reçoivent des données. Chaque protocole IoT dans l'architecture du système IoT permet une communication appareil à appareil, appareil à passerelle, passerelle à centre de données ou passerelle à cloud, ainsi que la communication entre les centres de données.

❖ **Couche Application**

La couche Application sert d'interface entre l'utilisateur et l'appareil avec un protocole IoT donné.

- AMQP (Advanced Message Queuing Protocol)

Couche logicielle qui assure l'interopérabilité entre les intergiciels de messagerie. Celle-ci permet à un large éventail de systèmes et d'applications de travailler ensemble, créant ainsi une messagerie normalisée à l'échelle industrielle.

- CoAP (Constrained Application Protocol)

Protocole optimisé pour les bandes passantes et les réseaux contraints, conçu pour les appareils dont la capacité de connexion est limitée dans le cadre d'une communication machine à machine. CoAP est également un protocole de transfert de documents qui s'exécute sur le protocole UDP (User Datagram Protocol).

- DDS (Data Distribution Service)

Protocole de communication pair à pair polyvalent qui fait tout, de l'exécution de petits appareils à la connexion de réseaux hautes performances. DDS rationalise le déploiement, renforce la fiabilité et réduit la complexité.

- MQTT (Message Queue Telemetry Transport)

  Protocole de messagerie conçu pour une communication machine à machine légère, et principalement utilisé pour les connexions à faible bande passante vers des emplacements distants. MQTT utilise un modèle éditeur-abonné et est idéal pour les petits appareils qui nécessitent une utilisation efficace de la bande passante et de la batterie

❖ Couche Transport

Dans un protocole IoT, la couche Transport permet la communication et protège les données lorsqu'elles circulent entre les couches.

- TCP (Transmission Control Protocol)

Protocole utilisé pour la majorité des connexions internet. Il offre une communication d'hôte à hôte, en divisant de grands ensembles de données en paquets individuels, et en renvoyant et réassemblant les paquets en fonction des besoins.

- UDP (User Datagram Protocol)

Protocole de communication qui permet la communication entre processus et s'exécute sur IP. UDP améliore les taux de transfert de données sur TCP et répond aux exigences des applications qui ont besoin d'une transmission de données sans perte.

❖ Couche Réseau

La couche Réseau d'un protocole IoT permet à des appareils individuels de communiquer avec le routeur.

- IP

De nombreux protocoles IoT utilisent IPv4, tandis que les exécutions plus récentes utilisent IPv6. Cette récente mise à jour du protocole IP achemine le trafic sur internet, et identifie et localise les appareils sur le réseau.

- 6LoWPAN

Ce protocole IoT fonctionne mieux avec les appareils de faible puissance qui ont des capacités de traitement limitées.

❖ **Couche Liaison de données**

La couche Données fait partie d'un protocole IoT qui transfère les données au sein de l'architecture système, en identifiant et en corrigeant les erreurs trouvées dans la couche physique.

- IEEE 802.15.4

Norme radio relative aux connexions sans fil à faible consommation. Elle est utilisée avec ZigBee, 6LoWPAN et d'autres normes pour créer des réseaux sans fil incorporés.

- Liaison sans fil à faible consommation énergétique (LPWAN)

Les réseaux étendus à basse consommation (LPWAN) permettent la communication sur des distances de 500 mètres à plus de 10 kilomètres à certains endroits. LoRaWAN est un exemple de LPWAN optimisé pour une faible consommation d'énergie.

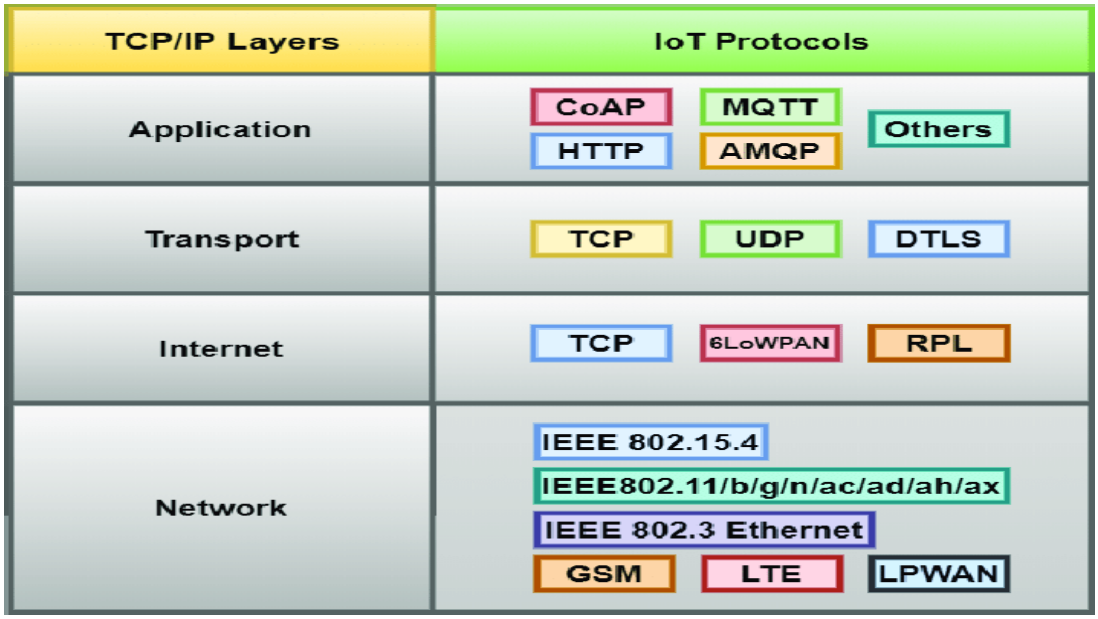


Figure 9: Principaux protocoles IoT -modèle TCP/IP

1.6. Historique de l'internet des objets

Le concept de l'IdO a été présenté en 1999 par Kevin Ashton. Ashton affirmait que les quantités de données allaient augmenter de façon si drastique que l'humanité aurait besoin de l'aide des machines pour les exploiter judicieusement. Dix ans plus tard, il déclarait que grâce aux données collectées par les appareils de l'IdO,

« [...] nous serons capables de tout surveiller et de compter, de réduire considérablement le gâchis, les pertes et les coûts. » « Nous saurons déterminer quand quelque chose doit être remplacé, réparé ou renvoyé, quand quelque chose est frais ou périmé » (Ashton 2009).

À l'image d'internet, dans sa vision, l'IdO allait changer le monde. Et sa prédiction est devenue une réalité. En 2003, on comptait environ 500 millions d'appareils connectés. En 2010, 12,5 milliards. Le département de recherche de Cisco avait prédit qu'il y aurait 25 milliards d'objets connectés dans le monde d'ici à 2015 et approximativement 50 milliards en 2020 (Cisco, 2011). Ce même chiffre a été avancé en 2018 (Davis, 2018).

Cette évolution témoigne de la croissance notable et rapide du nombre d'appareils connectés (voir figure 10). De nombreux professionnels s'accordent sur le fait que cette croissance n'est pas près de s'arrêter.

À l'avenir, de plus en plus d'appareils seront connectés et leurs fonctionnalités vont se diversifier.

Il est donc essentiel de s'intéresser à ces changements, car ils pourraient avoir (et auront très certainement) un impact énorme sur les travailleurs, les petites et moyennes entreprises (PME), mais aussi sur nos vies personnelles.

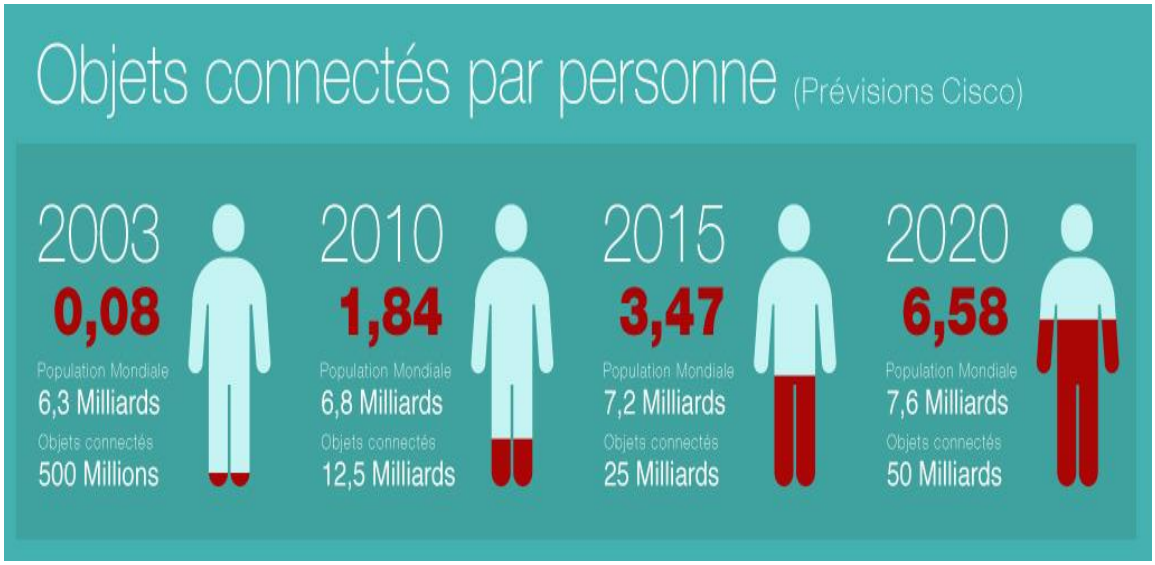


Figure 10: Evolution du nombre d'objets connectés de l'IoT

1.7. Domaines d'applications

On en entendait à peine parler il y a quelques années, et ils sont maintenant partout. Les objets connectés ont envahi notre quotidien sans même que nous y prêtions attention. De la télé intelligente à la voiture connectée, nos loisirs, nos déplacements sont facilités par ces nouveaux outils qui augmentent grandement notre confort.

Les applications sont variées et recouvrent de nombreux domaines : industrie, sciences, santé...

L'utilisation de l'IoT permettra le développement de plusieurs applications intelligentes qui toucheront essentiellement ceux qu'on citera. Dans ce qui suit, nous citons brièvement des exemples d'applications de l'IoT :

- **La domotique** [7] :

La domotique regroupe l'ensemble des technologies informatiques, électrotechnique et électronique qui permettant l'automatisation des équipements d'un habitat et transforment une maison en une maison intelligente. C'est l'ensemble des techniques visant à intégrer à l'habitant tous les automatismes en matière de sécurité (comme les alarmes), de gestion de l'énergie (optimisation de l'éclairage et du chauffage, etc.), de communication (contacts et discussion avec des personnes extérieures), etc. [7].

- **Automobile** [8] :

Avec le nombre croissant de véhicules intelligents, presque tous les véhicules vendus aujourd'hui dans le monde contiennent des capteurs et des moyens de communication pour faire face aux embouteillages, à la sécurité et au trafic [7].

L'objectif est que le véhicule puisse communiquer de manière autonome avec d'autres véhicules ou une station de surveillance pour éviter les accidents, réduire le trafic et sauver des vies [7].

Par exemple : si la voiture a un accident, elle demande automatiquement de l'aide et explique son emplacement et sa capacité à communiquer avec les utilisateurs [7].

Aujourd'hui, les constructeurs automobiles travaillent sur des projets de véhicules autonomes (sans conducteur) capables de se déplacer d'un point A à un point B sans aucune intervention humaine [7].

- **La santé** [9] :

Le secteur de la santé a connu un très grand nombre d'applications permettant à un patient et à son docteur de recevoir des informations, parfois même en temps réel, qu'il aurait été impossible de connaitre avant l'apparition d'IoT [7].

Par exemple, il existe un médicament qu'il s'appelle Porteuse Digital Heath qui est le premier médicament connecté sur le marché grâce à un capteur directement intégré dans l'être humain qui permet après ¸cela le suivi des patients à distance [7].

Aussi, il existe plusieurs autres dispositifs qui sont disponibles, fixés autour du poignet et permettent également de suivre l'activité physique quotidienne du patient, mesurer le taux de sucre, compter le nombre de pas et les kilomètres parcourus, le nombre de calories brûlées, le dispositif lui envoie une alerte dans les cas anormaux [7].

- **L'agriculture** :

L'agriculture intelligente a pour objet de renforcer la capacité des systèmes agricoles, de contribuer à la sécurité alimentaire en intégrant le besoin d'adaptation et le potentiel d'atténuation dans les stratégies de développement de l'agriculture durable [7].

Cet objectif a été atteint enfin par l'utilisation des nouvelles technologies, telles que l'imagerie satellitaire et l'informatique, les systèmes de positionnement par satellite de comme GPS, aussi par l'utilisation des capteurs qui vont s'occuper de récolter les informations utiles sur l'état du sol, taux d'humidité, taux des sels minéraux, etc. Et envoyer ces informations au fermier pour prendre les mesures nécessaires garantissant la bonne production [7].

- **Les villes intelligentes** :

Les villes intelligentes ou smart city sont en croissance dans les pays qui connaissent une avancée technologique. Il existe, dans ce cas, des systèmes qui permettent de contrôler le fonctionnement de la ville, les activités des populations, la gestion des bâtiments, la sécurité. Pour la sécurité, l'internet des objets permet d'effectuer la gestion du trafic dans les lieux de grande affluence, le suivi des caméras de télésurveillance publiques, l'éclairage connecté. Les enjeux d'une ville connectée sont, entre autres, l'optimisation des ressources économiques, la gestion de la population et l'assainissement de la ville [8].

- **L'industrie** :

Le déploiement de l'IoT dans l'industrie sera certainement un support pour le développement de l'économie et du secteur des services, puisque L'IoT permettra d'assurer un suivi total des produits, de la production à la distribution, par la gestion automatisée, la surveillance à distance, et le renforcement de la comptabilité. Ce travail compte développer les techniques de production en entreprises ainsi que le renforcement des capacités de gestion [8]. Donc la technologie IoT permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et en plus d'améliorer la sécurité des employés [8].

- **Le Sport** :

De nombreux objets connectés comme des montres ou des bracelets connectés nous permettront pendant la journée de calculer le nombre de pas effectués, la distance parcourue, votre temps d'activités, les calories brulées, ainsi que durant la nuit en calculant vos heures de sommeil. Pour les passionnés de high-tech, c'est un grand marché qui s'ouvre à eux ! De la montre connectée au téléviseur connecté en passant par les appareils photos, les montres, les drones, les lunettes (Google Glass) [26].

- **Sécurité** :

Pour le cabinet en stratégie, ces entreprises vont rapidement se positionner comme des alliés des personnes qui résident dans leur domicile. En fournissant des données relatives à la consommation d'énergie aux foyers, ces groupes vont apparaitre comme des arguments contre le facteur EDF pour les fournisseurs d'énergie la précision sera difficile à tenir, car ils seront probablement contraints d'accompagner leurs clients dans une baisse de leurs facteurs énergétique [27].

- **Militaire** :

Comme dans le cas de plusieurs technologies, le domaine militaire a été un moteur initial pour le développement des réseaux de capteurs. Le déploiement rapide, le coût réduit, l'auto-organisation et la tolérance aux pannes des réseaux des capteurs sont des caractéristiques qui rendent ce type de réseaux un outil appréciable dans un tel domaine. Comme exemple d'application dans ce domaine, on peut penser à un réseau de capteurs déployé sur un endroit stratégique ou difficile d'accès, afin de surveiller toutes les activités des forces ennemies, ou d'analyser le terrain avant d'y envoyer des troupes (détection d'agents chimiques, biologiques ou de radiations). Des tests concluants ont déjà été réalisés dans ce domaine par l'armée américaine.[28]

- **L’environnement** :

Le contrôle des paramètres environnementaux par les réseaux de capteurs peut donner naissance à plusieurs applications. Par exemple,

- ❖ **Les réseaux de capteurs sans fils** aident à l’étude de phénomènes complexes tels que les tremblements de terre, les éruptions volcaniques, les ouragans et les tsunamis. Ils fournissent des données permettant d’établir des modèles de prévision. Pour quelques applications présentées dans cette section, des systèmes filaires existaient déjà, mais étaient plus difficiles à déployer et n’offraient parfois pas autant de fonctionnalités.
- ❖ **La prévention des risques d’incendie ou d’inondation** fait partie des domaines où les réseaux de capteurs sans fils apportent les plus grandes perspectives. Dans ce type d’applications, les capteurs sans fil sont chargés de la détection de tous les phénomènes anormaux observés dans leur périmètre d’action. Il peut s’agir d’une brusque augmentation de la température ou du taux d’humidité caractéristique d’un début d’incendie ou d’inondation.
- ❖ **L’observation des animaux dans leur habitat** prend une place importante dans les applications environnementales. Les capteurs sans fil déployés dans une réserve naturelle donnent des informations de localisation sur les animaux, sur leur état de santé, sur leur intégration dans un nouvel habitat. Les réseaux de capteurs sans fils ont permis l’observation d’oiseaux sans troubler leur habitude en évitant une intervention humaine.[29]

- **Commerces** : pour les commerçants, l’IoT offre des opportunités illimitées pour augmenter l’efficacité de la chaîne d’approvisionnement, développer de nouveaux services et réorganiser l’expérience du consommateur.
- **Les usines intelligentes** : la technologie de l’IoT permet aujourd’hui aux usines de maximiser l’efficacité opérationnelle, d’optimiser la production, et d’augmenter la sécurité des travailleurs.

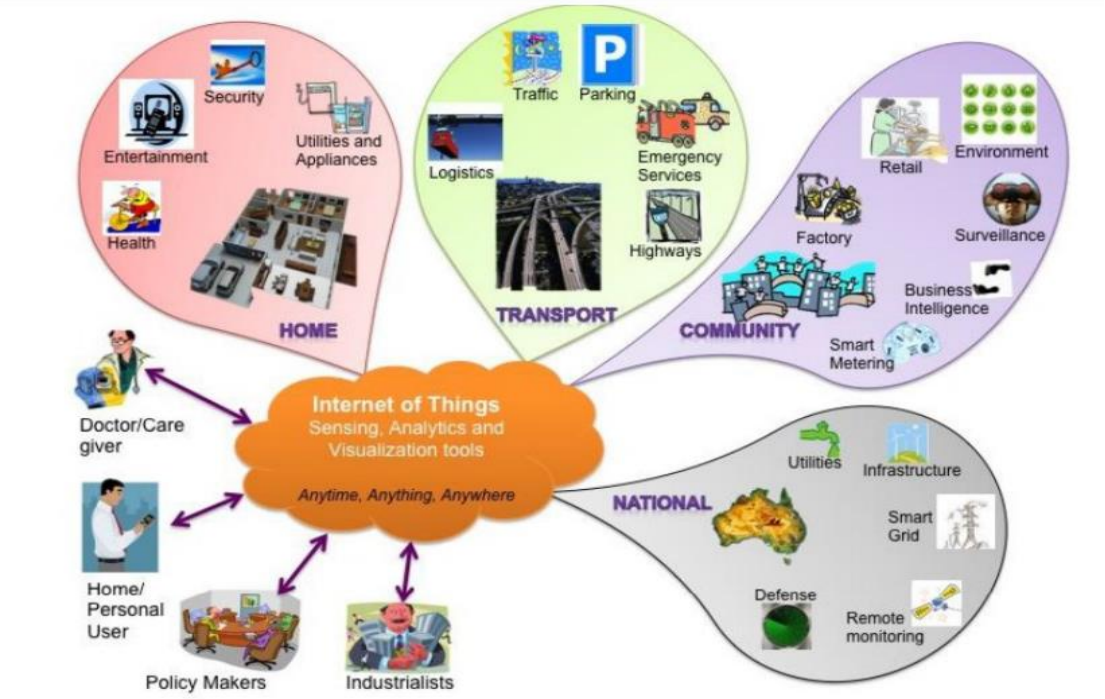


Figure 11: Domaines d'application de l'IoT

1.8. Les avantages et les inconvénients de l'IoT

1.8.1. Les avantages

Les avantages des IoT sont nombreux, nous pouvons citer les avantages suivants :

- Accès ubiquitaire à l'information pour un monde plus intelligent et un mode de vie sophistiqué et confortable.
- Amélioration de la qualité de service et de la télésurveillance dans différents domaines d'applications, à savoir le domaine industriel, médical, etc.
- Améliorer les services traditionnels généraux comme le transport et les parkings.
- La surveillance et la maintenance des lieux publics.
- Suivre le taux de la validité des instructions pour le travail.
- Réduire le temps perdu dans les transactions administratives dans la ville.
- Économiser du temps.
- Renforcer la sécurité routière.
- L'organisation et l'amélioration de la qualité d'Airlines.
- Économiser la consommation de l'énergie dans la ville.
- L'éclairage intelligent.

1.8.2. Les inconvénients

- La protection des données, la vie privée et la sécurité sont souvent les principales inquiétudes des sceptiques de l'IoT. Pour calmer ces inquiétudes, il serait utile de donner aux clients les informations relatives au lieu de stockage et à la nature des données qui les concernent [7].

- Les risques pour la sécurité de l'information : la mise en œuvre de l'IoT au sein d'une entreprise comporte un obstacle de taille qu'il importe de surmonter : la sécurité. Une atteinte à la sécurité pourrait avoir d'importantes répercussions sur la réputation et la crédibilité de l'entreprise et se traduire par une perte de temps et d'argent, en plus d'entraîner des conséquences juridiques.
- L'IoT et la confidentialité : qu'il soit lié à l'IoT ou non, tout cyber incident augmente considérablement les risques de vol, de divulgation ou d'altération de l'information. Ainsi, l'information concernant votre entreprise, vos employés et vos clients pourrait être détruite, altérée, volée ou publiée, ou même « retenue en otage » jusqu'au versement d'une rançon.
- Les appareils connectés collectent de grandes quantités de données, ce qui représente un motif de préoccupation pour la confidentialité et l'intégrité des données de l'entreprise.
- Quand un appareil connecté contrôle des biens matériels et des opérations, comme un véhicule intelligent ou une pompe à insuline, la menace que fait planer un cyber incident éventuel ne se limite pas à une brèche dans la sécurité de l'information. L'utilisation non autorisée ou la prise de contrôle à distance d'un objet connecté pourraient endommager les données et l'équipement de votre entreprise ou causer des dommages physiques à des personnes. Ces dommages pourraient s'avérer coûteux, si vous devez réparer les systèmes et équipements de votre entreprise et rétablir sa réputation. Le rôle que jouent de nombreux objets est bien plus important que l'information qu'ils emmagasinent. Pensez aux conséquences juridiques et financières que pourraient entraîner la défaillance ou le piratage d'un appareil connecté.

1.9. Les défis

L'augmentation exponentielle du nombre d'objets connectés entraîne parallèlement l'explosion du volume des données générées par ces derniers. Cette évolution engendre de nouveaux défis, principalement autour de la sécurisation et de l'accessibilité en temps réel aux données. En effet, les enjeux portent sur l'intégration transparente, sécurisée et efficace de l'hétérogénéité des technologies de communications utilisées et des interfaces de connexion associées (les objets connectés doivent pouvoir communiquer facilement non seulement sur le réseau, mais aussi entre eux), de l'hétérogénéité de la nature des objets et des technologies qu'ils utilisent, et bien sûr aussi de l'hétérogénéité des données générées selon différents formats. Ainsi, pour permettre son propre développement et accompagner la conception d'applications sûres et efficaces, l'IoT doit à minima relever les défis suivants :

- **L'hétérogénéité des dispositifs** : Un défi majeur pour l'IdO à la fois technique et utile, c'est de pouvoir gérer l'hétérogénéité technologique et des normes d'objets couplées à des multitudes de besoins, d'applications et d'usages en termes de services de sécurité. Sachant que ces besoins peuvent évoluer dans le temps selon le contexte et le goût. En effet, comment assurer l'authentification individuelle de plusieurs millions d'objets hétérogènes, dotés des technologies de communication hétérogènes, à travers des domaines administratifs multiples ? [VER 2011]. Ceci soulève des problèmes de gestion et de sécurité des objets dans un milieu hétérogène au niveau physique et

logique. Il est donc important d'instaurer des politiques de sécurité claires, adaptatives selon le contexte d'utilisation et d'établir les responsabilités des faits et des actions sur l'environnement physique des objets. « En effet, l'internet des objets est un système complexe dans lequel interagissent des personnes avec un écosystème technologique à base d'objets intelligents à travers des processus complexes. Les interactions de ces quatre composantes de l'IdO (personnes, objets intelligents, écosystème technologique, processus) font émerger une dimension systémique à la sécurité de l'IdO » [CHA 2012]. Par la suite, les tensions sur la sécurité de l'IdO sont créées lors de l'interaction des objets intelligents avec son environnement. Ces tensions (confiance, responsabilité, identification et auto-immunité) sont caractérisées par une dimension cognitive et systémique induite par l'autonomie grandissante des objets [CHA 2012].

- **Les ressources limitées** : historiquement, l'IoT s'est développé au travers de dispositifs intelligents ayant des ressources limitées afin tant de minimiser les coûts que de conserver des objets compacts. Bien sûr, aujourd'hui, des objets plus puissants sont disponibles grâce aux progrès dans la miniaturisation et l'intégration des composants, conjointement à la baisse de leurs coûts de production. Toutefois, le plus souvent, objet connecté rime encore avec ressources limitées. Les contraintes de ressources matérielles portent sur la puissance de traitement (CPU et mémoire RAM), la capacité de stockage (mémoire Flash), sur l'autonomie énergétique, sur les communications, etc. L'énergie de fonctionnement est souvent fournie par des piles ou des batteries et parfois, l'autonomie est assurée par des panneaux solaires ou d'autres systèmes de récupération d'énergie.
- **La mobilité** : de plus en plus fréquemment, dans l'IoT, les dispositifs intelligents sont maintenant capables de se mouvoir. Parmi ces objets, on peut trouver des drones, mais aussi des robots aspirateurs, des véhicules connectés. Afin de fournir un accès permanent et transparent aux données qu'ils produisent, mais aussi pour leur permettre d'accéder à d'autres services de l'IoT, ces dispositifs en mouvement (qu'il soit permanent ou ponctuel) conduisent à introduire de la dynamique dans le réseau avec de multiples connexions et déconnexions en temps réel. Il peut s'agir de réseaux dynamiques formés pour un instant par plusieurs dispositifs ou de réseaux statiques (préexistants) auxquels les dispositifs se rattachent le temps nécessaire. La gestion de tels réseaux dynamiques devient très difficile dans de grands environnements distribués, car déterminer si un dispositif peut être accepté dans le réseau revient à déterminer le niveau de confiance qu'on lui accorde. C'est donc, infime, une problématique de sécurité. Dans les réseaux dynamiques, la gestion de la mobilité peut se faire de plusieurs façons. Le dispositif intelligent (dont on rappelle qu'il est intégré à un dispositif physique, c'est-à-dire un objet) doit détecter son mouvement afin d'identifier qu'il va probablement quitter l'emplacement qu'il occupe alors dans la topologie du réseau pour se connecter à un autre endroit ou même à un autre réseau. Cette détection peut se faire par un scan passif des messages des participants aux réseaux ou via le suivi des émissions de balises (« beacons ») [34]. Une autre façon de gérer la mobilité est l'intégration dans les protocoles de messages de signalisation et de contrôle de la localisation des nœuds dans le réseau [35]. Il est à noter que la mobilité augmente la surface d'attaque et qu'elle va par conséquent de pair avec la sécurité.

