الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليـم العالـي والبحـث العلمـي

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia

Faculté des Sciences Exactes

Département d'Informatique

MEMOIRE DE MASTER

DOMAINE : Mathématiques et Informatique

FILIERE : Informatique

SPECIALITE : Réseaux et Systèmes Distribués

Thème

Protection des données dans l'Internet des Objets

Réalisé par :

- ***REDDAF Nassim***
- ***RAOUACHE Yakoub***

Devant le jury composé de :

Examinateur : **Dr. M.Mohammedi** M.C.B U.A/Mira Béjaia

Examinatrice : **Dr. K.Ouazine** M.C.B U.A/Mira Béjaia

Promotrice : **Dr. L. HAMZA** M.C.A U.A/Mira Béjaia

Promotion : 2020/2021

REMERCIEMENTS

Avant tout, louanges et remerciements au Dieu Tout-Puissant pour ses bénédictions tout au long de notre travail de recherche pour mener à bien ce projet.

Nous tenons à exprimer notre profonde et sincère gratitude à notre encadreur, le Dr Hamza Lamia, pour son soutien continu pour sa patience, sa motivation et ses immenses connaissances. Elle nous'a aidé pendant tout le temps de la recherche et de la rédaction de ce mémoire. Sans lui, nous ne serait pas en mesure d'atteindre ce succès.

Travailler avec vous a été un tel honneur.

Nous tenons à remercier vivement les membres du jury d'avoir consacrer de leur temps à la lecture de ce manuscrit, et d'accepter de juger et d'évaluer ce travail.

Une grande partie du mérite revient à notre parents qui nous'ont soutenu, encouragé non seulement dans cette thèse mais à chaque étape de notre vie, vous éclairez notre vie de votre présence et rien ne pourrons jamais vous remplacer, qu'Allah vous préserve et vous protège.

Enfin, nous tenons à remercier notre frères et sœurs, nos camarades de classe, nos amis et tous ceux qui ont contribué, même avec les plus petits efforts, à la réalisation de ce projet. si reconnaissant de t'avoir à nos côtés.

REDDAF Nassim

RAOUACHE Yakoub

TABLE DES MATIÈRES

Page

Table des figures **vi**

Liste des tableaux **vii**

Liste d'abréviations **viii**

Introduction **3**

1 Sécurité dans l'Internet des objets **3**

1.1 Aperçu sur l'Internet des objets 4

1.1.1 Historique 4

1.1.2 Definition 4

1.1.3 Composants 4

1.1.4 Domaine d'application 5

1.2 Sécurité dans l'IoT 6

1.2.1 Principaux objectifs de la sécurité dans IoT 6

1.2.2 Menaces sur l'IoT 7

1.2.2.1 Menaces généraux 7

1.2.2.2 Menaces sur la vie privée 8

1.2.2.3 Menaces sur les systèmes et l'environnement physique des objets 8

1.2.3 Dimensions de la sécurité de l'IoT 8

1.3 Conclusion 9

2 Blockchain **10**

2.1 Evolution de blockchain 11

2.2 Définitions 14

2.2.1 Blockchain 14

2.2.2 Bloc . . . 14
2.2.3 Transaction . . . 16
2.2.4 Nœud . . . 17
2.2.5 Adresse et porte-monnaie . . . 17
2.3 Fonctionnement de la blockchain . . . 18
2.4 Architecture de la Blockchain . . . 19
2.5 Types de blockchain . . . 20
2.6 Système blockchain . . . 20
2.7 Applications de blockchain . . . 20
2.8 Les défis de blockchain . . . 21
2.8.1 Évolutivité . . . 21
2.8.2 Perte de la vie privée . . . 22
2.8.3 Exploitation minière égoïste . . . 22
2.9 Conclusion . . . 23

3 Etat de l'art sur l'Internet des objets et la blockchain 24
3.1 Intégration Blockchain IoT (BIoT) . . . 25
3.1.1 Architectures de conception de l'infrastructure IoT de la blockchain 25
3.1.1.1 Conception de l'architecture IoT Peer to IoT Peer : . . . 26
3.1.1.2 Conception de l'architecture IoT Peer to Blockchain . . . 26
3.1.1.3 Conception d'une architecture hybride . . . 27
3.1.2 Scénarios d'intégration futurs pour BIoT . . . 28
3.1.2.1 Extension de l'espace d'adressage pour les appareils IoT 28
3.1.2.2 Contrôle d'accès intelligent basé sur un contrat et partage de données pour les systèmes IoT . . . 29
3.2 Applications BIoT . . . 30
3.2.1 Algorithmes cryptographiques pour les applications BIoT . . . 31
3.2.1.1 Cryptographie à clé publique . . . 31
3.2.1.2 Fonctions de hachage . . . 32
3.2.2 Algorithmes de consensus et leurs effets sur les objets connectés . 32
3.3 Défis actuels rencontrés dans les applications BIoT . . . 36
3.3.1 Anonymisation . . . 36
3.3.1.1 Anonymisation liée au modèle et algorithme matheuristiques . . . 36
3.3.1.2 Anonymisation liéé au apprentissage automatique . . . 37

3.3.2 Sécurité 38
3.3.3 Évolutivité, débit et latence 40
3.3.4 Calcul, traitement, taille de la blockchain, bande passante et infrastructure 40
3.3.5 Orientations et recommandations futures 40
3.4 Conclusion 42

4 Propostion et implèmentation **43**
4.1 Motivation 44
4.2 Approche proposée 44
4.2.1 Evaluation de la fitness 45
4.3 Description de l'algorithme proposé 46
4.4 Conception et Simulation 48
4.4.1 Description de l'application 48
4.4.2 Description de l'enemble de données test 50
4.4.3 Simulation et Discussion 51
4.5 Conclusion 53

Bibliography **55**

TABLE DES FIGURES

1.1 Domaines d'Internet des Objet. 6
1.2 Dimensions de la sécurité d'Internet des objets. 9

2.1 Fonctionnement des contrats intelligents 12
2.2 Structure d'un bloc 15
2.3 Enchainement des blocs 15
2.4 Arbre de Merkle 16
2.5 Fonctionnement de la blockchain 18
2.6 Réseau basé sur les Serveurs vs Réseau P2P 19

3.1 Les différences interactions entre les appareils IoT et les pairs 28
3.2 Organigramme du modèle de système proposé pour le contrôle d'accès intelligent basé sur un contrat 30

4.1 Diagramme de l'algorithme proposé 47
4.2 Interface graphique de l'application proposée 49
4.3 Echantillon de données originales (adult.data) 50
4.4 Aperçu des données test après l'étape de prétraitement 51
4.5 Perte d'informations en fonction de k 51
4.6 Perte d'informations en fonction de nombre de particules crées (k=2, nombre de cycle= 500) 52

LISTE DES TABLEAUX

2.1 Comparaison entre les différentes générations de blockchain 14

3.1 Comparaison entre les différents algorithmes de consensus et les blockchains qui les mettent en œuvre 35
3.2 Solutions de confidentialité de l'apprentissage machine basées sur la blockchain pour les appareils et réseaux IoT 38
3.3 Littérature sur les différentes approches de sécurité qui a été envisagées pour les applications BIoT 39

LISTE D'ABRÉVIATIONS

A	ACC	Contrôle des Contrats d'accès:(Access Aontracts Control).
	ANI	Autorité de Numérotation Internet.
B	$BIoT$	Blockchain Internt of Things.
C	CPS	Cyber-Physical Systems.
D	$DApps$	Des Applications Décentralisées .
	$DBFT$	Delegated Byzantine Fault Tolerance.
	DLT	Distributed Ledger Technology.
	$DPoS$	Proof of Stake Delegated.
E	ECC	Elliptical Curve Cryptography.
	$ECDSA$	Elliptic Curve Digital Signature Algorithm.
F	FFM	Fast, Feeless and Minerless.
G	GMO	Une société japonaise de services en ligne.
H	$HPSO$	Hierarchical Particle Swarm Optimization.
I	IA	Intelligences Artificielle.
	IoT	Internet of Things.
	$IOTA$	est une cryptomonnaie expérimentale et un protocole open-source.
J	JC	Judge Contracts.
K	$KECCAK-256$	La fonction de hachage utilisée par la fonction Ethereum SHA3.
N	NCP	Normalized Certainty Penalty.
	NFC	Near-Field Communication.
P	$P2P$	PEER TO PEER.
	$PBFT$	Practical Byzantine Fault Tolerance.
	$PoAC$	Proof-of-Activity.
	PoS	Proof-of-Stake.
	PoW	Proof of Work.
	PSO	Particle Swarm Optimization.
R	RC	Registry Contracts.
	$RFID$	Radio Fréquence ID.

INTRODUCTION GENERALE

Nous vivons dans un monde de plus en plus connecté où on génère et crée de plus en plus de données de nature différente. À cause des réseaux sociaux, du Big Data et maintenant avec l'émergence de l'Internet des Objets (IoT : Internet of Things), une quantité énorme de données personnelles est mise en jeu et divulguée parfois même sans que les intéressés en soient conscients. Face à ce risque de sécurité un nouveau concept apparu s'appelle la BIoT qui est l'intégration de la blockchain dans IoT. La blockchain qui semblait avoir un niveau de protection décent à des défis, cela nous à incité à explorer des pistes de recherche dans ce domaine.

Ces dernières années, la technologie Blockchain a considérablement mûri et est considérée comme une solution prometteuse grâce à sa sécurité intrinsèque. En fait,la blockchain est un système de sécurisé par conception qui peut atténuer les risques de sécurité grâce à ses capacités telles que l'immuabilité, la transparence, l'auditabilité, le cryptage des données et la résilience opérationnelle.

L'objectif de ce mémoire est de définir proprement les deux concepts la sécurité dans l'IoT et la blockchain, qui offre une foule de propriétés qui peuvent être intéressantes pour les applications IoT avec tous ces avantages dans le coté sécurité. Un autre objectif est d'examiner l'état de l'art dans le monde du BIoT et les progrès réalisés dans la recherche, avec une contribution par une proposition représenté dans une idée sur l'anonymisation qui combine entre les algorithmes matheuristiques et un algorithme de clustering blockchain avec Machine Learning. .

Structure du mémoire

Ce mémoire s'articule autour de quatre chapitres:

Le premier chapitre est " **Sécurité dans l'Internet des objets**" presente un aperçu sur l'IoT et définit l'aspect de la sécurité dans l'IoT.

Le deuxième chapitre "**Blockchain**" donne la propre définition,les notions des base,le fonctionnement et les défis reliés à cette technologie de blockchain.

Le troisième chapitre" **Etat de l'art sur l'Internet des objets et la blockchain**" expose un état de l'art général sur l'intégration de la bolckchaine dans les applications IoT, actuel défis de mise en œuvre et perspectives d'avenir.

Le dernier chapitre " **Propostion et implèmentation** " présente notre approche proposée qui est une combinaison entre une métaheuristique PSO et un algorithme de clustering blockchain avec Machine Learning.

CHAPTER 1

SÉCURITÉ DANS L'INTERNET DES OBJETS

Introduction

Durant les dernières années, les chercheurs se sont dirigés vers l'IoT et son impact sur notre vie quotidienne, spécialement après l'augmentation du nombre d'objets connectés autour du monde qu'aujourd'hui dépasse même le nombre de personnes. L'utilisation accélérée et massive de l'IoT (Internet of Things) soulève des nouvelles problématiques sérieuses relatives au sujet de la sécurité. En effet, des rapports récents sur la cybernétique ont mis en évidence la vulnérabilité des réseaux d'objets, les risques ne cessent d'accroitre d'une façon exponentielle surtout avec le déploiement des réseaux intelligents. Pour éviter les conséquences désastreuses, la sécurité doit être intégrée afin de vérifier un ensemble de critères, à savoir : la résistance aux attaques, le contrôle d'accès, assurer l'authenticité des données et la vie privée des d'utilisateurs. Ce chapitre est organisé en deux sections : La section 1.1 décrit un aperçu sur l'IoT. La section 1.2 définit l'aspect de la sécurité dans les réseaux d'objets ainsi les différentes menaces et ces dimensions de liés à l'IoT.

1.1 Aperçu sur l'Internet des objets

1.1.1 Historique

À l'origine, le terme Internet des objets a été utilisé pour la première fois en 1999 par Kevin Ashton [59] pour décrire des objets équipés de puces d'identification par radio fréquence (ou puce RFID). Chaque objet identifié de manière unique et universelle et peut alors être rattaché à un ensemble d'informations le concernant, ces dernières étant lisibles par d'autres machines. Le concept a toutefois évolué avec le temps et s'est généralisé vers une approche consistant à connecter un très grand nombre d'objets du quotidien au réseau Internet, les dotant ainsi d'une identité propre et leur permettant, entre autres, d'offrir des services et de collecter des informations de manière autonome [59].

1.1.2 Definition

Certaines définitions insistent sur les aspects techniques de l'IoT (« des objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés »), d'autres portent sur les usages et les fonctionnalités (« la convergence des identifiants numériques ») notant qu'il devient possible d'identifier de manière unifiée des éléments d'information numérique (adresses) et des éléments physiques (une palette dans un entrepôt, ou un animal dans un troupeau). Une définition plus synthétique est la suivante l'IoT est « un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant » [8].

1.1.3 Composants

Le concept d'Internet des objets exige la coordination des dispositifs suivants [16] :

- Une étiquette physique identifie chaque objet / une étiquette virtuelle identifie chaque lieu.

- Un dispositif mobile (téléphone cellulaire, organiseur, ordinateur portable) doté d'un logiciel additionnel, lit les étiquettes physiques ou localise les étiquettes virtuelles.
- Un réseau sans fil relie le dispositif portable à un serveur contenant l'information relative à l'objet étiqueté.
- Les informations sur les objets sont gérées dans des pages existantes du web.
- Un dispositif d'affichage (écran d'un téléphone mobile) permet de consulter les informations relatives à l'objet ou à un ensemble d'objets.

1.1.4 Domaine d'application

L'IoT couvrira un large éventail d'applications et touchera quasiment à tous les domaines que nous affrontons au quotidien, ceci permettra l'émergence d'espaces intelligents, on peut citer:

- Les villes intelligentes : l'IoT permettra une meilleure gestion des réseaux divers qui alimentent nos villes en permettant un contrôle continu en temps réel et précis. Des capteurs peuvent être utilisés pour l'économie de l'eau et pour améliorer la gestion des parkings et du trafic urbain et diminuer les embouteillages et les émissions en CO2 [41].
- Le Transport : Des voitures connectées ou autonomes aux systèmes de transport/logistique intelligents, l'IoT peut sauver des vies, réduire le trafic et minimiser l'impact des véhicules sur l'environnement [10].
- La santé : dans le domaine de la santé, l'IoT permettra le déploiement de réseaux personnels pour le contrôle et le suivi des signes cliniques, notamment pour des personnes âgées, les objets connectés permettent de suivre la tension, le rythme cardiaque, la qualité de respiration ou encore la masse graisseuse. Ceci permettra ainsi de faciliter la télésurveillance des patients à domiciles, et apporter des solutions pour l'autonomie des personnes à mobilité réduite [42].
- L'industrie : La technologie IoT permettra un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et d'améliorer la sécurité des employés [8].

- L'énergie : L'Internet des objets permet aux innombrables appareils qui composent le réseau électrique de partager des informations en temps réel pour une distribution et une gestion plus efficace de l'énergie.

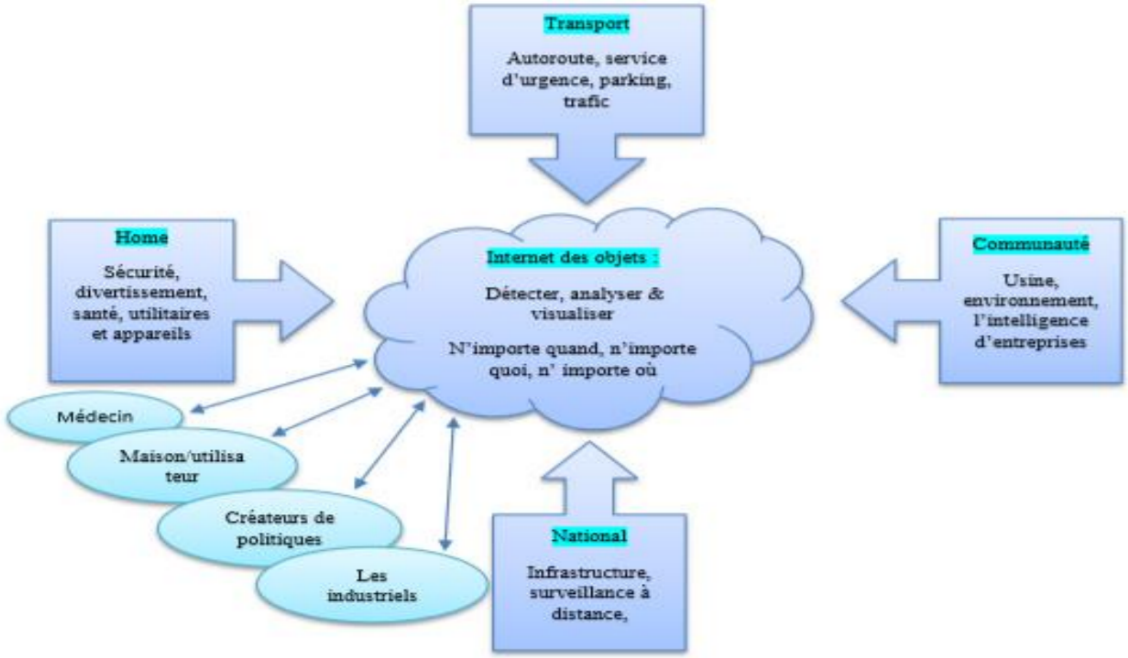

Figure 1.1 – Domaines d'Internet des Objet [31].

1.2 Sécurité dans l'IoT

1.2.1 Principaux objectifs de la sécurité dans IoT

La sécurité de l'information regroupe l'ensemble des moyens organisationnels,technologiques, humains et juridiques permettant de gérer les risques et leurs impacts à l'égard de la disponibilité de l'information, de sa confidentialité et de son intégrité [34] [35] [36].

