الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت بلحاج بوشعيب
Université de Ain Temouchent- Belhadj Bouchaib
Faculté des Sciences et de la Technologie
Département de Mathématiques et Informatique

Projet de Fin d'Etudes
Pour l'obtention du diplôme de Master en Informatique
Domaine : Mathématique et Informatique
Filière : Informatique
Spécialité : Réseau et Ingénierie de données

Thème

Une approche d'intégration Blockchain-Fog computing

Réalisé par :
1) Melle Ahmed Meriem
2) Melle Zeroual Asma

Soutenu le : 27 /06/2022

Devant le jury composé de :

Dr BENZERBADJ Ali	MCB	UAT.B.B (Ain Temouchent)	Président
Dr BEDAD Fatima	MCB	UAT.B.B (Ain Temouchent)	Examinatrice
Dr MEDEDJEL Mansour	MCA	UAT.B.B (Ain Temouchent)	Encadrant

Année Universitaire 2021/2022

RÉSUMÉ

L'adoption de l'Internet des objets (IoT) connaît une croissance importante et réussie dans de nombreux domaines. Néanmoins, la demande croissante d'appareils connectés entraîne le besoin d'architectures IoT évolutives qui sont capables de rapprocher le traitement, la communication et le stockage des appareils et des utilisateurs finaux tout en mutualisant les ressources locales. Ainsi, le Fog Computing (FC) peut être utilisé comme plate-forme intermédiaire entre les appareils IoT et le cloud traditionnel pour répondre aux exigences des applications sensibles à la latence en réduisant le temps de traitement et la quantité de données à transférer vers le cloud. La Blockchain (BC) fait partie des technologies révolutionnaires qui pourraient influencer de nombreux domaines. Un tel déploiement de cette technologie offrirait des moyens plus efficaces d'effectuer des tâches de manière décentralisée (peer-to-peer) en fournissant une gestion des données fiable, immuable et sécurisée. Ces critères peuvent être d'une grande importance pour l'IoT et le Fog computing. Par conséquent, l'intégration de ces deux technologies (BC-FC) pourrait aider à résoudre de nombreux problèmes auxquels sont confrontés les environnements IoT, tels que le stockage des données, la sécurité, la gestion des identités et la réduction des coûts. A travers ce projet de fin d'étude, nous avons simulé cette intégration en implémentant deux algorithmes de consensus, à savoir PBFT et PoET pour augmenter la sécurité, minimiser la consommation d'énergie et être plus adaptable aux contraintes des objets connectés. L'étude menée a démontré la fiabilité et la faisabilité des algorithmes de consensus mis en œuvre en termes de temps de réponse.

Mots clés : Blockchain, Fog computing, Internet des objets, Consensus.

REMERCIEMENTS

Tout d'abord, on remercie Dieu tout Puissant de nous avoir donné la force et la patience nécessaire pour achever ce travail de mémoire.

Nos sincères remerciements à notre honorable encadrant Mr MEDEDJEL Mansour tout d'abord d'avoir proposé ce thème qui nous a été trop bénéfique, ensuite pour sa disponibilité, son soutien continu, sa motivation, ainsi que pour ses précieux conseils, ses remarques enrichissantes et la confiance qu'il nous a accordée.

Nous remercions aussi les membres du jury : Mr BENZERBADJ Ali et Mme BEDAD Fatima d'avoir accepté de faire partie du jury.

À nos parents, nos frères et soeurs pour leur amour et support inconditionnel.

Enfin, on adresse nos remerciements à ceux qui nous ont aidé et soutenu de près plus précisément notre amie LAOUARI DOUNYA ou de loin pour l'accomplissement de ce travail.

DÉDICACES

Je dédie ce modéste travail à :

Ma chère mère,
Mon chèr père,

Qui n'ont jamais cessé de formuler des prières a mon égard, de me soutenir et de m'épauler pour que je puisse atteindre mes objectifs.

A mon frère,
A petite soeur,
A mon support dans ma vie,

Pour leur soutien moral et leurs conseils précieux tout au long de mes études.

A ASMA ma chère soeur avant d'être un binôme,

Pour sa sympathie et sa patience.

A mes amies, DOUNYA, YOUSSRA, FATIMA,

Pour leurs aides et support dans les moments difficiles.

MERIEM

A ma très chère mère,

Quoi que je fasse ou que je dis, je ne saurais point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes cotés a toujours été ma source de force pour affronter les différents obstacles.

A mon très cher père,

Tu as toujours été à mes côtés pour me soutenir et m'encourager. Que ce travail traduit ma gratitude et mon affection.

A Lhadja Zeroual pour son encouragement permanent et son soutien moral A ma soeur, mes frères

Pour leur appui et leur soutien moral.

A tous qui sont proches en particulier Medjat Mohammed
A mon amie Laouari Dounya et Rajaa Boulefdaoui

Sans oublier

Mon binôme

ASMA

SOMMAIRE

TABLE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

L'Internet des objets (Internet of Things, IoT) désigne l'ensemble des objets, des technologies et des réseaux mis en place pour permettre la communication et l'interaction entre ces objets physiques à travers l'internet. Récemment, l'IoT a gagné en importance en raison du grand impact qu'il a eu sur tous les aspects de notre vie. On s'attend à ce que l'IoT change complètement notre vie en introduisant un large éventail d'applications dans divers domaines. Ces applications incluent, à titre non exhaustif, la maison intelligente(Smart home), la ville intelligente(Smart city), la santé, les véhicules intelligents et la surveillance à distance.

Selon Cisco [9], d'ici 2025 il y aura 75 milliards de dispositifs IoT connectés dans le monde entier.

Ce grand nombre d'appareils connectés impose des contraintes élevées sur la structure et la conception du système en termes de couverture réseau, fiabilité du système, sécurité, confidentialité, quantité de données générées et interopérabilité avec d'autres réseaux existants, ainsi que les contraintes de latence et de bande passante pour certaines applications.

Le Cloud computing, se positionne comme étant un élément clé pour l'IoT qui fournit un pool de ressources à grande capacité et peut être utilisé pour combler les limites en ressources des objets connectés. Cependant, le Cloud constitué principalement d'un ensemble de centres de données éloignés des objets, rend son utilisation désavantageuse face aux containtes des applications IoT qui sont souvent sensibles aux délais. En outre, le grand nombre des capteurs et dispositifs IoT génère un volume de données important dont le transfert et le traitement dans le Cloud risque d'encombrer le réseau.