C’est pourquoi une solution de sécurité pour les dispositifs IoT devrait prendre en compte leur mobilité [36].

- **La sécurité** : les objets intelligents étant souvent déployés dans des environnements ouverts dans lesquels ils ne sont pas surveillés (milieux qu’on considère souvent comme adverses). Par exemple, afin de récupérer des données environnementales (température, pression, humidité, luminosité, etc.), si des capteurs fonctionnant sur batterie sont déployés sur le terrain (pour remonter les données à une station de base), ils ne sont généralement pas sous la surveillance physique à tout instant de l’opérateur les exploitant. En revanche, un adversaire peut lui y accéder physiquement pour conduire des attaques telles que la copie des données collectées (atteinte en confidentialité), la modification ou la suppression des données collectées (atteinte en intégrité). Les nœuds eux-mêmes peuvent être clonés et/ou modifiés à l’insu de leur propriétaire [36, 37]. Par ailleurs, en raison des ressources limitées des objets de l’IoT, les mécanismes de protection des communications ne sont souvent pas utilisés, ce qui peut permettre à l’adversaire d’écouter les communications, de falsifier des échanges, etc.

1.10. Conclusion

L’internet des objets, en tant qu’une évolution de l’internet actuel, permet une amélioration considérable de notre mode de vie et de la façon dont les objets intelligents dans notre entourage interagissent entre eux. Dans ce chapitre, nous avons expliqué la notion d’internet des objets qui constitue l’avenir de plusieurs domaines. Néanmoins, les problèmes d’ordre sécuritaire sont des défis à relever dans cette technologie.

Chapitre 2 : Sécurité de l'IoT

2.1. Introduction

« The National Intelligence Council (NIC) » américain considère que les avancées technologiques combinées à une forte demande des marchés encourageraient une adoption et un déploiement à large échelle de l'IdO. Néanmoins, la plus grande crainte est que les objets du quotidien deviennent des risques d'attaque de sécurité. Pire encore, la pénétration à large échelle de l'IdO diffuserait ces menaces d'une façon beaucoup plus large que l'internet d'aujourd'hui [39]. En effet, l'ubiquité de l'IdO amplifiera les menaces classiques de sécurité qui pèsent sur les données et les réseaux. Mais en plus, le rapprochement du monde physique et du monde virtuel à travers l'IdO ouvre la voie à de nouvelles menaces qui pèseront directement sur l'intégrité des objets eux-mêmes, les infrastructures et processus (monde physique) et la vie privée des personnes. Dans ce chapitre, nous allons d'abord définir la différence entre une vulnérabilité, une menace et un risque. Avant de présenter les différents services de sécurité. Ensuite, parler des vulnérabilités et enfin des attaques qui sont présentes dans le monde de l'IdO.

2.2. La différence entre vulnérabilité, menace et risque

La sécurité est un compromis entre les trois termes suivants :

2.2.1. Vulnérabilité

C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier. Ou bien « Une faiblesse dans un système ou dans sa conception qui permet à un intrus d'exécuter des commandes, d'accéder à des données non autorisées et / ou de mener des attaques par déni de service ».

2.2.2. Menace

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci : accident, erreur, malveillance passive si elle porte sur la confidentialité, malveillance active si elle modifie le contenu de l'information ou le comportement des systèmes de traitement.

2.2.3. Risque

C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.

2.3. Les propriétés de sécurité

Face aux menaces, il est fréquent de définir les propriétés de sécurité à assurer dans un système. Lors de la conception d'une solution de sécurité visant à pallier les menaces identifiées, une fois les propriétés de sécurité souhaitées sont exprimées, celles-ci se nomment sous le terme d'exigences de sécurité.

Il convient d'identifier les exigences fondamentales en sécurité informatique, qui caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques au regard de la sécurité :

- La confidentialité : seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- L'intégrité : il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- La disponibilité : il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.
- La non-répudiation : une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.
- L'authentification : elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.
- L'anonymat : est une forme particulière de confidentialité, puisqu'elle consiste généralement à protéger une donnée particulière : l'identité.
  Dans un système IoT, l'anonymat consiste à garder secrète ou indiscernable (c'est-à-dire en pratique semblable à un aléa) toute information permettant d'identifier une entité communicante. En effet, une entité est anonyme si elle n'est pas identifiable. Lors d'une communication entre un émetteur et un récepteur, l'anonymat est garanti si l'analyse d'un message ne permet pas d'identifier son émetteur et/ou son récepteur.



Figure 12: les propriétés de sécurité

Afin de fournir et d'assurer chacun des services énumérés ci-dessus, différents mécanismes de sécurité doivent être mis en place. Le tableau suivant montre quelques mécanismes associés à chaque service.

Tableau 3: la relation entre les services et les mécanismes de sécurité

Principes de sécurité	Mécanisme de sécurité
Confidentialité	Les mécanismes cryptographiques Symétriques/asymétriques (AES, RSA, …)
Authentification	Le code d'authentification de message et le chiffrement
Intégrité	Les fonctions de hachage (md5, SHA, …) et les signatures numériques
Non répudiation	Les signatures numériques
Disponibilité	Le contrôle d'accès

2.4. Les vulnérabilités de l'internet des objets

OWASP a défini un top dix des vulnérabilités de l'internet des objets :

- **Mot de passe faible, devinable ou codé en dur** :
  Utilisation d'informations d'identification facilement forcées, accessibles au public ou non modifiables, y compris des portes dérobées dans un micrologiciel ou un logiciel client qui accorde un accès non autorisé aux systèmes déployés.
- **Services réseau non sécurisés** :
  Services réseau inutiles ou non sécurisés s'exécutant sur l'appareil lui-même, en particulier ceux exposés à internet, qui compromettent la confidentialité, l'intégrité, l'authenticité ou la disponibilité des informations ou permettent un contrôle à distance non autorisé.
- **Interfaces d'écosystème non sécurisées** :

Interfaces Web, API, backend, cloud ou mobiles non sécurisées dans l'écosystème en dehors de l'appareil, ce qui permet de compromettre l'appareil ou ses composants associés.

Les problèmes courants incluent un manque d'authentification/ d'autorisation, un cryptage manquant ou faible et un manque de filtrage d'entrée et de sortie.

- **Absence de mécanisme de mise à jour sécurisée** :
  Manque de capacité à mettre à jour l'appareil en toute sécurité. Cela inclut le manque de validation du micrologiciel sur les appareils, le manque de livraison sécurisée (non chiffrée en transit), le manque de mécanismes anti-rollback et le manque de notifications de changements de sécurité en raison des mises à jour.
- **Utilisation de composants non sécurisés ou obsolètes** :
  Utilisation de composants / bibliothèques de logiciels obsolètes ou non sécurisés qui pourraient permettre à l'appareil d'être compromis. Cela inclut la personnalisation non sécurisée des plates-formes du système d'exploitation et l'utilisation de logiciels ou de composants matériels tiers provenant d'une chaîne d'approvisionnement compromise.
- **Protection de la vie privée insuffisante** :
  Les informations personnelles de l'utilisateur stockées sur l'appareil ou dans l'écosystème qui sont utilisées de manière non sécurisée, incorrecte ou sans autorisation.
- **Transfert et stockage non sécurisés des données** :
  Absence de cryptage ou de contrôle d'accès des données sensibles n'importe où dans l'écosystème, y compris au repos, en transit ou pendant le traitement.
- **Manque de gestion des appareils** :
  Manque de prise en charge de la sécurité sur les appareils déployés en production, y compris la gestion des actifs, la gestion des mises à jour, la mise hors service sécurisée, la surveillance des systèmes et les capacités de réponse.
- **Paramètres par défaut non sécurisés** :
  Les périphériques ou systèmes livrés avec des paramètres par défaut non sécurisés ou n'ont pas la capacité de rendre le système plus sécurisé en empêchant les opérateurs de modifier les configurations.
- **Absence de durcissement physique** :
  Absence de mesures de durcissement physique, permettant aux attaquants potentiels d'obtenir des informations sensibles qui peuvent aider lors d'une future attaque à distance ou de prendre le contrôle local de l'appareil.



Figure 13: Les 10 vulnérabilités de l'IOT selon OWASP

2.5. Les attaques visant l'IdO

Les cybers délinquants peuvent attaquer le hardware ou le software de n'importe quel composant au sein d'un système d'IdO. Parmi les types de cyberattaques par l'IdO figurent les catégories d'attaques suivantes :

1) Les attaques actives

Une attaque active consiste à capturer et à modifier les informations d'un système, voire à en injecter. Aussi, dans le contexte de la sécurité des communications, il faut considérer que l'attaquant a un accès total au canal de communication. Il peut donc ajouter, modifier ou supprimer les messages.

- Attaques d'usurpation d'identité (spoofing attack) : c'est lorsqu'une entité malveillante réussit à se faire passer pour une autre, obtenant ainsi les droits d'accès et les avantages de la victime [30].
- Usurpation de l'adresse e-mail : lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur, mais il est possible de changer l'adresse. Ainsi, un attaquant peut envoyer un e-mail en usurpant l'adresse d'un autre utilisateur.
- Usurpation de l'adresse IP (IP spoofing) : c'est une technique consistant à remplacer l'adresse IP de l'expéditeur par l'adresse IP d'une autre machine. Cette technique permet ainsi à un attaquant d'envoyer des paquets anonymement.
- Attaques de rejeu : c'est quand un utilisateur malicieux copie et renvoie un ou plusieurs message(s) déjà transmis afin d'exploiter les vulnérabilités du système [30].
- Attaques par force brute : en effet, le principe de ces attaques consiste à tester un grand nombre de mots de passe dans l'espoir de deviner le bon. Il peut également s'agir d'une opération de déchiffrement de données où l'attaquant essaie toutes les clés possibles jusqu'à ce que la clé correcte soit trouvée (recherche de clé exhaustive) [30].
- Le concept de Man-in-the-Middle (MITM) : désigne une attaque menée par un pirate informatique qui cherche à interrompre et à intercepter une communication entre

deux systèmes distincts. Ce type d'attaque peut être dangereux, car le pirate informatique intercepte discrètement les messages entre deux parties pour les retransmettre, alors qu'elles pensent communiquer directement entre elles. En possession du message d'origine, l'attaquant est en mesure de piéger le destinataire en lui faisant croire que le message qu'il reçoit est légitime.

- Attaques par cryptanalyse : cette catégorie concerne l'étude du flux de chiffrement (cipher), du texte chiffré ou des crypto-systèmes, afin de trouver des vulnérabilités qui permettent de récupérer le texte en clair à partir du texte chiffré [30].
- DOS (Denial Of Service) : ce type d'attaque est une tentative de rendre une machine ou une ressource réseau indisponible pour les utilisateurs auxquels elle est destinée. En raison de capacités mémoires insuffisants et de ressources de calcul limitées, la majorité des périphériques dans l'IoT sont vulnérables aux attaques d'environnement [31].
- Attaque Jamming : une attaque bien connue dans les communications sans fil, qui consiste à occuper le canal radio en envoyant des informations inutiles sur la bande de fréquence utilisée. Ce brouillage peut être temporaire, intermittent ou permanent et résultera dans l'incapacité des nœuds légitimes du réseau à envoyer et/ou recevoir des données [32].
- Attaque du trou noir (black holeattack) : un nœud falsifie des informations de routage pour forcer le passage des données par lui. Plus tard, son seul objectif est alors de ne rien transférer, créant ainsi un puits ou un trou noir dans le réseau [33].
- Attaque d'inondation « HELLO » : de nombreux protocoles de routage utilisent le paquet "HELLO" pour découvrir les nœuds voisins et ainsi établir une topologie du réseau. L'attaque la plus simple pour un attaquant consiste à envoyer une inondation de tels messages pour inonder le réseau et empêcher les autres messages d'être échangés [33]. Cette attaque peut être considérée comme une attaque de type jamming.

2) Une attaque passive

Une attaque passive consiste à surveiller, à capturer ou à utiliser les informations d'un système sans que cela ait de répercussion ou de modification sur son bon fonctionnement ou sur les données échangées. En effet, ce type d'attaque n'a aucun impact sur les communications entre les entités du système. Ces attaques sont souvent des étapes préliminaires à une attaque active.

Typiquement, les données sont envoyées et reçues de façon apparemment normale et ni l'émetteur ni le récepteur ne sont conscients qu'un tiers a lu les messages ou a analysé le trafic. Il existe deux types d'attaques passives

- Lecture du message : les données sont envoyées en clair (conversation téléphonique, e-mails, fichier, etc.). Ces données peuvent contenir des informations sensibles ou confidentielles : pour empêcher la lecture des messages, on peut utiliser le cryptage.
- Analyse du trafic : si les messages sont illisibles, l'adversaire ne peut pas les lire, mais peut analyser le trafic. L'adversaire peut déterminer l'emplacement et l'identité des hôtes de la communication et peut observer la fréquence et la longueur des messages

échangés. Ces informations peuvent être utiles pour deviner la nature de la communication qui se déroule.

Tableau 4: Les différentes types d'attaque dans l'IdO

Nom de l'attaque	But et résultat de l'attaque	Menace	Active ou Passive
Dos	-Saturer un serveur ou bloquer le trafic. -Rendre un service non disponible	-Intégrité -Disponibilité -Confidentialité	Active
Man-in-the-Middle	-Intercepter les communications entre deux parties et contrôler la conversation -Ecouter, modifier ou supprimer des données.	-Intégrité -Confidentialité	Active
L'usurpation d'identité	-Vol d'identité	-Confidentialité - Authentification	Active
Lecture du message	-Ecouter et lire les données envoyées entre deux entités.	-Confidentialité	Passive
Analyse du trafic	-Analyse des informaions concernant les données transmises.	-Confidentialité	Passive
Rejeu	-Ecouter, modifier ou supprimer des données.	-Intégrité -Confidentialité -Disponibilité	Active
Modification des messages	- Modifier, retarder, Réordonner des données.	-Intégrité -Disponibilité	Active

2.6. L'Authentification dans l'IoT

Comme indiqué précédemment, l'authentification est la sécurité fondamentale dans l'environnement IoT. L'authentification est le processus qui permet aux gens, souvent aux employés, d'identifier qui ils sont afin qu'ils puissent accéder aux installations ou au réseau informatique de l'entreprise. Le processus est extrêmement important pour aider à prévenir l'accès non autorisé, ce qui peut mener à des atteintes catastrophiques aux données. Il existe une grande variété de méthodes d'authentification, allant de la simple (un mot de passe unique) à la complexe (authentification multifacteurs qui peut inclure des mots de passe, des codes uniques et des données biométriques).

2.6.1. Les différentes techniques d'authentification

L'authentification est le mécanisme de sécurité qui permet de prouver l'identité d'une entité. En effet, il existe plusieurs méthodes d'authentification qu'on peut classer en 4 catégories :

- L'authentification avec ce qu'on sait, c'est-à-dire que l'entité prouve son identité avec une information secrète, qui n'est connue que par un nombre limité d'objets légitimes. Généralement, le nombre d'objets concernés ne dépasse pas deux (ex. un client et un serveur). Les mécanismes les plus utilisés dans cette catégorie sont les mots de passe et les numéros personnels d'identité (Personal Identity Number (PIN)) ;
- L'authentification avec ce qu'on possède. Dans cette catégorie, une entité s'authentifie grâce à une donnée stockée. Cette donnée peut être secrète comme les clé pré-partagées (Pre-Shared Key (PSK)), ou publique comme les certificats numériques et les jetons ;
- L'authentification avec ce qu'on est. Ça concerne généralement les utilisateurs humains, qui ont des caractéristiques biométriques qui leur sont uniques telle que la voix, l'empreinte digitale, l'iris et les veines ;
- L'authentification de comment on se comporte. Cette dernière catégorie est basée sur les profils comportementaux de chaque utilisateur. Chaque entité a une façon de travailler particulière, par exemple, sa façon de taper sur un clavier, les horaires de travail habituels, l'environnement de travail habituel, etc.

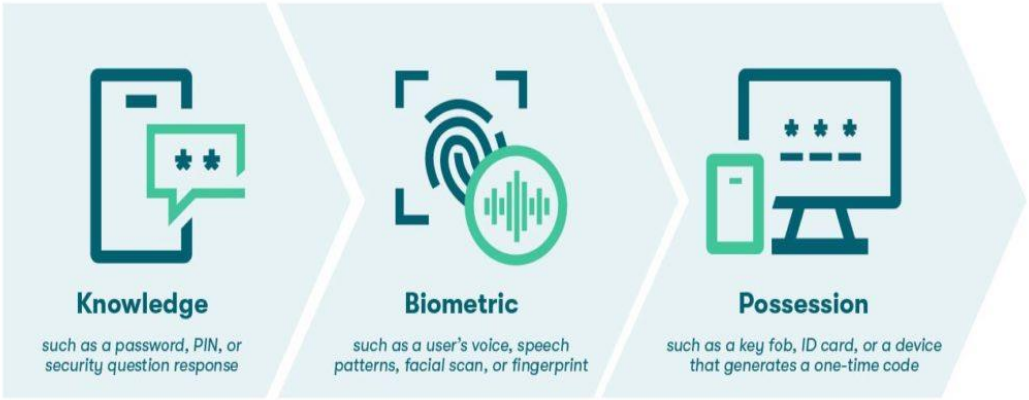


Figure 14: schéma de différents types d'authentification

2.6.2. Les risques liés aux techniques d'authentification

Les risques de sécurité les plus fréquents dans la sphère IoT actuelle sont liés aux fragilités des identités et aux techniques d'authentification. Ils concernent :

- L'authentification faible : l'utilisation d'authentifiants faibles proposés par défaut donne aux pirates un accès à grande échelle aux appareils, propice au déploiement de malwares.
- Les authentifiants codés en dur : le codage en dur de mots de passe ou de clés dans des logiciels ou micrologiciels, suivi de l'intégration de ces authentifiants au format texte dans le code source, simplifie la tâche des développeurs, mais aussi celle des hackers.
- Les clés partagées et non protégées : de nombreux cas de chiffrement symétrique (plutôt qu'asymétrique), liés à des problématiques de stockage et d'activation des clés de chiffrement (même asymétriques), facilitent la compromission des appareils. La problématique du stockage devient particulièrement délicate à grande échelle.
- Le chiffrement faible : le recours à des algorithmes faibles aboutit à un chiffrement facile à casser. Ce problème est lié au fait que les plus petits appareils IoT, à la puissance de calcul limitée, peinent à générer des nombres suffisamment aléatoires (à entropie trop faible).
- Les micrologiciels non signés : si la signature de code atteste de l'authenticité et de l'intégrité du code, de nombreux appareils IoT ne vérifient pas cette signature, ce qui les rend vulnérables aux mises à jour de micrologiciels malveillants.

2.6.3. Les solutions pour la sécurisation des appareils IoT

Malgré ces difficultés, la sécurité de l'internet des objets est à notre portée. Fonder sa stratégie de sécurité sur une solide infrastructure à clés publiques est un excellent choix. Une analyse approfondie révèle qu'une PKI peut renforcer la sécurité des appareils IoT de six manières essentielles :

- Identités uniques : l'utilisation de certificats assure à chaque appareil une identité vérifiable au moyen d'une méthode cryptographique, gage d'un accès réseau et d'une exécution de code sécurisés. À noter que ces certificats peuvent être actualisés ou révoqués de façon unitaire.
- Standard ouvert et universel : l'infrastructure PKI est un standard ouvert et compatible avec toute racine de confiance et protocoles d'enregistrement, de gestion et de révocation de certificats, permettant ainsi de prendre en charge divers scénarios d'utilisation.
- Haut degré d'évolutivité : l'émission de certificats uniques, à partir d'une même autorité de certification (AC) digne de confiance, facilite l'authentification respective des appareils en l'absence de serveur centralisé.
- Sécurité performante : un programme PKI correctement géré offre une authentification renforcée, les clés de chiffrement étant d'un niveau de sécurité nettement plus élevé que les méthodes de type mots de passe et jetons.
- Faible encombrement : les clés asymétriques, peu encombrantes, s'avèrent idéales pour les appareils IoT dotés de peu de puissance de calcul et de mémoire.

- Solution éprouvée : l'infrastructure PKI est une approche testée et éprouvée, validée par les experts qui considèrent cette solution comme pratique et évolutive pour une sécurité renforcée contre une grande variété d'attaques.
  Cependant, avec l'évolution de l'écosystème IoT, la massification des données nous mène à nous poser des questions sur la protection de celle-ci et la blockchain peut y répondre. La blockchain n'est pas seulement destinée à des échanges de crypto-monnaies. Elle a pour vocation de sécuriser les différents types de transaction, notamment celle des données. En effet, la blockchain nous promet une protection maximale des données, notamment pour le transfert de celles-ci.

2.7. Conclusion

L'internet des objets (IoT) représente la prochaine ère de la communication. Cette technologie a largement contribué au développement de différents secteurs et à automatiser divers créneaux. Cela étant, l'IoT est confronté à de sérieux défis et challenges concernant la sécurité. En effet, l'internet des objets fait face à de nombreuses vulnérabilités qui le rendent sensible à plusieurs cyberattaques. La sécurité est un volet très important qui ne peut être négligé. C'est pourquoi nous avons étudiés les techniques d'authentifications ainsi que leurs risques, sans oublier les solutions pour faire face à la sécurisation des objets IoT.

Ainsi notre prochain chapitre fera l'objet de l'étude de la technologie Blockchain qui, avec l'IoT et la massification des données, apparaît comme la solution la plus propice pour protéger les données.

Dès lors, nous pouvons nous demander si IoT et blockchain évolueront ensemble ou non.

Chapitre 3 : La technologie blockchain

3.1. Introduction

La blockchain a changé la vision d'internet en faisant en sorte que l'information soit distribuée mais, non copiée. Une blockchain ne nécessite que des coûts d'infrastructure comme dans tout autre cas. Mais cela ne nécessite aucun coût de transaction. Dans sa forme la plus simple, on peut définir l'IoT comme les choses qui sont câblées pour envoyer et recevoir des données dans le monde d'internet pour contrôler l'appareil ou analyser et manipuler les données partagées. La technologie blockchain peut être utilisée comme un outil efficace pour la protection de la vie privée et la sécurité des données à l'ère de l'IdO. Le principal défaut de l'architecture IoT actuelle est "d'avoir une structure correcte et robuste pour partager les données sur le réseau", qui est surmontée par une blockchain qui crée certainement la structure correcte et robuste pour partager les données.

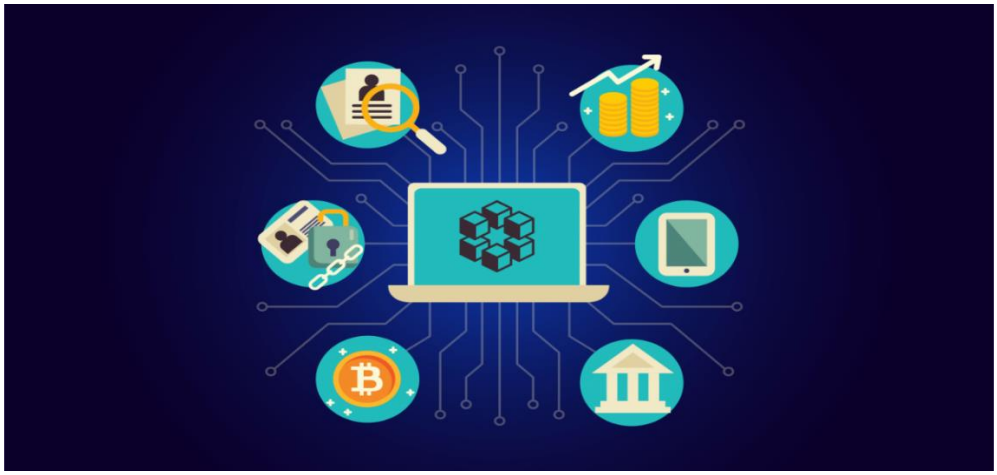


Figure 15: Schéma de la blockchain

3.2. Définition de la blockchain

De nombreuses définitions de la blockchain existent. Pour faire simple, il s'agit d'une technologie de stockage et de transmission d'informations. Elle fonctionne sans aucun organe central de contrôle. C'est pourquoi elle offre à ses utilisateurs de hauts standards de transparence et de sécurité. La blockchain est une technologie qui ne cesse de gagner en popularité dans les quatre coins du monde : Europe, Chine, Hong Kong…

Tous les utilisateurs partagent simultanément la blockchain, sans intermédiation. Ces utilisateurs ont ainsi la possibilité d'y inscrire des données. Le tout, en respectant des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie.

3.3. Historique de la blockchain

Les origines de la première blockchain de l'histoire remontent à 1995… Cette révolution figure sur le New York Times, dans la rubrique « Annonces et objets trouvés », depuis plus de 25 ans. Mais qui sont les chercheurs à l'origine de la première blockchain ?

En 1991, Stuart Haber et Scott Stornetta, chercheurs en cryptographie, posent les bases de cette révolution informatique, permettant l'horodatage des documents numériques. Ils instaurent alors un système de certification totalement décentralisé. Ce système repose sur un grand cahier libre, gratuit, infalsifiable et distribué dans le monde entier. Le tout, grâce à des méthodes de cryptographie bien précises qui empêchent l'antidatage ou l'altération de ce cahier.

Face à leur découverte, les deux chercheurs décident d'inscrire une suite de caractères cryptographiés dans la rubrique « Annonces et objets trouvés » du New York Times… C'est le début de la blockchain.

En 2004, Hal Finney, informaticien, lance un système appelé RPoW (« Reusable Proof of Work » pour « preuve de travail réutilisable »). Ce système ingénieux a permis de créer un jeton non échangeable et possédant une signature RSA. Ce dernier pouvait être transféré d'une personne à une autre. Les professionnels de la blockchain considèrent alors que ce système est le premier « prototype » de la cryptomonnaie. Fin 2008, Satoshi Nakamoto crée le premier système de paiement électronique décentralisé de pair à pair : le Bitcoin.