La sécurité des systèmes d'information vise les objectifs suivants :

- La disponibilité : Un système doit fonctionner sans faille durant les lages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

- L'intégrité : Les données doivent être intactes, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.

- La confidentialité : Seules les personnes autorisées et avec les habilitations requises ont accès aux informations.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que :

- La traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont journalisés et que les journaux sont conservés et exploitables [37] [38].
- L'authentification : Validation de l'identité des utilisateurs (et systèmes) afin de gérer les accès aux informations et les services et maintenir la confiance.
- La non-répudiation (irrévocabilité) et l'imputation : Aucun utilisateur (système) ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

1.2.2 Menaces sur l'IoT

1.2.2.1 Menaces généraux

- Ressources disponibles limitées:
  - Faible capacité en batterie.
  - Mémoire et vitesse de traitement alors on ne peut pas supporter les mesures de sécurité habituelles.
- Manque d'intérêt pour les données : les données de l'IoT ne sont pas forcément vues comme importante,alors elle deviennent vulnérables .
- Disponibilité des outils : tous les outils pour modifier/analyser/étudier les objets connectés sont disponibles pour tous.
- Pas besoin d'un accès physique : utilisation de communication sans fil.
- Interface différente et limitée : les rapports d'erreurs et de sécurité peuvent être facilement ignorés.
- Des ports d'accès physiques : utilisés pour la programmation ou le débogage .

1.2.2.2 Menaces sur la vie privée

Tous les pronostics envisagent le développement d'une informatique ambiante avec potentiellement des dizaines d'objets par personne y compris dans leur sphère privée et intime. Sans régulation stricte, une protection accrue de la vie privée, un degré élevé de contrôle des objets par les usagers, l'adoption de l'IoT serait un échec. Elle conclue que la protection de la vie privée ne doit pas se limiter à des solutions technologiques, mais doit comprendre des mesures juridiques, une régulation du marché et des considérations socio-éthiques [13].

1.2.2.3 Menaces sur les systèmes et l'environnement physique des objets

L'IoT fera partie intégrante du monde physique et des systèmes complexes. En conséquence, un disfonctionnement quelconque, un déni de service, ou un comportement byzantin des objets n'entravera plus uniquement l'intégrité du monde virtuel (composé de données et d'informations), mais directement les processus sous leur contrôle en causant des dommages collatéraux importants. En 2009, une équipe de recherche d'IOActive avait démontré l'existence de failles de sécurité dans des dispositifs utilisés dans des « smart grids » pour le contrôle de distribution de l'énergie. Cette faille permettait à un hacker potentiel de diffuser un code malicieux et de couper l'alimentation en électricité des foyers [13].

1.2.3 Dimensions de la sécurité de l'IoT

L'Internet des objets est une technologie largement répandue dans le monde physique et omniprésente parmi les utilisateurs. Les diverses applications potentielles de l'IoT, l'hétérogénéité de ses technologies habilitantes et sa forte dimension humaine et socioéconomique rendent sa sécurité un sujet difficile et complexe. En plus des problèmes de sécurité des technologies qui le constitueront, l'IoTaccentue les problèmes de sécurité des personnes qui l'utiliseront, et fait émerger de nouveaux problèmes liés à la sécurité des systèmes sous son contrôle [1] [2]. Comme nous l'illustrons sur la Figure 1.2, la sécurité dans l'IoTpeut être abordée de trois angles complémentaires qui reflètent ses dimensions technologique, humaine et systémique.

La protection technique concerne principalement la sécurité des données, des infrastructures de communication et des réseaux, nécessaire pour faire face aux attaques classiques et futures contre l'intégrité, l'authenticité et la confidentialité des données, ainsi que les attaques contre les infrastructures, les réseaux et leurs fonctions. La pro-

tection personnelle fait référence à la protection de la vie privée des utilisateurs. En plus des solutions techniques, il est également nécessaire de prévoir des réglementations appropriées sur les responsabilités en cas de litiges juridiques ou les systèmes et processus qu'ils contrôlent.

Figure 1.2 – Dimensions de la sécurité d'Internet des objets [17].

Comme on focalise sur la sécurité dans l'IoT,il existe une technologie très connecté au ce concept s'appelle la blockchain cette dernièrre on va la voir et la présenter dans le deuxième chapitre.

1.3 Conclusion

Dans le premier chapitre, nous décrivons la technologie Internet des objets (IoT) à partir de l'historique en passant par la définition et les composants jusqu'à les différents domaines d'application, puis décrivons les concepts de sécurité de base et les diverses menaces et modèles de l'Internet des objets.L'accent mise sur la sécurité des données dans l'Internet des objets nous amène à un nouveau terme appelé blockchain qui est le sujet du chapitre 2.

CHAPTER 2

BLOCKCHAIN

Introduction

Les nouvelles technologies prennent de plus en plus d'importance dans notre société. Cryptomonnaie et blockchain sont des mots qui continuent d'apparaître dans les conversations sur la subversion technologique actuelle ou future. Pour certains, c'est le nom de l'une des plus grandes révolutions technologiques de l'histoire de l'humanité.

Blockchain représente un protocole pair-à-pair décentralisé (ou peer-to-peer en anglais, c'est-à-dire un modèle d'échange dans lequel chaque entité du réseau est à la fois un client et un serveur), et il peut être considéré comme un plus grand livre avec informations ajoutées et stockées d'une manière immuable et sûre. Cette technologie peut également être utilisée pour prendre en charge des réseaux privés.

Dans ce chapitre, nous allons présenter un aperçu sur la blockchain:l'evolution,la propre définition et les notions des base reliées à cette technologie.

2.1 Evolution de blockchain

Depuis la création du Bitcoin en 2008 par Satoshi Nakamoto, la technologie n'a cessé d'évoluer et de s'enrichir, de sorte qu'aujourd'hui nous ne comptons pas moins de 900 crypto-monnaies. Une étape majeure dans le développement de la technologie Blockchain a été représentée par la création d'Ethereum en 2015, avec une volonté d'appliquer la technologie sous-jacente au Bitcoin au-delà d'un usage monétaire. Ethereum reprend les caractéristiques de la technologie Blockchain en y ajoutant des fonctionnalités supplémentaires, notamment la possibilité de créer des contrats intelligents.

En résumé, la blockchain peut être classés en quatre catégories : Blockchain 1.0, 2.0,3.0 et 4.0 :

- Blockchain 1.0 :

  La première génération de blockchain, Blockchain 1.0, est issue du concept de technologie des registres distribués (Distributed Ledger Technology):(DLT) [63] [71]. Le grand livre ou le registre distribué est une base de données qui est partagée de manière consensuelle entre plusieurs participants, ce qui permet aux témoins publics d'éliminer les scénarios de double dépense. L'application la plus importante de la DLT est la crypto-monnaie, où le bitcoin joue un rôle central. Le bitcoin est ainsi devenu la "monnaie de l'internet" et a ouvert la voie à "l'internet de l'argent" [5]. Après son lancement en 2009, le bitcoin a prouvé sa stabilité, sa fiabilité, son efficacité, sa simplicité, son indépendance et sa sécurité pour garder une trace des enregistrements des transactions et transférer l'autorité de ces enregistrements d'un utilisateur à un autre directement. Il utilise essentiellement des mécanismes de consensus et de minage pour échanger des crypto-monnaies.

- Blockchain 2.0 :

  Le gaspillage de minage et la faible évolutivité de la première génération de Blockchain ont incité Buterin [11] à étendre le concept de Blockchain au-delà de la monnaie. Cela a conduit à l'avènement de la l'avènement de la deuxième génération de Blockchain, à savoir Ethereum, qui repose sur de nouveaux concepts de contrats intelligents et de mécanismes de consensus de type Proof of Work.La figure 2.1 montre le fonctionnement des contrats intelligents. La première étape est la formulation du contrat entre deux parties. Elle implique que les termes, les règles et les conditions de l'accord doivent être acceptés par les deux parties et traduits en un code. Aucune modification ne peut être apportée au contrat sans le consentement des parties concernées. Le contrat intelligent est ensuite déployé sur

la blockchain. Dès que les événements mentionnés dans le contrat se produisent, le code s'exécute automatiquement. Un exemple pratique de ces événements peut être l'expiration d'une police d'assurance ou la livraison de marchandises. Une fois l'exécution du code terminée, le contrat transfère automatiquement la valeur au destinataire concerné. Le règlement est donc effectué instantanément, de manière sûre et efficace. Ce transfert est également enregistré dans la blockchain.

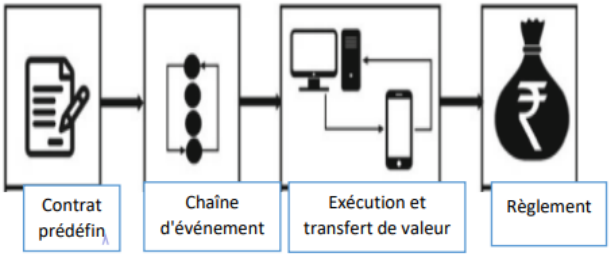

Figure 2.1 – Fonctionnement des contrats intelligents [11].

- Blockchain 3.0 :

  Le principal inconvénient des blockchains 1.0 et 2.0 est qu'elles ne sont pas du tout évolutives, qu'elles reposent principalement sur la preuve de travail et que la confirmation des transactions prend des heures. Tout ceci a permis la naissance de la génération actuelle de Blockchain appelée Blockchain 3.0 qui vise à rendre les crypto-monnaies viables au niveau mondial. En dehors des contrats intelligents, la troisième génération de Blockchain implique principalement des applications décentralisées (dApps) [6]. Il s'agit de programmes numériques qui s'exécutent sur un réseau d'ordinateurs de la blockchain plutôt que sur un seul ordinateur et qui échappent ainsi à toute autorité centrale. Cette génération est donc capable de promouvoir les transactions inter-chaînes à l'aide de techniques telles que le sharing. Il implique que chaque nœud de la blockchain ne contient qu'une partie des données qu'il contient et non l'ensemble des informations. Cela permet de répartir la charge et de rendre le système plus efficace et à l'abri des intrusions. Blockchain 3.0 utilise également les mécanismes de consensus Proof of Stake et Proof of Authority [19] pour permettre une vitesse et une puissance de calcul accrues pour les contrats intelligents, sans frais de transaction séparés. Bien que Blockchain 3.0 n'en soit qu'à ses débuts, elle vise à améliorer l'évolutivité, l'interopérabilité, la confidentialité et la durabilité des générations précédentes car elle est conçue sur le concept "FFM", acronyme de Fast, Feeless and Minerless. La

blockchain 3.0 élimine donc la dépendance à l'égard des mineurs pour vérifier et authentifier les transactions. Et utilise à la place des mécanismes intégrés pour cela. Elles sont donc extrêmement rapides pour des milliers de transactions par seconde, contrairement aux générations précédentes.

Cependant, la troisième génération de blockchain présente également plusieurs inconvénients, tels que la correction des bugs ou la mise à jour en raison de leur nature décentralisée. Les mécanismes de consensus appliqués sont comparativement compliqués.

- Blockchain 4.0 :

  Une autre progression favorable à venir dans l'évolution de la blockchain est la blockchain 4.0. Elle vise à fournir la technologie Blockchain en tant que plateforme utilisable par les entreprises pour créer et exécuter des applications, convertissant ainsi la technologie en un courant dominant. Elle a la possibilité d'intégrer d'autres technologies prospères telles que l'intelligence artificielle à la blockchain.La première plate-forme à mettre en avant les utilités de Blockchain 4.0 est Unibright [55] qui permet un amalgame de plusieurs modèles commerciaux de blockchain. Un autre exemple est la plateforme (SEELE) qui permet l'intégration dans l'espace blockchain en autorisant la communication croisée entre différents protocoles à travers divers services de manière harmonieuse. La quatrième génération a le potentiel de permettre la vitesse de transaction jusqu'à 1 million de transactions par seconde, ce qui est actuellement impossible dans les générations existantes.

Paramètres	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
principe sous-jacent	Technologie du grand livre distribué (DLT)	Contrats intelligents	Applications décentralisées (d'Apps)	Blockchain et IA
mécanisme de consensus	Preuve de travail	Preuve de travail déléguée	Preuve d'enjeu, Preuve d'autorité	Preuve d'intégrité
vérification	Par les mineurs	Par des contrats intelligents et des mineurs	Mécanisme de vérification intégré via les dApps	Vérification automatisée via Sharding
évolutivité	Non évolutif	Faiblement évolutif	Evolutif	Hautement évolutif
interopérabilité	Non interopérable	Non interopérable	Interopérable	Hautement interopérable
intercommunication	Non autorisé	Non autorisé	Autorisé	Autorisé
vitesse	7TBS	15 TBS	1000 S EN TBS	1M TBS
coût	Coûteux	Moins cher	Plus économique	Coût effectif
consommation d'énergie	Plus élevé	Modéré	Efficacité énergétique	Très efficace
exemple	Bitcoin	Ethereum	IOTA, Cardano, Anion	SEELE, Unibright
application	Secteur financier	Secteur non financier	Plateformes d'affaires	Industrie 4.0

Table 2.1 – Comparaison entre les différentes générations de blockchain [55].

2.2 Définitions

2.2.1 Blockchain

La Blockchain est fondamentalement une technologie de stockage et de transmission d'informations sécurisées, à l'image d'une base de données distribuée, en y intégrant en plus une protection cryptographique des données et en permettant la conservation de l'historique de tous les échanges effectués entre ses participants. Echange de valeurs, transfert de propriété, ou encore notarisation des transactions qui se réalisent grâce à une chaîne de blocs contenant les données, d'où le terme 'block' - 'chain'. Mais à la différence d'une base de données classique, la Blockchain introduit un nouveau type de gouvernance décentralisée, intégrée et gérée par la technologie, sans intermédiaire qui ne requiert pas la présence d'une tierce autorité de contrôle [46].

En résumé, la technologie Blockchain repose sur trois principes techniques de base : Architecture décentralisée ou architecture peer-to-peer pour assurer la stabilité du système. L'utilisation de cryptographie asymétrique pour assurer la sécurité de l'information. La mise en place d'un algorithme, appelé consensus, pour éliminer le risque de fraude et garantir la confiance au sein du système.

2.2.2 Bloc

Un bloc contient un en-tête et un corps,comme affichés dans la figure 2.2:

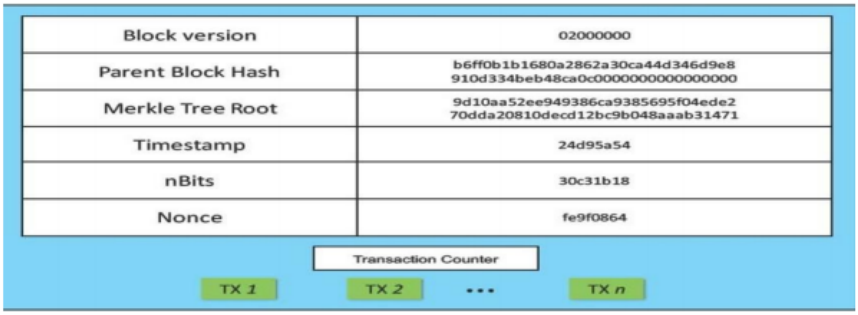

Figure 2.2 – Structure d'un bloc [96].

En particulier, l'en-tête de bloc comprend :

- Version de bloc : indique le jeu de règles de validation de bloc à suivre.
- Hachage de bloc parent : valeur de hachage de 256 bits qui pointe vers le blocprécédent. (Voir figure 2.3) :

Figure 2.3 – Enchainement des blocs [46]

- Hachage racine Merkle Tree : la valeur de hachage de toutes les transactions du bloc.

Les arbres de Merkle constituent un moyen très efficace de vérifier si une transaction spécifique appartient à un bloc particulier. S'il existe « n » transactions dans une arborescence Merkle (éléments feuille), cette vérification prend alors juste le temps déconnexion (n), comme illustré à la figure 2.4 [5].

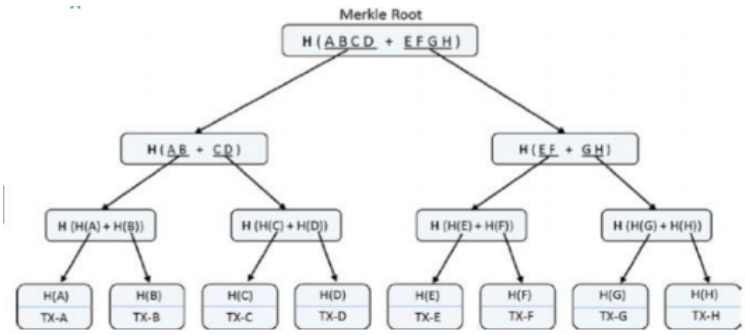

Figure 2.4 – Arbre de Merkle [46].

Pour vérifier si une transaction ou tout autre élément feuille appartient à un arbre Merkle, nous n'avons pas besoin de toutes les transactions ni de l'arbre complet.

Pour garantir l'intégrité d'un bloc téléchargé par rapport à l'ensemble des données, il suffit de posséder les hashs des frères, les hashs des oncles et le hash-sommet. De plus, seul le hash-sommet doit être récupéré de manière sûre pour garantir l'intégrité de l'ensemble des données représentées par l'arbre.

- Horodatage : horodatage actuel en secondes.
- Bits : cible de hachage actuelle dans un format compact.
- Nonce : un champ de 4 octets, qui commence généralement par 0 et augmente pour chaque calcul de hachage.

2.2.3 Transaction

La Blockchain permet le partage et l'échange d'informations entre nœuds. Cet échange s'effectue au moyen de fichiers contenant des informations de transfert d'un nœud à l'autre, générées par un nœud source et diffusées sur l'ensemble du réseau à des fins de validation. L'état actuel de Blockchain est représenté par ces transactions, qui sont générées en permanence par les nœuds, puis rassemblées en blocs.