Pour surmonter ces défis et atteindre une plus grande efficacité des systèmes, connectants ce grand nombre d'appareils et d'objets, de nouveaux paradigmes et technologies de communication sont déployés tels que le Fog computing. Ce dernier permet de décentraliser les services traditionnellement fournis par le Cloud sur l'ensemble des équipements réseaux. Il permet d'utiliser les ressources de calcul et de stockage des équipements réseaux tels que les routeurs et les switchs localisés entre les objets connectés et les centres de données du Cloud. Cependant, une telle architecture décentralisée n'est pas toujours suffisante pour gérer certaines transactions et données privés. À ce stade, la technologie de la Blockchain s'impose comme une solution prometteuse et efficace pour résoudre certains problèmes persistant avec le Fog computing.

Le déploiement des paradigmes de Blockchain et le Fog computing pour les réseaux IoT, permet une décentralisation qui offre divers avantages, notamment la gestion des ressources informatiques décentralisées, l'augmentation de la flexibilité globale du système, l'amélioration de la sécurité du système en empêchant diverses menaces et attaques, ainsi que la réduction des coûts de fonctionnement du système.

Dans ce contexte, ce projet de fin d'études, met l'accent sur l'utilisation de la Blockchain et le Fog computing pour résoudre certains problèmes qui émergent du concept global d'intégration entre la Blockchain et l'IoT.

Dans ce mémoire, nous avons mené une étude théorique et expérimentale sur l'approche d'intégration de ces deux concepts. Le manuscrit est organisé comme suit : le premier chapitre présente les concepts fondamentaux de la technologie Blockchain. Le deuxiéme chapitre est consacré au paradigme du Fog computing. Dans le troisiéme chapitre nous présentons la convergence de Blockchain et l'IoT en mettant l'accent sur l'intégration Blockchain-Fog computing qui constitut ainsi l'objet d'une étude expérimentale(Simulation) dans le quatrième chapitre. Une conclusion est donnée à la fin de ce manuscrit.

CHAPITRE 1

LA BLOCKCHAIN

1.1 Introduction

Aujourd'hui, notre monde est de plus en plus mouvant et évolue au rythme des inventions et des nouvelles technologies. Blockchain, un phénomène à la pointe de l'innovation qui a introduit un bouleversement comparable à celui que nous avons connu avec Internet dans les années 90.

Cette technologie apporte ce qu'il manquait à Internet : la possibilité de transférer de la valeur directement entre les internautes sans intermédiaire. Plus précisément, la Blockchain a donné naissance à «l'Internet des valeurs », ou le transfert de valeur se fait librement, immédiatement, sans frais, sans considération ni de volume ni de distance.

La Blockchain a gagné en popularité après l'introduction du Bitcoin en 2008 par Satoshi Nakamoto [10]. Beaucoup de gens confondent et pensent que la Blockchain est du Bitcoin. Mais, le Bitcoin est une application de cette technologie avec des concepts cryptographiques. La Blockchain a créé un nouveau paradigme de confiance. Ce nouveau modèle de confiance hérite de registre distribué (Distributed Ledger Technology "DLT")

[11]. Bien que cette Dernière et le grand livre distribué semblent similaires, il existe quelques différences entre les deux. La Blockchain peut être classée comme un type de grand livre distribué, mais vous ne pouvez pas classer chaque grand livre distribué comme une chaine de bloc .

Ce premier chapitre présente les notions générales de la technologie Blockchain, incluant l'historique, les domaines d'application, l'architecture et le fonctionnement.

1.2 Définitions

Définition 1

Une Blockchain **(BC ou chaîne de blocs en français)**, est une suite des blocs reliés entre eux sous forme d'une chaîne. Chaque bloc contient un enregistrement de tous les échanges effectués entre les utilisateurs de la Blockchain, en un intervalle de temps donné. Les différents blocs fournissent un historique de toutes les transactions crées depuis la création de la Blockchain et permettent ainsi à chacun de contrôler l'exactitude des données échangées [1].

Définition 2

Une Blockchain se compose de plusieurs nœuds, qui ne se font pas confiance, qui exécutent les services demandés dans un environnement et valident les transactions grâce à une méthode de confiance déployé par l'ensemble du réseau [12].

1.3 Histoire de la Blockchain

La technologie de la Blockchain est l'une des plus grandes innovations du 21 ème siècle. L'histoire de la Blockchain remonte au début des années 1990 [13].

— En 1991 : L'architecture derrière la technologie de la Blockchain a été décrite dès 1991 quand les chercheurs Stuart Haber et W. Scott Stornetta ont travaillé sur une chaîne de blocs sécurisée de manière cryptographique, selon laquelle la personne ne pouvait altérer l'horodatage des documents [12].

— En 1992 : Ces chercheurs ont mis à niveau leur système afin d'incorporer les arborescences Merkle, ce qui permet l'amélioration d'efficacité, et ainsi la possibilité de collecter des documents sur un seul bloc, cependant cette technologie tomba dans l'oubli.

— En 1995 : Le NY Times met en place la première Blockchain dans le journal.

— En 2004 : L'informaticien et l'activiste cryptographique Hal Finney, lance un système appelé RPoW (Reusable Proofs of Work). RPoW a résolu le problème de la double dépense, conçu pour permettre à n'importe quel utilisateur à travers le monde de vérifier son exactitude et son intégrité en temps réel.

— En 2008 : La première Blockchain est apparue fin 2008 avec la monnaie numérique Bitcoin, développée par un inconnu sous le pseudonyme de Satoshi Nakamoto [14]. Le logiciel Bitcoin original a été mis à la disposition du public en janvier 2009. Il s'agissait d'un logiciel open source. Il consiste en un système expérimental de transfert et de vérification de propriété reposant sur un réseau peer-to-peer sans aucune autorité centrale.

— En 2013 : Vitalik Buterin, programmeur et fondateur du magazine Bitcoin, a fondé Ethereum, une Blockchain plus volatile, qui n'était pas uniquement utilisée pour les monnaies.

— En 2015 : Vitalik Buterin, a lancé Ethereum qui est un réseau de Blockchain publique distribué qui vise à exécuter le code de n'importe quelle application décentralisée "Contrats intelligents" [15].