En 2009, la blockchain est implémentée en tant que composant principal du Bitcoin. À noter que plusieurs monnaies virtuelles utilisent les blockchains pour leur sécurité.

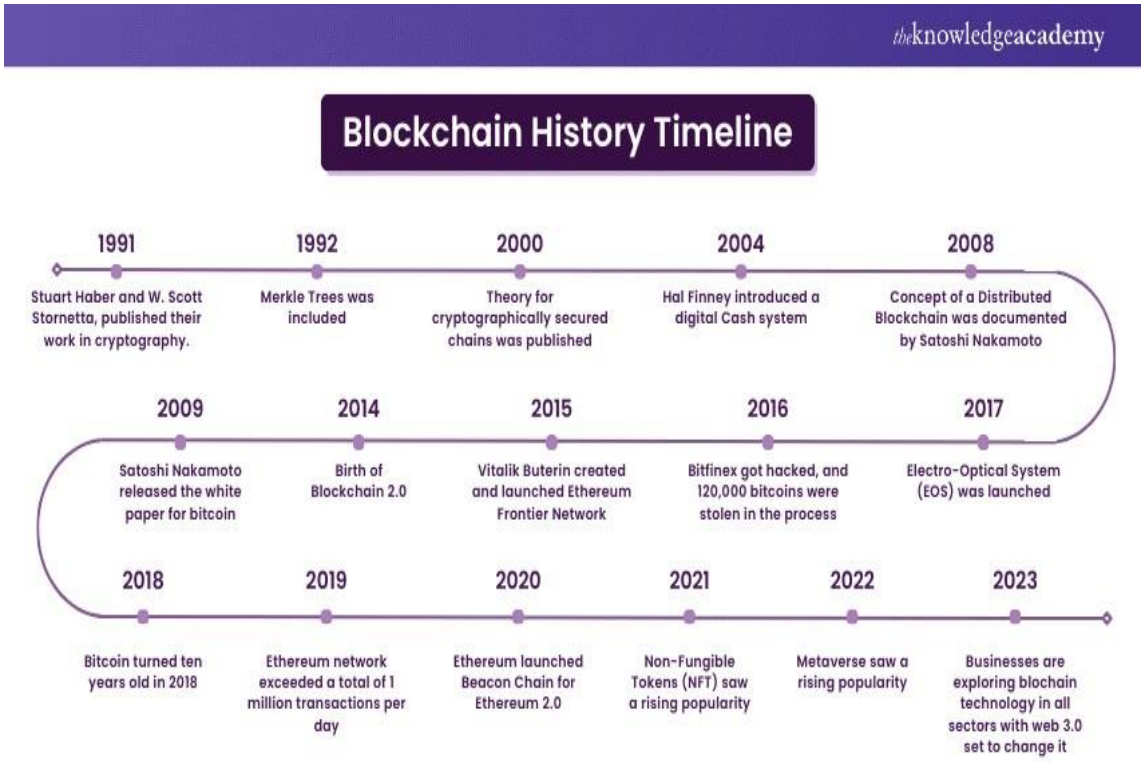


Figure 16: Historique de la technologie blockchain Source : blockchain 101.com

3.4. Le système blockchain

Pour faire partie d'un système blockchain, les entités participantes installent et exécutent chacune un logiciel qui connecte leur ordinateur ou leur serveur à d'autres participants du réseau. En exécutant ce logiciel, les participants agissent comme des validateurs individuels,

appelés nœuds de réseau. Lorsqu'un nœud se connecte au réseau pour la première fois, il télécharge une copie complète de la base de données blockchain sur son ordinateur ou son serveur ; le réseau de nœuds gère la base de données, également appelée blockchain. Les nœuds sont des points d'entrée pour de nouvelles données, ainsi que la validation et la propagation de nouvelles données qui ont été soumises à la blockchain.

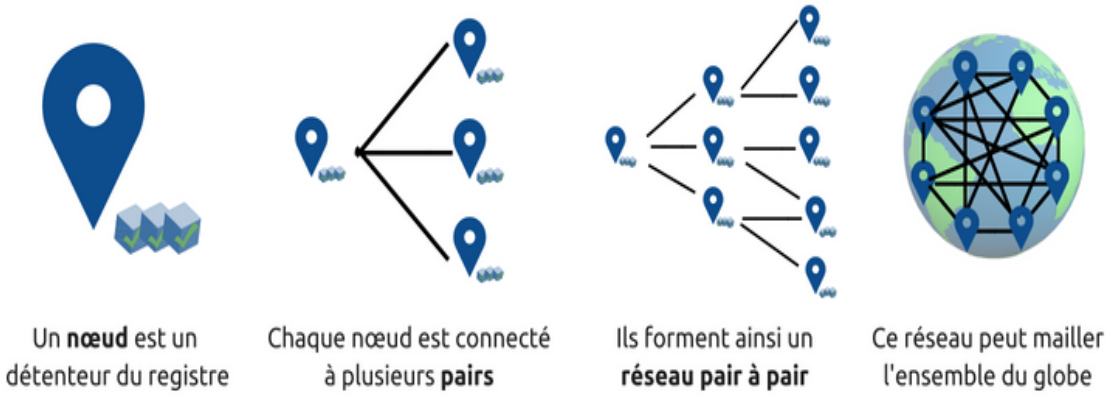


Figure 17: Le réseau des nœuds [18]

3.5. Les types de réseaux de blockchain

Il existe plusieurs types de réseaux de blockchain. Un réseau peut être public, privé, à autorisation ou construit par un consortium.

- Réseaux publics de blockchain : les blockchains publiques sont ouvertes, consultables et utilisables par tout individu depuis leurs interfaces internet, sans barrière à l'entrée. Pour effectuer une transaction ou partager des données sur une blockchain, il suffit à l'utilisateur de choisir, parmi les solutions existantes, un « portefeuille » (appelé aussi parfois porte-clés, ou wallet en anglais) qui lui permettra à la fois de conserver ses clés privées de façon sécurisée et de générer une adresse unique pour envoyer et recevoir des données. L'historique des transactions est accessible à tous, non seulement aux utilisateurs, mais également à tout visiteur de la plate-forme. De même, chacun peut se constituer en nœud et ainsi participer à la validation des transactions, à leur regroupement dans un bloc et au chaînage des blocs. En d'autres termes, une blockchain publique n'est soumise à aucune autorisation de lecture ou d'écriture. Ces blockchains sont principalement destinées à des échanges entre individus, constituant actuellement le plus souvent des transactions monétaires, mais pouvant être d'autre nature. De fait, la blockchain publique la plus connue et la plus mature à ce jour est celle du Bitcoin, qui permet d'effectuer des transactions monétaires :
- Réseaux de blockchain privés : tout comme le réseau de blockchain public, le réseau de blockchain privé est un réseau décentralisé de pair à pair, mais gouverné par une organisation. Celle-ci contrôle qui est autorisé à participer, exécute le protocole de consensus et assure la maintenance du grand livre partagé. Selon le cas d'utilisation, cela peut renforcer considérablement la confiance entre les participants. Une blockchain

privée peut être exécutée derrière un pare-feu d'entreprise et même être hébergée sur site.

- Blockchains hybrides : les blockchains hybrides combinent des éléments des réseaux de blockchain privés et publics. Les entreprises peuvent mettre en place des systèmes privés à base d'autorisations, parallèlement à un système public. Elles peuvent contrôler l'accès à des données spécifiques stockées dans la blockchain tout en maintenant le reste des données publiques. Les blockchains hybrides permettent également aux membres publics de vérifier si des transactions privées ont été effectuées.
- Blockchains de consortiums : plusieurs organisations peuvent se partager la responsabilité de la maintenance d'une blockchain. Ces organisations présélectionnées déterminent qui peut envoyer des transactions ou accéder aux données. Une blockchain de consortium est idéale pour les entreprises dès lors que tous les participants doivent disposer d'une autorisation et qu'ils ont une responsabilité partagée dans la blockchain.

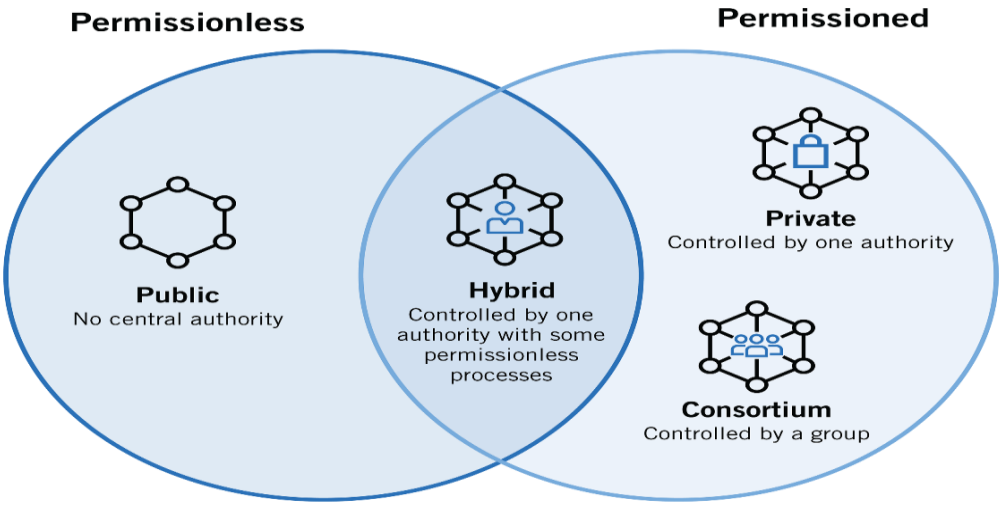


Figure 18: Schéma des différents types de blockchain

3.6. Les composants d'une blockchain

- Les nœuds sont les entités participantes à la création et à la validation de nouveaux blocs dans une blockchain. Chaque nœud détient une copie de cette dernière, ce qui fait qu'il doit nécessairement disposer d'une capacité de stockage mémoire suffisante et d'une puissance de calcul élevée.[24]
- Le contrat intelligent est un programme auto-exécutable ayant pour devoir de vérifier et d'imposer le respect des négociations établies entre les entités du réseau, tout en décentralisant et en sécurisant les transactions.
- Portefeuille de cryptomonnaie : c'est un dispositif virtuel ou physique spécifique à chaque nœud et il est stocké dans la blockchain, permettant ainsi le stockage de la cryptomonnaie. Il contient une clé privée et une clé publique. La clé privée permet au nœud de déclencher des transactions et de dépenser de la cryptomonnaie. La clé

publique lui permet de recevoir des récompenses (des cryptomonnaies) à la suite d'une validation d'un nouveau bloc ou de recevoir des paiements. [24,25]

- Algorithme (protocole) de consensus : c'est un accord permettant une gestion décentralisée, la validation et l'ajout de nouveaux blocs dans la blockchain, assurant ainsi la sécurité de cette dernière. Le consensus d'une blockchain est défini à sa création par les fondateurs de celle-ci. Plusieurs algorithmes de consensus existent tels que la preuve de travail et la preuve d'enjeu.[26]

3.7. Fonctionnement de la blockchain

Le processus de blockchain commence par une transaction en ligne entre deux parties ou plus. Cette transaction est ensuite envoyée sous la forme d'une requête à toutes les machines (des ordinateurs, généralement) du réseau de pairs de cette blockchain, chacune d'elle contenant une copie complète du registre numérique (autrement dit, l'historique de transactions de l'intégralité de la blockchain). Chaque ordinateur compare ensuite la requête à des critères et des règles techniques et métier préétablis qui encadrent l'ajout de nouvelles données. Chaque ordinateur valide la transaction et l'indique aux autres machines de la chaîne.

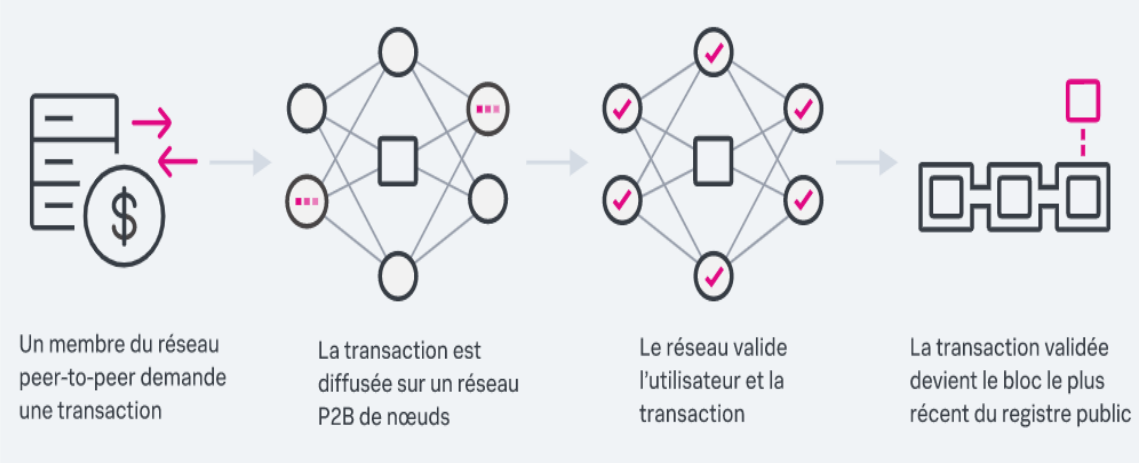


Figure 19: Fonctionnement de la blockchain

Dans une blockchain, l'ensemble des transactions est enregistré sous forme de blocs. Chacun des blocs doit ensuite être validé par les nœuds du réseau (ordinateurs) qui utilisent une méthode de cryptographie algorithmique. Dès que le bloc est validé, il est ajouté à la chaîne de blocs et devient visible de tous les utilisateurs. Voir le schéma ci-dessous qui illustre ce principe de fonctionnement.

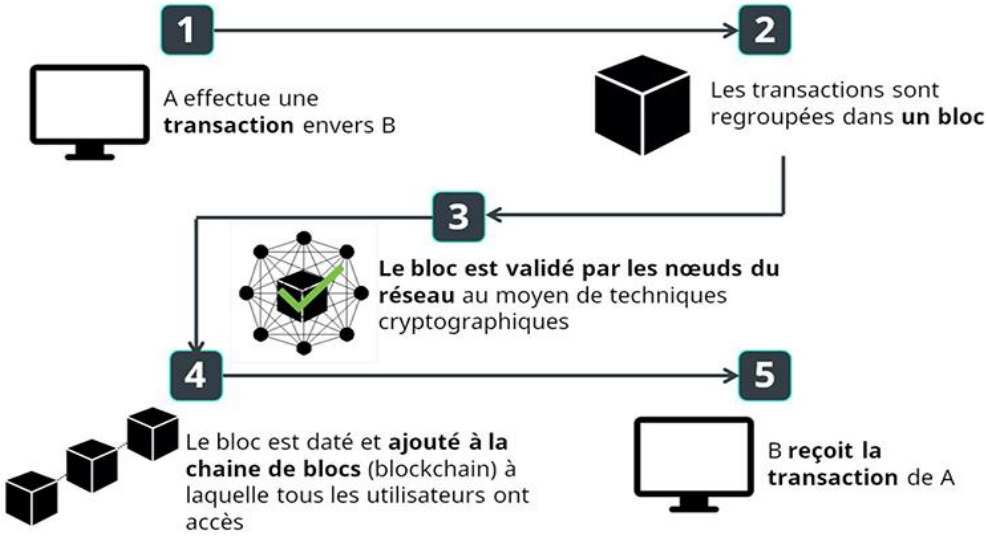


Figure 20: schéma récapitulatif expliquant le fonctionnement d'une blockchain publique lors d'une transaction

Pour expliquer son fonctionnement, prenons en exemple deux personnes qui souhaitent s'échanger une valeur pour le règlement d'un service ou d'un produit. A va transmettre une somme à B.

La première étape de la constitution de la chaine de bloc est l'inscription dans le registre de la transaction entre A et B. Ce registre se compose d'un bloc regroupant plusieurs transactions, il n'affiche pas seulement les transactions de A ou de B, mais toutes celles que la blockchain reçoit aléatoirement.

Traditionnellement, un organisme certificateur comme une banque commencerait par vérifier que A dispose bien des fonds pour que B soit réglé. Comme l'organisme certificateur, un acteur de la blockchain appelé le mineur, va vérifier premièrement à l'intérieur des registres antérieurs que A dispose bien de la somme nécessaire pour régler B et deuxièmement qu'il n'a pas par la même occasion tentée d'utiliser ces mêmes fonds pour payer une autre personne.

Dès lors que la transaction est valide et que l'ensemble des transactions du bloc le sont, le mineur va réaliser ce qu'on appelle la preuve de travail. Il va cryptographier et dater le bloc afin de le sécuriser. Le bloc validé va alors s'ajouter à la chaine de blocs.

La transaction est validée et devient visible pour l'ensemble du réseau. Un ensemble de blocs représente une chaîne et chaque chaîne est hébergée par un mineur. Dans la suite, nous allons présenter la structure d'une chaine de blocs.

3.8. Structure d'une chaine de blocs

La chaîne de blocs est une technologie de registres (ledgers) partagés décentralisée. Le registre est une liste de transactions qui sont dupliquées sur un certain nombre d'ordinateurs, plutôt que d'être stockées sur un seul serveur central. Chaque transaction (ou souvent une suite de

transactions sur une période donnée) est appelée un bloc ; chaque bloc possède un horodatage qui est lié au précédent bloc.

La fiabilité et l'intégrité de la blockchain reposent sur le fait qu'il n'y a aucune chance que des données ou des transactions frauduleuses, telles qu'une double dépense, soient acceptées ou enregistrées.

- **Le hachage** : est la pierre angulaire de la technologie dans son ensemble et les éléments clés du maintien de cette fiabilité. Le hachage est le processus qui consiste à prendre une entrée de n'importe quelle longueur et à la transformer en une sortie fixe cryptographique par un algorithme mathématique (Bitcoin utilise SHA-256, par exemple).

Il peut s'agir, par exemple, d'un court élément d'information tel qu'un message ou d'un énorme cache contenant divers éléments d'information tels qu'un bloc de transactions ou même l'ensemble des informations contenues sur l'Internet.

La décentralisation est l'un des aspects fondamentaux de la blockchain technologique. Et bien sûr, cela implique que n'importe qui, de n'importe quelle partie du monde, peut être ajouté au réseau et y opérer. Cela provoque à son tour qu'il n'y a pas de code de temps universel. C'est parce que nous pouvons nous connecter depuis n'importe quel fuseau horaire. L'horodatage est un horodatage qui est calculé en fonction de différents paramètres**.**

- **L'horodatage** : l'une des principales utilisations de l'horodatage est d'établir les paramètres du processus d'extraction **.** En effet, ces horodatages permettent aux nœuds d'ajuster correctement la difficulté de minage à utiliser pour chaque période de génération de bloc. Les horodatages aident le réseau à déterminer combien de temps il faut pour extraire des blocs pendant une certaine période, et à partir de là, à ajuster le paramètre de difficulté de minage.
- **Data** : les données à stocker (exemple : liste de transactions)
- **Other** information : ces informations définies par l'utilisateur peuvent être la version, la date, la difficulté, le nonce du bloc, etc. Les utilisateurs dans ces réseaux signent leurs transactions grâce à des clés cryptographiques publiques et privées lors de la phase de signature et de la vérification. La clé privée est gardée confidentielle et est utilisée pour signer une transaction et crypter les données. La clé publique est connue de tous et est utilisée pour valider et décrypter les données dans la phase de vérification de la transaction, confirmant ainsi l'authenticité des données. Une valeur de nonce est essentiellement une valeur de quatre octets commençant par zéro et s'incrémente chaque fois qu'un calcul de hachage est effectué. La valeur n bits détermine la valeur seuil cible d'un hachage de bloc valide.

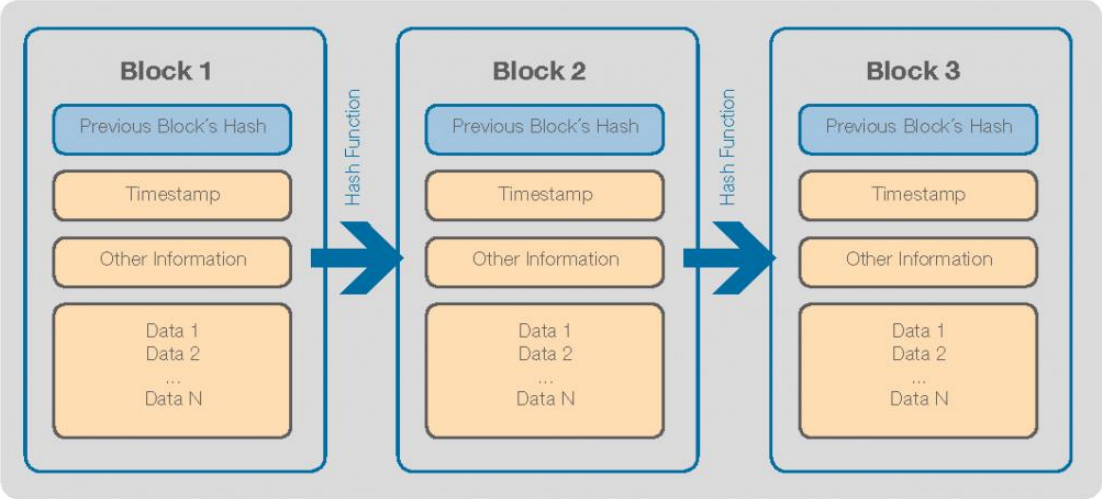


Figure 21: Structure de base de la chaine de blocs

3.9. Écosystème blockchain

L'écosystème de blockchain (figure 22) comporte plusieurs participants :

- **Dirigeants**

Le leader dans un écosystème blockchain fait référence à l'organisation qui visualise l'écosystème et sa valeur commerciale. Les leaders des écosystèmes blockchain sont généralement les créateurs du projet et les principaux bénéficiaires du travail dans les écosystèmes.

- **Groupe de base**

Le groupe central est également l'un des ajouts notables parmi les composants des écosystèmes blockchain. Il représente un groupe d'organisations actives ou de premier plan chargées de contrôler, de rationaliser et d'optimiser les activités opérationnelles. Le groupe central peut pareillement faire référence aux organisations activement impliquées dans la gestion de l'écosystème.

- **Participants actifs**

Les participants actifs de l'écosystème blockchain font référence à l'ensemble des principaux participants du réseau qui sont responsables de la contribution et de la gouvernance du flux de travail et des données.

- **Utilisateurs**

Les utilisateurs des écosystèmes blockchain sont les participants qui bénéficient des avantages du réseau et ont la possibilité d'accéder à leurs propres données. Cependant, les utilisateurs n'ont aucune responsabilité dans la gestion active du réseau.

- **Fournisseurs de services tiers**

Le dernier élément à ajouter aux composants de l'écosystème blockchain serait les fournisseurs de services tiers. Il s'agit en fait des tiers qui proposent des services au réseau. Ces services

peuvent inclure des services d'assistance informatique, d'infrastructure ou d'assistance aux applications, ainsi que de nombreux autres services, notamment payants.

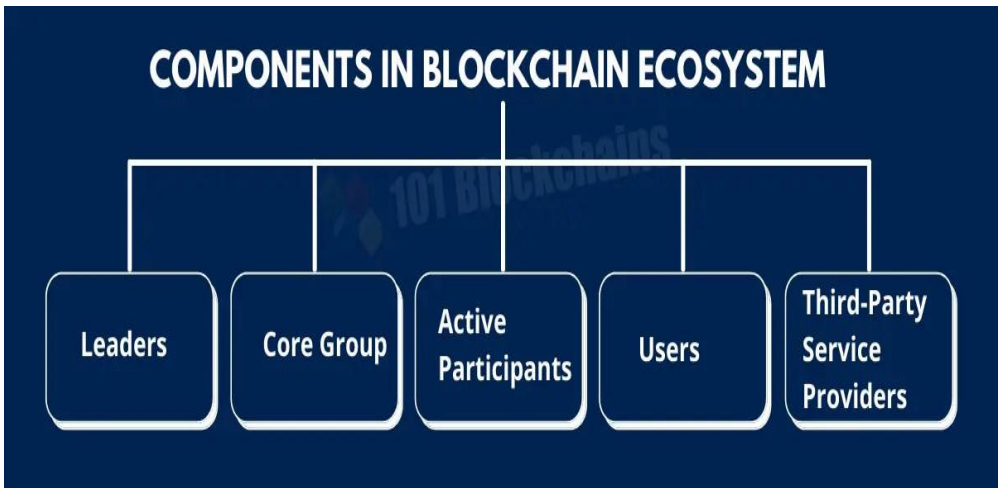


Figure 22: Ecosystème de blockchain

3.10. Les caractéristiques essentielles d'une blockchain

Blockchain a un certain nombre de caractéristiques uniques qui attirent l'attention des gens, telles que :

- **Immuabilité** : la formation d'un grand livre immuable est l'un des principaux concepts de la blockchain. Toute base de données centralisée est susceptible d'être piratée et nécessite la confiance du tiers pour la rendre plus sécurisée. Un bloc qui est une fois écrit dans la blockchain ne peut pas changer. Être immuable signifie que quelque chose reste immuable dans le temps. Il offre un grand avantage à des fins d'audit. En tant que fournisseur de données et destinataire de données, il est possible de prouver que les données n'ont pas été modifiées ou altérées.
- **Décentralisé** : traditionnellement, les transactions nécessitent l'approbation d'autorités de régulation telles qu'un gouvernement ou une banque.
  Cependant, avec une blockchain, les transactions sont effectuées avec le consensus mutuel des utilisateurs et les intermédiaires sont supprimés, ce qui permet des transactions par conséquent moins coûteuses. Les transactions par blockchain ne comportent, par ailleurs, aucun coût de transaction.
- **Fiabilité** : les mécanismes de validation derrière les blockchains permettent de réduire de manière considérable les erreurs et les fraudes. Pour effectuer de fausses transactions dans une blockchain, il faudrait ainsi pirater chaque nœud et modifier les bases de données de chacun des acteurs. Une opération, en pratique, irréalisable.
- **Transparence** : blockchain offre un haut niveau de confidentialité en s'assurant que les détails des transactions sont partagés entre les parties impliquées dans ces transactions. Chaque participant qui a accès au réseau blockchain peut voir de manière transparente les détails qui y sont stockés.