Une transaction est un message structuré. Ce message structuré a 2 représentations [74] :

- Un format binaire, utilisé pour le calcul de hachage, la signature et le transfert réseau.
- Un format source arbitraire

Le format binaire est le seul format "officiel". En effet, le format source est hors de portée de la spécification du protocole. Par conséquent, tout processus applicable à une transaction sera appliqué à ce format binaire. Les règles de conversion pour sérialiser un format source dans un format binaire sont les suivantes [74] :

- La plupart des nombres sont codés avec la convention de Little-Endian sur 32 bits.
- Un code de hachage est considéré comme un grand nombre sur 256 bits, codé avec la convention de Little-Endian.
- Une quantité est un nombre entier sur 64 bits, codé avec la convention de LittleEndian.
- Un tableau commence par le nombre d'entrées, codé sur un octet, suivi d'une séquence de toutes les entrées.
- Toute autre donnée commence par la taille des données codées sur un octet.

2.2.4 Nœud

C'est un ordinateur relié au réseau Blockchain qui utilise un programme relayant les transactions. Les nœuds conservent une copie du grand registre Blockchain et sont répartis partout dans le monde. Il existe trois types de nœud [74] :

- Un nœud complet : c'est un nœud qui contient l'ensemble des transactions et des blocs. Il participe à la sécurité du réseau Blockchain.
- Un nœud mineur : c'est un nœud complet qui fait des calculs de hash pour la sécurité de la Blockchain, il est difficile et couteux de sorte que les gens ne font pas fonctionner un nœud mineur gratuitement d'où l'algorithme de Blockchain les récompense par un token ou une crypto monnaie pour leur service.
- Un nœud simple : c'est un nœud qui contient les derniers blocs valides complets, ainsi que l'empreinte (hash) des transactions et blocs plus anciens.

2.2.5 Adresse et porte-monnaie

Les adresses sont généralement des caractères alphanumériques courts utilisés comme point de transaction de l'expéditeur et du destinataire. Différentes implémentations de blockchain utilisent différentes manières de dériver les adresses.Et les utilisateurs du réseau blockchain doivent stocker leurs clés privées dans un endroit sûr.

Le logiciel utilisé pour stocker les clés privées est appelé "wallets". Outre les clés privées, les portefeuilles peuvent également stocker les adresses et les clés publiques des utilisateurs. Les portefeuilles sont utilisés pour calculer le nombre de actifs numériques détenus par un utilisateur de confiance particulier.

2.3 Fonctionnement de la blockchain

La transparence de ce système repose sur le fait que tous les échanges effectuent entre les utilisateurs depuis la création de la chaine y sont inscrits.

Au moment que les utilisateurs de réseau effectuent des transactions, ces transactions seront regroupées en bloc chaque bloc est validé par les nœuds du réseau ou ”mineurs” selon des techniques qui dépendent du type de la blockchain [74].

Les ”mineurs” sont des particuliers qui permettent de vérifier la validité des transactions bloc par bloc. Ils sont rémunérés pour mettre à disposition la puissance de calcul de leurs processeurs. Le fonctionnement d'une transaction peut schématiquement être décrit par la figure 2.5 [74] :

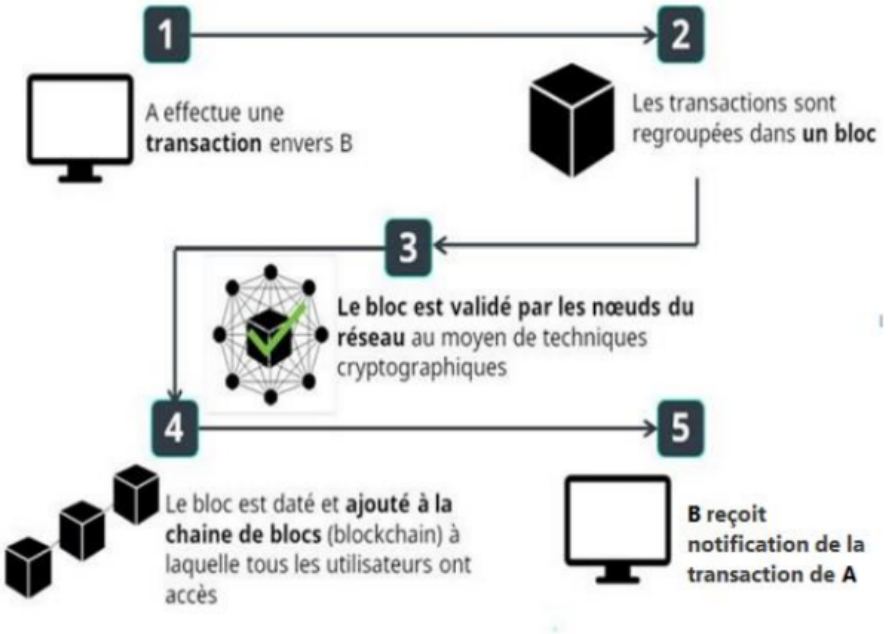

Figure 2.5 – Fonctionnement de la blockchain [74].

Au niveau de l'étape 3 du schéma, la puissance de calculest nécessaire afin de vérifier si le bloc est valide ou non. Pour cela, il faut utiliser la puissance des ordinateurs connectés sur le réseau afin de valider les transactions contenues dans le bloc. Ensuite,l'ajout de ce bloc à la base de données publique déjà existante. A ce moment se pose la question de comment être sûr qu'il ne s'agit pas d'une transaction frauduleuse ? Pour pallier à ce problème,il faux exploiter le système de Preuve de travail aussi appelé Proof of Works , qui réside dans le principe de la résolution d'un problème mathématique reposant sur un principe de cryptographie. La première machine à obtenir la solution à ce problème, propose son bloc au réseau afin de le vérifier et de valider le bloc. Si une majorité de gens approuve ce bloc, il est alors ajouté à la blockchain. Si ce n'est pas le cas, le block est alors rejeté [74].

2.4 Architecture de la Blockchain

L'architecture d'un réseau distribué Blockchain est Peer to Peer, le réseau d'égal à égal, également appelé P2P, fait référence à un groupe d'ordinateurs agissant en tant que nœuds pour partager des fichiers entre eux-mêmes. La Blockchain fonctionne donc sur un réseau distribué de serveurs, également appelé nœuds. Ces nœuds du réseau ont pour objectif de fournir un consensus sur l'état de la blockchain à tout moment, et contiennent une copie de la blockchain. L'application fondamentale de la Blockchain est un grand livre de transactions, un peu comme un grand livre public sécurisé, qui stocke toutes les transactions qui ont lieu dans le réseau. Cela en fait un système décentralisé très sécurisé et transparent.

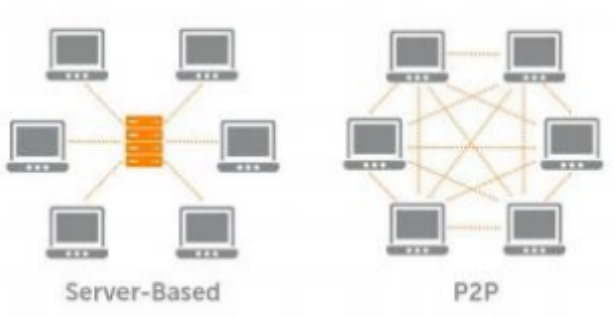

Figure 2.6 – Réseau basé sur les Serveurs vs Réseau P2P [74].

2.5 Types de blockchain

Les systèmes de Blockchain actuels peuvent être grossièrement classés en trois types :

- Blockchains publiques : sont des grands réseaux distribués accessibles, ouvert à tous et à tous les niveaux, et ont un code source ouvert que leur communauté maintien à jour comme Bitcoin.
- Blockchains consortium : sont des réseaux distribués qui contrôlent les rôles de chaque nœud dans les réseaux tels que Ripple, le code source peutêtre ouverte ou non.
- Blockchains privées : sont plus petites que les autres types, leur accès est complétement contrôlé.

2.6 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.

Le nœud télécharge une copie complète de la base de données blockchain sur son ordinateur ou son serveur, lorsqu'il se connecte au réseau pour la première fois.

Le réseau de nœuds gère la base de données, également appelée blockchain. Les nœuds sont des points d'entrée pour de nouvelles données pour asurer la validation et la propagation de ces données qui ont été soumises à la blockchain [45].

Un bloc est créé en regroupant des transactions similaires. Ces blocs sont ajoutés dans l'ordre chronologique, d'une manière qui ressemble à une chaîne. Les nœuds stockent ensuite ces nouveaux blocs dans la base de données blockchain locale sur leur ordinateur ou serveur [45].

2.7 Applications de blockchain

‘

- Smart contacts :ou contrats intelligents représentent un des cas d'usages les plus prometteurs de la Blockchain. Ce sont des programmes informatiques reposants

sur la technologie Blockchain et conçus pour exécuter automatiquement les termes d'un contrat dès lors que certaines conditions sont réunies. Ces programmes sont accessibles et auditables par toutes les parties autorisées, leur exécution est donc contrôlée et vérifiable. Enfin, la Blockchain garantit la fiabilité et l'immuabilité de ces contrats [29].
On donne un exemple du E-Commerce : Un internaute commande un objet sur une boutique en ligne lui garantissant un achat sécurisé grâce au contrat intelligent. Ce contrat est passé entre le ecommerçant, le transporteur et le client et prévoit certaines conditions : Si le colis est bien livré au client, alors le e-commerçant et le transporteur sont rémunérés. Et si le colis est perdu ou endommagé par le transporteur, le client est remboursé et le transporteur doit des indemnités au e-commerçant.

- Stockage cloud ou l'art de partager son disque dur :La blockchain peut être utilisée pour décentraliser le stockage des données dans le cloud. L'idée est de mettre à disposition des autres utilisateurs l'espace de stockage dont vous disposez sur le serveur cloud mais que vous n'utilisez pas contre rémunération en cryptomonnaie.Microsoft Azure et Amazon web services cloud Storage sont deux grands exemples sur cette application.

- Automatisation du paiement des salaires :Utiliser cette technologie pour gérer la paie des salariés fait donc totalement sens [29]. Exemple : La société "GMO" est la première dans l'utilisation réelle de la monnaie numérique "Bitcoin" cryptée, versée comme un salaire aux employés de l'entreprise.

2.8 Les défis de blockchain

Même si la technologie blockchain présente un potentiel important, certains défis limitent son application à une plus grande échelle. Les principaux défis sont les suivants [75] :

2.8.1 Évolutivité

En raison de l'augmentation du nombre de transactions de temps en temps, la taille et le volume de la blockchain deviennent également plus importants de jour en jour. Chaque nœud doit collecter toutes les transactions et les valider sur la blockchain. En outre, la

blockchain est limitée par la taille des blocs et le temps nécessaire à leur publication. Seules 7 transactions par seconde peuvent avoir lieu. Cela peut ne pas suffire pour traiter une grande quantité de données en temps réel. De plus, comme la taille du bloc est petite, les mineurs ont tendance à préférer valider les transactions avec des frais plus élevés, ce qui retarde les petites transactions. Certains développements pour résoudre ces problèmes sont l'optimisation du stockage et la refonte de la blockchain.

2.8.2 Perte de la vie privée

Dans la blockchain, une quantité considérable de vie privée est maintenue en utilisant le mécanisme de cryptographie à clé publique dans les transactions pour garder l'identité de l'utilisateur anonyme. Cependant, l'anonymat transactionnel ne peut être assuré par la blockchain car les identités de toutes les transactions et les soldes de chaque clé cryptographique sont accessibles au public. Il est donc possible de reconnaître l'utilisateur en gardant la trace des transactions.

2.8.3 Exploitation minière égoïste

La blockchain est plus sujette à des attaques de ce type. Le minage égoïste est une stratégie où un mineur trop ambitieux conserve secrètement ses blocs sans les publier. Ils ne seront révélés au public que si certaines conditions sont remplies. Ce minage secret des chaîne privées qui sont plus longues que la chaîne actuelle ouvertement disponible, tous les autres mineurs seraient d'accord avec elle. En conséquence, les mineurs honnêtes auraient gaspillé leurs ressources sur une chaîne qui va être abandonnée. De cette façon, les mineurs égoïstes peuvent être récompensés par des incitations plus importantes. De même, la blockchain est sensible à de nombreuses attaques comme les attaques Sybil, les doubles dépenses, les attaques 51, etc. Néanmoins, la blockchain a transformé à la fois l'industrie et le monde universitaire grâce à ses propriétés distinctes comme la décentralisation, l'anonymat, l'intégrité et la transparence. Les applications de la blockchain vont au-delà des crypto-monnaies et des transactions. La nature décentralisée de la blockchain sur l'Internet existant est très intéressante en termes de redondance et de survie des données. Parmi toutes les solutions, la blockchain est la solution parfaite pour les problèmes où la confiance est une préoccupation majeure. Même si la blockchain n'a pas atteint sa maturité, elle continue de convenir à des applications dans différents domaines au niveau mondial.

2.9 Conclusion

Dans ce chapitre, nous avons présenté les fondamentaux de la technologie blockchain et son principe de fonctionnement. La blockchain est encore une technologie émergente. En tant qu'elle s'accompagne d'une multitude de problèmes qui peuvent ou non être résolus dans les années à venir. Cependant, la communauté blockchain a montré que des solutions peuvent être imaginées et des problèmes contournés. Parmi ces problèmes, une blockchain optimisée pour l'IoT qui permettrait aux appareils de se connecter à la blockchain sans avoir besoin d'un serveur ou d'une passerelle n'a pas encore vu le jour. Malgré cela, la blockchain offre une foule de propriétés qui peuvent être intéressantes pour les applications IoT.

CHAPTER 3

ETAT DE L'ART SUR L'INTERNET DES OBJETS ET LA BLOCKCHAIN

Introduction

Avec l'avènement des technologies de l'Internet des objets (IoT), un grand nombre d'appareils intelligents ont été développés et intégrés dans la vie quotidienne. Les technologies IoT ont obtenu un succès sans précédent tant en ce qui concerne l'évolutivité que les scénarios applicables. Cette technologie émergente fournit des applications innovantes. En raison des contraintes sous lesquelles fonctionnent la plupart des appareils IoT (énergie limitée ou stockage faible), de plus en plus de fabricants d'appareils préfèrent lancer des applications basées sur la communication de groupe (par exemple, les systèmes de maison intelligente et de soins de santé) pour augmenter les bénéfices.

Cependant, avec le nombre croissant d'appareils et la complexité de la communication entre eux, les applications IoT, en particulier celles basées sur la communication de groupe, sont progressivement devenues la cible principale des attaques de piratage. Alors la meilleure solution contre ce piratage est d'intégrer la blockchaine dans les applications IoT et definir un nouveau concept : la BIoT.

Dans ce chapitre on donne un état de l'art général sur l'intégration de la bolckchaine dans les applications IoT, actuel défis de mise en œuvre et perspectives d'avenir.

3.1 Intégration Blockchain IoT (BIoT)

L'IoT, depuis sa création et son adoption massive, a montré un grand potentiel en matière de sa capacité à transformer et optimiser les activités manuelles et à les intégrer dans la révolution numérique. Le principal moyen par lequel l'IoT est devenu une telle superpuissance est le cloud computing [75].
Au cours des dernières années, le cloud computing a fourni l'infrastructure centrale de communication et d'intégration du stockage pour les implémentations IoT. Grâce à l'utilisation d'analyses avancées, qui peuvent être intégrées dans des plateformes d'informatique en nuage, des actions et des connaissances en temps réel peuvent être dérivées de la grande quantité d'informations produites par les dispositifs IoT [72]. Cette forme d'intégration avec l'informatique en nuage a nécessité la mise en place d'architectures centralisées pour garantir l'agrégation et la distribution correctes des données.
Cela a entraîné des problèmes de confiance et des préoccupations sur la confiance et d'inquiétude de la part des acteurs de l'IoT. La principale préoccupation concernant ces architectures centralisées est que le stockage et la récupération des données sont présentés comme des boîtes noires pour les acteurs de l'IoT.
Les fournisseurs de cloud computing ne donnent généralement pas d'indications claires sur la manière dont les données sont stockées sur leurs plateformes, mais ils font plutôt de vagues déclarations sur la sécurité de leurs systèmes, qui ne peuvent pas toujours être vérifiées. Les acteurs de l'IoT ont également tendance à s'inquiéter de savoir qui a accès à leurs données. Les blockchains reposent sur la confiance, l'immuabilité des données et la décentralisation. Ces caractéristiques des chaînes de blocs peuvent constituer des avantages majeurs et des solutions révolutionnaires aux problèmes rencontrés par les systems IoT si elles sont intégrées correctement.Ce type d'intégration peut s'avérer utile dans les cas où les données IoT doivent être partagées. Les principales préoccupations que la blockchain peut facilement contribuer à résoudre dans le paradigme de l'IoT sont les suivantes: le contrôle d'accès aux données et le partage des données en toute transparence des données, l'évolutivité, la confidentialité et la fiabilité [75].

3.1.1 Architectures de conception de l'infrastructure IoT de la blockchain

La communication entre dispositifs homologues de l'IoT est un aspect qui ne peut être ignoré dans les mises en œuvre de l'IoT. Elle constitue le cœur des interactions

IoT. Cela conduit à la formation de réseaux P2P pour les interactions entre dispositifs IoT où chaque dispositif IoT est représenté comme un nœud du réseau dans le cas de l'intégration de la blockchain dans l'IoT [88]. Ces types d'interaction sont illustrés dans la figure 3.1.

Les progrès réalisés dans le domaine de l'informatique en brouillard [92] ont conduit à son incorporation et à son utilisation dans des architectures de conception hybrides, ce qui a permis d'améliorer encore l'intégration des IoT et des blockchains. Les différentes méthodologies de conception sont développées comme suit :

3.1.1.1 Conception de l'architecture IoT Peer to IoT Peer :

Comme on a vue dans le chapitre 2 que la blockchain est basée sur une architecture peer to peer alors l'application de blockchain dans IoT donne un nouveau concept qui est :l'architecture IoT Peer to IoT Peer, cette méthode de conception est employée dans des scénarios où une faible latence et de hautes performances sont requises. Dans ce cas, seules les métadonnées des transactions entre dispositifs pairs IoT sont stockées sur la blockchain mais toutes les autres données sont transférées entre les dispositifs pairs IoT directement. Cette architecture nécessite des techniques de routage et des techniques de découverte. Cela permet de s'assurer que les données d'un dispositif IoT pair trouvent leur chemin vers l'autre dispositif IoT pair de manière efficace. Cette architecture fonctionnera mieux dans les cas où les dispositifs appartiennent à un même domaine, sont situés dans la même zone où se trouvent sur le même réseau. Cela permet de réduire la complexité de la découverte et du routage requis.