1.4 L'évolution de la Blockchain

Les fonctionnalités de la technologie Blockchain ont évolué au fil du temps [16].

— **Blockchain 1.0 :** Les applications liées aux liquidités, telles que le transfert de devises et les systèmes de paiement numérique, ont permis de former la couche technologique supportant la création de la Blockchain 1.0. Le premier type de transactions a été le Bitcoin qui utilise une cryptomonnaie virtuelle.

— **Blockchain 2.0 :** L'ensemble des applications économiques, commerciales et financières requièrent des fonctionnalités plus larges que de simples transactions monétaires. La Blockchain 2.0 a vu le jour, elle a permis l'utilisation du modèles de «Contrats intelligents».

— **Blockchain 3.0 :** La Blockchain 3.0 est un concept d'application au-delà de la cryptomonnaie. Elle s'appuie sur les contrats intelligents pour développer des organisations décentralisées. Cette Blockchain 3.0 est encore au stade de concept.

1.5 Caractéristiques de la Blockchain

Plusieurs caractéristiques sont associées à la Blockchain, parmi lesquelles, nous pouvons citer :

• **Désintermédiation :** Les transactions ne sont pas gérées par une autorité centralisée. Mais plutôt par échange de pair à pair (peer-to-peer). L'information est transférée directement entre les tiers concernés. Par exemple, quand on achète un objet dans un magasin et qu'on paye avec du cash, l'argent va directement au gérant. En revanche, si l'on paie par carte bancaire, l'échange ne s'effectue plus de pair à pair mais plutôt par une autorité centralisée : la banque dans ce cas. Le Bitcoin est donc, théoriquement une forme de cash digital.

• **Traçabilité et transparence :** Tous les utilisateurs de la Blockchain peuvent voir toutes les transactions effectuées depuis la création du premier bloc.

• **Consensus distribué :** Chaque Blockchain dispose d'un mécanisme de consensus distribué. Dans ce mécanisme, les blocs doivent être validés en appliquant un algorithme exécuté par plusieurs utilisateurs.

• **Immuable :** Une fois qu'un bloc est créé, il ne peut pas être effacé et sa modification engendrera forcément la création d'un autre bloc.

• **Structure distribuée** : Le système n'est pas centralisé. C'est-à-dire que pratiquement tous les usagers sont reliés entre eux et gèrent le système sur un pur mode peer-to-peer.

• **Résilience :** La Blockchain est très résistante aux pannes et aux attaques car toutes les données sont copiées dans plusieurs serveurs. En effet, s'il est possible d'attaquer à un ou plusieurs ordinateurs, il sera plus compliqué d'attaquer un ensemble de blocs d'informations copiés dans plusieurs ordinateurs connectés au réseau.

• **Sécurité :** La résilience offre à la Bockchain un haut niveau de sécurité. Par conséquent, les fonctions cryptographiques appliquées rendent les informations stockées infalsifiables.
• **Confiance :** Le système repose sur une confiance automatisée, réciproque des utilisateurs. Il n'y a pas d'organisme central, le système est alors géré par tous suivant les principes de la décentralisation.

1.6 La Blockchain en couches

Les composants technologiques sous-jacents de la Blockchain comprennent les transactions, les blocs, les consensus, les applications et les contrats intelligents qui construisent l'écosystème de la Blockchain peuvent être divisés en six couches répertoriées comme suit : couches de réseau, de transaction, de Blockchain, de confiance, d'application et de sécurité. Chacune de ces couches a des propriétés et des caractéristiques différentes, comme le montre la Figure 1.1.
La couche réseau fait référence à un réseau P2P. La couche de transaction fait référence aux transactions déclenchées par les utilisateurs ou le contrat intelligent. La couche Blockchain fait référence au statut de bloc contenant toutes les informations nécessaires, tandis que la couche de confiance se réfère au protocole de consensus pour la validation de bloc et de transactions. La couche d'application englobe les applications et les contrats intelligents. La couche de sécurité est essentielle pour la technologie Blockchain car la Blockchain est vulnérable à de nombreux types d'attaques (l'attaque de 51 % est la plus connue) [1].

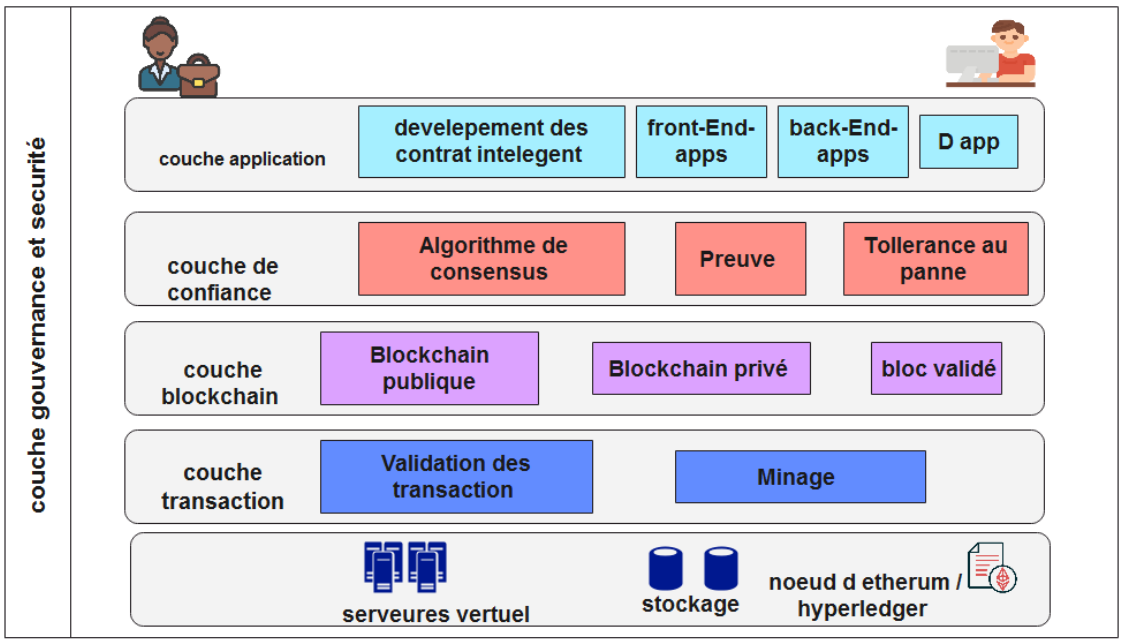

FIGURE 1.1 – Les couches de Blockchain [1]

1.7 Types de Blockchain

1.7.1 La Blockchain publique

Une Blockchain publique ou sans permission est un réseau décentralisé qui fonctionne de pair-à-pair et sans autorité centrale. C'était le premier type de Blockchain qui existait. Un exemple de ce dernier est Bitcoin, Ethereum, Tiret, Monero Zcash.
Ce type de Blockchain garde ses données, ses logiciels et son développement ouverts au public, afin que chacun puisse les revoir, les auditer, les développer ou les améliorer [17].