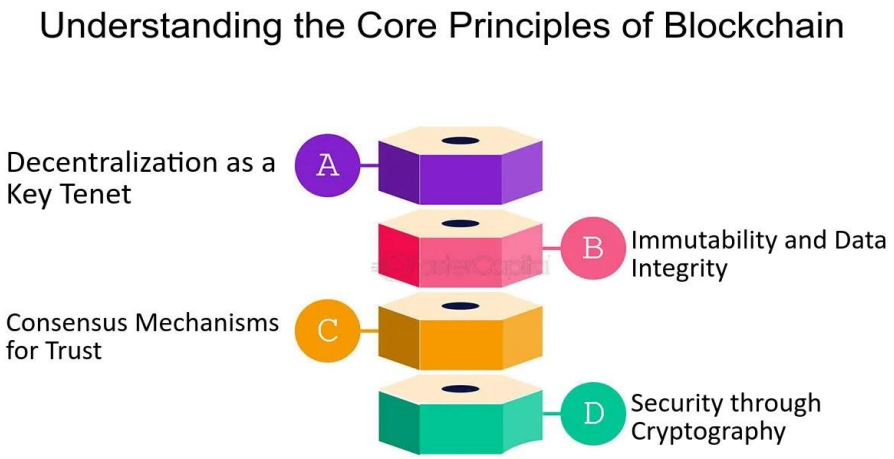


Figure 23: Architecture des caractéristiques d'une blockchain

3.11. Les mécanismes de validation des blocs

Lorsqu'on parle de blockchain, on parle souvent d'une suite de blocs composant un réseau et d'un processus décentralisé, sécurisé et fiable. Il existe différents processus de consensus possédant chacun leurs avantages et leurs inconvénients.

Une blockchain est généralement indépendante d'une seule société ou d'une personne, car elle fonctionne par l'alliance de multiples acteurs. Chaque acteur participe à la sécurisation du réseau en vérifiant que chaque transaction et interaction soit possible et qu'aucun autre acteur ou participant n'essaye de tricher au détriment des autres.

Ce fastidieux processus de vérification permet de s'assurer que l'historique de transaction de la blockchain est correct et infalsifiable. Tous les acteurs doivent se mettre d'accord pour valider une entrée dans le registre de la blockchain, c'est ce qu'on appelle un algorithme de consensus.

Ce consensus, obtenu sur l'état du registre, est régi par des règles et des procédures communes partagées entre les nœuds du réseau pair-à-pair, selon une périodicité déterminée, y compris en présence de nœuds défaillants. Il existe plusieurs types de mécanismes de consensus selon le protocole utilisé :

a) Preuve de travail ou Proof of work (pow)

La preuve de travail est l'algorithme de consensus le plus populaire. Bitcoin, Litecoin et Ethereum l'utilisent [15]. Il a été conçu par Satoshi Nakamoto lorsqu'il l'a utilisé dans son implémentation du Bitcoin. Cependant, c'est aussi le moyen le plus inefficace de parvenir à un consensus dans une blockchain, car il nécessite une puissance de calcul considérable. Il fonctionne en demandant aux mineurs de résoudre des problèmes mathématiques complexes. Une fois le hachage résolu, le bloc est miné et la transaction est validée en même temps.

En résolvant ces problèmes, ils créent des blocs qui sont ensuite ajoutés à la blockchain. Pour que cela fonctionne, 50% du travail doit toujours être honnête.

Parmi les avantages de la POW

- La preuve de travail aide à protéger le réseau contre de nombreuses attaques différentes. Une attaque réussie nécessiterait beaucoup de puissance de calcul et beaucoup de temps pour faire les calculs, et donc elle serait inefficace, car le coût encouru serait supérieur aux récompenses potentielles pour attaquer le réseau [15].
- La preuve de travail est sécuritaire, l'historique de la chaine de blocs est impossible à falsifier [15].
- Il est nécessaire de posséder au moins 51 pour 100 de la puissance de calcul du réseau pour le saturer de fausses transactions [15].

Comme inconvénients, on peut signaler les points suivants :

- L'exploitation minière nécessite un matériel informatique coûteux qui consomme une grande quantité d'énergie. Même si c'est ce qui garantit la sécurité du réseau, ces calculs d'exploration de données ne peuvent pas être utilisés au-delà. [17]
- Quantité massive de puissance de traitement et d'énergie sous forme d'électricité. [17]
- Couts élevés associés aux ressources matérielles. [17]
- Temps de latence nécessaire pour valider une transaction. [17]
- Le gain décroissant des mineurs augmenterait le risque de corruption du réseau, puisque la fiabilité de la chaine de blocs nécessite qu'aucun opérateur hostile ne détienne plus de la moitié de la puissance de calcul de la chaine (attaque de type 51 pour 100) [15].

b) Preuve d'enjeu ou Proof of stake(pos)

Un algorithme de consensus proof-of-stake (PoS) est un ensemble de règles régissant un réseau blockchain et la création de sa cryptomonnaie native, c'est-à-dire qu'il a le même objectif qu'un algorithme proof-of-work (PoW) dans le sens où il est un instrument pour parvenir à un consensus. Contrairement au PoW, aucun mineur n'est impliqué dans le processus.

En revanche, avant de pouvoir se lancer dans la validation des transactions et la création de nouveaux blocs dans un réseau proof-of-stake, les participants au réseau doivent posséder une certaine quantité de cryptos de ce réseau, lesquelles sont également stockées dans des wallets reliés à cette blockchain. C'est ce qu'on appelle une « mise en jeu » ou un « enjeu ». Un créateur de blocs dans un système PoS se limite à créer des blocs proportionnels à sa participation dans le réseau.

Ainsi, les réseaux PoS sont basés sur des algorithmes déterministes, ce qui signifie que les validateurs de blocs sont élus en fonction de la nature de l'enjeu. Par exemple, la sélection du solde du compte comme seul critère pour définir la validité du prochain bloc dans une blockchain risquerait d'entraîner une centralisation non souhaitée. Par conséquent, les membres riches d'un réseau bénéficieraient de grands avantages.

- D'une part, la PoS comble certaines des lacunes d'un système PoW sur lequel fonctionnent les cryptomonnaies comme le bitcoin. La PoS élimine essentiellement les obstacles à l'entrée du processus de validation. Les utilisateurs n'ont plus besoin

d'investir dans des ordinateurs spécialisés dans le seul but d'avoir une chance de gagner cette récompense de bloc si difficile à obtenir. C'est pour cette raison que la PoS nécessite moins de puissance informatique et a donc également moins d'impact sur l'environnement que la PoW.

- D'autre part, certains réseaux PoS présentent des défauts majeurs, selon les variantes utilisées pour définir l'enjeu d'un réseau. Les créateurs de blocs de certaines cryptomonnaies peuvent exercer une puissance incroyable s'ils sont peu nombreux dans le réseau et qu'ils valident toutes les transactions. Cependant, le pouvoir d'un créateur peut être automatiquement révoqué à tout moment s'il fait agir à l'encontre de l'intérêt du réseau. Par exemple, si un créateur de cryptomonnaies EOS ne parvient pas à travailler sur des blocs pendant 24 heures, une sauvegarde prend rapidement sa place.

c) Preuve d'enjeu Délégué (Delegated Proof of stake)

La preuve de participation déléguée est une variante de la preuve de participation qui a été développée pour relever certains des défis associés à l'algorithme standard de preuve de participation. Dans DPoS, les nœuds sont sélectionnés pour valider les transactions et les ajouter à la blockchain en fonction du nombre de votes qu'ils reçoivent des autres nœuds du réseau. L'idée derrière DPoS est que les nœuds avec le plus de votes sont les plus fiables et les plus fiables, et devraient donc être ceux responsables de la validation des transactions.

DPoS est un algorithme de consensus rapide et efficace, car il ne nécessite qu'un petit nombre de nœuds pour valider les transactions. Cependant, il est également considéré comme moins sécurisé que la preuve de travail ou la preuve de participation, car la sélection des nœuds de validation est basée sur le nombre de votes qu'ils reçoivent plutôt que sur la quantité de puissance de calcul ou de jetons qu'ils prennent. Certains cryptos DPoS sont Tron (TRX), EOS (EOS) et Stemm (STEEM).

- L'avantage de ce type de construction, c'est qu'elle réduit les interactions entre les nœuds et permet un plus grand nombre de transactions et une validation plus rapide.
- Le principal inconvénient, c'est une plus grande centralisation, avec des risques de vulnérabilité, de censure et de cartellisation.

d) La preuve d'autorité (PoA)

Comme le PoW et bien d'autres, le Proof of Authority (PoA) est un algorithme de consensus ayant pour but la mise en application du protocole de la blockchain. Il permet dès lors de valider les transactions et autres interactions avec le réseau, mais aussi de mettre à jour son registre plus ou moins distribué. Ce droit est donné à un nombre restreint et désigné d'acteurs.

En effet, ce sont une ou plusieurs machines qui vont avoir pour rôle de générer chaque bloc de transactions qui sera inclus dans la blockchain. Chaque bloc peut alors être accepté sans vérification, à l'unanimité ou à la majorité en fonction de la configuration choisie. Cela explique qu'un nombre de validateurs soit défini et désigné dès le départ en ce sens.

Le Proof of Authority (PoA) a plusieurs avantages et inconvénients.

- Tout d'abord, il permet de s'affranchir de la concurrence technique liée au système de minage puisque le mécanisme ne nécessite pratiquement aucune puissance de calcul. Un avantage certain en matière d'économie d'énergie.
- Grâce au nombre restreint d'acteurs, la mise à jour se fait plus fréquemment, ce qui permet la réduction du blocktime et l'augmentation de la block size avec des frais proches de zéro. Le Proof of Authority (PoA) permet aussi de se passer d'actifs natifs et n'immobilise pas non plus de capital particulier.

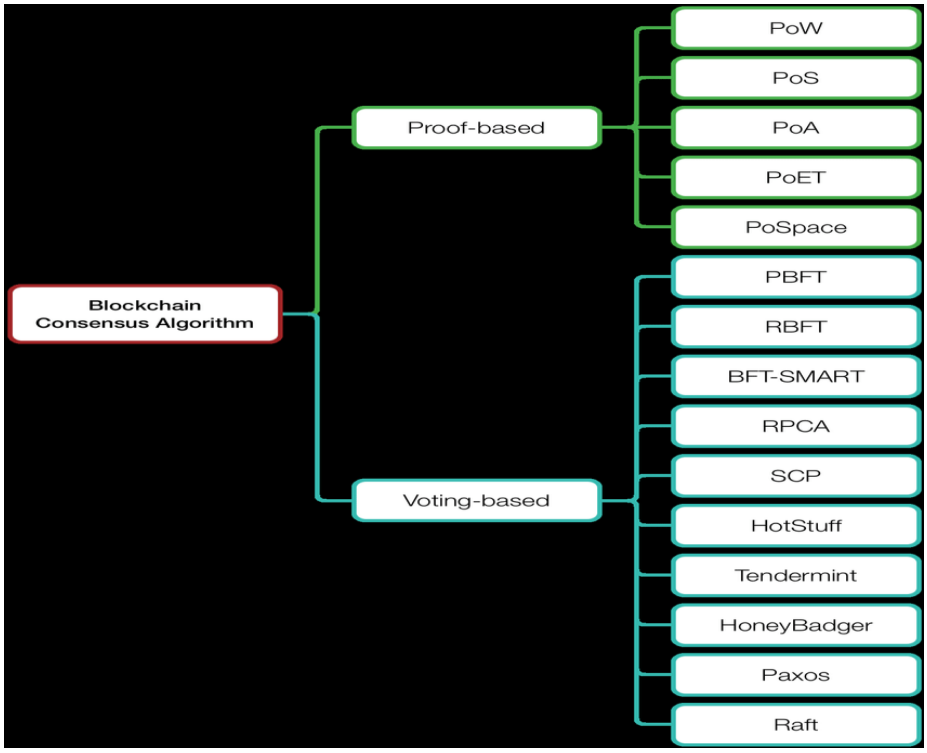


Figure 24 : Classification des algorithmes de consensus Blockchain par mécanisme

Tableau 5: Avantages et inconvénients de la preuve de travail (POW), de la preuve d'enjeu (POS) et d'une forme hybride des deux modes de preuve (OPECST, d'après Giang-Truong Nguyen and Kyungbaek Kim23(*))

Critères	Preuve de travail	Preuve d'enjeu	Forme hybride entre preuve de travail et preuve d'enjeu
Consommation énergétique	Très importante	Faible	Très importante
Besoin de matériel informatique spécialisé spécialisé	Très important	Pas nécessaire	Important

Risque de séparation du réseau (forking)	Possible, lorsque deux nœuds trouvent le bon hash au même moment	Très improbable	Probable
Vulnérabilités aux attaques des 51 %	Existante	Faible	Existante, mais moins que pour la preuve de travail simple
Vitesse de création des blocs	Lente, dépend de plusieurs variables	Rapide	Lente, dépend de plusieurs variables
Risque de regroupement en pools	Oui, mais peut être prévenu	Oui mais difficile à prévenir	Oui
Exemples	Bitcoin	Nextcoin	PPcoin, Blackcoin

3.12. Plateformes de la blockchain

Nous présentons ci-dessous une liste des plateformes de la technologie blockchain [27] :

1) Bitcoin

Fondée en 2009, Bitcoin a été la première cryptomonnaie et reste la plus échangée. La monnaie a été mise au point par Satoshi Nakamoto, qui serait le pseudonyme d'une personne ou d'un groupe de personnes dont l'identité précise reste inconnue.

Tout le principe du Bitcoin est de créer un système de monnaie décentralisé. Il ne doit pas y avoir de serveur central. Il utilise donc la blockchain (et son principe du peer to peer) pour échanger des fichiers entre ordinateurs sans autorité centrale (ici les banques) : les ordinateurs s'accordent entre eux grâce à l'algorithme du Bitcoin. Chaque ordinateur qui possède une copie de la blockchain est appelé un « nœud » du réseau.

2) Ethereum

Créé par Vitalik Buterin en 2014, 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. Il s'agit de la cryptomonnaie la plus populaire après Bitcoin. 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.

3) Hyperledger Fabric

Hyperledger Fabric est une blockchain open-source privée, créée par la Linux Foundation, plus précisément par IBM. Utilisé dans des centaines de projets, Fabric, le framework phare d'Hyperledger, domine les applications de la blockchain pour l'industrie. Contrairement aux blockchains publiques comme Bitcoin ou Ethereum, Hyperledger, créé en décembre 2015 par un large consortium d'éditeurs, ne propose pas un seul réseau blockchain, mais des structures logicielles open source, des Frameworks, facilitant l'utilisation des outils développés dans l'univers de la blockchain pour créer son propre réseau.

4) Litecoin

Cette monnaie ressemble le plus à Bitcoin, mais a évolué plus rapidement pour développer des innovations, notamment des paiements plus rapides ainsi que des processus permettant un plus grand nombre de transactions.

5) Binance Coin

Le Binance Coin est natif de Binance, la plus grande plateforme d'échange de cryptomonnaies au monde en 2022. Les frais de transaction pour cet échange sont réduits pour les utilisateurs qui paient en BNB. Ce qui a encouragé l'adoption du Binance Coin, qui est devenu l'une des plus grandes cryptomonnaies du marché. Pour assurer la stabilité de sa valeur, Binance détruit ou « brûle » un pourcentage fixe des coins en circulation.

6) IOTA

IOTA est une crypto-monnaie dont l'architecture repose sur le concept du graphe orienté acyclique. Le « Tangle » matérialise cette chaîne de blocs non-linéaires. Avec ce système, IOTA espère bénéficier d'une scalabilité qui ne fera que croître avec le nombre grandissant de transactions. IOTA a pour objectif premier de devenir la cryptomonnaie de l'Internet des choses (IoT). Afin de faciliter les microtransactions inhérentes à cet écosystème, il n'y a pas de frais de transaction.

7) Tendermint

Tendermint est une plateforme open source de Blockchain permettant l'exécution de smart-contract multi-langages dont l'algorithme de consensus PBFT résiste à la panne, même si 1/3 des acteurs sont malveillants ou déconnectés.

3.13. Domaines d'applications de la blockchain

Dans cette section, nous allons présenter certaines des applications potentielles de la technologie Blockchain [65] - [68], Ces applications sont : Chaîne d'approvisionnement, Banque et finance, gouvernement et santé.

- **Chaîne d'approvisionnement** : la chaîne d'approvisionnement est un segment très complexe et il est devenu plus difficile d'avoir une visibilité transparente sur l'ensemble de la chaîne d'approvisionnement. Il est devenu plus difficile de suivre le flux de matériel et les canaux de distribution, ce qui a entraîné divers comportements contraires à l'éthique dans les entreprises, allant du commerce illégal aux produits de contrefaçon et aux dommages environnementaux. Tout au bout de la chaîne d'approvisionnement,

les consommateurs ne disposent pas des informations selon lesquelles un produit final a été importé tout au long de la chaîne d'approvisionnement. De nos jours, vous pouvez perdre vos colis par la poste. En tirant parti de la convergence du paradigme IoT et des contrats intelligents, vous pourrez enregistrer la position à tout moment de vos colis grâce à la connexion de capteurs à chaque étape.

- **Banque et finance** : les banques et autres institutions financières comptent parmi les premiers à adopter la technologie blockchain. Ils l'utilisent pour rationaliser les processus, réduire les coûts et réduire le risque de fraude. Par exemple, les banques utilisent la blockchain pour régler les paiements transfrontaliers plus rapidement et plus efficacement.
- **Gouvernement** :la blockchain pourrait être utilisée pour assurer au public que les politiciens agissent correctement avec l'argent, et peut également lutter contre le crime financier. Grâce à la technologie, chaque transaction peut être enregistrée sans manipulation, ce qui rend la destination ultime transparente pour le public.
- **Soins de santé** : les établissements de santé doivent faire face à des problèmes de sécurité et de confidentialité lorsqu'ils partagent des données sur plusieurs plates-formes. L'amélioration de la collaboration de données entre fournisseurs signifie l'amélioration de nombreux aspects du domaine de la santé, tels que la précision des diagnostics et l'efficacité des traitements. Blockchain peut créer cet environnement sécurisé pour permettre aux établissements de santé, aux payeurs et aux autres acteurs de ce domaine de partager l'accès à leur réseau avec des garanties d'intégrité des données.

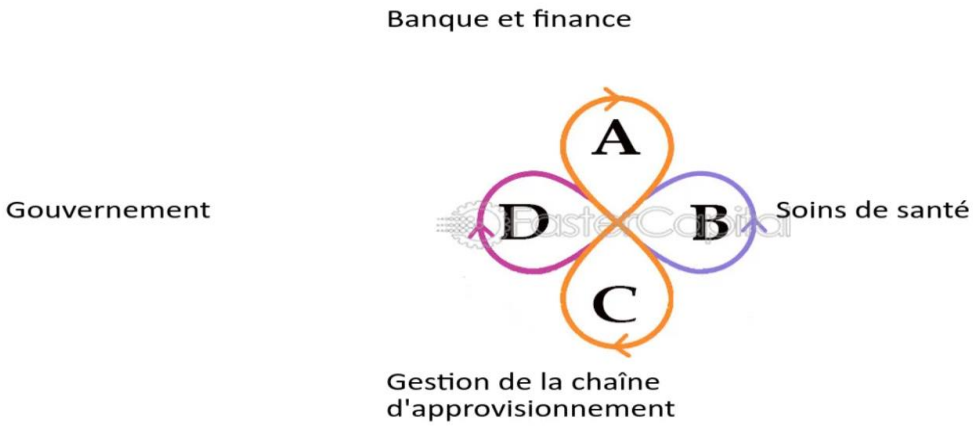


Figure 25: domaines d'application de la blockchain

3.14. Avantages, inconvénients et défis de la blockchain

Les blockchains sont suffisamment souples et puissante pour rendre en charge de nombreuses applications et services nouveaux et passionnants. Mais dans sa forme actuelle, la technologie

blockchain présente également un certain nombre d'inconvénients. Nous allons citer quelques avantages et inconvénients de la blockchain.

3.14.1. Avantages

- Une meilleure transparence

La technologie blockchain se veut être un système transparent. Le contrôle des informations repose sur les utilisateurs. Tous ont donc accès à un contrôle complet de leurs transactions.

- Une sécurité renforcée

Grâce à la cryptographie, l'authenticité des informations est assurée. Rappelons-nous aussi qu'une fois le bloc validé, celui-ci n'est plus modifiable. Pour qu'un éventuel changement ait lieu, la majorité des membres du réseau doivent être d'accord. Enfin, les informations étant distribuées sur plusieurs ordinateurs, les données sont bien plus sécurisées en cas de défaillance sur un réseau.

- Des transactions plus rapides

Généralement, il est nécessaire d'attendre plusieurs jours pour qu'un virement soit réellement effectué. Avec la technologie blockchain, cela ne prend que quelques minutes.

- Des coûts de transactions plus faibles

Cette technologie est aussi bénéfique pour les utilisateurs en termes de coûts. Ceux-ci sont largement réduits sans l'intervention d'un organisme tierce. La technologie blockchain est aujourd'hui de plus en plus utilisée grâce à un mécanisme sécurisé et à la facilité des transactions. Pour fournir un service plus rapide, de meilleure qualité et plus fiable aux utilisateurs, la blockchain fait donc son apparition dans les cryptomonnaies, les domaines de la santé, juridique, gouvernemental, dans l'industrie automobile ou encore dans les banques et les marchés d'actions.

- La décentralisation

Les données blockchain étant souvent stockées dans des milliers de dispositifs sur un réseau distribué de nœud, le système et les données sont très fortement résistants aux défaillances techniques et aux attaques malveillantes. Chaque nœud du réseau peut créer une copie de la base de données. C'est pour cette raison qu'il n'existe pas de point de défaillance unique : si un nœud se déconnecte, cela n'affecte pas la disponibilité ou la sécurité du réseau.

À l'inverse, les bases de données traditionnelles reposent sur un ou plusieurs serveurs et sont vulnérables aux pannes et aux cyberattaques.

- La traçabilité :

Il est possible de tracer chaque échange de valeur physique ou immatérielle en toute transparence en scrutant le registre. Cela constitue alors un historique inviolable de chaque action réalisée. Ainsi, la blockchain peut consigner tout type d'engagement et prouver la détention ou la validité historique de données.

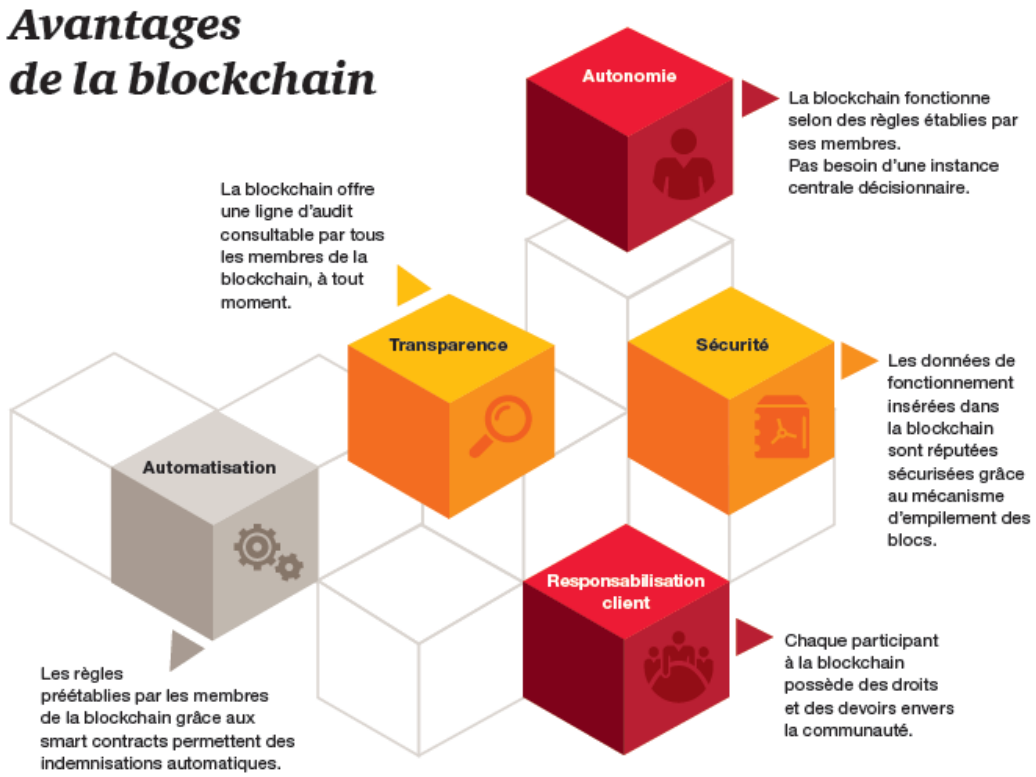


Figure 26: Avantages de la blockchain, Source : « Blockchain, catalyseur de nouvelles approches en assurance », PwC, mars 2017

3.14.2. Les inconvénients

- La forte consommation d'énergie

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

- Immutabilité des données :

L'immutabilité des données a toujours été l'un des plus gros inconvénients de la blockchain. Il est clair que plusieurs systèmes en bénéficient, notamment la chaîne d'approvisionnement, les systèmes financiers, etc. Cependant, il souffre du fait qu'une fois les données écrites, elles ne peuvent pas être supprimées. Chaque personne sur terre a droit à la vie privée. Cependant, si la même personne utilise une plate-forme numérique qui fonctionne sur la technologie blockchain, alors elle ne pourra pas supprimer sa trace du système lorsqu'elle ne le souhaite pas. En termes simples, il n'y a aucun moyen de supprimer sa trace laissant les droits à la vie privée en morceaux. [39]

- Interopérabilité :

Plusieurs réseaux de chaînes de blocs travaillant dur pour résoudre le problème du grand livre distribué rendent difficile de les relier ou de les intégrer les uns aux autres. Cela rend la communication entre les différentes chaînes qui sont difficiles. [39]

❖ La cryptographie à clé publique :

C’est une bénédiction mitigée qui fait partie intégrante de la technologie blockchain. Le cryptage sécurise le réseau, mais les utilisateurs qui perdent leurs clés privées peuvent perdre l’accès à tous leurs fonds. Des utilisateurs ont perdu des millions d’euros simplement en perdant les clés privées de leurs comptes blockchain.