3.1.1.2 Conception de l'architecture IoT Peer to Blockchain

Dans ce schéma, tous les dispositifs pairs de l'IoT n'ont pas de lien direct ou un moyen de connexion entre eux. Toutes les interactions et communications se font via la blockchain. Cela signifie que toutes les données qui sont associées à une interaction entre deux ou plusieurs dispositifs IoT pairs peuvent être enregistrées et capturées sur la blockchain. Ainsi, la blockchain peut aider à atteindre l'objectif de surveillance et de vérification des transactions entre les dispositifs IoT. Cela permet de fournir une traçabilité et une transparence élevées des interactions entre les dispositifs. Ce type d'architecture peut être essentiellement utilisé pour les applications BIoT qui fournissent des services d'échange et de location, comme Slock.it[69]. Cela pourrait également être bénéfique pour les dispositifs homologues IoT qui sont issus de domaines différents et qui exigent une haute-fidélité des données partagées entre eux lors des transactions.

- L'inconvénient de cette architecture serait la forte bande passante et les exigences en matière de données qui seraient nécessaires aux dispositifs homologues de l'IoT pour fonctionner et communiquer de cette manière. Une faible latence est une exigence pour les applications IoT, mais les blockchains sont connues pour avoir des problèmes d'évolutivité et de latence d'aprés Bisw as et al [43].Ainsi, la latence des interactions serait augmentée pour ce type d'architecture, car toutes les informations devraient être stockées sur la blockchain. La mise en œuvre de ce type d'architecture signifierait également que les dispositifs pairs IoT devraient agir comme des nœuds dans la blockchain. Il faudrait pour cela que les dispositifs disposent des ressources informatiques nécessaires pour agir en tant que nœuds de la blockchain.

3.1.1.3 Conception d'une architecture hybride

Les premières années du développement de l'infrastructure IoT ne prévoyaient pas que les dispositifs IoT fassent beaucoup de traitement et d'analyse des données. Cette situation a changé ces dernières années grâce à une approche appelée edge computing [51]. Cette approche permet une intercommunication avancée et le traitement d'un plus grand nombre de données sur les dispositifs IoT.

La conception de l'architecture hybride tire parti de la puissance de technologies telles que l'intelligence artificielle, le fog computing et l'edge computing pour créer un environnement d'interaction transparent pour les dispositifs IoT. Même si l'edge computing a permis la production de dispositifs IoT dotés d'une puissance de calcul et de ressources accrues, ils n'ont pas encore le niveau requis pour fonctionner comme des nœuds de blockchain efficaces (comme indiqué dans le cadre des défis de la conception IoT peer to blockchain). Ainsi, le fog computing permet de réduire la consommation d'énergie et la charge de calcul nécessaires aux dispositifs IoT. Il peut également contribuer à atténuer certains des problèmes de bande passante et de latence évoqués précédemment. La couche d'informatique en brouillard qui est incorporée dans ce type d'architecture se chargerait de toutes les tâches lourdes lorsqu'il s'agit d'interactions avec la blockchain.

Elle fournit également une plateforme pour l'exécution d'algorithmes d'IA, ce qui peut aider à prendre des décisions critiques concernant ces appareils pairs IoT. Le point fort de cette conception est que toutes les interactions IoT ne vont pas directement à la blockchain. Cela signifie que toutes les interactions de la blockchain seront effectuées par la couche d'informatique en brouillard et serviront de nœuds sur la blockchain. Il peut y avoir une source supplémentaire de redondance lorsque les brouillards peuvent

être connectés à une infrastructure en nuage (comme le montre la figure 3.1).

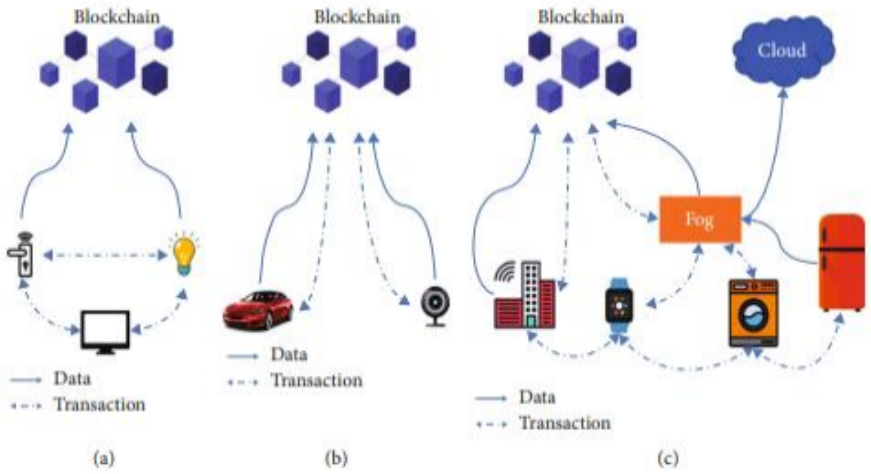

Figure 3.1 – Les différences interactions entre les appareils IoT et les pairs [88].

3.1.2 Scénarios d'intégration futurs pour BIoT

Il existe de nombreuses façons d'intégrer la blockchain à l'IoT pour résoudre des problèmes spécifiques. Voici quelques scénarios qui le montrent :

3.1.2.1 Extension de l'espace d'adressage pour les appareils IoT

Le nombre d'appareils IoT mis en ligne continue d'augmenter de jour en jour. Chaque appareil nécessite une adresse IP pour lui acheminer les communications et les interactions. L'espace d'adressage IPv4 est limité et ne peut pas répondre à cette augmentation. IPv6 a été utilisé dans de nombreux IoT déploiements [50]. IPv6 a bien fonctionné pour les scénarios IoT, car il dispose d'un espace d'adressage de 128 bits par rapport à l'espace d'adressage de 32 bits fourni par IPv4, mais le nombre d'appareils IoT ne cesse d'augmenter. La blockchain utilise des algorithmes cryptographiques avancés qui utilisent un schéma de clé publique-clé privée. La clé publique générée par l'algorithme de signature de courbe elliptique, par exemple,a une longueur de 160 bits (c'est-à-dire 20 octets) [98]. Cela signifie effectivement que si une clé publique de 160 bits est utilisée pour adresser des appareils IoT, il y aurait environ 146×1018 espaces d'adressage pour les nœuds IoT. Ce serait suffisant pour fournir un identifiant unique aux nœuds et appareils IoT. Si une telle chose est mise en œuvre, il n'y aurait pas besoin d'une autorité de numérotation Internet(ANI) [4] pour attribuer des adresses IP puisque tout

cela serait sur la chaîne de blocs et géré par des contrats intelligents.Cela aiderait à résoudre certains des problèmes d'évolutivité et de sécurité auxquels seraient confrontés les futurs déploiements IoT.

3.1.2.2 Contrôle d'accès intelligent basé sur un contrat et partage de données pour les systèmes IoT

Dans [94], un cadre basé sur un contrat intelligent a été proposé pour effectuer la tâche de contrôle d'accès pour les appareils IoT. Ce cadre est destiné à résoudre le problème des mauvais acteurs imitant d'autres appareils IoT et à les empêcher d'effectuer des activités malveillantes. Le cadre est composé de trois éléments principaux : les contrats de contrôle d'accès (ACC):access contracts control, les contrats de juge (JC):judge contracts et les contrats de registre (RC) :registry contracts. Une opération standard du cadre consiste à avoir plusieurs ACC, un JC et un RC sur la blockchain. Chaque ACC a pour tâche d'accorder à chaque couple sujet-objet une méthode de contrôle d'accès.

L'ACC valide les droits d'accès pour chaque couple sujet-objet en effectuant deux types de tâches de validation : une validation de droit d'accès dynamique et une validation de droit d'accès statique. La validation du droit d'accès statique est effectuée sur la base de politiques prédéfinies, et la validation du droit d'accès dynamique vérifie le comportement du sujet. Le JC reçoit les rapports de l'ACC dynamique et procède à l'évaluation des comportements inappropriés et pénalise les sujets contrevenants. Dans [44], un modèle pour améliorer la structure de pénalité du JC a été proposé. Cette conception proposée donne des sanctions aux parties contrevenantes sous la forme de périodes limitées dans le temps d'impossibilité d'exécuter des transactions. Le RC enregistre toutes les activités de l'ACC et du JC ainsi que l'exécution des méthodes de gestion telles que les enregistrements, les mises à jour et la suppression qui sont effectuées par les ACC et le JC. Le fonctionnement de ce cadre est illustré à la figure 3.2 .

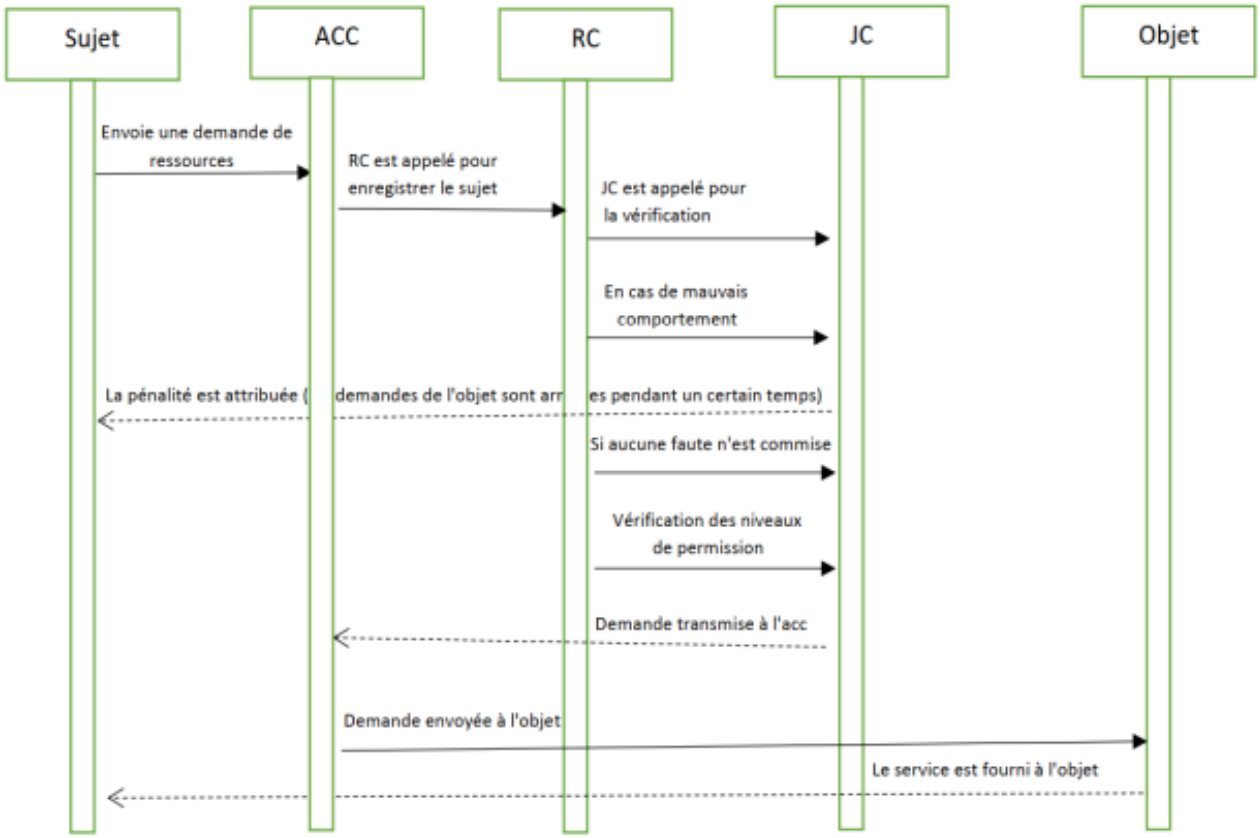

Figure 3.2 – Organigramme du modèle de système proposé pour le contrôle d'accès intelligent basé sur un contrat [84].

3.2 Applications BIoT

BIoT est un terme formé en combinant blockchain avec des applications IoT. En raison de certains problèmes de confidentialité et de sécurité des solutions IoT ainsi que de la sensibilité des données qui en sont obtenues, en particulier dans des domaines tels que les soins de santé et la gestion de la chaîne d'approvisionnement, certaines implémentations actuelles ont infusé la blockchain dans leurs systèmes IoT. Certains exemples incluent des applications dans les appareils portables, les soins de santé, le stockage de données, le système de transport intelligent et les villes intelligentes.

Le domaine de l'agriculture IoT intelligente a également vu d'excellentes applications. Dans [87], un système de blockchain de traçabilité alimentaire a utilisé l'identification par radiofréquence (RFID) comme schéma d'authentification pour aider à identifier les produits alimentaires ainsi que tous les participants de la chaîne d'approvisionnement al-

imentaire. Dans [24], les chercheurs ont également proposé une architecture de calcul de brouillard pour aider à alimenter les applications IoT agricoles basées sur la blockchain. L'argument principal était basé sur la faible capacité de calcul des appareils IoT, et donc, l'utilisation de l'architecture de brouillard s'est avérée très bénéfique pour que les appareils IoT servent uniquement de nœuds pour le transfert, et le gros du travail (extraction et validation) est fait par le nœud de brouillard.

Dans [15], les auteurs proposent une solution pour les mises à jour sécurisées du micro logiciel sans fil pour les appareils IoT. Cela fonctionnerait de telle manière qu'un fabricant aurait tous ses appareils IoT en tant que participants sur le même réseau blockchain. Le fabricant aurait alors un contrat intelligent sur la blockchain qui exécuterait les mises à jour du micro logiciel, et le hachage de ce contrat intelligent serait intégré aux appareils IoT. Ces appareils peuvent interroger périodiquement le contrat pour vérifier les nouvelles mises à jour du micro logiciel, puis demander la mise à jour actuelle par son hachage et la recevoir via un système de fichiers distribué peer-to-peer. Cela améliorerait considérablement la sécurité et la disponibilité des mises à jour du micro logiciel sur ces appareils, car même si le nœud du fabricant n'est pas disponible ou même si le fabricant a cessé de diffuser cette mise à jour pour l'appareil, cet appareil est sur la blockchain, il peut recevoir la mise à jour dont il a besoin des autres appareils IoT sur la blockchain.

3.2.1 Algorithmes cryptographiques pour les applications BIoT

Il est à noter que les blockchains ont deux principales cryptographiques implémentations qui les prennent en charge qui sont les suivantes : Fonctions de hachage et cryptographie à clé publique.

3.2.1.1 Cryptographie à clé publique

La puissance de calcul des appareils IoT est limitée et les appareils IoT peuvent avoir du mal à mettre en œuvre la cryptographie à clé publique standard qui est essentiellement utilisée pour assurer la sécurité et la confidentialité dans la blockchain. L'algorithme Rivest-Shamir Adleman (RSA) est un schéma cryptographique très puissant, mais l'allocation de ressources, en termes de puissance nécessaire à sa mise en œuvre, est assez élevée [85]. Les appareils IoT seront plus lents à le mettre en œuvre.

Une alternative au RSA qui a été suggérée dans la littérature est lacryptographie à courbe elliptique (ECC) qui est plus légère et s'est avérée plus performante en termes de puissance exigences et vitesse [83] sur une faible puissance de calcul dispositifs.

Une recherche récente effectuée par [83] montre des niveaux de sécurité plus élevés et une consommation d'énergie plus faible par un système basé sur ECC schéma cryptographique appelé Elliptic curve digital signature algorithm (ECDSA). Il surpassait RSA lorsque le niveau de sécurité était augmenté. Cela nécessite encore des recherches et une évaluation plus approfondie.

3.2.1.2 Fonctions de hachage

Les fonctions de hachage jouent un rôle très important dans les blockchains car elles sont utilisées pour signer des transactions. Il est important que la fonction de hachage utilisée sur un appareil IoT soit rapide, légère, consomme peu d'énergie et soit sécurisée (afin d'éviter les collisions). La fonction de hachage populaire utilisée dans les blockchains est KECCAK-256 (utilisée par la fonction Ethereum SHA3), SHA-256d (utilisée par Bitcoin), SHA-256 (utilisée par Emercoin) et Scrypt (utilisée par Litecoin). SHA-256 a été testé sur un certain nombre d'appareils IoT, y compris des appareils portables [57] même s'ils sont beaucoup plus anciens, mais les schémas plus récents présentés dans [27], respectivement, suggèrent que l'AES devrait être utilisé pour les appareils IoT en raison de sa faible consommation d'énergie. Dans [89], d'autres chercheurs ont suggéré la fonction de hachage BLA KE2x qui se décline en deux versions (BLAKE2b pour les plates-formes 64 bits et BLAKE2s pour les plates-formes 8 à 32 bits) [95].

3.2.2 Algorithmes de consensus et leurs effets sur les objets connectés

Proof of Work (PoW) : L'algorithme de consensus le plus populaire qui est devenu bien connu avec Bitcoin était la preuve de travail (PoW). Il s'agissait d'une tentative d'empêcher les attaques Sybil en obligeant les validateurs à effectuer une tâche appelée exploitation minière, d'où le terme mineur. Cela signifiait que chaque mineur du réseau devait effectuer un problème mathématique complexe qui consiste à trouver un nombre aléatoire appelé nonce.