1.7.2 La Blockchain privée

Ce type de Blockchain a généralement les mêmes éléments qu'une Blockchain publique, cependant une Blockchain privée dépend d'une unité centrale qui contrôle toutes les actions en son sein. Les transactions sont émises et validées par tous les nœuds, par contre l'ajout des blocs à la chaîne ainsi le choix du protocole de consensus se fait par l'autorité centrale.
Les Blockchain avec permission sont principalement utilisés par les entreprises afin d'assurer leurs confidentialité. L'un des développements les plus importants de la Blockchain privée dans le monde de la cryptographie est Hyperligue [18].

1.7.3 La Blockchain consortium

La Blockchain de consortium, également connue sous le nom de Blockchain fédérée, est similaire à une blockchain hybride, est une fusion entre les Blockchain publiques et privées. Ce type de Blockchain peut être considéré comme partiellement décentralisé, car le droit d'accès au réseau peut être limité à un certain nombre de participant.
Dans cette Blockchain, il existe généralement deux types d'utilisateurs. L'un est l'utilisateur qui a tous les contrôles sur la Blockchain, tandis que les autres sont ceux qui accèdent simplement à la Blockchain.

1.7.4 La différence entre Blockchain publique, privée et consortium

Le tableau suivant montre la différence entre les trois types de Blockchain :

	Privé	Publique	Consortium
Caractéristique	L'accés limité par autorité central. L'accés au registre d'information est privé.	Tout le monde fait partie Fonctionnenement du réseau est totalement transparent. Pas de tierce de confiance.	Pas de minage. L'accés au information est publique.
Avantage	+control d'accès. +perfermance.	+Indépendance. +transparance. +confiance.	+control d'acces. +scalabilite. +sécurité.
Désavantage	-Confiance. -Auditabilité.	-Perfermance. -Scalabilite. -Sécurité.	-Transparance.
Exemples de cas d'usage	Supplychain.	Cryptomonnaie.	Médical.

TABLE 1.1 – Comparaison entre différents types de Blockchain

1.8 Architecture de la Blockchain

La Blockchain se compose de deux composants principaux : une base de données et un réseau de nœuds, comme illustre la Figure 1.2.

Ce réseau de noeuds se compose de plusieurs types de nœuds en fonction des données qu'il conserve [16].

— **Nœud complet :** Un nœud complet (full node en anglais) comme son nom l'indique, contient une copie complète de la chaîne de bloc. Ainsi, un nœud complet participe au processus de validation et d'insertion des transactions et nouveaux blocs dans la Blockhain.

— **Nœud léger :** Les nœuds légers(Lightweight node en anglais) permettent également de vérifier les transactions du réseau, sans avoir à télécharger et mettre à jour toute la Blockchain. Ils utilisent pour cela une fonctionnalité nommée SPV (Simplified Payment Verification), afin de vérifier de façon spécifique certaines transactions. Ils se reposent sur des nœuds complets, qui leur permettent d'accéder aux données nécessaires.

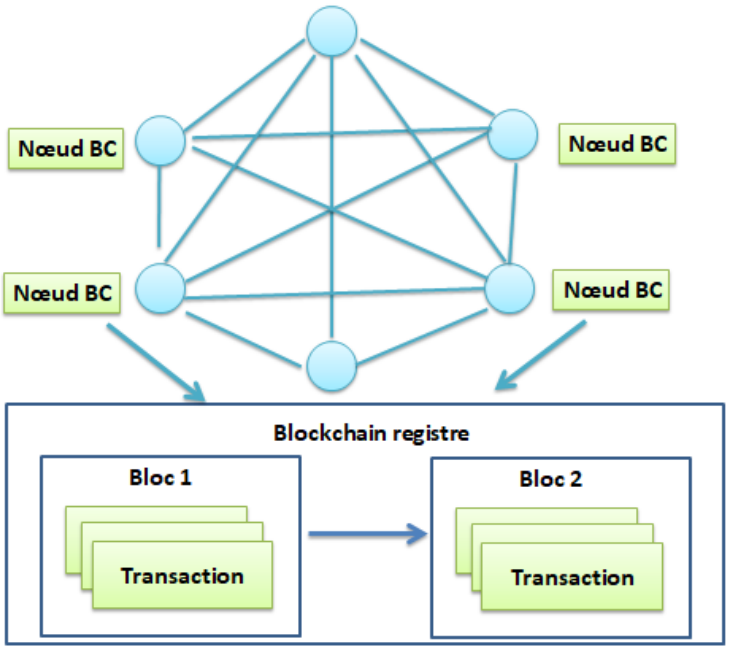

FIGURE 1.2 – Éléments architecturaux de la Blockchain [2]

La base de données d'une Blockchain est un magasin distribué, partagé, inviolable et tolérant aux pannes qui garde une trace des enregistrements sous forme de transactions. Les blocs sont formés en regroupant un certain nombre de transactions et chaque bloc est lié à son prédécesseur par un hachage. Ce qui fait que chaque bloc se compose de deux parties : la partie entête (header), et la partie contenant la liste des transactions.

1.8.1 L'en-tête du bloc

— **Hach du bloc précédent :** Est l'élément responsable du chainage de la Blockchain. Par exemple, le bloc 31 pointe vers le bloc 30. Le tout premier bloc d'une chaîne est un peu spécial et tous les blocs confirmés et validés sont dérivés de ce bloc (Genesis block en Anglais).

— **Indexe :** C'est le numéro du bloc dans la chaine.

— **L'horodatage :** Est un mécanisme qui consiste à associer une date et une heure à toute transaction et tout un bloc. Afin d'enregistrer l'instant de chaque opération.