3.14.3. Les défis

❖ **Sécurité et confidentialité des données** :

Le premier et le plus important défi concernent la sécurité est la confidentialité des données. Avec la mise en œuvre d'applications basées sur la technologie de la blockchain, la nécessité pour un tiers d'effectuer une transaction est éliminée. Étant donné que le mécanisme de blockchain permet à l'ensemble de la communauté, plutôt qu'à un seul tiers de confiance, de vérifier les enregistrements dans une architecture de blockchain, les données sont exposées à des risques en matière de sécurité et de confidentialité. Étant donné que tous les nœuds peuvent accéder aux données transmises par un nœud, la confidentialité des données ne sera pas active. En cas d'absence d'une tierce partie pour l’autorisation, le patient doit sélectionner un ou plusieurs représentants qui peuvent accéder à ses informations et / ou à ses antécédents médicaux en son nom, en cas d'urgence. Désormais, ce représentant peut également autoriser un ensemble de personnes à accéder aux enregistrements du même patient, ce qui peut créer une menace énorme pour la sécurité et la confidentialité des données. L'implication de mécanismes de haute sécurité dans les données entraînera à son tour des obstacles pour le transfert des données d'un bloc à un autre et, par conséquent, les destinataires auront accès à des données limitées ou incomplètes. En outre, les réseaux blockchain sont sujets à une sorte de violation de la sécurité connue sous le nom d'attaque 51%. Cette attaque implique une équipe de mineurs qui possèdent plus de 50% des blocs d'un réseau blockchain. Les mineurs obtiennent une autorité du réseau et pourraient empêcher toute nouvelle transaction en ne leur donnant pas leur consentement. Cinq cryptomonnaies ont récemment été victimes de cette attaque. En outre, un dossier patient peut contenir des données sensibles qui ne conviennent pas pour figurer dans la chaîne de blocs.

❖ **La mise à jour des blockchains** :

Le défi technologique majeur des blockchains réside dans la distribution d’un tel registre. Il faut s’assurer que l’ensemble des acteurs s’accordent sur une version commune de la blockchain, mais aussi empêcher des entités malicieuses de prendre le contrôle de l’ajout de blocs à la blockchain. Ce problème, qui a déjà été beaucoup étudié par les informaticiens dans le cadre des modèles dits « à permission » (c’est-à-dire des modèles où l’ensemble des acteurs sont connus et contrôlés) est connu sous le nom du « problème des généraux byzantins ».

S’il existe de nombreux protocoles permettant de parvenir à un consensus dans un cadre maîtrisé où tous les acteurs sont préalablement connus, ceux-ci ne fonctionnent plus quand des acteurs non authentifiés peuvent prendre part au protocole ou s’en désister à leur gré. La principale innovation de Bitcoin est d’avoir proposé un protocole permettant de parvenir à un consensus dans un tel environnement « sans permission » en utilisant des puzzles cryptographiques appelés « preuves de travail ».

Les blockchains les plus utilisées aujourd'hui ne sont pas adaptées au déploiement à grande échelle d'applications et de services. Les blockchains Bitcoin et Ethereum gèrent moins de 50 transactions par seconde. Des solutions technologiques se profilent à l'horizon, mais l'évolutivité limitée reste un inconvénient majeur qui compromet les performances des applications blockchain actuelles.

3.15. Conclusion

La blockchain pourrait devenir la couche économique et financière du Web. Elle permettra d'effectuer de façon décentralisée des paiements, des échanges, des transferts d'actifs, d'émettre et d'exécuter des contrats intelligents. Son domaine d'application peut aller au-delà des seuls aspects économiques et financiers.

Comme pour toute nouvelle technologie, l'implémentation de la blockchain peut connaître des obstacles et des limites. C'est à la communauté de ses acteurs qu'il revient de trouver les moyens permettant de les dépasser. Dans le chapitre suivant, nous allons évoquer les méthodes d'authentification basées sur la blockchain pour sécuriser l'IoT.

Chapitre 4 : Méthodes d'authentification basées sur la blockchain pour sécuriser l'IoT

4.1. Introduction

Dans un monde de fausses nouvelles, d'escroqueries et de vol d'identité, il devient plus difficile que jamais d'établir des relations d'affaires fondées sur la confiance. L'authentification blockchain pourrait aider à prouver l'intégrité et l'authenticité des enregistrements et même fournir une preuve numérique d'identité pour les personnes.

Sur un réseau IoT, la blockchain peut non seulement faciliter les transactions financières, mais aussi sécuriser les échanges de messages entre appareils. En opérant selon des contrats intelligents intégrés, deux parties peuvent partager de la data sans compromettre leur confidentialité pour son propriétaire. Si la blockchain ne résout pas tous les problèmes de sécurité pour les équipements de l'internet des objets, à l'instar du piratage des appareils pour une utilisation dans les botnets DDoS, elle aide toutefois à protéger la data des acteurs malveillants.

Si la blockchain a déjà attiré l'attention de nombreux acteurs du secteur bancaire, elle intéresse désormais les professionnels de l'IoT. D'autant que cette technologie de rupture arrive avec la promesse de faire progresser la sécurité.

C'est ainsi que nous allons étudier dans ce chapitre les différentes méthodes d'authentification possibles basées sur la blockchain pour pallier les problèmes de sécurité dans l'IoT.

4.2. Pourquoi l'IoT a-t-il besoin de la blockchain ?

Les déploiements IoT posent de nombreux défis, notamment en matière de sécurisation, de confidentialité et d'échange de données. Bien qu'il s'agisse de problèmes distincts, ces enjeux sont étroitement liés. La blockchain permet de les résoudre**.** Cette technologie, qui enregistre des informations et les transmet de manière immuable, transparente et sécurisée, est particulièrement adaptée aux enjeux de non-falsification et de traçabilité des données de l'IoT industriel. Les données générées par les machines sont ancrées dans la blockchain, et chaque équipement IoT y dispose d'une identité propre. La blockchain assure ainsi la confiance dans les données générées, garantissant qu'elles ne sont pas falsifiées ou compromises.

4.3. Le contrôle d'accès dans l'IoT

Les techniques de contrôle d'accès nécessitent deux phases essentielles, à savoir l'authentification et l'autorisation.

L'authentification est le processus de vérification de l'identité d'une entité. L'authentification est la première phase de tout mécanisme de contrôle d'accès qui peut déterminer l'identité exacte de la partie accédant afin d'établir la confiance du système.

Dans la plupart des cas, l'authentification est initiée entre un humain et une machine dans un processus pour se connecter au portail bancaire internet en entrant les identifiants.

Toutefois, dans ce scénario, l'entité qui sollicite l'accès n'a pas de garantie quant à l'identité de l'entité qui accorde l'accès. Afin de surmonter cette préoccupation, l'authentification

mutuelle doit être établie entre les entités, en vérifiant l'identité de l'entité octroyant l'accès avec la participation d'un TTP (tiers de confiance), tel qu'une autorité de certification. [27]

De plus, l'étape d'autorisation garantit qu'un utilisateur authentifié ne peut effectuer que les actions autorisées. Il peut être de trois types différents : basé sur des politiques, basé sur des jetons ou basé sur la cryptographie. Ces types peuvent être combinés pour avoir : des approches basées sur la politique et la cryptographie ou la cryptographie et les jetons [28].

4.3.1. L'authentification mutuelle

L'authentification mutuelle ou l'authentification bidirectionnelle (à ne pas confondre avec l'authentification à deux facteurs) désigne le fait que deux parties s'authentifient en même temps dans un protocole d'authentification. C'est un mode d'authentification par défaut dans certains protocoles (IKE, SSH) et optionnel dans d'autres (TLS). L'authentification mutuelle est une caractéristique souhaitée dans les schémas de vérification qui transmettent des données sensibles, afin d'assurer la sécurité des données. L'authentification mutuelle peut être effectuée avec deux types d'identifiants : les noms d'utilisateur et les mots de passe, et les certificats de clé publique. L'authentification mutuelle est souvent utilisée dans l'internet des objets (IdO). La rédaction de schémas de sécurité efficaces dans les systèmes IdO peut devenir difficile, en particulier lorsque les schémas doivent être légers et avoir des coûts de calcul faibles. L'authentification mutuelle est une étape de sécurité cruciale qui peut se défendre contre de nombreuses attaques antagonistes, qui autrement peuvent avoir de grandes conséquences si les systèmes IdO sont piratés. Le manque d'authentification mutuelle a été considéré comme une faiblesse des schémas de transmission des données [29].

4.3.2. La cryptographie

La cryptographie vise à assurer des fonctionnalités qui sont essentielles pour protéger l'information, dont les principales sont les suivantes :

- La confidentialité : elle assure que les données ne sont compréhensibles qu'aux personnes ou entités autorisés.
- L'intégrité : elle assure que les données ne sont pas altérées de façon non autorisée pendant leur transmission ou leur stockage.
- L'authentification : elle prouve que la personne ou l'entité qui envoie les messages est exactement celle qu'elle prétend être.

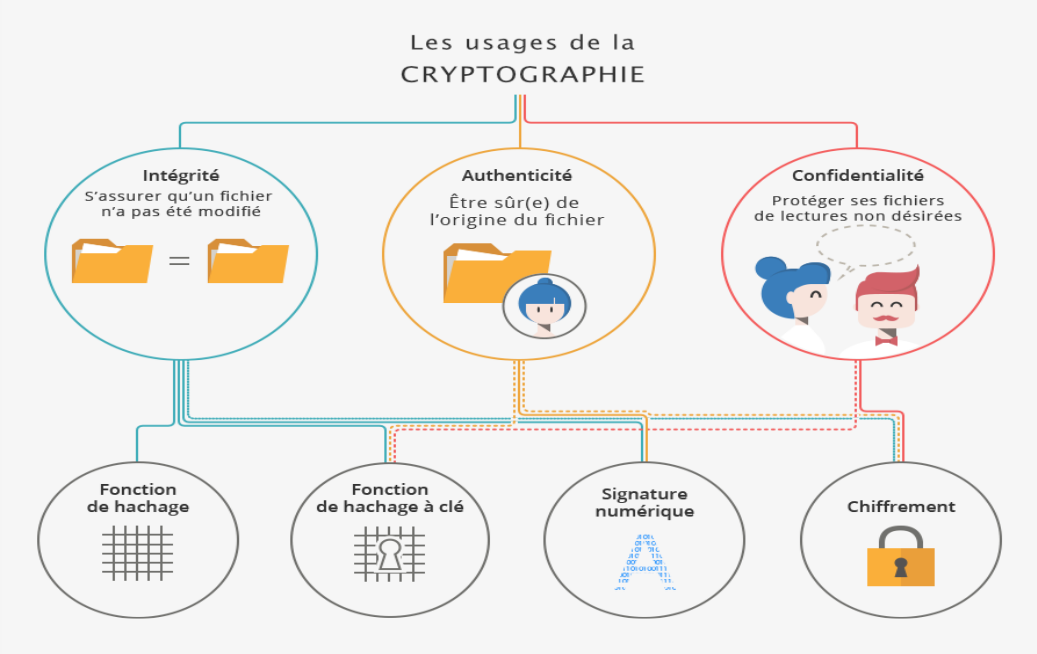


Figure 27: Les fonctionnalités de la cryptographie

La cryptographie permet ainsi de protéger un message clair, généralement par l'utilisation d'un secret, afin d'obtenir un chiffré compréhensible uniquement par l'utilisateur légitime. Il s'agit de l'une des deux disciplines de la cryptologie, l'autre étant la cryptanalyse qui consiste à analyser un chiffré sans la connaissance du secret pour en déduire des informations sur le message clair ou sur le secret. La cryptographie n'est considérée que depuis peu comme une science, mais il s'agit d'une discipline qui existe depuis l'antiquité.

4.3.2.1. La cryptographie moderne

Ce type de cryptographie repose sur une clé, qui doit pouvoir prendre suffisamment de valeurs différentes afin d'empêcher une attaque exhaustive qui consiste à tester toutes les valeurs de clé possibles. L'ensemble des techniques utilisées aujourd'hui peut se diviser en quatre principales catégories : les fonctions de hachage cryptographiques, les codes d'authentification de message (MAC en anglais pour "Message Authentication Code"), les schémas de chiffrement à clé publique et les schémas de chiffrement à clé secrète.

- ❖ Fonctions de hachage cryptographique :

Une fonction de hachage est aussi appelée fonction de hachage à sens unique ou "one-way hash function" en anglais. Ce type de fonction est très utilisé en cryptographie, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage.

De façon générale, l'empreinte d'un message produit avec une fonction de hachage cryptographique doit dépendre de tous les bits de message. En parallèle, une fonction de hachage cryptographique doit être un procédé assez complexe de façon que si un bit du message est modifié, le haché ne doit plus avoir aucune liaison avec le haché du message précédent. Mis à part ces propriétés de conception génériques, une fonction de hachage est dite avoir des

bonnes propriétés cryptographiques si elle est résistante aux préimages, aux secondes préimages et aux collisions. Les trois problèmes suivants doivent donc être difficiles.

- Préimage : étant donné un haché h choisi aléatoirement, trouver un message m tel que H(m) = h.
- Seconde préimage : étant donné un message m choisi aléatoirement, trouver un message m′ tel que H(m) = H (m′).
- Collision : trouver deux messages m, m′ tels que m m′ et H(m) = H (m′).

❖ Codes d'authentification de messages ou MAC :

Ces mécanismes cryptographiques permettent à la fois d'assurer l'intégrité du message envoyé et d'authentifier son expéditeur. Pour réussir cela, lors de l'envoi du message, le code d'authentification est ajouté au message. Un MAC peut être construit à partir d'une fonction de hachage, par exemple la construction HMAC ou enveloppe MAC, à partir d'une fonction de hachage universelle (UMAC) ou encore d'un chiffrement par bloc, comme dans OMAC ou CBC-MAC.

❖ La cryptographie asymétrique

- Fonctionnement : un schéma de chiffrement à clé publique ou asymétrique manipule deux clés. L'une est publique, transmissible sans restriction, et est utilisée par la fonction de chiffrement. L'autre est privée, connue uniquement de son propriétaire, et est utilisée par la fonction de déchiffrement.

  Un des tout premiers schémas de chiffrement à clé publique, et le plus célèbre, a été proposé en 1978 par R. Rivest, A. Shamir et L. Adleman et est désigné par RSA (pour "Rivest-Shamir-Adleman ") [RIVEST et al. 1978]. Le RSA repose sur l'exponentiation modulaire, sa clé publique est composée d'un entier *e* et d'un entier *n* qui doit être le produit de deux nombres premiers *p* et *q*, et sa clé privée est un entier *d* tel que ed ≡ 1 modulo (*p* - 1) (*q* - 1). Pour chiffrer un message M, il suffit alors de calculer C = M*e* modulo *n*, qui pourra bien être déchiffré en calculant M = C*d* modulo *n*, d'après le théorème d'Euler en arithmétique modulaire [EULER, 1763]. Il est à noter que les fonctions de chiffrement et de déchiffrement du RSA peuvent être utilisées pour effectuer une authentification. En effet, il suffit d'appliquer la fonction de déchiffrement avec la clé privée sur un message clair connu de tous afin d'obtenir un chiffré à transmettre pour vérification. N'importe qui peut alors appliquer la fonction de chiffrement avec la clé publique sur le chiffré pour s'assurer que le message ainsi obtenu correspond bien au message clair.

➢ Avantages :

- Pas besoin d'établir un canal sûr pour la transmission de la clé.
- Plusieurs fonctions de sécurité : confidentialité, authentification et non répudiation.

➢ Inconvénients :

- Le principal problème du chiffrement à clé publique réside dans la lenteur à laquelle se font les opérations de chiffrement et de déchiffrement.
- D'autres problèmes de cette méthode de chiffrement est qu'elle nécessite un nombre très important de calculs : généralement dix fois plus lent que le cryptage symétrique.

- Problème d'implémentation sur les équipements disposant de faible puissance de calcul (exemple : cartes bancaires, stations mobiles, etc.).
- Clés longues.
- Complexité algorithmique de la méthode (exemple : réalisation des opérations modulo n).

➢ Solution : utilisation du cryptage asymétrique pour l'échange des clés secrètes de session d'un algorithme symétrique à clés privées.

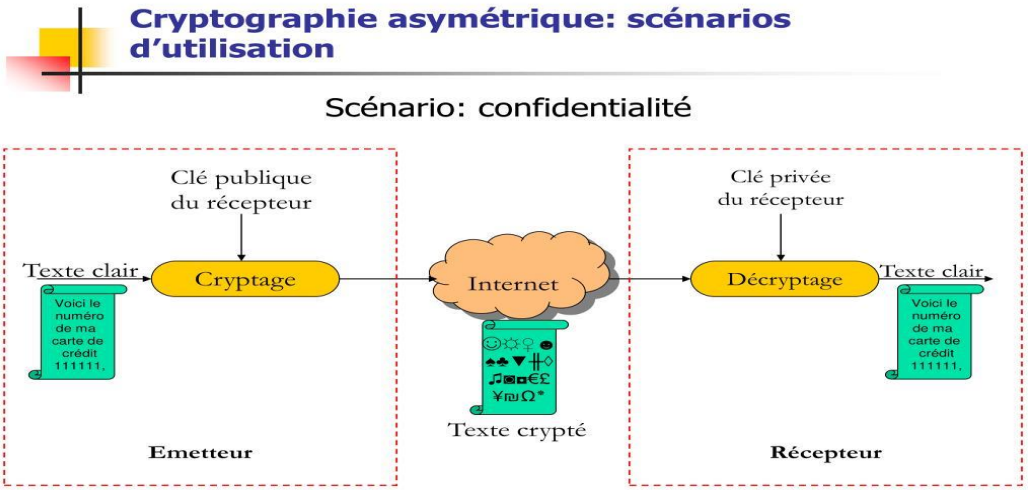


Figure 28: Chiffrement à clé publique

❖ La cryptographie symétrique

➢ Fonctionnement : la cryptographie symétrique, ou cryptographie à clé secrète, est la plus ancienne forme de cryptographie. Elle se base sur l'utilisation d'une clé différente pour chaque communication.
Cette clé, qui sert à la fois à chiffrer et à déchiffrer les messages échangés, est connue par les deux personnes impliquées dans la communication.

La cryptographie symétrique comprend plusieurs types de constructions qui sont employés pour assurer la confidentialité, l'intégrité ou l'authenticité de la communication. Cette exigence selon laquelle les deux parties ont accès à la clé privée. Les Principales constructions sont :

Les systèmes de chiffrement par bloc : un chiffrement par bloc est une transformation inversible d'un bloc de taille fixe n paramétré par une clé secrète k. Pour chiffrer un message de taille quelconque, celui-ci est découpé en blocs de taille n et ces blocs sont ensuite chiffrés les uns après les autres. Pour chaîner les blocs chiffrés, un mode opératoire est utilisé. Le chiffrement par bloc le plus utilisé aujourd'hui est l'algorithme AES. Il a été conçu par Joan Daemen et Vincent Rijmen [DR00b, FIP01] et sélectionné comme norme internationale lors d'une compétition publique organisée par le NIST. Il a ainsi remplacé le standard précédent, DES [FIP99], qui a dû être abandonné à cause de la taille trop courte de sa clé.

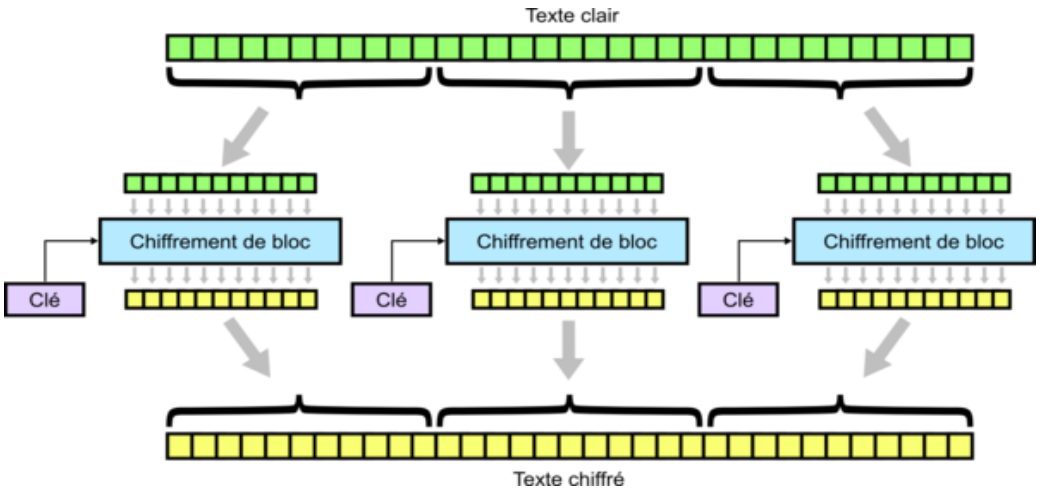


Figure 29: Schéma d'un chiffrement par bloc

- Les systèmes de chiffrement à flot : le principe du chiffrement à flot, également appelé chiffrement à la volée, consiste en la combinaison du message clair avec une suite chiffrant de taille égale à la taille du message à chiffrer, par une opération de ou exclusif (XOR). Cette suite est générée à l'aide d'un générateur pseudo-aléatoire, qui a été initialisé avec une valeur secrète relativement courte, dérivée de la clé secrète du chiffrement. La sécurité du système est alors basée sur la qualité du générateur. Une suite chiffrant doit ressembler le plus possible à une suite aléatoire, aucune propriété structurelle ne doit pouvoir être exploitée. Les systèmes de chiffrement à flot sont utilisés dans les contextes où il est primordial de pouvoir chiffrer et déchiffrer très rapidement et où les ressources matérielles, par exemple la taille du circuit ou la capacité de stockage, sont très restreintes. Ceci est la raison pour laquelle les chiffrements à flot sont implantés dans les téléphones mobiles et dans d'autres dispositifs embarqués.

➢ Avantages :

- Un avantage important des chiffrements asymétriques par rapport aux chiffrements symétriques est qu'aucun canal secret n'est nécessaire pour pratiquer l'échange de la clé publique. Le récepteur doit simplement être sûr de l'authenticité de la clé publique. Les chiffrements symétriques demandent un canal secret pour envoyer la clé secrète générée d'un côté du canal de communication vers l'autre côté.
- Le chiffrement/déchiffrement est très rapide, les algorithmes de chiffrement symétrique sont généralement beaucoup moins complexes que les algorithmes de chiffrement asymétrique.
- Utilise peu de ressources systèmes, toujours dans le même principe d'algorithme moins complexe.

➢ Inconvénients :

L'un des principaux inconvénients du cryptage à clé symétrique par rapport au cryptage à clé publique est : une "clé" ici est en fait un secret partagé entre plusieurs parties, ce qui permet de maintenir un lien vers des informations confidentielles.

- Le chiffrement symétrique n'assure que la confidentialité des données.
- Une clé symétrique correspond à un échange entre deux personnes. Pour communiquer avec d'autres personnes, il faudra une autre clé symétrique.

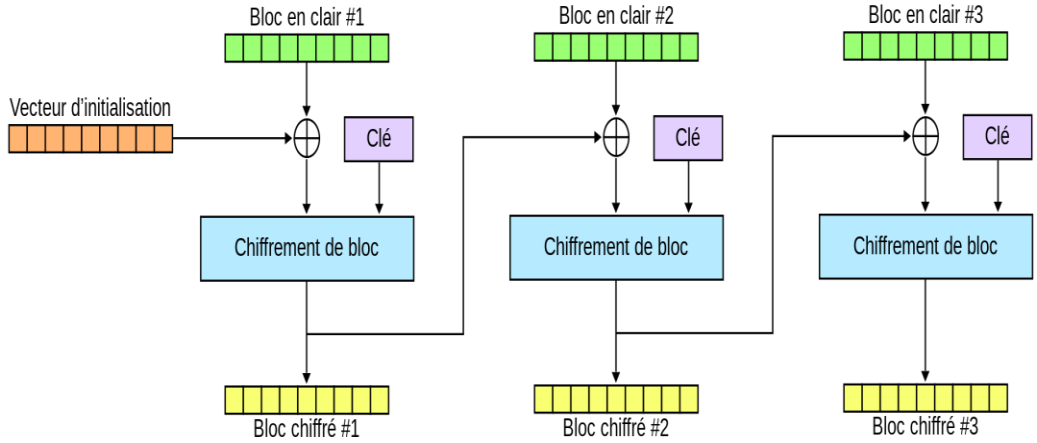


Figure 30: Schéma d'un chiffrement à flot

Tableau 6: Comparaison entre cryptographie symétrique et cryptographie asymétrique (Source : 10 /01/2015, Pr BELKHIR Abdel Kader)

	Symétriques	Asymétriques
Avantages	-Rapidité (jusqu'à 1000 fois plus rapide) -Facilité d'implantation sur hardware - Taille de clé : 128 bits (16 caractères mémorisables)	-Distribution des clés facilitées : pas d'authentification -Permet de signer des messages faciles -Nombre de clé à distribuer est réduit par rapport aux clés symétriques

Inconvénients	-Nombre de clés à gérer -Distribution des clés (authentification, confidentialité) -Certaines propriétés (p.ex. signatures) sont difficiles à réaliser	-Taille des clés -Vitesse de chiffrement

Ce tableau comparatif montre les principales différences entre le chiffrement symétrique et le chiffrement asymétrique.

Il faut considérer le rôle de la clé dans la sécurisation de la communication. Le chiffrement à clé symétrique utilise la même clé pour le chiffrement et le déchiffrement. Dans ce cas, l'expéditeur et le destinataire partagent la même clé et doivent la garder secrète. Le cryptage symétrique présente l'avantage d'être plus rapide et plus efficace. Toutefois, le principal inconvénient réside dans le partage sécurisé de la clé entre les deux parties.

Alors que le cryptage asymétrique utilise une paire de clés. L'expéditeur peut librement distribuer la clé publique à n'importe qui, mais il doit conserver la clé privée en lieu sûr. L'avantage du cryptage asymétrique est qu'il élimine la nécessité d'une distribution sécurisée des clés, puisque chaque partie génère sa paire de clés. Cependant, elle est plus lente et moins efficace.

4.3.3. Protocoles d'authentification

Les protocoles d'authentification ont chacun leur propre manière d'authentifier un utilisateur ou une machine. Ils utilisent différents algorithmes et différentes techniques. Cependant, ils ont tous quasiment le même principe de fonctionnement qui est à base de clés.