Le résultat de cette opération était de faire en sorte que le hachage SHA-256 ait un nombre requis de zéros au début. Une fois cette opération effectuée correctement, elle permet aux autres nœuds de vérifier facilement les résultats obtenus. Cela présentait de sérieux inconvénients qui étaient évidents dans sa consommation d'énergie élevée, son faible débit et son évolutivité [68]. Ce sont des problèmes qui ne sont souhaitables dans aucune application IoT. En raison des problèmes rencontrés par l'algorithme de preuve

de travail, d'autres méthodes de consensus ont été développées pour aider à résoudre le problème. Les plus prometteurs d'entre eux sont les suivants :

- Proof-of-Stake (PoS) : Il a été démontré que cela a un taux de consommation d'énergie inférieur à celui du PoW. Il y a eu plusieurs approches de la stratégie PoS. Une approche consiste à visualiser les mineurs sur le réseau et à déterminer lequel d'entre eux a un taux de participation élevé [68]. Cela peut être prouvé sur une blockchain publique de cryptomonnaie en voyant l quantité de monnaie dont dispose un mineur. Sur cette base, on peut dire que ce mineur est moins susceptible d'attaquer le réseau ; ainsi, ce mineur peut être autorisé à extraire plus de blocs. Cela a été considéré comme injuste car les mineurs les plus riches contrôleraient la chaîne. L'autre approche adoptée par Peer coin consiste à considérer l'âge de la monnaie du mineur. Plus le mineur a de pièces, plus il a de chances d'exploiter un bloc [28]. Cela améliore considérablement le débit et s'adapte bien.

- Proof of Stake Delegated (DPoS): dans ce schéma, les parties prenantes et les nœuds délèguent certains mineurs pour valider les blocs au lieu de le faire eux-mêmes. Cela s'adapte très bien car il y a moins de nœuds impliqués dans le processus de validation. Ce processus est sécurisé par le fait que, puisque moins de nœuds valident les transactions, il est facile d'identifier si un mineur ou un nœud se comporte de manière malhonnête et une décision peut facilement être prise pour expulser ce nœud du réseau [23].

- Proof-of-Activity (PoAC) : Cette approche a été développée comme une accumulation sur le système de PoS [58]. Un mineur peut avoir de vieilles pièces et être devenu passif sur le réseau ; ainsi, l'âge des pièces ainsi que son temps d'activité sont vérifiés avant que ce nœud ne gagne le droit d'exploiter un bloc.

- Tolérance pratique aux pannes byzantines (PBFT:Practical Byzantine Fault Tolerance) : Dans [12], les auteurs décrivent comment cet algorithme de consensus résout le problème des généraux byzantins. PBFT suppose qu'un tiers des nœuds du réseau sont malveillants et qu'un mineur leader est donc sélectionné pour valider la transaction et 2/3 de tous les nœuds activement connus sur le réseau doivent être en accord avec ce leader.

- BFT délégué (DBFT:Delegated Byzantine Fault Tolerance) : Il fonctionne de la même manière que DPoS. Certains nœuds particuliers sont sélectionnés pour

les transactions minières et s'ils montrent des signes de malhonnêteté, ils sont expulsés.

- Bitcoin-NG : Cela implémente une variante de l'algorithme de consensus Bitcoin qui vise à améliorer l'évolutivité, le débit et la latence.

Dans le tableau 3.1, nous avons décrit les différents algorithmes de consensus avec leurs limites. Nous proposons également des façons dont ces algorithmes de consensus peuvent être utilisés dans les applications BIoT pour les rendre encore efficaces. La liste des algorithmes de consensus répertoriés dans le tableau 3.1 n'est pas exhaustive mais fournit un bon moyen d'adaptation de ceux mentionnés pour les applications IoT.

Algorithme de consensus	Adaptation basée sur la blockchain	Type	Performance	Limitation	Adaptation pour l'IoT
Preuve de travail (PoW)	Bitcoin [21]	Concurrence consensus	Robuste contre les attaques DDoS et aux attaques de Sybil	Forte consommation d'énergie Faible débit et faible évolutivité Risque de double dépense	Les points d'accès serviraient de mineurs à la place des nœuds individuels (dispositifs IoT). Ainsi, en prenant la charge de calcul des appareils IoT
Proof-of-stake (PoS)	Peercoin [99] Nxt [100]	Consensus de compétition	Difficile et plus coûteux à attaquer Consommation d'énergie plus faible	Injuste car les mineurs les plus riches contrôleraient contrôleraient la chaîne	Tous les dispositifs IoT peuvent être sélectionnés comme validateurs
Preuve d'activité (PoAC)	Decred [101]	Concurrence consensus	Topologie de réseau Consommation électrique Consommation d'énergie	Susceptible de subir une attaque par double dépense	L'architecture du réseau de brouillard peut être adaptée. Chaque couche de brouillard comporterait un nœud mineur qui crée un en-tête de bloc vide. Les dispositifs IoT dérivent N parties prenantes pseudo-aléatoires en utilisant le hachage de l'en-tête de bloc
Tolérance pratique aux fautes	byzantines	Tolérance aux fautes byzantines (PBFT)	_____	Moins de consommation d'énergie Faible variance de la récompense	Nombre élevé de communications entre les nœuds, donc un nombre accru dennœuds se traduira par une augmentation du nombre de messages envoyés Les frais généraux de communication augmentent exponentiellement lorsqu'un nouveau nœud est ajouté.
BFT délégué (DBFT)	Néo [103]	Compétition consensus	Moins de consommation d'énergie Faible puissance de calcul nécessaire	Les nœuds délégués fonctionnent sous identités réelles	Un système de vote doit être mis en œuvre parmi les nœuds, avec une décision aléatoire sur le nœud à déléguer

Table 3.1 – Comparaison entre les différents algorithmes de consensus et les blockchains qui les mettent en œuvre [68].

3.3 Défis actuels rencontrés dans les applications BIoT

L'utilisation des blockchains dans les applications IoT présente de nombreux avantages, mais elle comporte également son propre ensemble de défis. Les systèmes IoT, ces dernières années, ont connu des avancées émergentes dans les technologies qui les alimentent. Ces progrès ont été réalisés dans le domaine des technologies de communication telles que les communications 4G/5G[70],[44], les systèmes d'authentification et de sécurité tels que RFID et NFC [32] et les systèmes cyber-physiques (CPS)[26],[25]. L'ajout de la blockchain à l'IoT introduit des problèmes qui affectent l'évolutivité, la puissance et le temps de traitement, le stockage, la confidentialité et le débit global de ces implémentations. Les défauts et les lacunes du BIoT sont discutés dans les sous-sections suivantes :

3.3.1 Anonymisation

L'anonymat de la blockchain est quelque chose qui est implicite mais pas assuré. En effet, les appareils et les utilisateurs de blockchains sont identifiés par leur clé publique ou leur hachage. Ainsi, les attaquants et les tiers peuvent étudier leurs clés publiques et leurs hachages et en déduire les identités des nœuds ou des participants [22]. Il s'agit d'une grave préoccupation en ce qui concerne les appareils IoT, car ces appareils stockent ou transmettent généralement des informations sensibles et personnelles, et une fois qu'une telle trace peut être obtenue, elle met les appareils et leurs propriétaires en danger [69].

3.3.1.1 Anonymisation liée au modèle et algorithme matheuristiques

L'anonymisation a suscité beaucoup d'intérêt ces dernières années, suite à quoi de nombreuses approches ont été proposées sur les différents modéles comme MODELE L-DIVERSITE,T-PROXIMITE et K-ANONYMAT avec des algorithmes matheuristiques: Lin et Wei [4] ont proposé une approche de clustering basée sur un algorithme génétique pour atteindre le k-anonymat. Dans cette approche, la population initiale de l'algorithme génétique est créée sur la base de la méthode hybride proposée dans [53]. Une solution candidate de la population est codée par un chromosome contenant au moins k gènes, où chaque gène indique l'index d'un enregistrement dans l'ensemble de données d'origine. Run et al [77] ont proposé une méthode de recherche hybride basée sur la recherche tabou

et l'algorithme génétiques pour atteindre le k-anonymat. Dans la méthode proposée, une recherche taboue est intégrée dans un algorithme génétique traditionnel pour jouer le rôle de mutation. L'objectif est de surmonter la limitation de la capacité « d'escalade » de la recherche tabou traditionnelle à partir d'un seul point de départ, en mettant en œuvre une recherche locale à partir de plusieurs points de départ, provenant de l'algorithme génétique. L'algorithme proposé commence par la construction d'un treillis de l'espace des solutions (hiérarchies de généralisation de domaine) représentant les stratégies de généralisation. Sur la base de ce treillis, l'algorithme génétique crée lapopulation initiale qui est utilisée par la recherche taboue pour trouver la stratégie de généralisation optimale.Wai et al [56] ont proposé une approche de protection de la vie privée dans les Big Data, basée sur l'optimisation hiérarchique à l'essaim de particules (HPSO). L'approche proposée est basée sur l'infrastructure Hadoop MapReduce4 pour résoudre les problèmes d'évolutivité des Big Data. Elle se compose de deux étapes, principales, réalisées à l'aide de tâches MapReduce ; Une première étape de clustering, consistant à produire un nombre prédéfini de clusters de tailles supérieures ou égale à k (chaque cluster représente une particule). Suivit d'une étape de généralisation, consistant à transformer les données en leurs formes anonymisées.

3.3.1.2 Anonymisation liéé au apprentissage automatique

Les systèmes d'authentification d'identité automatique pour les applications IoT sont également mentionnés dans [80], où les chercheurs ont présenté un système basé sur la blockchain pour les applications IoT qui obtiendrait automatiquement les signatures des appareils IoT en identifiant les appareils et les utilisateurs. Certaines solutions d'apprentissage automatique basées sur la blockchain ont été présentées pour les solutions IoT, et celles-ci sont répertoriées dans le tableau 3.2. Nos résultats, répertoriés dans le tableau 3.2, montrent l'efficacité de l'utilisation d'approches basées sur l'apprentissage automatique dans les solutions de confidentialité. La solution apportée par Mendis et al. [61] utilise une approche d'apprentissage en profondeur. Cela fonctionne de manière distribuée afin que toute la formation ne se déroule pas sur un seul appareil (Raspberry Pi). Nous n'avons trouvé aucune implémentation qui utilise l'apprentissage par renforcement pour une telle préservation de la vie privée.les chercheurs peuvent considérer dans ce sens comme un élément constitutif du travail effectué dans [61]. En effet, une fois que la formation peut être effectuée de manière distribuée, il ne serait alors que prudent d'avoir une mise en œuvre efficace qui recycle le modèle produit de manière similaire.

Ref	Attaque	Cas d'utilisation	Métrique	Algorithme	Blockchain utilisée	Description
Shen et al. [79]	Confidentialité des données (modèle du texte chiffré, connu sous le nom de modèle d'arrière-plan)	Villes intelligentes	Précision	SVM (secureSVM)	–	Un algorithme de formation SVM sécurisé dans scénarios multipartites a été créé sur des données IoT. L'algorithme de consensus Proof-of-work a été utilisé. Précision : 93,89 %.
Mendis et al. [61]	Fuite de données	Polyvalent /général	Précision	CNN	Ethereum	Algorithme de consensus par preuve d'enjeu utilisé. Cette recherche a porté sur les formations modèles d'apprentissage automatique de manière distribué sur plusieurs Raspberry Pi 3.
Arachchige et al. [7]	Confidentialité des données	IoT industriel	–	ML fédéré	Ethereum	Un cadre a été introduit appelé PriModChain qui empêche la fuite de données sensibles des IoT vers des réseaux adversaires

Table 3.2 – Solutions de confidentialité de l'apprentissage machine basées sur la blockchain pour les appareils et réseaux IoT

3.3.2 Sécurité

Pour qu'un système BIoT soit considéré comme sécurisé, il doit répondre aux conditions et exigences suivantes : ‘

- Intégrité.
- Confidentialité.
- Disponibilité.

Plusieurs approches ont été envisagées pour assurer la sécurité des applications BIoT. Certains ont utilisé des approches d'apprentissage automatique, et d'autres ont opté pour des approches plus conventionnelles. Ceux-ci peuvent être vus dans le tableau 3.3 :

Références	Domaine d'étude	Contribution à la recherche
Ding et al. [20] **Ali et al. [3]**	Contrôle d'accès	Les chercheurs ont utilisé une approche de la délégation autorisée par blockchain pour aider à contrôler l'accès aux données des dispositifs IoT. Cela permet de protéger les informations vitales des dispositifs IoT.
Mohanta et al. [65] **Huh et al. [40]** **Xie et al. [90]** **Maw et al. [60]**	Assurance de la confiance	De nombreuses applications IoT fonctionnent sur des systèmes centralisés où l'intégrité des données est assurée par des tiers. Les auteurs de ces articles ont proposé meilleurs processus de gestion de la confiance pour aider à maintenir l'intégrité des données dans les implémentations BIoT
Li et al. [47], **Biswas et al. [9],** **Dorri et al. [21]**	Évolutivité	Les problèmes d'évolutivité des applications BIoT ont été abordés par ces auteurs qui ont fourni des cadres surla manière de les rendre plus évolutives.
Shen et al. [64], Lv et al. [54], **Hassan et al. [39], Sagirlar et al. [78],** **Xu et al. [2]**	Préservation de la confidentialité des données	Les auteurs de ces articles proposent des techniques de cryptage basées sur la blockchain pour aider à préserver la des utilisateurs et des nœuds de la blockchain.
Liu et Seo [52], Mohanta et al. [66], **Hammi et al. [33], Mohsin et al. [67],** **Lin et al. [49], Gope et al. [30],** **Zhang et al. [93], Conti et al. [133].**	Authentification	L'authentification du dispositif est l'un des facteurs importants considérés dans ces articles. Les auteurs ont utilisé différentes approches pour aborder le problème de l'authentification les schémas d'authentification basés sur la RFID, l'authentification déléguée, PSO-AES, authentification mutuelle, et l'authentification distribuée pour les implémentations IoT.
Si et al. [81], Li et al. [48], Roy et al. [76], **Danzi et al. [18], Pan et al. [73],** **Zhou et al. [97], Yang et al. [91],** **Li et al. [82]**	Échange d'informations	Les auteurs de ces articles ont discuté et proposé l'échange d'informations basé sur la blockchain dans le cadre d'applications IoT.

Table 3.3 – Littérature sur les différentes approches de sécurité qui a été envisagées pour les applications BIoT

Nos résultats ont mis en lumière différentes manières dont la sécurité a été assurée dans certaines implémentations BIoT. Certaines de ces approches utilisaient des schémas tels que le contrôle d'accès, l'assurance de confiance et même l'authentification. Nous avons trouvé la littérature concernant le maintien de la sécurité tout en améliorant l'évolutivité de la blockchain très intéressante et un domaine qui demande encore plus de recherche. Les articles présentés examinent les implications de rendre les solutions BIoT plus évolutives tout en maintenant un niveau de sécurité élevé. Une fois qu'une application BIoT est rendue plus évolutive, cela se fait généralement au détriment d'un aspect de la blockchain qui à son tour peut provoquer des failles de sécurité.

3.3.3 Évolutivité, débit et latence

L'évolutivité est un problème majeur qui a tourmenté les blockchains au cours des années d'existence de la technologie. Il s'agit d'un problème causé par de nombreux facteurs tels que le haut niveau de cryptographie utilisé et les algorithmes de consensus utilisés (qui nécessitent généralement une puissance de calcul élevée). Il s'agit d'un aspect préoccupant lors de l'examen de la mise en œuvre du BIoT en raison des ressources limitées qui existent sur ces appareils IoT.

3.3.4 Calcul, traitement, taille de la blockchain, bande passante et infrastructure

La maintenance des réseaux blockchain sur un grand nombre de nœuds (pairs) coûte assez cher. Ces coûts découlent de la puissance de calcul, de l'énergie, du stockage et de la mémoire nécessaires pour participer à un réseau de chaînes de blocs. Dans [101], le grand livre de la blockchain était de près de 196 Go en 2018 et il est depuis passé à 306,86 Go en mai 2020. Il s'agit d'une grave préoccupation pour les solutions IoT. Cette limitation explique la raison pour laquelle la plupart des appareils IoT auraient des temps de transaction et une capacité d'évolutivité médiocres. Des solutions ont été proposées par les chercheurs pour décharger les tâches de calcul de ces appareils IoT vers des serveurs centralisés (ou des serveurs cloud) ou un serveur de brouillard, mais il a été constaté que celles-ci provoquaient des latences réseau [101].

3.3.5 Orientations et recommandations futures

À la lumière des progrès réalisés ces dernières années dans la mise en œuvre et les solutions BIoT, certains domaines nécessitent encore un examen plus approfondi. Pour améliorer davantage les applications et les solutions BIoT, des recherches et des enquêtes supplémentaires doivent avoir lieu dans certains domaines pour rendre les déploiements sûrs, sécurisés et évolutifs. Ces domaines comprennent les suivants :

- Solutions basées sur l'apprentissage automatique pour la confidentialité et la sécurité des applications BIoT. Certaines implémentations d'apprentissage automatique pour la confidentialité et la sécurité BIoT ont déjà été abordées et d'autres techniques d'apprentissage en profondeur et de clustering pour obtenir de meilleures performances, détection des intrusions et préservation de la vie privée.

- Défis techniques liés à la décentralisation. En raison de problèmes d'évolutivité, de sécurité et de confidentialité, la plupart des applications BIoT proposées jusqu'à présent ont dû ajouter une forme de centralisation à la blockchain. Des investigations et des recherches doivent être menées pour aider à réduire la tendance à la centralisation et s'orienter vers des architectures véritablement décentralisées et évolutives pour les applications BIoT.

- Infrastructure blockchain. La confiance est un élément essentiel de l'utilisation de l'IoT sur les blockchains. Un système de blockchain qui résout réellement la question de la confiance dans les implémentations BIoT, car les dispositifs IoT produisent des données très sensibles. De nombreuses approches ont été adoptées, mais elles dépendent principalement des politiques et des systèmes de contrôle interdomaines.