— **Compte ou porte-monnaie (wallet) :** Le porte-monnaie est un logiciel pour la sauvegarde de la clé privé et clé publique d'un utilisateur de Blockchain, ce logiciel peut être une application sur le web, téléphone mobile ou ordinateur. Il permet a cet utilisateur de contrôler son compte de crypto-monnaie, voir son montant et exécuter des transactions.

— **Hach du bloc :** Est un nombre hexadécimal calculé à partir des données du bloc. Il représente une empreinte digitale servant à identifier rapidement la donnée initiale. Il existe plusieurs fonctions de hachage, la plus connue est le SHA256.

1.8.2 La liste des transactions

Une transaction est le petit élément constitutif d'un système de Blockchain. Elle se compose d'une adresse de destinataire, l'adresse d'expéditeur et les données. Le concept des transactions repose en réalité sur la cryptographie asymétrique. Lorsque quelqu'un se lance dans le processus de création d'une transaction, il génère à l'aide de son porte-monnaie, une clé publique et une clé privée. La clé privée n'est transmise à personne et la clé publique est quant à elle, disponible pour tout le monde.

Une fois qu'une transaction est crée, elle doit être signée numériquement. Une signature numérique est un nombre généré à partir de la clé privée de l'expéditeur (cette clé ne doit être jamais transmise lors d'une transaction). La signature peut être vérifiée par la clé publique correspondante.

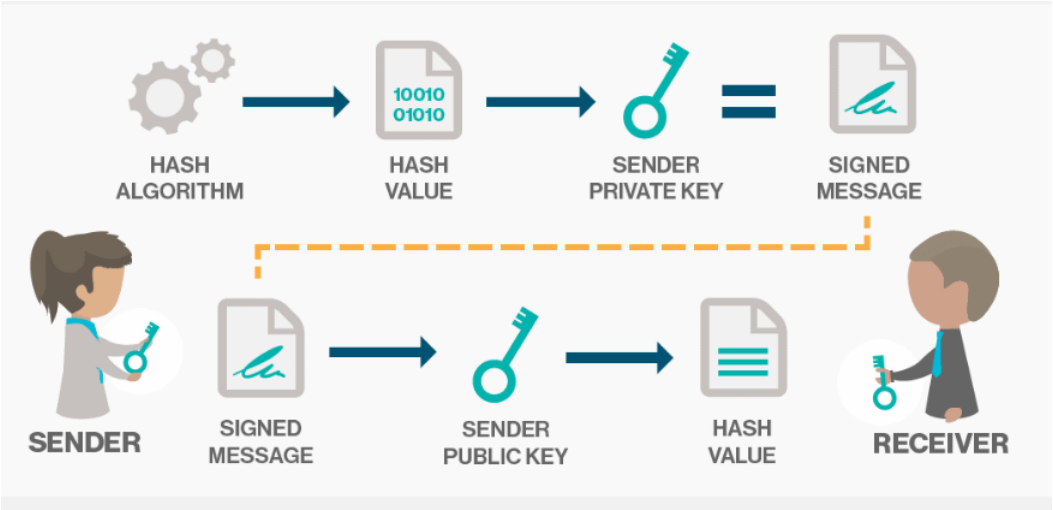

FIGURE 1.3 – La signature d'une transaction [3].

— **Cryptographie asymétrique :** Dans un chiffrement asymétrique (ou cryptographie à clés publiques), les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaitre (il s'agit de la clé privée). À partir de cette clé, ils déduisent la clé publique à l'aide d'un algorithme. Donc les clés existent par paires (le terme de bi-clés est généralement employé). Les utilisateurs s'échangent cette clé publique a travers un canal non sécurisé [19].

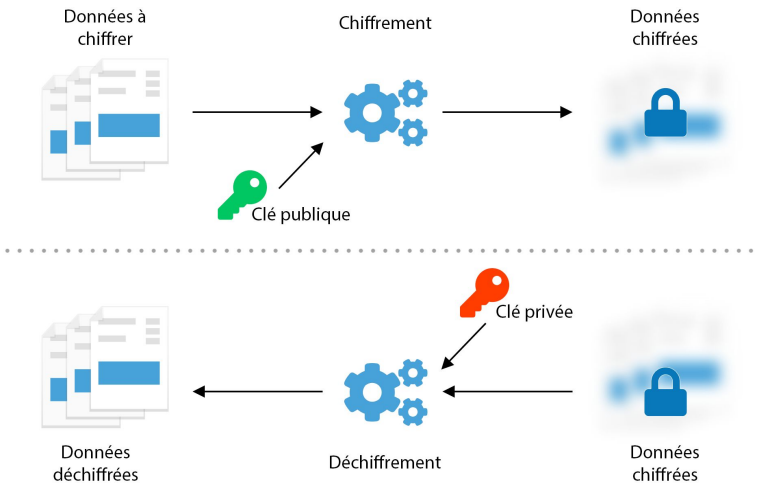

FIGURE 1.4 – Chiffrement Asymétrique

1.8.3 Les fonctions de hachage

Les fonctions de hachage sont des fonctions à sens unique «sans collision», générant une sortie de taille fixe (ou empreinte). Ces fonctions sont dites à sens unique car il est impossible de retrouver les données initiales à partir de l'empreinte. Une fonction est dite « sans collision » ou « injective » lorsqu'il est impossible de trouver deux sources différentes conduisant à un même résultat ainsi que la modification d'entrée engendra des modifications en sortie.
On distingue le hachage simple et le hachage arborescent appelé l'arbre de Merkle.
Dans l'approche de hachage simple, la fonction SHA256 est une veriante de SHA-2 qui génère une valeur de 256 bits [20].

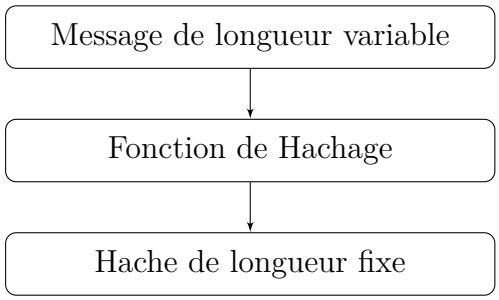

FIGURE 1.5 – Fonction de hachage.