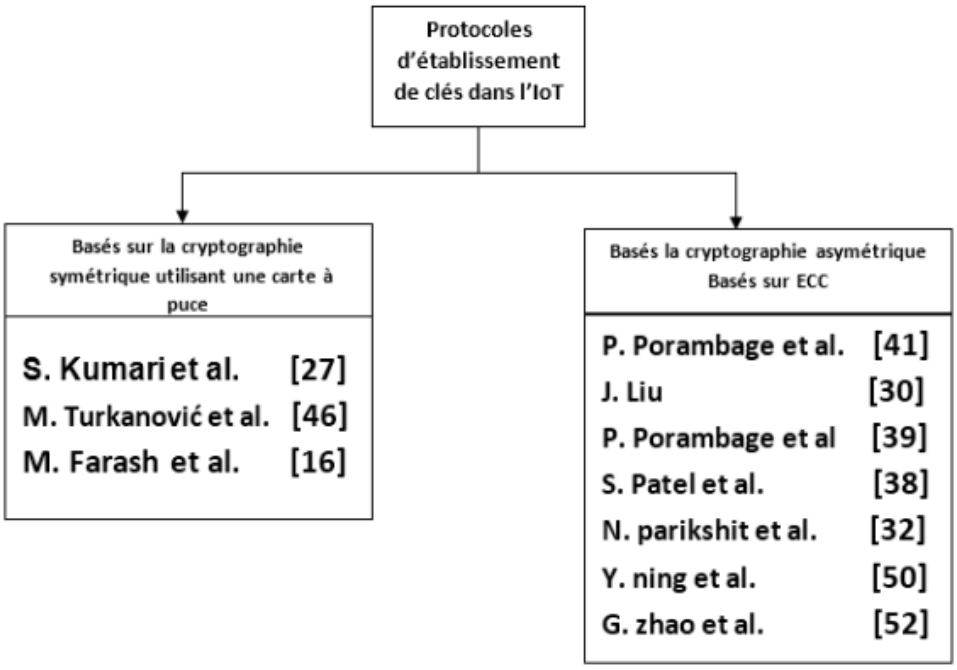


Figure 31: Classification des protocoles étudiés pour l'établissement de clé

4.3.3.1. Critère de comparaison des solutions

L'établissement de critères s'impose pour une bonne étude critique des protocoles proposés pour l'authentification et la gestion de clé. Dans le but de mener une étude objective des solutions proposées dans la littérature, et en tenant compte des besoins et des contraintes spécifiques de l'IoT, cela nous permettra de cibler les défis auxquels nous ferons face lors de notre contribution.

C'est ainsi que nous allons proposer une technique d'authentification qui consiste en un protocole de gestion de clé.

a) Résistances aux attaques

Les techniques de sécurité doivent résister tant que possible aux attaques. Plus la résistance est forte, plus les solutions sont meilleures.

b) Consommation énergétique

L'énergie est sans doute le facteur limitatif le plus important par rapport aux capacités d'un nœud capteur. La réserve énergétique limitée de chaque nœud capteur doit être gérée raisonnablement pour prolonger autant que possible sa durée de vie et ainsi que celle du réseau.

c) Complexité de mémoire de stockage

Un capteur ou un objet sont des petits dispositifs avec une mémoire très réduite et un espace de stockage limité. Donc pour construire un mécanisme de sécurité efficace, il est nécessaire de limiter la taille du code de l'algorithme de sécurisation.

d) Accord de clé

Un cryptage doit être défini à l'aide d'une clé de session partagée secrètement entre deux parties pour communiquer de manière sécurisée sur un réseau ouvert non sécurisé. Une clé de session est négociée en utilisant un protocole d'accord clé, dans lequel toutes les parties impliquées indépendamment et individuellement forment et influencent une clé.

e) Authentification mutuelle

Dans un système d'authentification, l'authentification mutuelle est d'une grande importance. Lorsqu'un utilisateur tente de se connecter à un réseau ou un serveur, il en a besoin pour être sûr de la légitimité du serveur, car un adversaire pourrait se faire passer pour un serveur légitime en exécutant une attaque man-in-the-middle. En revanche, un serveur doit également être sûr de la légitimité de l'utilisateur.

f) Scalabilité

On dit qu'un réseau a une bonne scalabilité quand on peut facilement augmenter le nombre de nœuds ou d'objets et qu'il n'y a aucun problème lors de cet ajout au réseau. Il est plus intéressant que le réseau assure le bon fonctionnement quel que soit le nombre de nœuds.

4.3.3.2. Étude de quelques protocoles d'authentification

Chaque protocole d'authentification a sa propre méthode pour authentifier un utilisateur ou une machine. Ils utilisent différents algorithmes et différentes techniques. Cependant, ils ont tous presque le même principe de fonctionnement (basé sur la clé). On va classer les protocoles étudiés en deux catégories principales. D'un côté il y a des protocoles basés sur la cryptographie symétrique qui utilise une seule clé pour le chiffrement et le déchiffrement ; et dans l'autre côté, nous avons des protocoles basés sur la cryptographie asymétrique qui utilise deux clés (la première est publique pour le chiffrement et la deuxième est privée pour le déchiffrement).

1) Protocoles basés sur la cryptographie symétrique utilisant une carte à puce

- **Protocole d'authentification et d'accord clé basé sur la cryptographie symétrique et une carte à puce [30]**

Ce protocole comprend quatre phases : phase d'enregistrement, phase de connexion, phase d'authentification et phase de changement de mot de passe.

- **La phase d'enregistrement** : dans cette phase, l'utilisateur Ui s'enregistre sur le serveur Si. Ui choisit d'abord son identifiant ID et son mot de passe Pwi.
- **La phase de connexion** : lorsqu'un utilisateur enregistré Ui veut accéder aux services de Si, il insère sa carte à puce SCi dans un terminal et saisit son identité et son mot de passe Pwi.
- **La phase d'authentification** : si et Ui procèdent à des calculs pour s'authentifier mutuellement, après qu'ils ont une clé de session commune.
- **La phase de changement de mot de passe** : cette phase est réalisée lorsque Ui souhaite remplacer son ancien mot de passe PWi par un nouveau. La carte SCi décide si la demande de changement de mot de passe est acceptable ou non.

Discussion et critique :

Le régime proposé assure l'authentification mutuelle et est résistant à diverses attaques, y compris attaque initiale, attaque de DoS et il fournit un accord clé de session, mais n'est pas complètement exempt d'attaques de sécurité, il souffre de l'attaque de supposition de mot de passe de carte à puce ou un attaquant peut lancer avec succès une attaque de supposition de mot de passe de carte à puce et de la violation de l'anonymat où un attaquant peut obtenir l'IDi de l'utilisateur. Le protocole proposé est coûteux en mémoire et en consommation d'énergie.

- **Un système d'authentification et d'accord clé basé sur une carte à puce et un nœud de passerelle pour l'IdO [31]**

Ce protocole est composé de quatre phases :

- **La phase de pré-déploiement** : pendant la phase de pré-déploiement, chaque nœud de capteur régulier est prédéfini avec son identité SID et une clé de mot de passe sécurisée XGWN générée au hasard, qui est partagée avec le GWN et stockée dans la mémoire du nœud. Le GWN est prédéfini avec une clé de mot de passe hautement sécurisée générée de manière aléatoire Xgwn.
- **La phase d'enregistrement** : deux phases d'enregistrement distinctes sont nécessaires après le déploiement. La première est une phase d'enregistrement entre GWN et un nœud de capteur régulier correspondant Sj, et après le déploiement. La deuxième phase d'enregistrement est entre une interface utilisateur et le GWN, et est initiée par l'utilisateur sur demande.
- **La phase de connexion :** après la phase d'enregistrement, l'utilisateur peut se connecter à un nœud de capteur désiré du réseau en lançant une phase d'authentification. Dans l'ordre de la phase d'authentification pour être lancée, l'utilisateur doit d'abord se connecter. Comme mentionné, le système utilise une carte à puce (SC) pour permettre à l'utilisateur de s'inscrire et de s'authentifier. Tout autre système de sécurité pour l'enregistrement sécurisé des données d'un utilisateur pourrait être utilisé à la place.
- **La phase d'authentification** : cette phase est initiée par l'utilisateur avec une authentification message à la fin d'une phase de connexion exécutée avec succès. L'utilisateur envoie le message d'authentification à un nœud de capteur souhaité du réseau et non le GWN. L'objectif de cette phase est de négocier une clé de session secrète entre l'utilisateur et le nœud du capteur d'une manière qui contribuera individuellement à la clé de la session avec un nonce secrètement choisi. Après avoir négocié avec succès la clé de session, ils peuvent l'utiliser pour communiquer en toute sécurité dans toute matière cryptée. Afin de réaliser la session sécurisée de négociation clé, une méthode d'accord clé légère est proposée qui implique une authentification mutuelle entre toutes les parties.

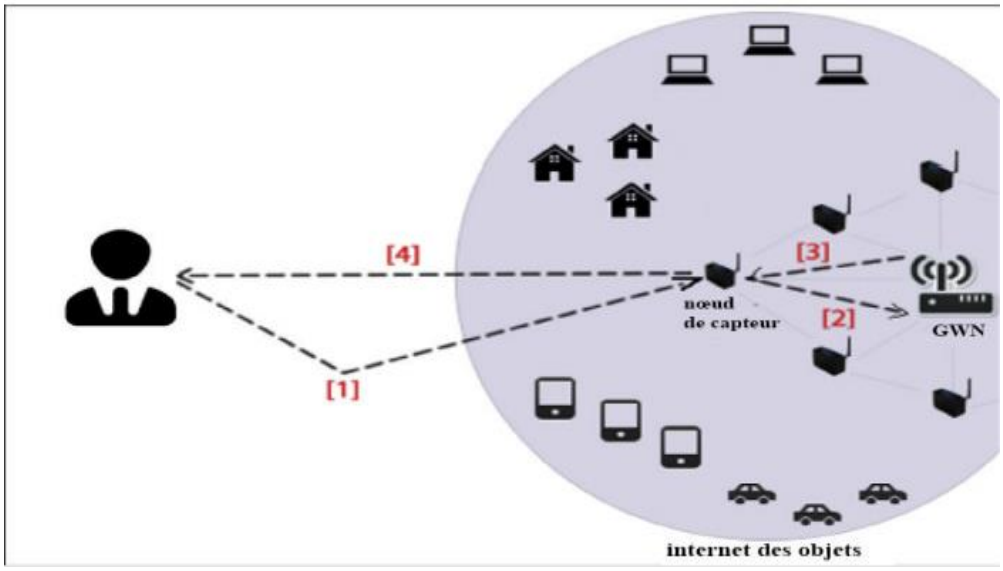


Figure 32: Un système d'authentification et d'accord clé basé sur une carte à puce et un nœud de passerelle pour l'Ido

Discussion et critique :

Le schéma proposé est également sûr et léger, car il utilise la cryptographie symétrique, ce qui est hautement souhaitable par l'architecture à contraintes de ressources du WSN. Le système garantit des caractéristiques importantes, comme la protection par mot de passe, le changement de mot de passe et l'ajout de nœuds dynamiques. En outre, il offre une grande sécurité, parce qu'il est résilient pour reporter les attaques d'adversaires privilégiées, infractions de cartes à puce, les attaques d'usurpation d'identité, les attaques d'identification quand plusieurs utilisateurs sont connectés avec la même connexion, les attaques de contournement GWN, les attaques de changement de mot de passe et les attaques DoS. Ils assurent une meilleure performance au sein de l'environnement de ressources limitées.

Ce schéma n'est pas adapté aux applications pratiques en raison de faiblesses de sécurité où de quelques défauts de sécurité et il est susceptible de quelques attaques cryptographiques. Il souffre d'une attaque par carte à puce et d'une attaque man-in-the-middle.

Le système proposé consomme plus de stockage, ou il nécessite plus d'espace de stockage à partir d'un GWN ou d'un nœud de capteur et beaucoup d'énergie environ. Ce protocole pose un problème de confidentialité lorsqu'un grand nombre de personnes est impliqué dans l'échange de clés (car il faudrait n (n - 1) /2 clés secrètes). Le système GWN devait conserver la clé partagée de chaque nœud capteur enregistré, ce qui signifie immédiatement que le nombre de nœuds utilisés dans le WSN est limité par la mémoire du GWN.

- **Un système d'authentification et d'accord clé basé sur une carte à puce et un nœud de passerelle pour l'IdO (UAKAS) [32]**

Ce système d'authentification des utilisateurs et d'accord clé (UAKAS) basé sur le modèle de Turkanović doit résoudre et éliminer toutes les lacunes et vulnérabilités. Il comprend trois phases :

- **La phase de pré-déploiement** : pour qu'un WSN (Wireless sensor network) puisse être activé, une phase de pré-déploiement est nécessaire. Selon le schéma de Turkanović, cette phase est effectuée hors ligne par un administrateur réseau. Chaque nœud de capteur du WSN est prédéfini avec son identité SIDj et un mot de passe sécurisé XGWN-Sj qui est partagé avec le GWN. Les deux variables sont stockées dans la mémoire d'un nœud de capteur Sj.
- **La phase d'enregistrement** : cette phase est divisée en deux parties : la phase d'enregistrement de l'utilisateur et la phase d'enregistrement du nœud de capteur. Le processus d'enregistrement de l'utilisateur se fait via le canal protégé par le GWN, et le résultat est que l'utilisateur utilise une carte à puce pour s'inscrire. Avant de commencer l'authentification, l'utilisateur Ui doit se connecter. Cela se fait hors ligne via la carte à puce SC.
- **La phase de connexion et d'authentification** : après une connexion réussie, SC prépare le processus d'authentification. Le but de la phase d'authentification est de permettre à l'utilisateur de négocier la clé de session secrète avec un nœud de capteur spécifique sans contacter le GWN. La clé de session sera ensuite utilisée pour une communication sécurisée (requête, réponse) entre l'utilisateur et le nœud capteur, et sera construite par les deux parties.

Discussion et critique :

La différence vitale et l'amélioration du schéma proposé par Turkanović et al permet à un GWN d'ajouter de nombreux nœuds supplémentaires au réseau sans remplir sa mémoire, car il est continuellement libéré après l'avoir enregistré. Les auteurs ont montré que le schéma proposé fournit un accord clé, ainsi est résistant à une attaque d'usurpation d'utilisateur, à un problème d'anonymat d'utilisateur, une attaque répétée, une attaque initiale privilégiée, et une attaque de déni de service, l'attaque de carte intelligente volée, l'attaque de man-in-the middle.

Ce protocole n'assure pas l'authentification mutuelle, ne pouvait pas résister à une attaque de carte à puce, à une attaque de déconnexion de mot de passe hors ligne, à une attaque d'information temporaire spécifique et ne désactive pas la traçabilité des utilisateurs. L'architecture de réseau utilisée dans ce protocole est inefficace pour les environnements auxquels l'énergie est un problème majeur. Le temps de fonctionnement total de ce protocole est de 0.0128 ms, le coût total de calcul est de 32 Th donc il est coûteux en mémoire et en termes de consommation d'énergie.

2) Protocoles basés sur la cryptographie asymétrique basés sur ECC

- **Un système d'authentification et d'établissement de clé utilise des certificats implicites (CA) basés sur ECC [33]**

Le schéma d'authentification proposé pour les applications WSN dans l'IdO distribué comprend deux phases.

- **La phase d'enregistrement** : les dispositifs de bordure du réseau (p. ex., nœuds de capteurs) et les utilisateurs finaux demandent des justificatifs de sécurité et des certificats à l'autorité de certification (AC). Le rôle de la phase d'enregistrement est d'établir une communication authentifiée, où le nœud capteur et l'utilisateur final

doivent avoir un certificat implicite d'une suite de chiffrement spécifique, et le nœud capteur demande des informations de sécurité et un certificat de sécurité. Dans un premier temps, le client envoie une suite de chiffrement de message, qui inclut un certificat implicite appelé le serveur. Le serveur accepte la suite de chiffrement et répond par un message ou supprime la poignée de main.

- **La phase d'authentification** : afin d'établir une communication authentifiée, les nœuds de bordure et les utilisateurs finaux devraient posséder des certificats implicites pour des suites de chiffrement particulières. Plusieurs transferts de message de la phase d'authentification entre le nœud client et le nœud serveur sont considérés. Le client envoie son certificat accompagné d'un nonce cryptographique aléatoire et la valeur MAC. Si la vérification MAC réussit, le serveur calcule la clé publique du client (QU) à l'aide du certificat CertU reçu et de la clé publique de l'AC (QCA). Semblable au côté serveur, le client vérifie MAC, calcule la clé publique du serveur et dérive la clé commune en utilisant sa propre clé privée et la clé publique du serveur :
  KUV = dUQV. À la fin, les deux nœuds de bord (clients) peuvent s'authentifier et établir une clé secrète commune et une liaison de communication pouvant être utilisée pour sécuriser d'autres acquisitions de données entre le client et le serveur.

Discussion et critique :

Le schéma d'authentification proposé est léger et peut être facilement déployé dans les dispositifs à ressources restreintes, ainsi qu'une sécurité raisonnablement élevée. En raison de la petite taille des certificats, il est possible de les déployer dans les WSN hétérogènes compatibles avec l'IoT. En outre, le schéma d'authentification proposé prend en charge l'addition du nouveau nœud (il est scalable) et la mobilité des périphériques de bord et des utilisateurs finaux. L'authentification proposée est basée sur ECC. L'avantage de l'utiliser est qu'il fournit une sécurité égale à celle pour RSA, mais avec moins de frais généraux. L'autorité de certification (CA) a été utilisée pour délivrer des certificats. Après avoir obtenu leur propre certificat, les nœuds peuvent se déplacer et changer leur emplacement.CA peut valider l'identité des capteurs et communiquer avec d'autres entités du réseau. Le schéma proposé offre une meilleure sécurité, il est sécurisé contre les attaques de déni de service (DoS), cependant, il a toujours des limites. Par exemple, les attaques de capture de nœud peuvent créer une quantité limitée de dommages à l'ensemble du réseau. Le schéma proposé :

La performance du schéma proposé montre qu'il offre une consommation d'énergie et des frais généraux moins élevés et qu'il consomme moins de mémoire sur chaque nœud capteur.

- **Protocole d'authentification basé sur le hashing et l'extraction des fonctionnalités [33]**

Ce protocole est basé sur l'algorithme de hachage SHA et l'extraction de fonction et la cryptographie de la courbe elliptique ECC. Il contient trois parties principales :

- **La phase d'initialisation** : dans cette phase, certains facteurs nécessaires sont prédistribués au nœud de la plateforme et du terminal. De la figure 33, nous pouvons voir que les facteurs du côté du nœud de terminal, y compris ID, compte, etc. Et les facteurs du côté de la plateforme, y compris toutes les informations concernant le nœud

terminal. Afin de comprendre clairement le schéma, nous avons besoin de faire quelques explications.

- **Vérification AC** : comme nous l'avons expliqué dans la partie précédente, il existe un centre CA qui peut être utilisé en toute sécurité pour vérifier les certificats des deux plateformes et le nœud terminal. L'authentification du certificat méthode est la même que celles existantes.
- **L'authentification mutuelle** : le système d'authentification mutuelle proposé est asymétrique pour les nœuds de plateforme et de terminal. En général, la plateforme a des structures relativement plus complexes et des capacités de processus plus élevées par rapport au nœud terminal, il est donc très difficile pour l'attaquant de prétendre être une fausse plate-forme pour communiquer avec le nœud terminal.

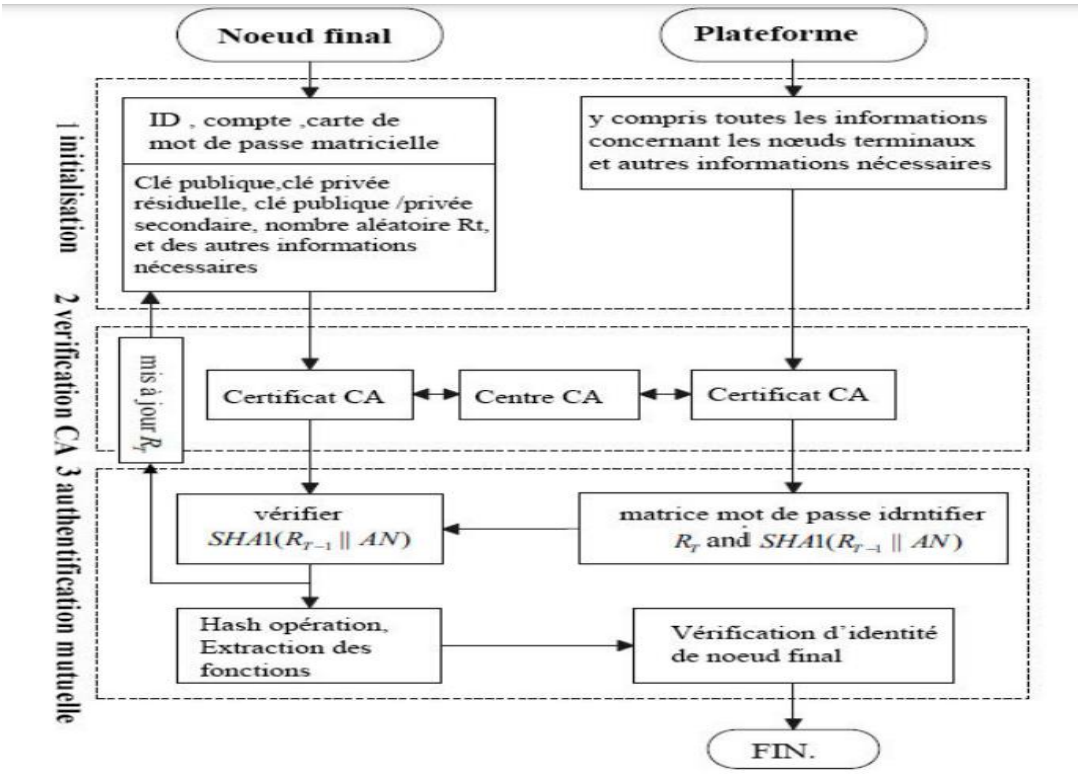


Figure 33 : Les étapes de protocole de hachage

Discussion et critique :

Les auteurs ont présenté un schéma d'authentification mutuelle pour l'IoT entre les plates-formes et les nœuds terminaux. Le schéma est basé sur le hashing et l'extraction des fonctionnalités. L'extraction des fonctions a été combinée avec la fonction hash pour éviter toute attaque de collision. Ce système fournit en fait une bonne solution pour l'authentification dans l'IoT. Le processus d'extraction des caractéristiques a les propriétés de l'irréversibilité nécessaires pour assurer la sécurité et est léger, ce qui est souhaitable dans l'IoT. Le schéma se concentre sur le processus d'authentification lorsque la plate-forme essaie d'envoyer des données aux nœuds terminaux et non pas le contraire. Bien que le système améliore la sécurité

tout en réduisant la quantité d'information réduite, cela ne fonctionne que sur la théorie et il n'y a pas de preuve pratique pour l'appuyer.

- **Une méthode efficace d'authentification basée sur ECC pour la couche de perception**

YE Ning et al [40] ont proposé une méthode efficace d 'authentification mutuelle établissant des paires de clés publique-privée, basée sur la cryptographie de courbe elliptique (ECC) pour la couche de perception de l'IdO. Cette méthode peut confirmer l'identité des deux côtés de la communication et établir une clé de session.

L'authentification comprend deux phases : une phase d'initialisation, d'authentification mutuelle où l'utilisateur doit négocier avec BS l'information secrète utilisée pour l'authentification lorsqu'il accède au réseau du capteur. Et une phase d'établissement de clés. Le schéma suivant décrit les différentes étapes.

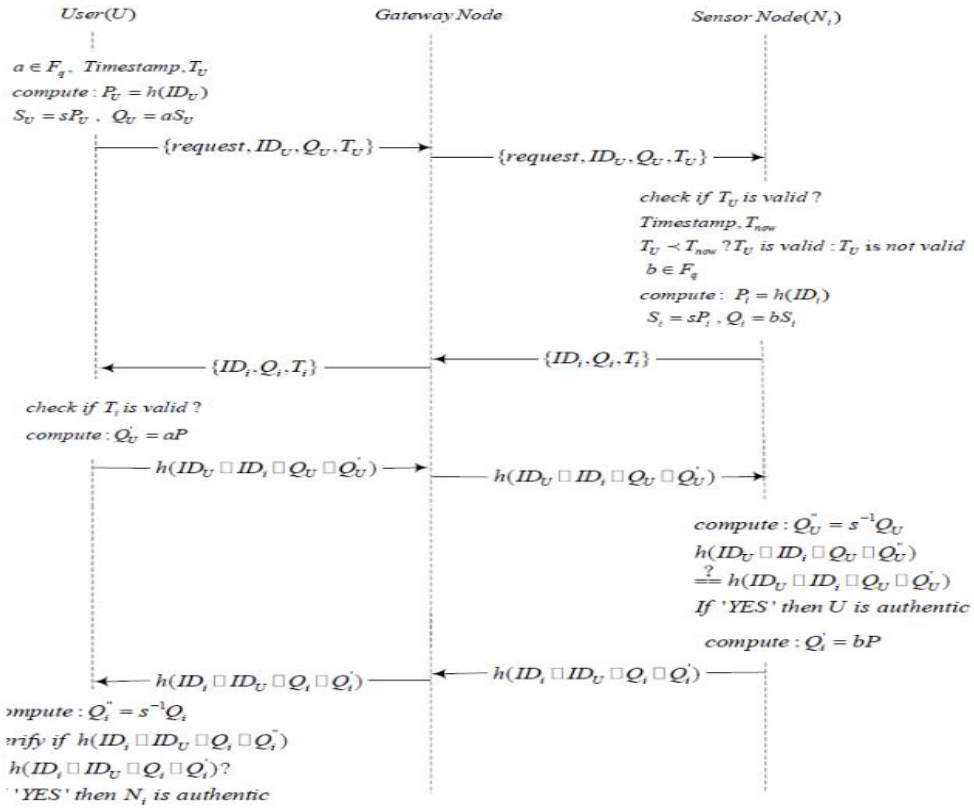


Figure 34: Mutual Authentication Key Establishment Phase

Discussion et critique :

L'auteur dit que son authentification résiste aux attaques suivantes : man in the middle, l'effraction, la capture de nœud, Dos, attaques de répétition. Les algorithmes cryptographiques traditionnels ne peuvent pas atteindre le poids léger, le manque d'authentification mutuelle entre les utilisateurs et les nœuds n'est pas adapté à l'environnement ouvert d'IoT. L'authentification mutuelle garantit la sécurité de la communication entre les utilisateurs et les

nœuds, dont le processus est simple pour résoudre le problème limité de ressources de la couche de perception IoT. ECC offre de meilleures performances, car il peut utiliser une taille de clé plus petite pour obtenir la même sécurité.