- Gouvernance, réglementation et aspects juridiques. Le monde de la blockchain, en raison de son niveau élevé de décentralisation, est considéré par beaucoup comme un « no man's land ». Il n'y a pas de réglementations et d'aspects juridiques majeurs qui lient l'utilisation des blockchains et leur mise en œuvre. L'ajout de l'IoT à un système dépourvu de cette forme de gouvernance peut être très dangereux. Nous ne suggérons pas que les blockchains devraient avoir des autorités entièrement centralisées, mais il devrait y avoir au moins des directives à suivre pour mettre en œuvre des solutions et des applications qui impliqueraient l'IoT.

En résumé, cette revue a examiné l'état de l'art dans le monde du BIoT et a examiné les progrès réalisés dans la recherche en utilisant les différentes approches proposées telles que l'anonymisation, l'apprentissage automatique, le clustering,etc. De là, nous avons eu une idée sur l'anonymisation cette idéé combine entre la technique qui base sur les modeles et les algorithmes matheuristiques avec la confidentialité de l'apprentissage machine basées sur la blockchain pour les appareils IoT.Cette idée réduit et se dresse devant les défits mentionnée danns la partie 3.3 : assurer l'anonymisation (3.3.1),augmenter la confidentialité avec l'apprentissage machine donc une amélioration de sécurité (3.3.2) en plus meilleure performance sur le coté calcule et traitement (3.3.3).On doit devloper et realiser cette idéé dans le prochain chapitre.

3.4 Conclusion

Nous concluons que l'IoT, tel que nous le connaissons, est venu pour rester et que les implémentations BIoT se généraliseraient bientôt, mais nous voulons faire savoir qu'il n'y a pas de réponse unique pour les applications BIoT en termes de choix architecturaux et structure du réseau. La technologie est encore en train de mûrir, et nous pouvons hardiment affirmer que cela laissera plus de place à l'avenir au développement de certaines applications qui perturberaient les industries et les entreprises. Mais pour aller de l'avant, nous prévoyons que l'utilisation plus large de cette technologie nécessitera la collaboration et la coopération des parties prenantes, des gouvernements et d'autres institutions et syndicats technologiques pour être en mesure de fournir la bonne gouvernance, la structure organisationnelle et la réglementation et les aspects juridiques pour pouvoir vraiment exploiter la puissance des applications BIoT et éviter les abus.

CHAPTER 4

PROPOSTION ET IMPLÈMENTATION

Introduction

L'utilisation des métaheuristiques hybrides s'est avérée efficace pour résoudre des problèmes de complexité élevée et pour plus de sécurité de données, ce qui nous a motivés à intégrer ce concept au problème d'anonymisation. Nous présentons, dans ce chapitre notre algorithme hybride, combinant une métaheuristique PSO avec un algorithme de clustering blockchain avec Machine Learning. Nous commençons, d'abord, par nos motivations. Nous décrivons, ensuite notre algorithme et son fonctionnement. Enfin, nous présentons sa mise œuvre et les résultats de son évaluation

4.1 Motivation

L'utilisation des algorithmes métaheuristiques inspirés de la nature pour résoudre des problèmes NP-difficiles est bien connue et assez efficace dans de nombreux domaines. Cependant, son application dans le domaine de la vie privée et de l'anonymat s'avère moins répandu, car la majorité des approches échouent à trouver le bon équilibre entre protection de la vie privée et l'utilité produisent des données mauvaise qualité.

Au cours des dernières années, l'intérêt pour les métaheuristiques hybrides a considérablement augmenté. Il a été démontré, dans de nombreux travaux que l'hybridation donne de meilleurs résultats qu'une métaheuristique hybride [86].

Le clustering, également connu sous le nom d'analyse de cluster, est devenu une technique importante dans l'apprentissage automatique utilisé pour découvrir le regroupement naturel des données observées. Souvent, une distinction claire est faite entre les problèmes d'apprentissage qui sont supervisés, également connus comme classification, et celles qui ne sont pas supervisées, appelées clustering. La première traite uniquement des données étiquetées tandis que le deuxième ne traite que des données non étiquetées. Dans de nombreuses applications réelles, il existe une grande quantité de données. Ce fait rend le regroupement plus difficile que la classification. Par conséquent, il y a un intérêt croissant pour un cadre hybride, appelé apprentissage semi-supervisé où les étiquettes de seulement une petite partie des données sont disponibles [14].

Notre approche consiste en une hybridation d'une métaheuristique avec une technique d'apprentissage automatique (Machine Learning) et d'exploration de données. Dans notre approche, un algorithme d'apprentissage non supervisé, à savoir le clustering blcokchain, est intégré à l'algorithme (PSO:Optimisation par essaims particulaires) pour améliorer la qualité de l'anonymisation. Nous avons choisi cette métaheuristique parce qu'elle a très peu été explorée, à savoir la vie privée et encore moins dans le processus d'anonymisation. De plus son fonctionnement est simple et facile à comprendre.

4.2 Approche proposée

L'approche proposée, dans ce travail, est une méthode hybride, qui combine la métaheuristique : "on a choisi l' algorithme d'optimisation par essaims particulaires (PSO)", avec une technique de clustering blockchain. L'algorithme commence par une population initiale de solutions candidates, générées aléatoirement par un algorithme de clustering. Chaque solution candidate est une solution k-anonyme, représentée par une particule.

La population de particules évolue vers la meilleure particule c'est-à-dire la solution k-anonyme ayant la plus petite perte d'information.

Après la création de solutions candidates avec l'algorithme de clustering, celles-ci doivent être codées pour être utilisées par l'algorithme d'optimisation PSO. Pour représente rcorrectement une solution, chaque particule est codée par un tableau d'entiers à une dimension, de taille égale au nombre d'enregistrements dans l'ensemble de données, où le ième indice indique le ième enregistrement et le ième élément indique l'identifiant du cluster auquel appartient le ième enregistrement.

Cette proposition et plus simple que le travail de Wai et al[56] à cause de l' algorithme d'optimisation choisie : le PSO dans notre approche plus simple que le HPSO dans [56]. De l'autre coté cette approche est un développement de la solution proposée de Mendis et al [61] par l'ajout de l' algorithme d'optimisation à l'apprentissage en profondeur.

4.2.1 Evaluation de la fitness

Pour évaluer la qualité d'une particule et sélectionner la meilleure particule, nous utilisons la fonction fitness proposée dans [57]. Cette fonction est une fonction de minimalisation, basée sur les paramètres de confidentialité (vie privée) et d'utilité. La fitness d'une particule X est calculée en utilisant l'équation suivante :

Fitness(X)=1/2*(confidentialité+utilité)... (1)

Les mesures de confidentialité et d'utilité sont exprimées comme suit :

Confidentialité(X)=F(X)

- F(X) = 0 si X satisfait k–anonymité... (2)
- F(X) = 1 sinon .

Utilité (X) =NCP (X) = la somme NCP de Xi (de i=1 jusqu'à N) ...(3)

Où Xi est le ième cluster dans la particule X. N est le nombre de cluster de X. NCP de Xi est le NCP [X] du cluster Xi.

NCP de Xi est calculé par l'équation (4) et (5), où NCP de t est le NCP d'un tuple dans le cluster Xi et |Xi| est la taille du cluster:

NCP de Xi =NCP de tuple * |Xi|...(4)

NCP de tuple = La somme NCP de j (de j=1 jusqu'à d)...(5)

Le calcul du NCP d'un attribut dépend de son type (numérique ou catégoriel). Les équations (6) et (7) expriment le NCP d'un attribut numérique et catégoriel, respectivement.

NCP de j = [|MAX(j)-MIN(j)|] /[|MAX-MIN|]...(6)

Où MIN(j)/MAX(j) correspondent aux valeurs minimales/maximales de l'attribut numérique j dans le cluster et MIN/MAX , les valeurs minimales et maximales de l'attribut dans toute la table.

NCP de j = size(Cj) /[|MAX-MIN|]...(7)

Où Cj est l'ancêtre commun, le plus proche, dans l'arbre de taxonomie des valeurs de l'attribut catégoriel j, dans le cluster. size(Cj) est le nombre de nœuds feuilles dans Cj.

4.3 Description de l'algorithme proposé

Le diagramme de l'algorithme est représenté sur la figure 4.1 :

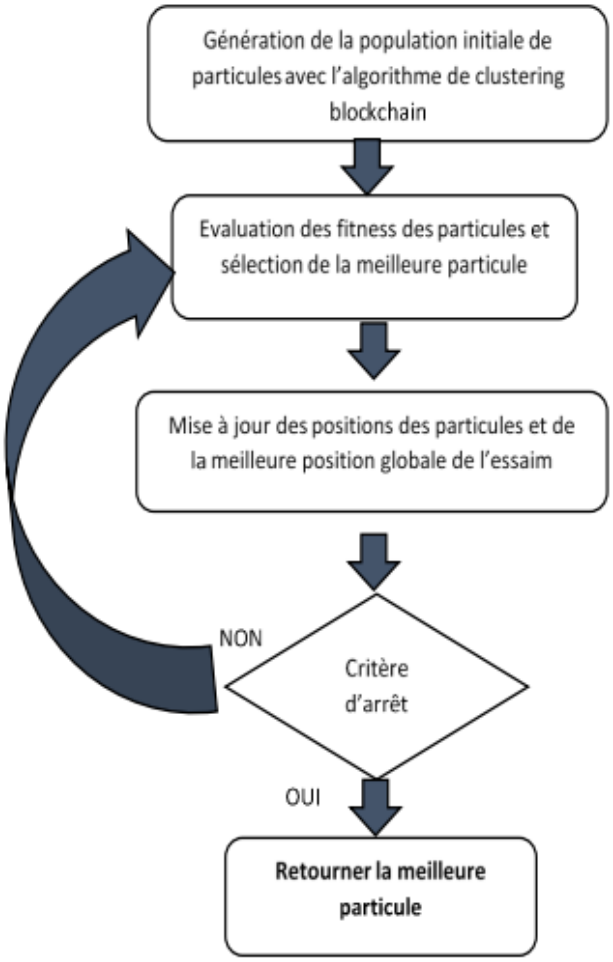

Figure 4.1 – Diagramme de l'algorithme proposé

- Génération de la population initiale : La population initiale de l'algorithme PSO se constitue d'un ensemble de particules. Chaque particule est créée, d'abord aléatoirement, avec l'algorithme de clustering et, ensuite, codée. Après cette étape, chaque particule de la population est représentée par sa position (position de chaque enregistrement, c.-à-d. son cluster) et sa fitness (qualité du clustering).
- Sélection de la meilleure particule : Après l'initialisation de la population, la fonction fitness de chaque particule est évaluée sur la base de l'équation (6) et la meilleure (avec la plus petite fitness) particule est sélectionnée.
- Mise à jour des positions :Dans cette étape, chaque particule mettra à jour sa position et calculera le fitness de la nouvelle position. Le fitness de la nouvelle

position est, ensuite, évalué, avec les équations (4) et (5) ; Si elle est inférieure à celle de la meilleure position de la particule, la position actuelle devient la meilleure position de la particule (pBest). Si elle est inférieure à la fitness de la meilleure position de la population (gBest), la position actuelle devient la meilleure position de la population.

4.4 Conception et Simulation

Après avoir décrit le fonctionnement de l'algorithme proposé, nous allons, dans cette partie,évaluer sa qualité. Pour ce faire, nous mesurons l'utilité des données anonymes, produites par notre algorithme, en termes de perte d'informations.

4.4.1 Description de l'application

Notre application a été développée avec le langage JAVA sous Windows 10 avec de 8GB de RAM, un processeur Intel i7-6500U CPU, à l'aide de l'environnement de développement Eclipse SE.
Notre application contient les classes principales suivantes :

- La classe Particle représente une particule. Elle possède les attributs position, fitness et velocity ainsi que les méthodes pour calculer/mettre à jour ces attributs.
- La classe EquivalenceClass représente une classe d'équivalence (un cluster) . Cette classe possède de nombreuses méthodes comme la méthode pour créer les clusters et attribuer les tuples aux différents clusters (clustering).
- La classe readFile est la classe principale de notre programme. Elle permet, entre autre, de lire l'ensemble de données test.

L'interface graphique de l'application est représentée dans la figure 3.5. Elle est simple à utiliser et permet d'utiliser des paramètres différents pour tester l'application. Ces paramètres sont :

- K représente le paramètre d'anonymisation. C'est le nombre minimum d'enregistrement que doit contenir chaque cluster.
- nbparticle représente le nombre de particules à générer (taille de la population).

- nbtuples représente le nombre d'enregistrements des données à anonymiser. iterations représente le nombre de cycle que le programme doit effectuer, c'est-à-dire le nombre de mise à jour de chaque particule. Ce paramètre constitue le critère d'arrêt de notre programme.

L'interface est, également, dotée de deux boutons « Exécuter » et « Quitter » permettant, respectivement, de lancer et d'arrêter l'exécution du programme. Après l'exécution du programme, la perte d'information et le temps d'exécution sont affichés dans les champs « Perte d'information » et « temps d'exécution », respectivement.

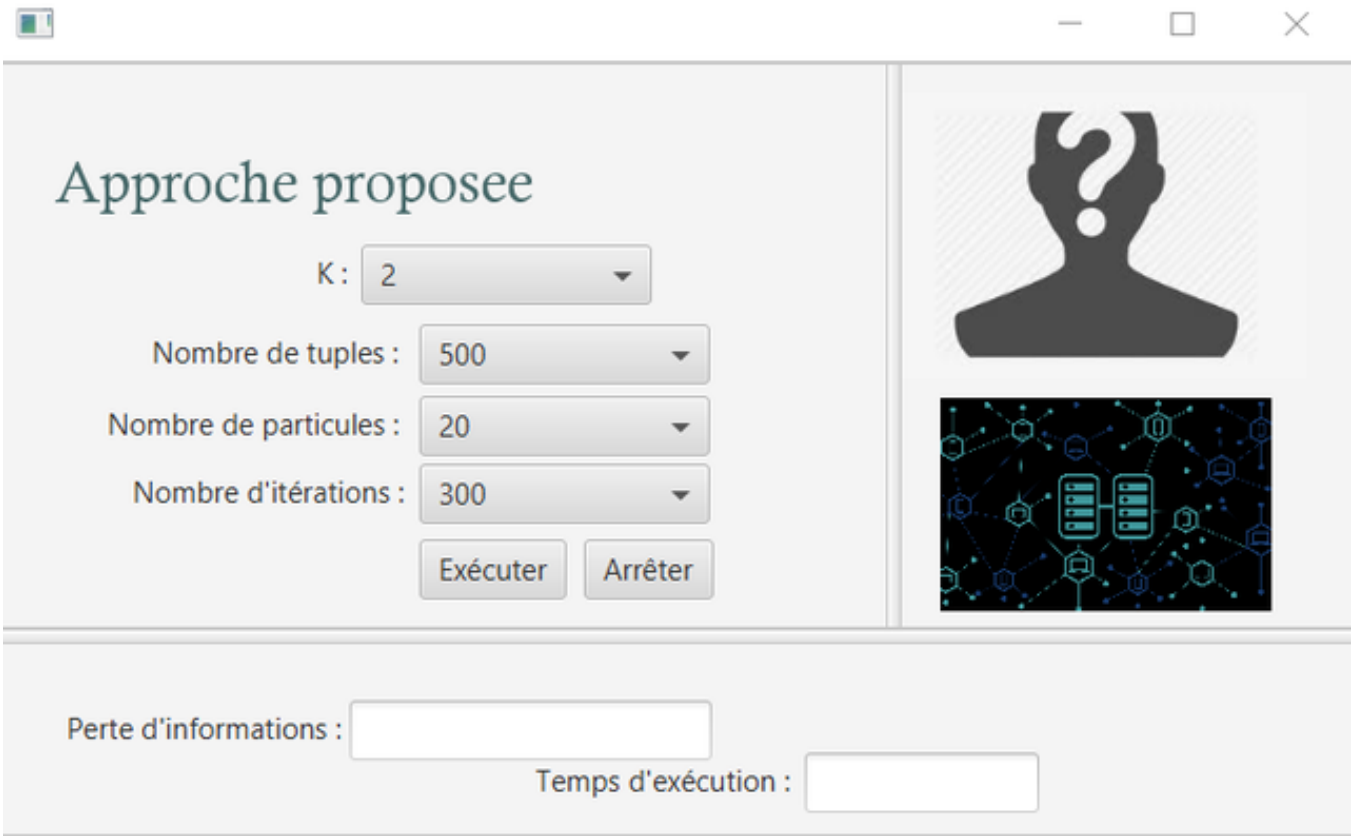

Figure 4.2 – Interface graphique de l'application proposée

4.4.2 Description de l'enemble de données test

Pour tester la qualité de notre algorithme, nous avons utilisé un ensemble de données réel adult.data (obtenue à partir de UC Irvine [62]), car c'est un référentiel pour tester la qualité d'une anonymisation. L'ensemble de données contient 32561 instances et 14 attributs. Chaque enregistrement décrit les informations personnelles d'un Américain ainsi que son revenu annuel (supérieur ou inférieur 50000 dollar). L'ensemble adult.data est destiné à des tâches de classification/prédiction dont le but est de prédire les niveaux des revenus annuels des américains en fonction de leurs informations personnelles tels que leurs âges et leurs niveaux d'études. La figure 4.3 représente un aperçu du data set. Avant de tester notre application avec ces données, nous leur appliquons une étape de

```
39, State-gov, 77516, Bachelors, 13, Never-married, Adm-clerical, Not-in-family, White, Male, 2174, 0, 40, United-States, <=50K
50, Self-emp-not-inc, 83311, Bachelors, 13, Married-civ-spouse, Exec-managerial, Husband, White, Male, 0, 0, 13, United-States, <=50K
38, Private, 215646, HS-grad, 9, Divorced, Handlers-cleaners, Not-in-family, White, Male, 0, 0, 40, United-States, <=50K
53, Private, 234721, 11th, 7, Married-civ-spouse, Handlers-cleaners, Husband, Black, Male, 0, 0, 40, United-States, <=50K
28, Private, 338409, Bachelors, 13, Married-civ-spouse, Prof-specialty, Wife, Black, Female, 0, 0, 40, Cuba, <=50K
37, Private, 284582, Masters, 14, Married-civ-spouse, Exec-managerial, Wife, White, Female, 0, 0, 40, United-States, <=50K
49, Private, 160187, 9th, 5, Married-spouse-absent, Other-service, Not-in-family, Black, Female, 0, 0, 16, Jamaica, <=50K
52, Self-emp-not-inc, 209642, HS-grad, 9, Married-civ-spouse, Exec-managerial, Husband, White, Male, 0, 0, 45, United-States, >50K
31, Private, 45781, Masters, 14, Never-married, Prof-specialty, Not-in-family, White, Female, 14084, 0, 50, United-States, >50K
42, Private, 159449, Bachelors, 13, Married-civ-spouse, Exec-managerial, Husband, White, Male, 5178, 0, 40, United-States, >50K
37, Private, 280464, Some-college, 10, Married-civ-spouse, Exec-managerial, Husband, Black, Male, 0, 0, 80, United-States, >50K
30, State-gov, 141297, Bachelors, 13, Married-civ-spouse, Prof-specialty, Husband, Asian-Pac-Islander, Male, 0, 0, 40, India, >50K
23, Private, 122272, Bachelors, 13, Never-married, Adm-clerical, Own-child, White, Female, 0, 0, 30, United-States, <=50K
32, Private, 205019, Assoc-acdm, 12, Never-married, Sales, Not-in-family, Black, Male, 0, 0, 50, United-States, <=50K
40, Private, 121772, Assoc-voc, 11, Married-civ-spouse, Craft-repair, Husband, Asian-Pac-Islander, Male, 0, 0, 40, ?, >50K
34, Private, 245487, 7th-8th, 4, Married-civ-spouse, Transport-moving, Husband, Amer-Indian-Eskimo, Male, 0, 0, 45, Mexico, <=50K
25, Self-emp-not-inc, 176756, HS-grad, 9, Never-married, Farming-fishing, Own-child, White, Male, 0, 0, 35, United-States, <=50K
32, Private, 186824, HS-grad, 9, Never-married, Machine-op-inspct, Unmarried, White, Male, 0, 0, 40, United-States, <=50K
38, Private, 28887, 11th, 7, Married-civ-spouse, Sales, Husband, White, Male, 0, 0, 50, United-States, <=50K
43, Self-emp-not-inc, 292175, Masters, 14, Divorced, Exec-managerial, Unmarried, White, Female, 0, 0, 45, United-States, >50K
40, Private, 193524, Doctorate, 16, Married-civ-spouse, Prof-specialty, Husband, White, Male, 0, 0, 60, United-States, >50K
```