1.8.4 L'Arbre Merkle

L'Arbre de Merkle est la structure utilisée par la Blockchain pour organiser le stockage des transactions dans chaque bloc.

Le Merkle Tree ("Arbre de Merkle") est une méthode permettant de structurer des données en vue d'y accéder et d'en vérifier la véracité plus rapidement. Le nom vient du fait que cette méthode organise les données en les regroupant par deux, donnant ainsi la forme d'un arbre inversé. En

effet, les transactions sont regroupées par groupe de deux, un hachage est ensuite applique à ce groupe. Les groupes sont ensuite regroupes par groupe de deux puis soumis au même procédé jusqu'au dernier hachage appelé la racine ("Merkle Root") qui lui est ajoute comme référence dans le "Header" du bloc. Cette organisation des transactions au sein d'un block va permettre aux mineurs lors de la vérification des nouvelles transactions, de remonter très rapidement vers la dernière transaction concernée et ainsi vérifier si il existe un fraude [21].

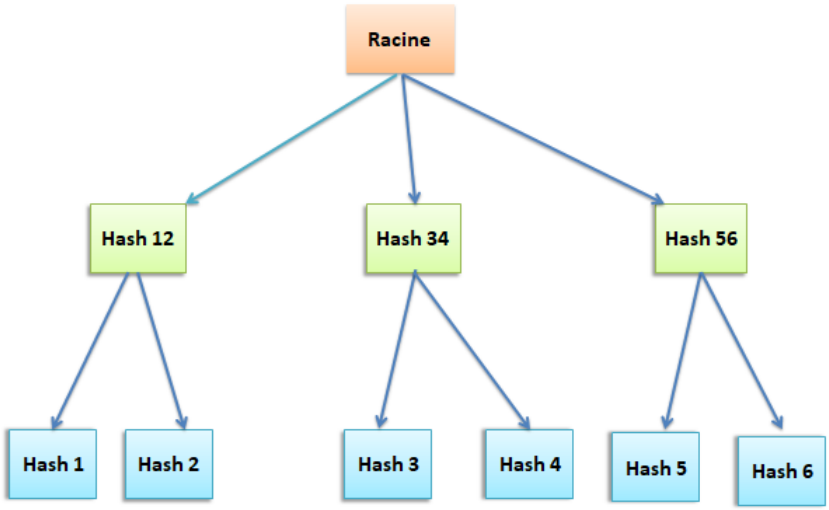

FIGURE 1.6 – Un arbre de Merkel

1.9 Fonctionnement de la Blockchain

Lorsqu'un utilisateur effectue une transaction à travers le réseau Blockchain, cette dernière est regroupée avec d'autres transactions connexes au sein d'un bloc. Elle est ensuite vérifiée et validée par des membres du réseau à l'aide des techniques cryptographiques. Cette étape dénommée minage, permet d'en vérifier l'authenticité et de s'assurer que la structure est correcte. Une fois validé, le bloc est immédiatement horodaté et ajouté à la Blockchain et ne peut plus être modifié, même en cas d'erreur. Lorsqu'une telle situation se produit, la rectification nécessite uniquement le rajout d'une nouvelle transaction. La validation d'une transaction est presque instantanée (généralement de l'ordre de 10 minutes en Bitcoin). Pour comprendre le fonctionnement d'une Blockchain, prenons un exemple simple d'une opération de virement dans le réseau Bitcoin. Alice désire envoyer 100 Bitcoin à Bob, chacun possède une adresse publique. Alice signe la transaction avec sa clé privé et lance la demande de virement au sein du réseau Bitcoin et passe en attente de validation avec d'autres transactions. Une fois la transaction est transmise aux participants du réseau P2P, les nœuds vont consulter l'historique des transactions et s'assurer qu'Alice qui souhaite effectuer la transaction, possède bien ce qu'elle prétend avoir et qu'il s'agit bien de lui(Alice) en vérifiant sa signature. Aprés vérification, le mineur applique la puissance de calcul (proof of work) sur le bloc pour obtenir un hach qui satisfait les exigences. Le mineur diffuse le hach du nouveau bloc à l'ensemble du réseau, ensuite un consensus intervient pour assurer qu'un mineur a bien fourni la puissance de calcul pour le hashage du nouveau bloc. Si le résultat

satisfait le consensus, le bloc est ajouté à la Blockchain, le mineur est rémunéré avec des tokens. Par conséquent, Bob reçoit les 100 Bitcoins.

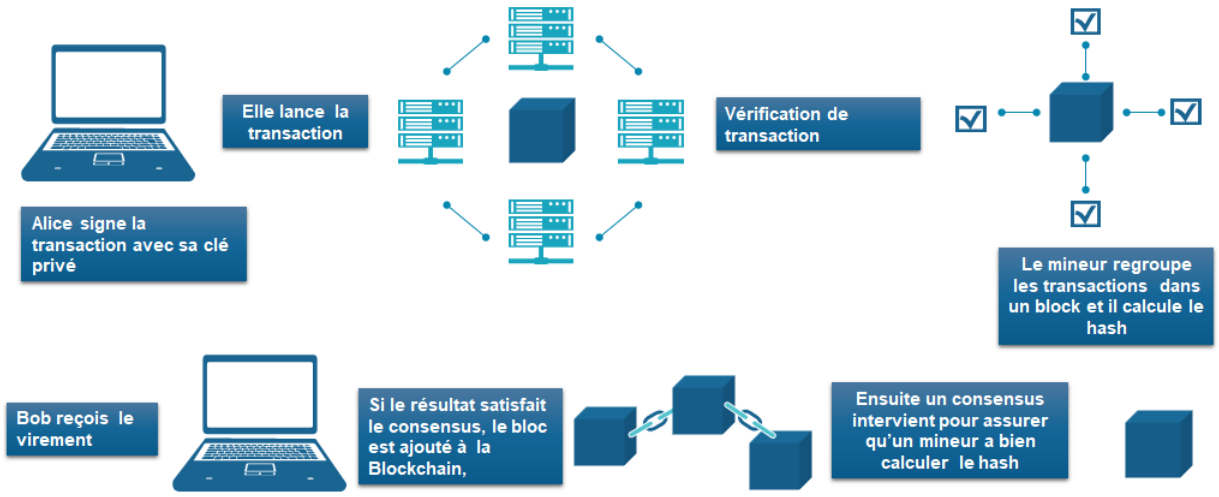

FIGURE 1.7 – Fonctionnement de la Blockchain [4]

1.9.1 La notion de fourchette

Il est possible que deux nœuds du réseau trouvent simultanément la solution d'un problème de minage, minant ainsi deux blocs différents au même moment. Ainsi, le réseau se retrouve dans un état indéterminé dans lequel il ne sait pas lequel utiliser des deux blocs crées. On obtiendra donc deux chaînes différentes. Les mineurs continuent leur travaille, et un nouveau bloc va être miné sur l'une ou l'autre des deux Bockchains, la rendant ainsi comme valide par défaut.
Le protocole de Blockchain prévoit ce type de problèmes, et oblige les nœuds du réseau à prendre comme seule et unique Blockchain valide la plus longue en termes de nombre de blocs.