Tableau 7: Tableau comparatif entre les protocoles de gestions de clé

		Résistance aux Attaques				Sca Labi Lité	Accord de clé	Optimisation de la consommation d'énergie	Complexité de calcul et mémoire de stockage	Anonymat	L'authentification mutuelle
		DOS	Man In the mid Dle	Répétition	Supposition de mot de passe						
Basé sur la cryptographie symétrique utilise carte à puce	M. Turkanovic et al.[10]	Oui	Non	/	Non	Oui	Non	Non	19Th 768 bits	Non	Oui
	S. Kumari et al.[45]	Oui	/	/	Non	/	Oui	Non	16 th +36t⊕ 768 bits	Non	Oui
	Farash et al.[18]	Oui	Oui	Oui	Non	Oui	Oui	Non	32 Th 512 bits	Oui	Non
Basé sur la cryptographie asymétrique	S. Patel et al.[31]	Oui	Oui	Oui		Oui	Oui	Oui	2TMac +Th +TRC5		Oui
	P. porambage et al.[39]	Oui	/	/		Oui	Oui	Oui	(n+5) PM + n+2 PA		Oui
	J.lui et al.[7]	Non	Oui	Oui		/	Oui	Non	Oui	Oui	Non

Basé sur (ECC)	N. pariksit et al. [G]	Non	Non			/	/	Oui	2Dh+2DMac +2DRCS		Non
	Y.ning et al. [C]	Oui	Oui	Oui		/	/	Non	R+Tnul+2Th		Oui
	G. Zhao et al.[ICM]	Oui	Oui	Oui		/	/	Non	Oui		Non
	P. poram bage et al.[50]	Oui	Non	/		Oui	Oui	Oui	ROM 22.875kB RAM 2.871kB		Oui

Dans ce tableau, nous constatons que pour le protocole d'authentification basé sur la cryptographie à clé symétrique utilisant une carte à puce, il résiste aux attaques DOS, man in the middle et aux attaques de répétition. Il y a aussi la présence d'authentification mutuelle garantissant l'accord de clé sans optimiser la consommation d'énergie.

Alors que le protocole d'authentification basé sur la cryptographie à clé asymétrique basé sur ECC résiste aux attaques DOS, man in the middle at aux attaques de répétition. Sauf que ECC ne garantit plus la sécurité avec les accords de clé et l'optimisation de la consommation d'énergie. Nous constatons aussi que le protocole d'authentification basé sur la cryptographie à clé asymétrique basée sur ECC est plus résistant aux attaques de répétitions qu'aux autres types d'attaques.

4.4. Authentification sécurisée basée sur la blockchain avec des performances améliorées pour le Fog Computing

4.4.1. Méthodologie proposée

Le système proposé utilise la blockchain Neo, des contrats intelligents et des registres pour, fournir une authentification décentralisée pour l'IoT et le calcul du brouillard. Les nœuds de brouillard exécutent des tâches de blockchain et conservent une copie des contrats intelligents et des registres décentralisés. L'architecture globale du schéma proposé est donnée dans 35.

Le système commence par la procédure dans laquelle un utilisateur envoie la demande d'authentification via l'utilisateur ou le périphérique. Cet appareil périphérique est connecté à

l'appareil de brouillard via un réseau. Le dispositif de brouillard est connecté aux nœuds de la blockchain et a accès au module d'exécution de contrat intelligent.

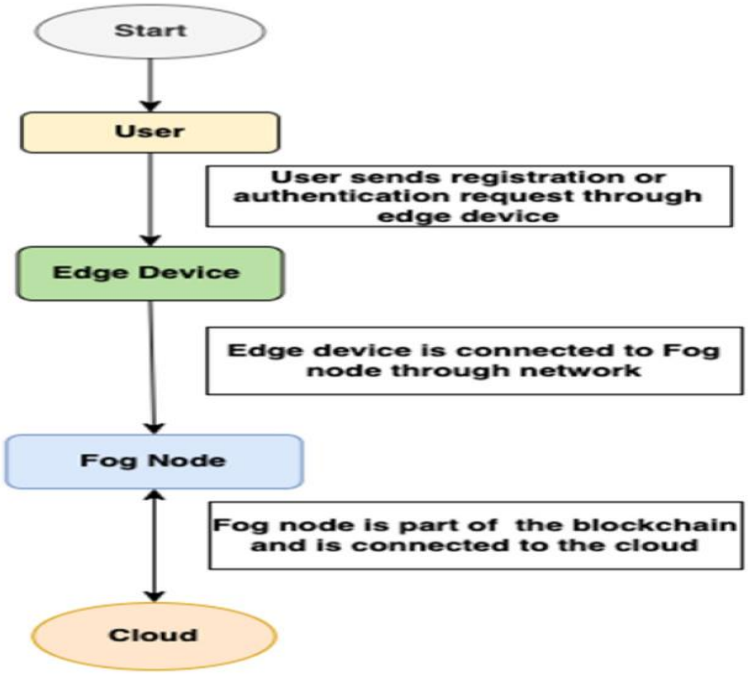


Figure 35 Organigramme de l'architecture globale du système proposé

4.4.2. Architecture du système

Le système d'authentification décentralisé proposé est décrit dans cette section, ainsi que les tâches qu'ils accomplissent. L'architecture complexe du système proposé est illustrée dans la figure 36. Il montre le système d'authentification construit sur la blockchain Neo utilisant des dispositifs de périphérie et de brouillard. Les composants impliqués dans cette architecture sont décrits ci-dessous :

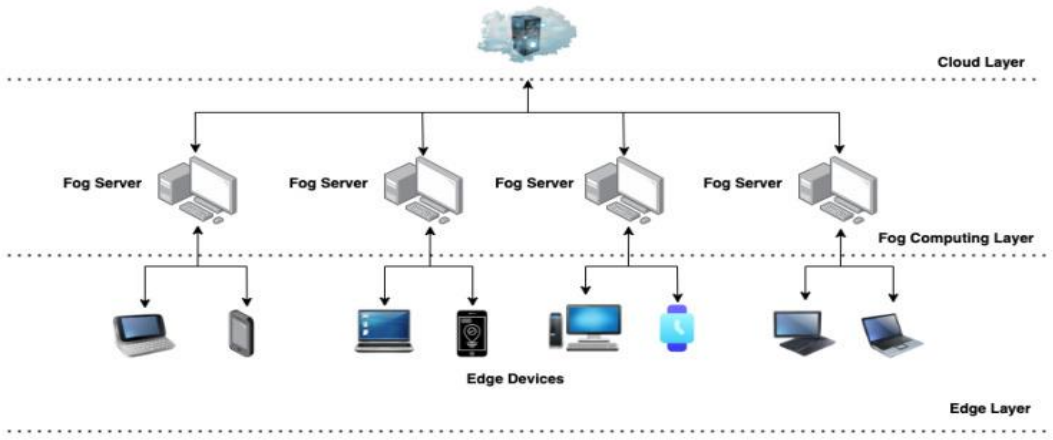


Figure 36: Système d'authentification basé sur la blockchain Neo et le Fog computing

4.4.2.1. Contrat Néo Smart

Les tâches d'authentification et d'enregistrement sont exécutées par le contrat dans ce système.

Le contrat nécessite des données telles que Username, Password et UserNeoAddress lors de l'enregistrement et de l'authentification et lorsque l'utilisateur interagit avec le système par la suite.

4.4.2.2. Nœud de brouillard

Il existe plusieurs nœuds de brouillard dans le réseau qui agissent comme des nœuds de blockchain, chacun ayant une copie de blockchain, ledger et SmartContract edger.

Une transaction d'enregistrement ou d'authentification Blockchain via un nœud de brouillard met à jour le grand livre pour les transactions Blockchain. Afin de pouvoir héberger ou faire partie de Blockchain, ces appareils ou serveurs de brouillard doivent répondre aux spécifications requises.

4.4.2.3. Utilisateurs

Pour que l'authentification et l'enregistrement réussissent, l'utilisateur doit fournir des données valides et effectuer une série de tâches. Un nom d'utilisateur, un mot de passe et une adresse UserNeoAddress valides doivent être fournis pour ces tâches.

4.4.2.4. Appareils périphériques

Lors de l'enregistrement et de l'authentification, ce sont les appareils des utilisateurs qui n'ont pas suffisamment de ressources pour héberger la blockchain.

4.4.2.5. Nuage

Les données sont les principales caractéristiques du cloud, qui est souvent décrit comme une grande unité de stockage capable d'héberger, de stocker et de calculer des données. Lors de la réception des données générées par les appareils IoT, Edge et Fog, ce serveur cloud les traite pour analyse et traitement.

4.4.3. Fonctionnement du système proposé

Le fonctionnement du système d'authentification proposé est décrit dans cette sous-section.

- ❖ Initialisation :

Dans le cadre du processus d'inscription, un nouvel utilisateur doit appliquer tous les facteurs nécessaires au fonctionnement du système d'authentification. Ces paramètres initialisés par la blockchain Neo sont valides UserNeoAdr (avec Neo Gas), Username et Password.

- ❖ Enregistrement de l'utilisateur

Afin de terminer la phase d'inscription, un nouvel utilisateur envoie une demande d'inscription et est invité à fournir un nom d'utilisateur et un mot de passe, ainsi que UserNeoAdr, à BlockChainNet ; les données sont transférées via le SmartContract et stockées dans le Ledger.

La blockchain identifie l'utilisateur comme un utilisateur valide et le Ledger stocke les données fournies par l'Utilisateur sur la blockchain. La figure 37 montre le processus d'enregistrement de l'utilisateur.

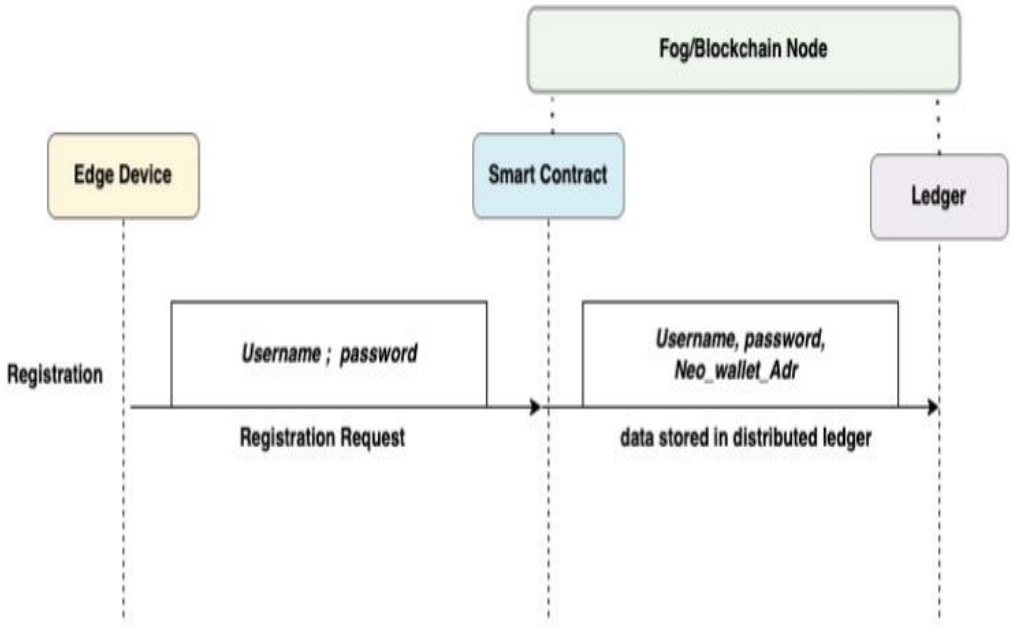


Figure 37 : Diagramme de flux pour l'enregistrement des utilisateurs

- Authentification d'utilisateur

Lorsque la phase d'authentification commence, l'utilisateur envoie une demande d'authentification avec le nom d'utilisateur et le mot de passe, et l'utilisateur doit également soumettre une UserNeoAddress valide. Dans le cadre de la blockchain, l'utilisateur est vérifié via le SmartContract et le Ledger.

Les données présentées par l'utilisateur déterminent si la tentative d'authentification est réussie. Des données valides sont requises de la part de l'utilisateur pour que l'authentification réussisse. Une représentation de l'authentification de l'utilisateur peut être trouvée dans la figure 38. Pour s'authentifier avec succès, l'utilisateur doit fournir des données qui correspondent aux paramètres requis par le système. Si l'authentification n'est pas réussie, l'utilisateur obtient une autre opportunité.

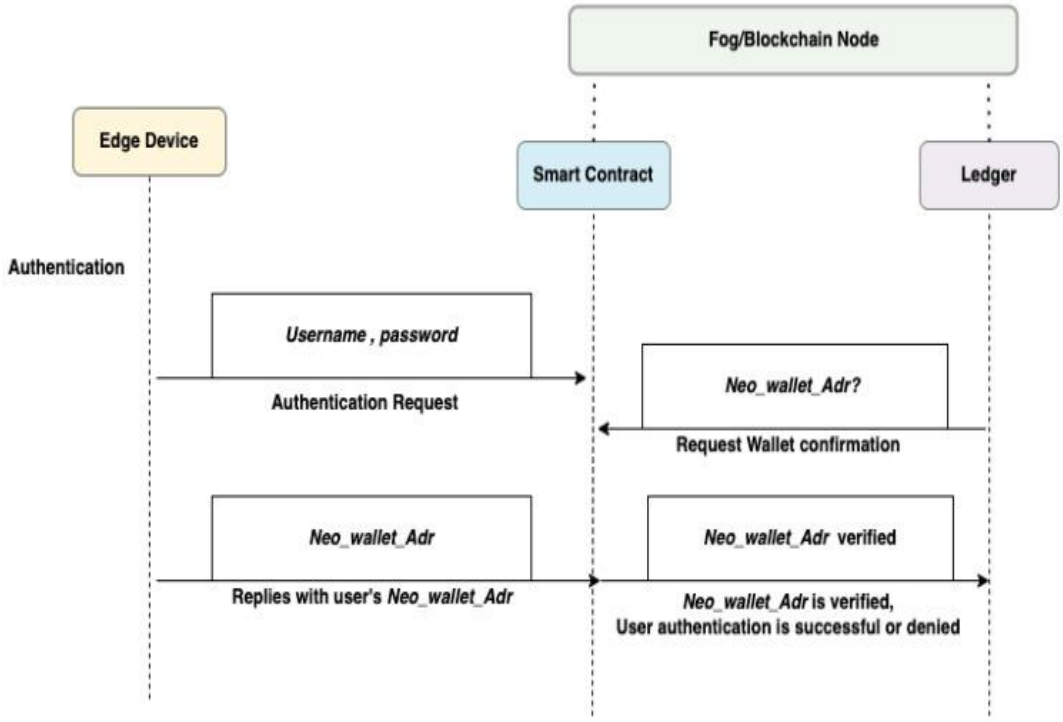


Figure 38 : Diagramme de flux pour l'authentification de l'utilisateur

4.5. Étude d'un nouveau protocole d'authentification basé sur la blockchain dans l'IoT

4.5.1. Schéma d'authentification basé sur la technologie blockchain dans l'IoT

a) L'authentification dans les WSN

Les réseaux de capteurs sans fil (WSN, une partie importante de l'IoT) se composent de nœuds de capteurs avec des capacités de traitement, de mémoire et d'énergie limitées. Les réseaux de capteurs sans fil font face à de nombreux dangers, car ils sont souvent distribués dans des régions non fiables. L'exactitude des données obtenues dans un WSN, où les menaces de sécurité ne peuvent être évitées, est également remise en question. Dans les WSN, l'authentification des ressources et des données peut être vérifiée avec le mécanisme d'authentification. L'authentification dans les WSN permet au nœud de vérifier si les données ont été envoyées à partir de sources autorisées et protège les données d'origine contre les modifications. Cependant, il existe certaines lacunes en termes de sécurité dans les protocoles d'authentification existants, telles que les attaques d'usurpation d'identité. De plus, la blockchain, l'une des technologies émergentes, donne des résultats significatifs dans les applications de sécurité. Sécurisé cryptographiquement, immuable, non répudiable, irrévocable, auditable et vérifiable peuvent être donnés comme caractéristiques liées à la sécurité de la blockchain.

Dans cette étude, un nouveau protocole d'authentification basé sur la blockchain a été développé pour les WSN. Sur la base du modèle de système de l'étude (figure 39), des nœuds de capteurs, des nœuds de cluster, une station de base et des réseaux de chaînes de blocs ont

été créés à l'aide d'une chaîne de blocs privée et d'utilisateurs. Une analyse de sécurité détaillée a été effectuée pour l'étude.

b) Architecture proposée :

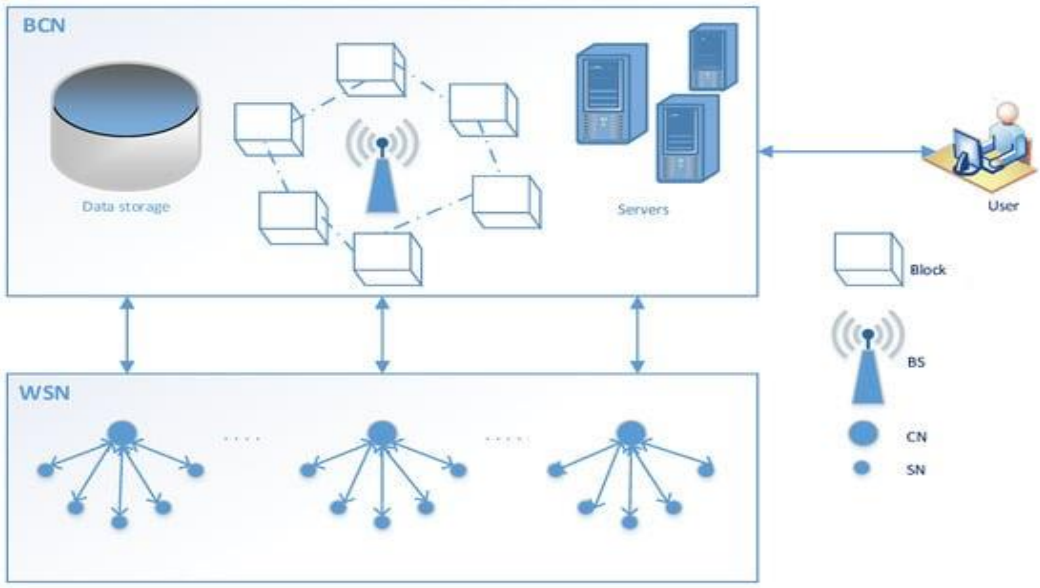


Figure 39: Modèle du système

Les réseaux de capteurs sans fil se composent de nœuds de capteurs, de nœuds de cluster, d'une station de base et d'un utilisateur. Les SN ont des capacités de calcul limitées, une énergie limitée et une capacité de stockage limitée. Les SN assurent la fonction de détection et la transmettent à leur CN leader. Les CN reçoivent les données transmises et les transmettent à la BS.

- ❖ Les acteurs du modèle

Dans le modèle de système proposé, il y a quatre acteurs différents. Il s'agit du nœud de capteur (SN), du nœud de cluster (CN), de la station de base (BS) et de l'utilisateur (U).

- ✓ SN : cela fait référence aux nœuds capteurs dans l'environnement. Ces nœuds transmettent les valeurs qu'ils perçoivent de l'environnement au CN dont ils sont membres. Les capacités et les énergies de traitement sont limitées.
- ✓ CN : il fait référence au nœud de cluster. Il transmet les données envoyées par les SN de son cluster à la BS. Les capacités et les énergies de traitement sont limitées dans les CN en tant que SN car les CN agissent comme des routeurs entre le SN et la BS.
- ✓ BS : cela fait référence à la station de base. Il reçoit les données transmises par les CN. Ces données sont également traitées sur le réseau blockchain. La BS est considérée comme illimitée en termes d'énergie, de mémoire et de capacité de traitement.
- ✓ U : il fait référence à l'utilisateur final. Il peut surveiller le WSN en se connectant au réseau quand il le souhaite.

- ❖ Mécanisme :

Cette étude utilise le mécanisme de consensus Proof of Authentication (PoAh). Le PoAh se compose de deux étapes. Dans la première étape, la source du bloc est authentifiée. Dans la deuxième étape, la valeur de confiance de chaque nœud d'authentification est augmentée de 1. Si le nœud s'authentifie de manière incorrecte, la valeur de confiance est diminuée de 1. Ensuite, le bloc validé est transmis à tous les nœuds pour mise à jour. La raison de l'utilisation de PoAh dans cette étude est qu'elle est plus efficace en fonction de la consommation d'énergie, des exigences du processus et des critères de délai par rapport à des mécanismes tels que PoW, PoS et PoA.

❖ Protocole utilisé

Le protocole proposé se compose de quatre étapes, qui sont la section d'initialisation, où les valeurs initiales sont générées, la section d'enregistrement, où les nœuds du réseau sont enregistrés, la section d'authentification, où les nœuds du réseau sont vérifiés, et la désinscription. Section, qui est la suppression des nœuds quittant le réseau pour une raison quelconque. Les opérations à ces étapes sont automatiques. L'ensemble du processus est effectué sous le commandement de la station de base. Les mêmes opérations sont répétées pour les nœuds concernés si de nouveaux nœuds sont ajoutés au réseau. Enfin, les informations de nœud nouvellement rejoint sont annoncées au réseau. Toutes les informations nécessaires pour le réseau telles que les identités des nœuds et les mappages SN-CN sont signalées aux nœuds par la station de base.

- Phase d'initialisation :

À ce stade, la BS prépare tous les nœuds. Chaque nœud a son propre ID unique. L'ID du nœud capteur i est spécifié comme IDSNi. L'ID du nœud de cluster i est spécifié comme IDCNi, tandis que l'ID du nœud BS est spécifié comme IDBS. La BS génère des clés publiques et privées pour SN-CN et pour elle-même. Les clés publiques et privées du nœud BS sont spécifiées comme PBKBS, PVKBS, les clés publiques et privées du nœud CN sont spécifiées comme iPBKCNi, PVKCNi, et les clés publiques et privées du nœud SN i sont spécifiées comme PBKSNi, PVKSNi.

Les clés sont utilisées pour vérifier l'intégrité des messages envoyés lors de la vérification et de l'enregistrement. Les informations ID et PVK des nœuds de capteur et de cluster sont transmises sous forme d'ID et de PVK dans un environnement sécurisé pour être stockées aux nœuds concernés. La carte d'identité est produite pour les CN. La carte d'identité comprend une signature créée à l'aide d'IDCNi, de PVKBS et de l'algorithme de signature numérique à courbe elliptique (ECDSA). Comme on le sait, l'algorithme de signature numérique à courbe elliptique (ECDSA) est un algorithme de signature numérique (DSA) qui utilise le cryptage à courbe elliptique. Sur la figure 40, le diagramme de séquence de la partie d'initialisation est donné.

La figure 40 illustre le déroulement de cette phase.

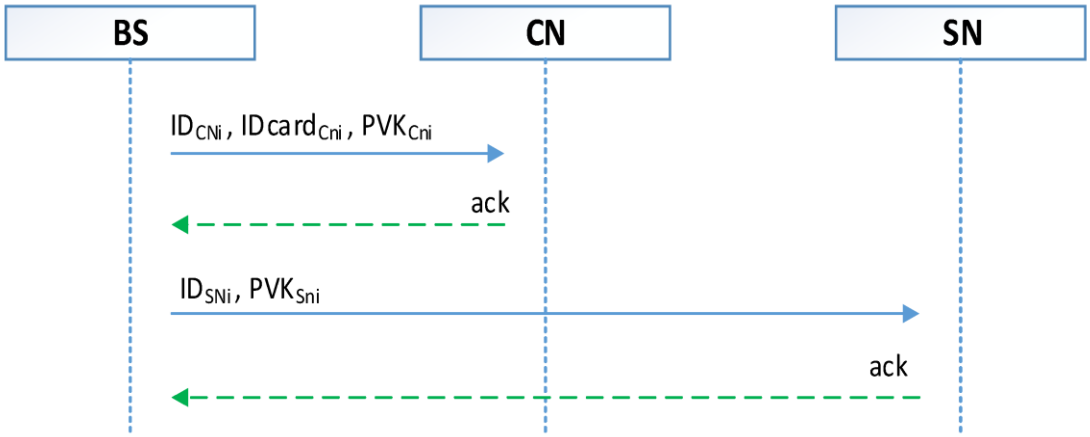


Figure 40: Diagramme de séquence de l'initialisation

- Phase d'inscription :

Après l'initialisation du réseau, il est temps de s'inscrire. Les CN demandent l'enregistrement en transmettant les informations IDCNi, IDcardCni et Time à BS. Ensuite, le contrat intelligent (algorithme 1) dans le BCN est déclenché. Tout d'abord, les informations de temps sont vérifiées. Ensuite, il est vérifié si le CN est enregistré dans le BCN. Enfin, IDCNi et PBKBS sont utilisés pour authentifier la carte d'identité. Si la vérification a lieu dans tous ces processus, le CN sera enregistré auprès du BCN.

Algorithme 1 : Enregistrement CN

Commencer

si time_check = erreur ; retourne l'erreur () ;

si ID $_{CNi}$ _check = erreur ; retourne l'erreur() ;

si IDcard $_{Cni}$ _check = erreur; retourne l'erreur() ;

enregistrer(ID $_{CNi,}$ IDcard $_{Cni}$);

Fin

Bien que les contrats intelligents puissent être utilisés dans les communications CN-BS/BCN, ces transactions ont été effectuées avec ECC car les communications SN-CN ont une capacité de stockage, de traitement et d'énergie insuffisante. La cryptographie à courbe elliptique est préférée car elle offre une sécurité élevée avec de faibles coûts de transaction [116]. Chaque SN du WSN est membre d'un seul CN. Les SN transmettent les informations IDSNi, Messageencyrypted et Time à des CN prédéterminés. Les CN vérifient d'abord les informations horaires. Ensuite, en utilisant le propre PVKSNi du nœud, ils vérifient le message chiffré avec

PBKSNi. S'il n'y a pas de problème jusqu'à présent, le CN envoie les informations IDCNi, IDSNi, IDcardCni et Time à la BS et demande la demande d'enregistrement du SN. Ensuite, le contrat intelligent (algorithme 2) dans le BCN est déclenché. Tout d'abord, les informations de temps sont vérifiées. Ensuite, il est vérifié si le CN et le SN sont enregistrés dans le BCN. Enfin, IDCNi et PBKBS sont utilisés pour authentifier la carte d'identité. Si la vérification se produit dans tous ces processus, le SN pertinent est enregistré auprès du BCN. Sur la figure 41, le diagramme de séquence de la partie d'enregistrement est donné.