Figure 4.3 – Echantillon de données originales (adult.data)

prétraitement qui se déroule en deux temps ; Les données seront, d'abord, nettoyées pour supprimer les doublons et les lignes/espaces vides. Les données nettoyées seront, ensuite, transformées, principalement pour des raisons d'efficacité, pour produire l'ensemble de données test. Cette transformation consiste, essentiellement, à coder les valeurs des attributs catégoriels, en valeurs numériques et à prendre en compte uniquement les quasi-identifiants (car ils constituent le maillon faible dans la protection de la vie privée). Nous avons retenu huit quasi-identifiants : age, work class, education-num, marital status, occupation, race, gender, native country. L'ensemble test résultant est une table à 8 colonnes et 30162 tuples. La figure ci-dessous est un aperçu de l'ensemble de données test, correspondant aux données brutes de la figure précédente.

```
0,39,0,13,0,0,0,0,0
1,50,1,13,1,1,0,0,0
2,38,2,9,2,2,0,0,0
3,53,2,7,1,2,1,0,0
4,28,2,13,1,3,1,1,1
5,37,2,14,1,1,0,1,0
6,49,2,5,3,4,1,1,2
7,52,1,9,1,1,0,0,0
8,31,2,14,0,3,0,1,0
9,42,2,13,1,1,0,0,0
10,37,2,10,1,1,1,0,0
11,30,0,13,1,3,2,0,3
12,23,2,13,0,0,0,1,0
13,32,2,12,0,5,1,0,0
14,34,2,4,1,6,3,0,4
15,25,1,9,0,7,0,0,0
16,32,2,9,0,8,0,0,0
17,38,2,7,1,5,0,0,0
18,43,1,14,2,1,0,1,0
19,40,2,16,1,3,0,0,0
```

Figure 4.4 – Aperçu des données test après l'étape de prétraitement

4.4.3 Simulation et Discussion

Dans cette section, nous allons mesurer la perte d'information des données produites avec notre application et la comparer avec celle de l'algorithme Median Mondrian [57], en raison de qualité des données qu'il produit.Nous avons testé notre application avec les paramètres suivants : k [2 ; 20], 100 tuples 50/100 itérations, c1=2 et c2=1, et mesurer la perte d'information avec la métrique NCP (équation (3.8)). Les résultats de la simulation sont décrits dans la figure 4.5. La figure 4.5 montre l'évolution de la perte

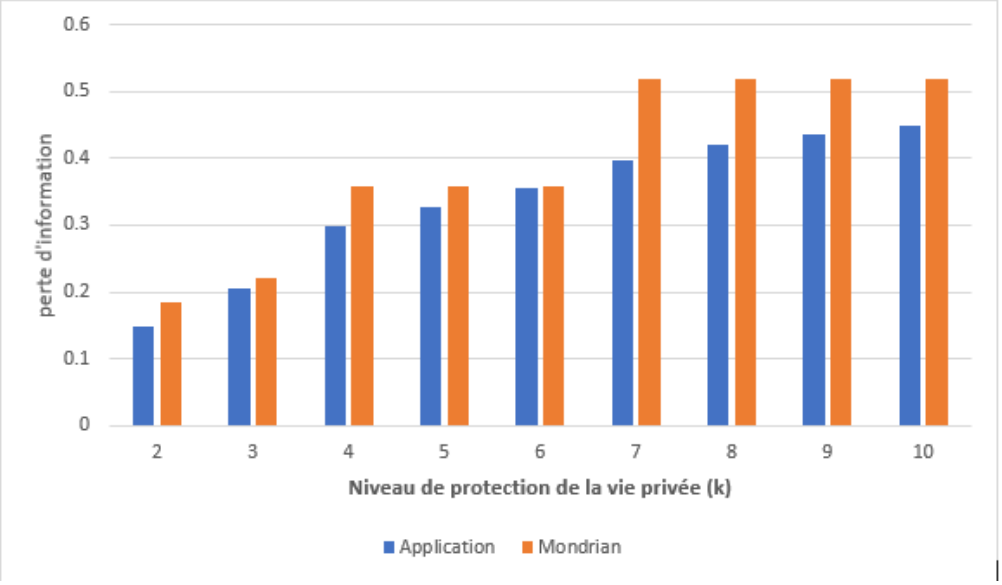

Figure 4.5 – Perte d'informations en fonction de k

d'information des deux algorithmes, en fonction de différents niveaux de protection de

vie privée, représentés par le paramètre k. Nous pouvons observer que quand la valeur de k augmente, la perte d'information, des deux algorithmes augmente. Étant donné que k représente le nombre minimal d'enregistrements dans chaque cluster, plus k est grand, plus il y a d'enregistrements dans un cluster, plus la différence entre les valeurs minimales et maximales de ce dernier est grande, et plus la perte d'informations est importante. De plus notre algorithme PSO introduit une perte d'informations plus petite que l'algorithme Mondrian et produit, donc, des données anonymes de meilleure qualité.

Une autre mesure, généralement utilisée, pour évaluer la qualité d'une métaheuristique, est la distance entre les solutions de départ et la solution finale (solution optimale). Une grande distance, signifie que la population initiale a bien évolué et c'est un gage de qualité pour la métaheuristique. Afin de mesurer cette distance, nous avons mené une deuxième expérimentation, dont le rôle est d'évaluer l'influence du nombre de particules sur la distance, et donc sur la qualité des données. Pour cela, nous avons varié le nombre de particules (50 ...500) et calculé la différence entre la perte d'information de la population initiale (moyenne) et la perte d'information de la meilleure particule. Les résultats obtenus sont représentés dans la figure 4.6. Le paramètre k et le nombre de cycle restent constants.

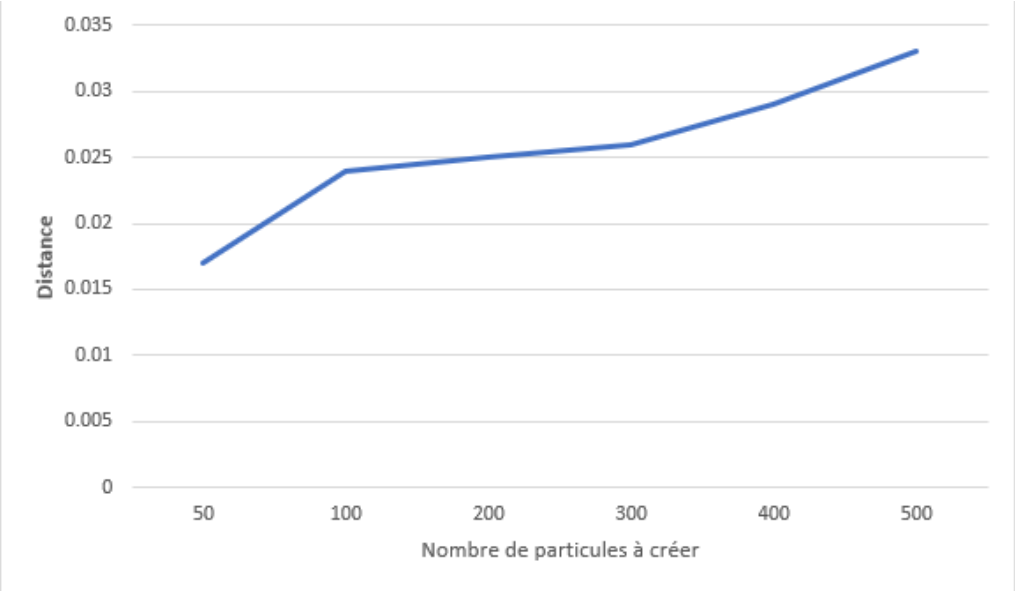

Figure 4.6 – Perte d'informations en fonction de nombre de particules crées (k=2, nombre de cycle= 500)

Nous pouvons observer, à partir de la figure 4.6, que la distance entre les solutions initiales et la solution optimale augmente proportionnellement avec l'augmentation du nombre de particules. Nous pouvons conclure que l'emploi d'une grande population de particules conduira vers une meilleure qualité de données, mais augmentera, également, le temps d'exécution.

4.5 Conclusion

Nous avons proposé, dans cette partie, notre algorithme basé sur la métaheuristique "PSO" et la technique de clustering blockchain . Nous avons décrit son fonctionnement et son implémentation. Ensuite, nous l'avons évalué, en termes de qualité de données, et comparer avec une k-anonymisation simple, implémentée avec l'algorithme Mondrian. Les résultats de l'évaluation démontrent que notre algorithme produit des données de meilleure qualité.

CONCLUSION GÉNÉRALE

L'IoT est considéré comme la prochaine étape vers l'évolution d'Internet. Il a la capacité de se connecter et 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.

Dans ce mémoires nous avons exposé un propre aperçu sur deux concepts:l'IoT et la blockchain contenant l'historique ,les définitions ,les domaines d'application, le fonctionnement et d'autres notions. Aprés nous avons présenté l'intégration de la blockchain dans l'IoT qui s'appelle la BIoT,en style d'un état de l'art avec les déférents approches proposées dans ce concept. Parmi les défis des applications BIoT, nous nous sommes focalisé sue l'anonymisation. Pour cela, nous avons eu l'idée de combiner entre la métaheuristique PSO et un algorithme de clustering blockchain avec Machine Learning.

Notre travail a été une tentative pour trouver le bon équilibre entre protection et qualité, à l'aide d'une métaheuristique combinée à une technique de clustering blockchain.Nous avons voulu démontrer, avec notre tentative, que l'intégration d'une métaheuristique hybride dans le modèle k-anonymat peut améliorer sa qualité.

En effet, nous avons comparé la qualité des données anonymisés par le k-anonymat (implémenté par l'algorithme Mondrian) et la qualité des données produites par notre algorithme, et nos données sont meilleurs. Cependant, les tests ont été réalisé sur un échantillon de l'ensemble de données. Nous proposons, comme perspective d'étendre ce travail à l'ensemble complet de données.

BIBLIOGRAPHY

[1] K. ADI, L. HAMZA, AND P. LIVIU, *Automatic security policy enforcement in computer systems*, computers & security, 73 (2018), pp. 156–171.

[2] K. ADI, L. HAMZA, AND L. PENE, *Formal modeling for security behavior analysis of computer systems*, in 2008 International MCETECH Conference on e-Technologies (mcetech 2008), IEEE, 2008, pp. 49–59.

[3] 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.

[4] R. ALSABAH, M. ALJSHAMEE, A. M. ABDULJABBAR, AND A. AL-SABBAGH, *An insight into internet sector in iraq.*, International Journal of Electrical & Computer Engineering (2088-8708), 11 (2021).

[5] A. M. ANTONOPOULOS, *Mastering Bitcoin: unlocking digital cryptocurrencies*, " O'Reilly Media, Inc.", 2014.

[6] A. M. ANTONOPOULOS AND G. WOOD, *Mastering ethereum: building smart contracts and dapps*, O'reilly Media, 2018.

[7] P. C. M. ARACHCHIGE, P. BERTOK, I. KHALIL, D. LIU, S. CAMTEPE, AND M. ATIQUZZAMAN, *A trustworthy privacy preserving framework for machine learning in industrial iot systems*, IEEE Transactions on Industrial Informatics, 16 (2020), pp. 6092–6102.

[8] P.-J. BENGHOZI, S. BUREAU, AND F. MASSIT-FOLLÉA, *L'Internet des objets / The Internet of Things: Quels Enjeux Pour L'Europe? / What Challenges for Europe?*, Les Editions de la MSH, 2009.

[9] S. BISWAS, K. SHARIF, F. LI, B. NOUR, AND Y. WANG, *A scalable blockchain framework for secure transactions in iot*, IEEE Internet of Things Journal, 6 (2018), pp. 4650–4659.

[10] B. BRAUNSCHWEIG, *Artificial intelligence: Current challenges and inria's engagement*, Inria white paper, (2016).

[11] V. BUTERIN ET AL., *A next-generation smart contract and decentralized application platform*, white paper, 3 (2014).

[12] M. CASTRO, B. LISKOV, ET AL., *Practical byzantine fault tolerance*, in OSDI, vol. 99, 1999, pp. 173–186.

[13] Y. CHALLAL, *Sécurité de l'Internet des Objets: vers une approche cognitive et systémique*, PhD thesis, Université de Technologie de Compiègne, 2012.

[14] S. S. CHAWATHE, *Clustering blockchain data*, in Clustering Methods for Big Data Analytics, Springer, 2019, pp. 43–72.

[15] K. CHRISTIDIS AND M. DEVETSIKIOTIS, *Blockchains and smart contracts for the internet of things*, Ieee Access, 4 (2016), pp. 2292–2303.

[16] A. COULON, *L'internet des objets : un gisement à exploiter*, La Lettre d'ADELI n°78, (2010).

[17] N. DAGORN, *Management de la sécurité de l'information: mise en oeuvre, évaluation et pilotage de la sécurité de l'information dans les organisations*, PhD thesis, Nancy 2, 2011.

[18] P. DANZI, A. E. KALØR, Č. STEFANOVIĆ, AND P. POPOVSKI, *Delay and communication tradeoffs for blockchain systems with lightweight iot clients*, IEEE Internet of Things Journal, 6 (2019), pp. 2354–2365.

[19] S. DE ANGELIS, L. ANIELLO, R. BALDONI, F. LOMBARDI, A. MARGHERI, AND V. SASSONE, *Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain*, Italian Conference on Cyber Security, Milan, Italy., (2018), p. 11 pp.

[20] S. DING, J. CAO, C. LI, K. FAN, AND H. LI, *A novel attribute-based access control scheme using blockchain for iot*, IEEE Access, 7 (2019), pp. 38431–38441.

[21] A. DORRI, S. S. KANHERE, R. JURDAK, AND P. GAURAVARAM, *Lsb: A lightweight scalable blockchain for iot security and anonymity*, Journal of Parallel and Distributed Computing, 134 (2019), pp. 180–197.

[22] P. DUNPHY AND F. A. PETITCOLAS, *A first look at identity management schemes on the blockchain*, IEEE security & privacy, 16 (2018), pp. 20–29.

[23] X. FAN AND Q. CHAI, *Roll-dpos: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems*, in Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2018, pp. 482–484.

[24] M. A. FERRAG, L. SHU, X. YANG, A. DERHAB, AND L. MAGLARAS, *Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges*, IEEE access, 8 (2020), pp. 32031–32053.

[25] P. FRAGA-LAMAS, T. M. FERNÁNDEZ-CARAMÉS, D. NOCEDA-DAVILA, M. A. DÍAZ-BOUZA, M. VILAR-MONTESINOS, J. D. PENA-AGRAS, AND L. CASTEDO, *Enabling automatic event detection for the pipe workshop of the shipyard 4.0*, in 2017 56th FITCE Congress, IEEE, 2017, pp. 20–27.

[26] P. FRAGA-LAMAS, T. M. FERNÁNDEZ-CARAMÉS, D. NOCEDA-DAVILA, AND M. VILAR-MONTESINOS, *Rss stabilization techniques for a real-time passive uhf rfid pipe monitoring system for smart shipyards*, in 2017 IEEE International Conference on RFID (RFID), IEEE, 2017, pp. 161–166.

[27] L. FU, X. SHEN, L. ZHU, AND J. WANG, *A low-cost uhf rfid tag chip with aes cryptography engine*, Security and Communication Networks, 7 (2014), pp. 365–375.

[28] P. GAŽI, A. KIAYIAS, AND A. RUSSELL, *Stake-bleeding attacks on proof-of-stake blockchains*, in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018, pp. 85–92.

[29] B. E. K. GHOGGALI, *Systeme des credits bancaire base sur la technologie blockchain*, Memoire de Master,Universite Mouhammed Khider de Biskra, (2020).