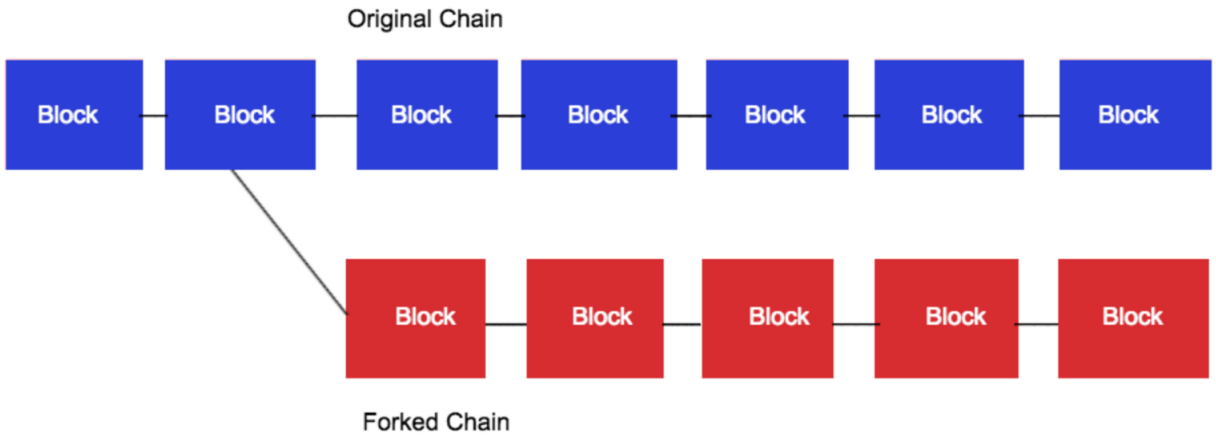

FIGURE 1.8 – Notion de fourchette [5].

1.10 Algorithme de consensus

L'algorithme de consensus est l'élément de base dans le contexte de la Blockchain. C'est un mécanisme qui garantit un registre unique, cohérent et honnête accepté par la plupart des nœuds du réseau pour faire face aux divers types d'attaques [22].

1.10.1 Critères de l'efficacité d'un mécanisme de consensus

Les algorithmes de consensus doivent respecter les critères d'efficacité ci-dessous :

— Être résilients aux pannes de nœuds, aux retards de transmission, aux messages corrompus.

— Faire face aux nœuds malveillants tentant de manipuler le consensus ou de le retarder.

Pour ce faire, une pluralité de mécanismes existent (PoW, PoS, DPoS, PoET, PoI, etc). Chacun d'entre eux dispose de ses propres caractéristiques en matière de synchronisation, d'émission de message (fréquence, taille), de tolérance aux pannes, de prévention contre les nœuds malveillants, de performance et de sécurité des messages échangés [22].

1.10.2 Preuve de travail (PoW : proof of work)

En 2009, Bitcoin a introduit une manière innovante d'utiliser la preuve de travail, comme algorithme de consensus. Dans ce cas, PoW est utilisé pour valider les transactions qui sont regroupées en blocs, qui sont liés entre eux pour former une Blockchain. Depuis lors, PoW s'est propagé pour devenir un algorithme de consensus largement utilisé et est maintenant déployé par de nombreuses crypto-monnaies.

Principe de fonctionnement de PoW :

— Les participants de la Blockchain (mineurs) doivent résoudre un problème de calcul complexe afin d'ajouter un bloc de transactions dans la Blockchain.

— Fondamentalement, la preuve de travail est un concept qui accorde de l'importance a la puissance de calcul des nœuds. Le nœud doit prouver qu'il dispose bien de cette puissance de calcul en faisant travailler son matériel informatique. Cela est fait pour s'assurer que les mineurs mettent de l'argent/des ressources (machines d'extraction) pour faire le travail, ce qui montre qu'ils ne nuiront pas au système de Blockchain, car nuire au système entrainera une perte de leur investissement [19].

— La difficulté du problème peut être modifiée lors de l'exécution, pour garantir un temps de blocage constant. Parfois, il y a une situation dans laquelle plus d'un mineur résout le problème simultanément. Dans ce cas, les mineurs choisissent l'une des chaînes et la chaîne la plus longue est considérée comme gagnante. La version de PoW de Bitcoin est basée sur l'utilisation des haches. Son fonctionnement est illustré dans les étapes suivantes ainsi que dans la Figure 1.9 :
  • Les mineurs sont chargés d'ajouter de nouveaux blocs dans la Blockchain. Pour ce faire,

les mineurs doivent essayer de deviner un nombre pseudo aléatoire (Nonce).
Ce nombre, lorsqu'il est combiné avec les données fournies dans le bloc et transmis via une fonction de hachage, doit produire un résultat qui correspond aux conditions données, par exemple, un hachage commençant par quatre zéros.

• Lorsqu'un résultat correspondant est trouvé, les autres nœuds vérifient la validité du résultat et le nœud mineur est récompense par la récompense de bloc (actuellement "12.5 Bitcoins", pour la Blockckaine de Bitcoins).