Algorithme 2 : Enregistrement SN

Commencer

si time_check = erreur ; retourne l'erreur () ;

si ID $_{CNi}$ _check = erreur ; retourne l'erreur () ;

si ID $_{SNi}$ _check = erreur ; retourne l'erreur () ;

si IDcard $_{Cni}$ _check = erreur ; retourne l'erreur () ;

registre (ID $_{SNi,}$ ID $_{Cni}$);

Fin



Figure 41: Diagramme de séquence de l'enregistrement

- Authentification :

Lorsque le SN numéro i veut interagir avec le CN dont il est membre, une authentification bidirectionnelle doit être effectuée en établissant un canal sécurisé IDSNi-IDCNi entre deux nœuds. IDSNi envoie un message de demande de connexion IDSNi, message chiffré, Time au CN dont il est membre. Le CN vérifie d'abord les informations de temps. Ensuite, en utilisant le propre PVKSNi du nœud, il vérifie le message chiffré avec PBKSNi. S'il n'y a pas de problème jusqu'à présent, le CN envoie les informations IDCNi, IDSNi, IDcardCni et Time à la BS et demande une vérification. Ensuite, le contrat intelligent (algorithme 3) dans le BCN est déclenché. Tout d'abord, les informations de temps sont vérifiées. Ensuite, il est vérifié si le CN et le SN sont enregistrés dans le BCN. Ensuite, IDCNi et PBKBS sont utilisés pour authentifier la carte d'identité. Enfin, on vérifie si l'IDSNi est membre de l'IDCNi.

Les algorithmes [3] et [4] nous montrent la procédure d'authentification.

Algorithme 3 : Authentification CN-SN

Commencer

si time_check = erreur ; retourne l'erreur () ;

si ID $_{CNi}$ _check = erreur ; retourne l'erreur () ;

// Le nœud est-il actif ?

// Le nœud est-il enregistré ?

si ID $_{SNi}$ _check = erreur ; retourne l'erreur () ;

// Le nœud est-il actif ?

// Est-ce que SN est membre du CN ici ?

si IDcard $_{Cni}$ _check = erreur ; retourne l'erreur () ;

// Les informations de signature sont-elles correctes ?

Retourner vrai ; //

Fin de connexion sécurisée

L'utilisateur U peut demander l'accès au BCN avec l'identifiant qui lui a été fourni. Le contrat intelligent (algorithme 4) est déclenché lorsque la demande arrive. En cas d'accord de cette

manière, U peut accéder au BCN. Un canal sécurisé est établi entre U et le BCN. Sur la figure 42, le diagramme de séquence de la section d'authentification est donné.

Algorithme 4 : authentification par algorithme 4 U

Commencer

si time_check = erreur ; retourne l'erreur () ;

si ID $_U$ _check = erreur ; retourne l'erreur () ;

// si autorisation OK

retourne true ;

//

Fin de connexion sécurisée

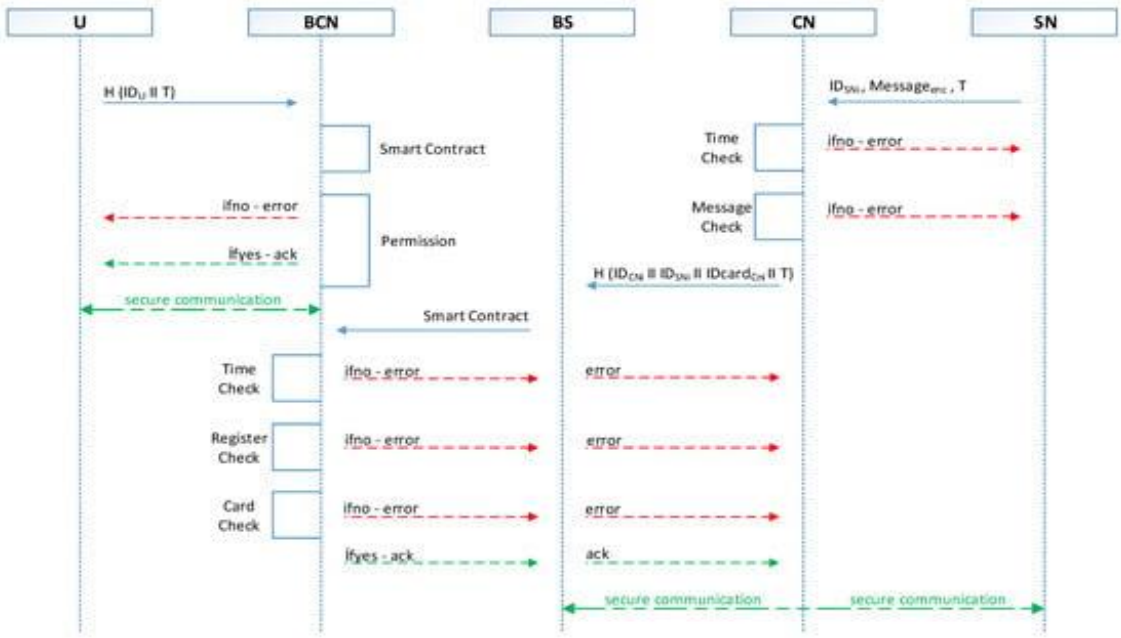


Figure 42 : Diagramme de séquence de l'authentification

- Désinscription :

Les SN qui sont membres des CN sont connus par les CN. Les CN tentent de communiquer avec des nœuds qui ne leur ont pas envoyé de messages depuis un certain temps. Si la communication ne se produit pas correctement, des résultats tels que l'épuisement, la corruption, la saisie et l'exposition de l'énergie du nœud aux attaques peuvent se produire. Dans

un tel cas, le CN demande au BCN l'annulation du nœud avec l'ID du nœud correspondant. Ensuite, le contrat intelligent (algorithme 5) est déclenché et une fois les processus de vérification terminés, il exécute le processus d'annulation.

Algorithme 5 : désinscription du SN

Commencer

si time_check = erreur ; retourne l'erreur () ;

si ID $_{CNi}$ _check = erreur ; retourne l'erreur () ;

si ID $_{SNi}$ _check = erreur ; retourne l'erreur () ;

si IDcard $_{Cni}$ _check = erreur ; retourne l'erreur () ;

Supprimer (ID $_{SNi}$) ;

Fin

4.5.2. Notre solution pour sécuriser la communication des objets connectés contre les attaques à répétition

Comme tous les réseaux informatiques, l'internet des objets fait aussi l'objet de différentes attaques. La meilleure solution pour protéger les informations circulant dans le réseau avec la technologie blockchain est d'utiliser la cryptographie asymétrique basée sur ECC. Car c'est une solution de sécurité qui est relativement beaucoup plus sûre. Les techniques appliquées doivent répondre aux exigences principales de sécurité telles que :

- L'authentification : qui consiste à protéger le réseau contre les attaques de vol d'identité en vérifiant bien que le nœud qui est déclaré est effectivement celui qu'il prétend être.
- L'intégrité : qui consiste à vérifier que les données n'ont pas été altérées pendant la transmission.
- La confidentialité : qui s'assure de ne pas faire circuler les données entre les nœuds en clair, que les attaquants ne puissent ni les comprendre, ni les interpréter.

Ainsi l'étude du tableau 7 nous a permis de porter notre choix sur la cryptographie asymétrique basée sur ECC. En effet, la cryptographie asymétrique utilise deux clés différentes, à savoir l'un pour le chiffrement et l'autre pour le déchiffrement message qui doit être envoyé et chiffré avec la clé publique puis diffusé dans l'ensemble du réseau et enfin à sa réception le message est déchiffré avec la clé privée du destinataire.

La cryptographie donne aussi la possibilité de messages chiffrés. Dès lors, si l'émetteur envoie un message chiffré au destinataire alors ce dernier le déchiffre avec sa clé privée. Ensuite, l'émetteur va vérifier la signature avec sa clé publique pour tester. Si l'authentification échoue, cela veut dire qu'elle sera rejetée.

Voilà en quelque sorte notre contribution pour pallier les problèmes de la sécurisation des objets connectés avec blockchain.

4.6. Conclusion et perspective

Dans ce chapitre nous, avons pu étudier quelques protocoles d'authentification qui servent à sécuriser les communications entre les objets connectés, ainsi que la résistance de ces derniers face à certains types d'attaques. Dans cette étude, nous avons décrit le fonctionnement des deux méthodes d'authentification étudiées, à savoir l'une basée sur la cryptographie symétrique et l'autre basée sur la cryptographie asymétrique.

Néanmoins, le nombre croissant d'objets connectés contraints, ou IoT, accentue le besoin d'avoir un meilleur compromis entre sécurité et performance qui n'étaient pas au centre de l'élaboration des premiers standards de cryptographie sur les courbes elliptiques.

Une des problématiques majeures de sécurité de ces nouveaux objets connectés est liée aux attaques dites physiques. Ce biais d'attaque dans le domaine de la cryptographie sur les courbes elliptiques amène de nouveaux enjeux lors d'une implémentation sur les courbes elliptiques. Or, il est très difficile d'ajouter des protections à une implémentation ou une arithmétique déjà existante sans en dégrader les performances. Malgré tout, l'ajout de contremesures est nécessaire pour garantir la sécurité d'une implémentation d'un algorithme cryptographique sur les courbes elliptiques dans un environnement IoT. Une cryptographie prenant en compte ces problématiques dès sa conception permettrait de garantir plus aisément une sécurité physique tout en garantissant des performances acceptables pour des objets IoT contraints.

C'est ainsi que nous avons proposé qu'un nouveau protocole d'authentification basé sur la blockchain a été développé pour les WSN avec ces mécanismes et algorithmes utilisés afin de pallier les attaques physiques rencontrées dans le monde de l'internet des objets.

Conclusion générale

L'IoT est considéré comme la prochaine étape vers l'évolution d'internet. Il a la capacité de se connecter et de communiquer sur internet pour augmenter l'information partagée. À l'aide de capteurs, l'IoT a la capacité de collecter, d'analyser et de déployer une quantité énorme de données qui seront à leur tour converties en des informations et des connaissances utiles pouvant être utilisé pour créer de nouvelles applications et de nouveaux services pour améliorer notre qualité de vie. Pour atteindre un bon niveau de protection dans l'IoT, tout en ayant une bonne qualité des données protégées de nombreuses approches ont été proposées dans ce concept, la blockchain avec ces avantages est une bonne solution pour la sécurité pour cela elle a bien été intégrée dans l'IoT et dans la majorité de ces approches.

La sécurité des données et l'exploration des données doivent figurer en tête de la liste des caractéristiques de sécurité de l'IoT à travers l'authentification. Il s'agit de la première étape pour empêcher tous les nœuds non authentifiés d'accéder aux appareils du réseau IdO. L'authentification fait face à plusieurs types d'attaque comme l'usurpation d'identité pouvant nuire au respect de la vie privée.

Plusieurs méthodes d'authentification des nœuds ont été proposées pour répondre aux questions de sécurité. Néanmoins, la plupart de ces solutions sont centralisées et souvent vulnérables face aux attaques de type DoS/DDoS. La technologie décentralisée offre d'énormes possibilités, notamment sur les questions de la sécurité. C'est dans cet élan que les chercheurs s'intéressent de plus en plus à cette technologie et ne cessent de proposer des protocoles et des schémas d'authentification pour les objets connectés.

Dans ce mémoire, nous avons passé en revue un bon nombre de ces protocoles et nous avons fait une analyse par rapport aux vulnérabilités des objets connectés. Ces méthodes ne peuvent cependant pas garantir une authentification à long terme à cause de l'évolutivité des objets connectés. Pour faire face à ces problèmes, nous avons proposé un nouveau protocole d'authentification de sécurité robuste qui est conçu par les auteurs proposent une conception d'architecture de haut niveau d'un système de protection résistant à plusieurs attaques, basé sur la blockchain et l'IoT, qui peut aider à traiter les trois types de propriétés, à savoir l'authentification, l'intégrité et la confidentialité des données.

BIBLIOGRAPHIE et REFERENCE

[1] Rolf H. Weber, “Internet of Things – New Security and Privacy Challenges,” Computer Law & Security Review 26, no. 1 (January 1, 2010): 23–30,

[2] Hamed HaddadPajouh, Ali Dehghantanha, Reza M. Parizi, “A Survey on Internet of Things Security: Requirements, Challenges, and Solutions - ScienceDirect,”

[3] I. Saleh : Les enjeux et les défis de l’Internet des Objets (IdO). In: Internet des objets (2017).

[4] Weber, Rolf H., et Evelyne Studer. « Cybersecurity in the Internet of Things: Legal Aspects ». Computer Law & Security Review 32, no 5 (1 octobre 2016): 715-28.

[5] D. Singh, G. Tripathi, & A. J. Jara: A survey of Internetof-Things: Future vision, architecture, challenges and services. In: In Internet of things (WF-IoT), world forum on IEEE (2014).

[6] A., Mayuri, et Sudhir T. « Internet of Things: Architecture, Security Issues and Countermeasures ». International Journal of Computer Applications 125, no 14 (17 septembre 2015): 1-4. https://doi.org/10.5120/ijca2015906251.

[7]https://courses.minnalearn.com/fr/courses/emerging-technologies/the-internet-of-things/an-introduction-to-the-internet-of-things/

[8]https://books.google.sn/books?id=3h1VEAAAQBAJ&lpg=PA57&ots=0rmauGWnWc&dq=domaines%20d'application%20de%20l'IoT&lr&pg=PA58#v=onepage&q=domaines%20d'application%20de%20l'IoT&f=false

[9]https://dspace.univ-guelma.dz/jspui/bitstream/123456789/11760/1/ALLELE_IMANE_F5_Informatique.pdf

[10] https://books.openedition.org/editionsmsh/84

[11]http://www.wikiwai.com/informatique-technologie/materiel_et_internet_des_objets/internet_des_objets_industriels/2020/supernova/internet-des-objets-architectures-protocoles-et-applications/

[12] file:///C:/Users/DELL/Downloads/2021LIMO0037%20(1).pdf

[13] https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/

[14] https://azure.microsoft.com/fr-fr/solutions/iot/iot-technology-protocols/

[15]https://www.alain-bensoussan.com/avocats/internet-des-objets-iot-enjeux/2016/09/06/

[16] https://blog.wallix.com/fr/securiser-l-iot-objets-connectes

[17] https://www.ovhcloud.com/fr-sn/learn/what-is-iot/

[18] https://www.maxicours.com/se/cours/les-objets-connectes/

[19] https://wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/

[20]https://www.google.com/search?q=M%C3%A9moire+fin+d%27%C3%A9tude+sur+IoT&ei=m6fWY8-

SCYiSxc8P1MaumA4&start=10&sa=N&ved=2ahUKEwiPzNz3oe38AhUISfEDHVSjC-MQ8NMDegQIBRAW&biw=1280&bih=648&dpr=1.5

[21] http://dspace.univ-bouira.dz:8080/jspui/bitstream/123456789/9310/1/Binder1.pdf

[22] Taleb Omar et Mankouri Abdelkrim, Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp, Mémoire Pour l'obtention du diplôme de MASTER Spécialité: Réseaux et Systèmes de Télécommunication, Université Abou BakrBelkaid Tlemcen, pp 7-13, 2016.

[23]https://www.academia.edu/73935424/Les_enjeux_et_les_d%C3%A9fis_de_l_Internet_des_Objets_IdO_

[24] Yassine HADDAB Professeur à l‟‟Université de Montpellier, Introduction à l‟‟internet des objets (IdO – IoT).

[25]https://www.ummto.dz/dspace/bitstream/handle/ummto/12608/LarrasMelissa.pdf?sequence=1&isAllowed=y

[26] https://learn.microsoft.com/fr-fr/azure/iot-fundamentals/iot-security-ground-up

[27] https://hal.science/cel-01965300/document

[28] http://archives.univ-biskra.dz/bitstream/123456789/13229/1/djeffal_leila.pdf

[29] http://dspace.univ-tlemcen.dz/bitstream/112/15750/1/Ms.Tel.RABHI.pdf

[30] https://techno-skills.com/le-piratage-dobjets-iot/

[31]https://iotsecurity2018.ca/wp-content/uploads/2019/03/OTA-top-iot-vulnerabilities_FR_REV_V2-March-2019.pdf

[31]https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.fgcsecurity.com%2Fowasp-top-10-de-vulnerabilidades-del-internet-de-las-cosas-iot%2F&psig=AOvVaw34CyhLYTXzeMAflw2wE4Th&ust=1675602687579000&source=images&cd=vfe&ved=0CA0QjRxqGAoTCKjTrcz4-_wCFQAAAAAdAAAAABDIAQ

[32] https://blog.octo.com/iot-et-securite-une-union-impossible/

[33]https://www.pingidentity.com/fr/resources/cybersecurity-fundamentals/threats/internet-of-things-attack.html

[34]https://www.placesdaffaires.com/les-10-cybermenaces-auxquelles-linternet-des-objets-iot-est-particulierement-vulnerable/

[35]https://iotindustriel.com/cybersecurite/cybersecurite-dans-liot-attaques-et-preventions/

[36] Yassine HADDAB Professeur à l‟‟Université de Montpellier, Introduction à l‟‟internet des objets (IdO – IoT).

[37] Mlle CHALAL Lina et M. SIROUAKNE Slimane, Gestion des clés dans l'internet des objets, Master en informatique, Spécialité : Réseaux et Systèmes Distribués.

[38] El Mouaatamid, O., Lahmer, M., & Belkasmi, “Internet of Things Security: Layered classification of attacks and possible Countermeasures’’, electronic journal of information technology (9), 2016

[39] file:///C:/Users/DELL/Downloads/BAYATE_BAYATE.pdf

[40] A. ARFAOUI “Context-Aware and Adaptive Security Solutions for the Internet of Things’’, université de Bourgogne, 15, 2019

[41] https://pastel.archives-ouvertes.fr/tel-01997261/document

[42]https://www.journaldunet.com/ebusiness/internet-mobile/1516265-securisation-de-l-iot-a-grande-echelle-comment-l-infrastructure-a-cles-publiques-pki-peut-aider/

[43] https://www.forceplus.com/blog/iot-blockchain-technologies-opportunite

[44] https://blogs.manageengine.com/fr/2022/12/16/comment-la-blockchain-releve-t-elle-les-defis-presentes-par-les-applications-iot.html

[45] G. ALI, N. AHMAD, Y. CAO, M. ASIF, H. CRUICKSHANK, AND Q. E. ALI, Blockchain based permission delegation and access control in internet of things (baci), Computers & Security, 86 (2019), pp. 318–334.

[46] https://www.sciencedirect.com/science/article/abs/pii/S1084804519303418

[47]https://www.taylorfrancis.com/books/edit/10.1201/9781003081487/blockchain-technology-applications-pethuru-raj-kavita-saini-chellammal-surianarayanan?refId=94a787ad-8c31-4639-a79b-5c4b58665a76&context=ubx

[48]https://youmatter.world/fr/definition/blockchain-definition-fonctionnement-et-domaines-application/

[49] https://academy.binance.com/fr/articles/history-of-blockchain

[50] https://www.leewayhertz.com/what-is-blockchain/

[51] https://www.ibm.com/fr-fr/topics/what-is-blockchain

[52] https://www.institutdesactuaires.com/magazine/article/schema-de-fonctionnement-de-la-blockchain/2371

[53] https://www.avg.com/fr/signal/what-is-blockchain

[54]https://www.lafinancepourtous.com/decryptages/finance-et-societe/nouvelles-economies/blockchain/quest-ce-que-la-blockchain/

[55]https://www.aura-niort.fr/wp-content/uploads/2022/01/memoire-Excelia-C.Moinnault.pdf

[56] https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf

[57]https://www.spiria.com/fr/blogue/culture-geek/la-technologie-de-la-chaine-de-blocs-blockchain/

[58] https://www.crypto-sous.fr/blockchain-fonctionnement/hashing/

[59] https://www.splunk.com/fr_fr/data-insider/what-is-blockchain.html

[60] https://cryptoast.fr/qu-est-ce-que-la-blockchain/

[61] https://www.senat.fr/rap/r17-584/r17-584_mono.html

[62] https://coinacademy.fr/academie/algorithme-consensus-blockchain/

[63]https://www.researchgate.net/publication/349583511/figure/fig4/AS:994937059426307@1614222888997/Classification-of-Blockchain-Consensus-Algorithm-by-mechanism.ppm

[64] https://www.archipels.io/faq/proof-of-authority-definition

[65]http://dspace.univ-jijel.dz:8080/xmlui/bitstream/handle/123456789/8575/Inf.ILM.06-20.pdf?sequence=1&isAllowed=y

[66]https://www.researchgate.net/profile/Oussama-Ayadi/publication/335174496/figure/fig7/AS:792035095244802@1565847290645/Historique-de-la-technologie-Blockchain-Source-blockchain101com.jpg

[67] https://www.inria.fr/fr/essentiel-technologie-blockchain

[68]https://www.pourlasolidarite.eu/sites/default/files/publications/files/na-2019-technologie-blockchFain_0.pdf

[69]https://www.bitpanda.com/academy/fr/lecons/algorithmes-de-consensus-la-proof-of-stake/

[70] https://actualiteinformatique.fr/blockchain/definition-algorithme-de-consensus

[71]https://www.cryptopolitan.com/fr/qu-39-est-ce-qu-39-un-algorithme-de-consensus-blockchain/

[72] https://bitcoin.fr/quest-que-le-dpos/

[73] https://monte-crypto.fr/blockchain/ecosysteme-blockchain/

[74] http://archives.univ-biskra.dz/bitstream/123456789/18909/1/Rahmani_Rokia.pdf

[75]https://rivieresdusud.uasz.sn/bitstream/handle/123456789/1662/ndiaye_m%C3%A9moire_2022.pdf?sequence=1&isAllowed=y

[76]https://kriptomat.io/fr/blockchain/avantages-et-inconvenients-de-la-technologie-blockchain/

[77]Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, et L. He, « A Comparative Study of Blockchain Consensus Algorithms », J. Phys.: Conf. Ser., vol. 1437, no 1, p. 012007, janv. 2020, doi: 10.1088/1742-6596/1437/1/012007.

[78]https://www.usinenouvelle.com/article/blockchain-pourquoi-hyperledger-fabric-s-est-impose-chez-les-industriels.N1808527

[79] https://lehub.bpifrance.fr/comment-fonctionne-blockchain/

[80] https://www.kaspersky.fr/resource-center/definitions/what-is-cryptocurrency

[81]https://n26.com/fr-fr/blog/les-differentes-crypto-monnaies#:~:text=L'ether%20est%20la%20cryptomonnaie,Ether%20n'est%20pas%20plafonn%C3%A9.

[82]https://www.researchgate.net/publication/335174496_CHAPITRE_III_Etat_de_l%27art_de_la_Blockchain

[83] https://www.cairn.info/revue-realites-industrielles-2017-3-page-98.htm

[84] https://www.finance-investissement.com/nouvelles/actualites/les-defis-insoupconnes-de-la-blockchain/

[85] https://www.cairn.info/revue-realites-industrielles-2017-3-page-20.html

[86]https://www.researchgate.net/figure/Entreprises-implementant-la-Blockchain_fig14_335174496

[87] Kumar, N.M., Mallick, P.K.: Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. 132, 1815–1823 (2018)

[88] Y.Ait Mouhoub et F.Bouchebbah. Proposition d'un modèle de confiance pour l'Internet des objets. Mémoire master de l'université Abderrahmane Mira Bejaia, 21 Juin 2015.

[89] Taleb Omar, Mankouri Abdelkrim. « Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp », Mémoire de master, Université de Tlemcen, Algérie, 2016.

[90] https://www.sciencedirect.com/science/article/pi i/S2542660519302288.

[91] https://www.andese.org/actrad/images/blockchain.png

[92] http://bib.univ-oeb.dz:8080/jspui/bitstream/123456789/14289/1/m%C3%A9moire.pdf

[93] http://www.senat.fr/rap/r17-584/r17-5847.htm

[94]https://www.innovauto.org/systemes-embarques/la-securite-des-donnees-le-blockchain

[95] https://www.asprom.com/application/blockchain_1.pd

[96] https://www.merciyanis.com/post/blockchain-iot-et-tracabilite

[97]https://www.capdigital.com/wp-content/uploads/2018/05/living-things-cr-blockchain-iot-v10.pdf

[98] https://www.usine-digitale.fr/article/avis-d-expert-l-integration-de-la-blockchain-dans-l-iot-opportunites-et-limites.N592593

[99] http://archives.univ-biskra.dz/bitstream/123456789/18916/1/AZIZI_MIYADA.pdf

[100] https://www.orange-business.com/fr/magazine/la-blockchain-en-passe-de-securiser-les-objets-connectes

[101]https://www.linkedin.com/pulse/comment-liot-peut-il-tirer-parti-de-la-blockchain-iex-ec/?originalSubdomain=fr

[102] https://www.mdpi.com/2079-9292/11/14/2225

[103] https://files.stample.co/browserUpload/d671d1d4-7373-473a-a813-17950fd4a61e

[104] http://www.univ-usto.dz/theses_en_ligne/doc_num.php?explnum_id=3442

[105]https://coinrivet.com/fr/how-blockchain-technology-is-helping-to-prove-authenticity/

[106]353346629_BLOCKCHAIN_ET_IDENTIFICATION_NUMERIQUE_Restitution_des_ateliers_du_groupe_de_travail_blockchain_et_identite_BCID_Octobre_2020_Version_10

[107]https://pastel.archives-ouvertes.fr/tel-01997261v1/preview/75456_HAMMI_2018_archivage.pdf#page=2

[108]https://www.researchgate.net/publication/326094774_Bubbles_of_Trust_a_decentralized_Blockchain-based_authentication_system_for_IoT

[109]https://www.cgi.com/sites/default/files/pdf/or16277_block_chain_white_paper-fr.pdf

[110] https://doi.org/10.3390/app13031526

[111] file:///C:/Users/DELL/Downloads/s42452-020-04089-9.pdf

[112] https://link.springer.com/article/10.1007/s42452-020-04089-9

[113] Sogani, A.; Jain, A. Schéma d'authentification rapide et sensible à l'énergie utilisant un chiffrement basé sur l'identité dans les réseaux de capteurs sans fil. Clust. Calcul. 2019 , *22* , 10637–10648. [Google Scholar] [CrossRef]

[114] https://theses.hal.science/tel-00767028/document

[115]http://www.univ-bejaia.dz/xmlui/bitstream/handle/123456789/18154/m%C3%A9moire_nassim_yakoub_m2_rsd%20_ref_latex_v_complete%20%282%29.pdf?sequence=1&isAllowed=y

[116] Chang, Q. ; Zhang, Y.; Qin, L. Un protocole d'authentification de nœud basé sur ECC dans WSN. Dans Actes de la conférence internationale 2010 sur la conception et les applications informatiques, Qinhuangdao, Chine, 25-27 juin 2010 ; p. 1–4. [Google Scholar]

[117]https://depot-e.uqtr.ca/id/eprint/10563/1/eprint10563.pdf

[118] https://doi.org/10.1016/j.clsr.2016.07.002.