[30] P. GOPE, R. AMIN, S. H. ISLAM, N. KUMAR, AND V. K. BHALLA, *Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure*

with secure localization services for smart city environment, Future Generation Computer Systems, 83 (2018), pp. 629–637.

[31] J. GUBBI, R. BUYYA, S. MARUSIC, AND M. PALANISWAMI, *Internet of things (iot): A vision, architectural elements, and future directions*, Future generation computer systems, 29 (2013), pp. 1645–1660.

[32] B. HAMMI, A. FAYAD, R. KHATOUN, S. ZEADALLY, AND Y. BEGRICHE, *A lightweight ecc-based authentication scheme for internet of things (iot)*, IEEE Systems Journal, 14 (2020), pp. 3440–3450.

[33] M. T. HAMMI, B. HAMMI, P. BELLOT, AND A. SERHROUCHNI, *Bubbles of trust: A decentralized blockchain-based authentication system for iot*, Computers & Security, 78 (2018), pp. 126–142.

[34] L. HAMZA, *Génération automatique de scénario d'attaques pour les systèmes de détection d'intrusion*, PhD thesis, Université de Béjaia-Abderrahmane Mira, 2005.

[35] L. HAMZA, *Modèle d'intrus pour générer des attaques complexes dans les systèmes informatiques*, In Proceedings of the 2018 International Symposium ISKO-Maghreb, (2018), pp. 81–86.

[36] L. HAMZA, *Intruder model for generating attack scenarios in computer systems*, International Journal of Information and Computer Security, 13 (2020), pp. 428–443.

[37] L. HAMZA AND K. ADI, *Formal technique for discovering complex attacks in computer systems*, in Proceedings of the 2007 conference on New Trends in Software Methodologies, Tools and Techniques: Proceedings of the sixth SoMeT_07, 2007, pp. 185–199.

[38] L. HAMZA, K. ADI, AND K. EL GUEMHIOUI, *Automatic generation of attack scenarios for intrusion detection systems*, in Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06), IEEE, 2006, pp. 205–205.

[39] M. U. HASSAN, M. H. REHMANI, AND J. CHEN, *Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions*, Future Generation Computer Systems, 97 (2019), pp. 512–529.

[40] S. HUH, S. CHO, AND S. KIM, *Managing iot devices using blockchain platform*, in 2017 19th international conference on advanced communication technology (ICACT), IEEE, 2017, pp. 464–467.

[41] E. JEANNE, *Actifs immobiliers sobres en carbone: analyse des cheminements élaboés par Climate Bonds Initiative pour certifier l'émission d'obligations climatiques*, PhD thesis, Université de Sherbrooke, 2019.

[42] D. KEULLER AND A.-C. JEANDRAIN, *Le secteur de la santé face à l'émergence de l'internet des objets: développement d'un outil d'aide à la décision*, Memoire Master Université de Louvain, (2016).

[43] N. KOBLITZ AND A. MENEZES, *A riddle wrapped in an enigma*, IEEE Security & Privacy, 14 (2016), pp. 34–42.

[44] N. KUMAR AND R. KHANNA, *A compact multi-band multi-input multi-output antenna for 4g/5g and iot devices using theory of characteristic modes*, International Journal of RF and Microwave Computer-Aided Engineering, 30 (2020), p. e22012.

[45] L. LESAVRE, P. VARIN, P. MELL, M. DAVIDSON, AND J. SHOOK, *A taxonomic approach to understanding emerging blockchain identity management systems*, arXiv preprint arXiv:1908.00929, (2019).

[46] M. LESUEUR, L. BIRONNEAU, G. LUX, AND T. MORVAN, *Reflections on using the blockchain for logistics and supply chain management.*, in 13ème Rencontres internationales de la Recherche en Logistique et en Supply Chain Management (RIRL 2020), 2020.

[47] S. LI, M. YU, C.-S. YANG, A. S. AVESTIMEHR, S. KANNAN, AND P. VISWANATH, *Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously*, IEEE Transactions on Information Forensics and Security, 16 (2020), pp. 249–261.

[48] Z. LI, L. LIU, A. V. BARENJI, AND W. WANG, *Cloud-based manufacturing blockchain: Secure knowledge sharing for injection mould redesign*, Procedia Cirp, 72 (2018), pp. 961–966.

[49] C. LIN, D. HE, X. HUANG, K.-K. R. CHOO, AND A. V. VASILAKOS, *Bsein: A blockchain-based secure mutual authentication with fine-grained access control*

system for industry 4.0, Journal of Network and Computer Applications, 116 (2018), pp. 42–52.

[50] R. LIU, Z. WENG, S. HAO, D. CHANG, C. BAO, AND X. LI, *Addressless: enhancing iot server security using ipv6*, IEEE Access, 8 (2020), pp. 90294–90315.

[51] X. LIU, J. YU, J. WANG, AND Y. GAO, *Resource allocation with edge computing in iot networks via machine learning*, IEEE Internet of Things Journal, 7 (2020), pp. 3415–3426.

[52] Z. LIU AND H. SEO, *Iot-nums: evaluating nums elliptic curve cryptography for iot platforms*, IEEE Transactions on Information Forensics and Security, 14 (2018), pp. 720–729.

[53] S.-E. LU, Y. LIN, AND W.-C. J. SHIH, *Analyzing excessive no changes in clinical trials with clustered data*, Biometrics, 60 (2004), pp. 257–267.

[54] P. LV, L. WANG, H. ZHU, W. DENG, AND L. GU, *An iot-oriented privacy-preserving publish / subscribe model over blockchains*, IEEE Access, 7 (2019), pp. 41309–41314.

[55] D. MACRINICI, C. CARTOFEANU, AND S. GAO, *Smart contract applications within blockchain technology: A systematic mapping study*, Telematics and Informatics, 35 (2018), pp. 2337–2354.

[56] S. MADAN AND P. GOSWAMI, *A privacy preserving scheme for big data publishing in the cloud using k-anonymization and hybridized optimization algorithm*, (2018), pp. 1–7.

[57] S. MADAN AND P. GOSWAMI, *A novel technique for privacy preservation using k-anonymization and nature inspired optimization algorithms*, in Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, 2019.

[58] S. MAHJOUM, D. RUFINO-RAMOS, L. PEREIRA DE ALMEIDA, M. L. BROEKMAN, X. O. BREAKEFIELD, AND T. S. VAN SOLINGE, *Living proof of activity of extracellular vesicles in the central nervous system*, International Journal of Molecular Sciences, 22 (2021), p. 7294.

[59] V. MATYAS, S. FISCHER-HÜBNER, D. CVRCEK, AND P. SVENDA, *The future of identity in the information society:4th ifip wg 9.2, .6/11.6, 11.7/ FIDIS international summer school Brno, Czech Republic, september 1-7, 2008 revised selected papers*, vol. 298, 01 2009.

[60] A. MAW, S. ADEPU, AND A. MATHUR, *Ics-blockops: Blockchain for operational data security in industrial control system*, Pervasive and Mobile Computing, 59 (2019), p. 101048.

[61] G. J. MENDIS, Y. WU, J. WEI, M. SABOUNCHI, AND R. ROCHE, *A blockchain-powered decentralized and secure computing paradigm*, IEEE Transactions on Emerging Topics in Computing, (2020).

[62] N. METROPOLIS, A. W. ROSENBLUTH, M. N. ROSENBLUTH, A. H. TELLER, AND E. TELLER, *Equation of state calculations by fast computing machines*, The journal of chemical physics, 21 (1953), pp. 1087–1092.

[63] D. C. MILLS, K. WANG, B. MALONE, A. RAVI, J. MARQUARDT, A. I. BADEV, T. BREZINSKI, L. FAHY, K. LIAO, V. KARGENIAN, ET AL., *Distributed ledger technology in payments, clearing, and settlement*, (2016).

[64] D. C. MILLS, M. WANG, KATHY, ET AL., *Distributed ledger technology in payments, clearing, and settlement*, (2016), pp. 8–30.

[65] B. K. MOHANTA, S. S. PANDA, U. SATAPATHY, D. JENA, AND D. GOUNTIA, *Trustworthy management in decentralized iot application using blockchain*, in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2019, pp. 1–5.

[66] B. K. MOHANTA, A. SAHOO, S. PATEL, S. S. PANDA, D. JENA, AND D. GOUNTIA, *Decauth: Decentralized authentication scheme for iot device using ethereum blockchain*, in TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 558–563.

[67] A. MOHSIN, A. ZAIDAN, B. ZAIDAN, O. S. ALBAHRI, A. S. ALBAHRI, M. ALSALEM, AND K. MOHAMMED, *Based blockchain-pso-aes techniques in finger vein biometrics: A novel verification secure framework for patient authentication*, Computer Standards & Interfaces, 66 (2019), p. 103343.

[68] D. J. MOROZ, D. J. ARONOFF, N. NARULA, AND D. C. PARKES, *Double-spend counterattacks: Threat of retaliation in proof-of-work systems*, arXiv preprint arXiv:2002.10736, (2020).

[69] C. NARTEY, E. T. TCHAO, J. D. GADZE, E. KEELSON, G. S. KLOGO, B. KOMMEY, AND K. DIAWUO, *On blockchain and iot integration platforms: current implementation challenges and future perspectives*, Wireless Communications and Mobile Computing, (2021).

[70] J. NAVARRO-ORTIZ, S. SENDRA, P. AMEIGEIRAS, AND J. M. LOPEZ-SOLER, *Integration of lorawan and 4g/5g for the industrial internet of things*, IEEE Communications Magazine, 56 (2018), pp. 60–67.

[71] S. OLNES, J. UBACHT, AND M. JANSSEN, *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*, Government Information Quarterly, 34 (2017), pp. 355–364.

[72] M. M. OTHMAN AND A. EL-MOUSA, *Internet of things & cloud computing internet of things as a service approach*, in 2020 11th International Conference on Information and Communication Systems (ICICS), IEEE, 2020, pp. 318–323.

[73] J. PAN, J. WANG, A. HESTER, I. ALQERM, Y. LIU, AND Y. ZHAO, *Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts*, IEEE Internet of Things Journal, 6 (2018), pp. 4719–4732.

[74] D. PUTHAL, N. MALIK, S. P. MOHANTY, E. KOUGIANOS, AND G. DAS, *Everything you wanted to know about the blockchain: Its promise, components, processes, and problems*, IEEE Consumer Electronics Magazine, 7 (2018), pp. 6–14.

[75] A. REYNA, C. MARTÍN, J. CHEN, E. SOLER, AND M. DÍAZ, *On blockchain and its integration with iot. challenges and opportunities*, Future generation computer systems, 88 (2018), pp. 173–190.

[76] D. G. ROY, P. DAS, D. DE, AND R. BUYYA, *Qos-aware secure transaction framework for internet of things using blockchain mechanism*, Journal of Network and Computer Applications, 144 (2019), pp. 59–78.

[77] C. RUN, H. J. KIM, D.-H. LEE, C. G. KIM, AND K. J. KIM, *Protecting privacy using k-anonymity with a hybrid search scheme*, International Journal of Computer and Communication Engineering, 1 (2012), p. 155.

[78] G. SAGIRLAR, B. CARMINATI, AND E. FERRARI, *Decentralizing privacy enforcement for internet of things smart objects*, Computer Networks, 143 (2018), pp. 112–125.

[79] M. SHEN, X. TANG, L. ZHU, X. DU, AND M. GUIZANI, *Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities*, IEEE Internet of Things Journal, 6 (2019), pp. 7702–7712.

[80] N. SHI, L. TAN, C. YANG, C. HE, J. XU, Y. LU, AND H. XU, *Bacs: A blockchain-based access control scheme in distributed internet of things*, Peer-to-peer networking and applications, 14 (2021), pp. 2585–2599.

[81] H. SI, C. SUN, Y. LI, H. QIAO, AND L. SHI, *Iot information sharing security mechanism based on blockchain technology*, Future Generation Computer Systems, 101 (2019), pp. 1028–1040.

[82] J. C. SONG, M. A. DEMIR, J. J. PREVOST, AND P. RAD, *Blockchain design for trusted decentralized iot networks*, in 2018 13th Annual Conference on System of Systems Engineering (SoSE), IEEE, 2018, pp. 169–174.

[83] M. SUÁREZ-ALBELA, T. M. FERNÁNDEZ-CARAMÉS, P. FRAGA-LAMAS, AND L. CASTEDO, *A practical performance comparison of ecc and rsa for resource-constrained iot devices*, in 2018 Global Internet of Things Summit (GIoTS), IEEE, 2018, pp. 1–6.

[84] T. SULTANA, A. ALMOGREN, M. AKBAR, M. ZUAIR, I. ULLAH, AND N. JAVAID, *Data sharing system integrating access control mechanism using blockchain-based smart contracts for iot devices*, Applied Sciences, 10 (2020), p. 488.

[85] N. TAHAT, A. A. TAHAT, M. ABU-DALU, R. B. ALBADARNEH, A. E. ABDALLAH, AND O. M. AL-HAZAIMEH, *A new rsa public key encryption scheme with chaotic maps.*, International Journal of Electrical & Computer Engineering (2088-8708), 10 (2020).

[86] E.-G. TALBI, *Metaheuristics: from design to implementation*, vol. 74, John Wiley & Sons, 2009.

[87] F. TIAN, *An agri-food supply chain traceability system for china based on rfid & blockchain technology*, in 2016 13th international conference on service systems and service management (ICSSSM), IEEE, 2016, pp. 1–6.

[88] M. TORKY AND A. E. HASSANEIN, *Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges*, Computers and Electronics in Agriculture, (2020), p. 105476.

[89] K.-L. TSAI, Y.-L. HUANG, F.-Y. LEU, I. YOU, Y.-L. HUANG, AND C.-H. TSAI, *Aes-128 based secure low power communication for lorawan iot environments*, Ieee Access, 6 (2018), pp. 45325–45334.

[90] L. XIE, Y. DING, H. YANG, AND X. WANG, *Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets*, IEEE Access, 7 (2019), pp. 56656–56666.

[91] J. YANG, Z. LU, AND J. WU, *Smart-toy-edge-computing-oriented data exchange based on blockchain*, Journal of Systems Architecture, 87 (2018), pp. 36–48.

[92] H. ZAHMATKESH AND F. AL-TURJMAN, *Fog computing for sustainable smart cities in the iot era: Caching techniques and enabling technologies-an overview*, Sustainable Cities and Society, 59 (2020), p. 102139.

[93] X. ZHANG, C. LIU, S. POSLAD, AND K. K. CHAI, *A provable semi-outsourcing privacy preserving scheme for data transmission from iot devices*, IEEE Access, 7 (2019), pp. 87169–87177.

[94] Y. ZHANG, S. KASAHARA, Y. SHEN, X. JIANG, AND J. WAN, *Smart contract-based access control for the internet of things*, IEEE Internet of Things Journal, 6 (2018), pp. 1594–1605.

[95] N. ZHENG AND Z. G. IVES, *Compact, tamper-resistant archival of fine-grained provenance*, Proceedings of the VLDB Endowment, 14 (2020), pp. 485–497.

[96] Z. ZHENG, S. XIE, H.-N. DAI, X. CHEN, AND H. WANG, *Blockchain challenges and opportunities: A survey*, International Journal of Web and Grid Services, 14 (2018), pp. 352–375.

[97] L. ZHOU, L. WANG, Y. SUN, AND P. LV, *Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation*, IEEE Access, 6 (2018), pp. 43472–43488.

[98] S. ZIEGLER, P. KIRSTEIN, L. LADID, A. SKARMETA, AND A. JARA, *The case for ipv6 as an enabler of the internet of things*, IEEE Internet of Things, (2015), pp. 395–399.

RÉSUMÉ

L'IoT, depuis sa création et son adoption massive, a montré un grand potentiel en matière de sa capacité à transformer et optimiser les activités manuelles et à les intégrer dans la révolution numérique.Pendant ce temps, assurer la confidentialité et la sécurité est une partie indissociable de cette technologie. Sans fournir une sécurité suffisante, les avantages prometteurs de cette technologie florissante seront mal utilisés et sans valeur. Pour cela la blockchain avec toutes ces augmentation pour la sécurité a intégré l'IoT et nous est apparu un nouveau concept qui s'appelle BIoT, cette technologie est encore en train de mûrir alors plusieurs mises a jour et adaptions sont proposées et réalisées dans ce concept pour l'endurance devant les différents défis actuels rencontrés.L'objectif de ce mémoire est de définir proprement les deux concpts la sécurité dans l'IoT et la blockchain, ensuite examiné l'état de l'art dans le monde du BIoT et les progrès réalisés dans la recherche, enfin présenter notre idée sur l'anonymisation qui combine entre les algorithmes matheuristiques et un algorithme de clustering blockchain avec Machine Learning. Cette idée réduit et se dresse devant les défits avec l'assurance de l'anonymisation,l'augmentation de la confidentialité et une augmentation aussi de performance sur le coté calcule et traitement.

Mots clés : IoT, Blockchain, BIoT, sécurité des données, Anonymisation, Apprentissage automatique, Machinig Leraning.

Abstract

The IoT, since its inception and mass adoption, has shown great potential in its ability to transform and optimize manual activities and integrate them into the digital revolution. Meanwhile, ensuring privacy and security is an inseparable part of this technology. Without providing sufficient security, the promising advantages of this flourishing technology will be misused and worthless. For this the blockchain with all these increases for security has integrated the IoT and a new concept appeared to us called BIoT, this technology is still in the process of maturing so several updates and adaptations are proposed and carried out in this concept for endurance in the face of the various current challenges encountered.The objective of this thesis is to properly define the two concepts of security in IoT and blockchain, then examined the state of the art in the world of BIoT and the progress made in research, finally presenting our idea on anonymization which combines between matheuristic algorithms and a blockchain clustering algorithm with Machine Learning. This idea reduces and stands up to the challenges with the assurance of anonymization, increased confidentiality and also increased performance on the compute and processing side.

Keywords : Internet of Things, IoT, Blockchain, BIoT, Data security , Anonymization, Machine Learning,.