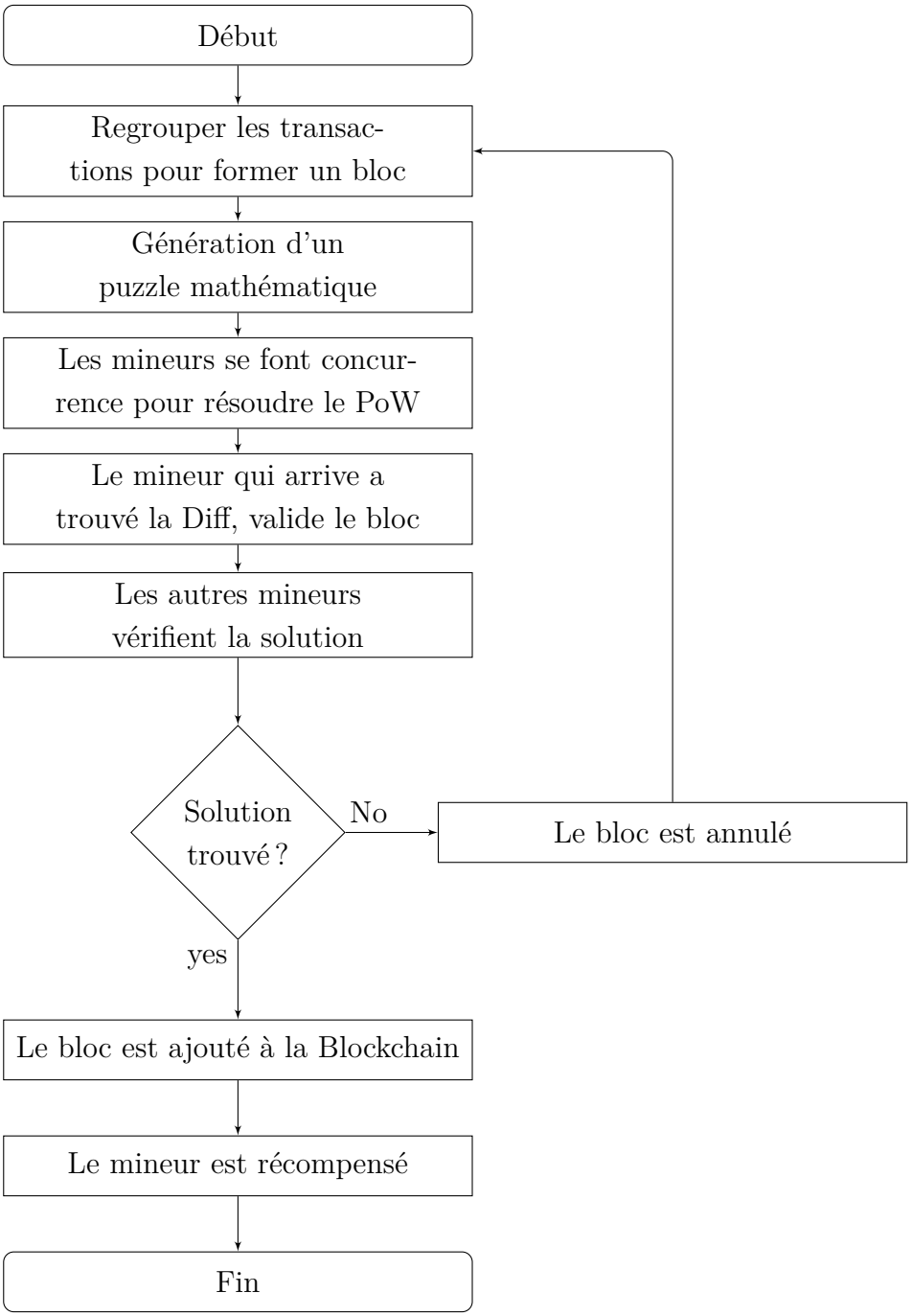

FIGURE 1.9 – La preuve de travail PoW.

Avantages de PoW :

On peut citer les avantages suivants :

1. La preuve de travail aide à protéger le réseau contre de nombreuses attaques différentes. Une attaque réussie nécessiterait beaucoup de puissance de calcul et beaucoup de temps pour faire les calculs et donc elle serait inefficace.
2. Il est nécessaire de posséder au moins 51 pour 100 de la puissance de calcul du réseau pour le saturer de fausses transactions.

Inconvénients de PoW :

Comme inconvénients, on peut signaler les points suivants :

1. Le proccesus de minage nécessite un matériel informatique coûteux qui consomme une grande quantité d'énergies.
2. La validation des blocs de la Blockchain entraine une augmentation de la latence.

1.10.3 Preuve d'enjeu (PoS : proof of stake)

La preuve d'enjeu a été créée comme une alternative à la preuve de travail (PoW), afin de résoudre les problèmes inhérents à cette dernière. Bien qu'ils partagent tous deux le même objectif de parvenir à un consensus dans la Blockchain, le processus pour atteindre l'objectif est assez différent. La preuve d'enjeu, elle est directement liée à la monnaie puisqu'elle lie la capacité de valider un bloc à la quantité d'argent (ou jeton) détenue. Les étapes de l'algorithme de PoS sont illustrées dans le diagramme de la Figure 1.10.

Avantages de PoS :

Le principal avantage de PoS est que la validation d'un bloc ne repose pas sur de puissants calculs algorithmiques qui consommeraient énormément d'énergie et auraient par conséquent un impact négatif sur l'environnement.

Inconvénient de PoS :

1. Stocker des jetons pour miner va donc limiter les échanges de jeton et donc nuire au développement de la crypto monnaie.
2. Monopolisation de la richesse, en effet plus on a de jeton plus l'on peut forger et plus on gagne de l'argent.
3. **Nothing at stake(rien en jeu) :** Dans un réseau PoW, il est rare que deux mineurs produisent un bloc presque simultanément grâce à un décalage dans le temps. Cette situation entraîne une confusion temporaire dans le réseau qui nécessite que les nœuds parviennent à un consensus sur le bloc valide. Par conséquent, les mineurs doivent choisir la version de la Blockchain à laquelle ils consacreront leurs ressources, contournant ainsi d'autres possibilités. Cependant, étant donné que dans le système PoS, la création de nouveaux

blocs nécessite peu de ressources, un validateur peut choisir de continuer à travailler sur plusieurs versions du fork et de forger de nouveaux blocs. Comme il n'y a pas de coûts d'opportunité pour forger dans une Blockchain en particulier, il n'y a «rien en jeu» pour les utilisateurs qui créent des blocs. C'est pourquoi les utilisateurs pourraient miner sur les branches concurrentes d'une Blockchain pour maximiser le montant des frais de transaction qu'ils reçoivent.

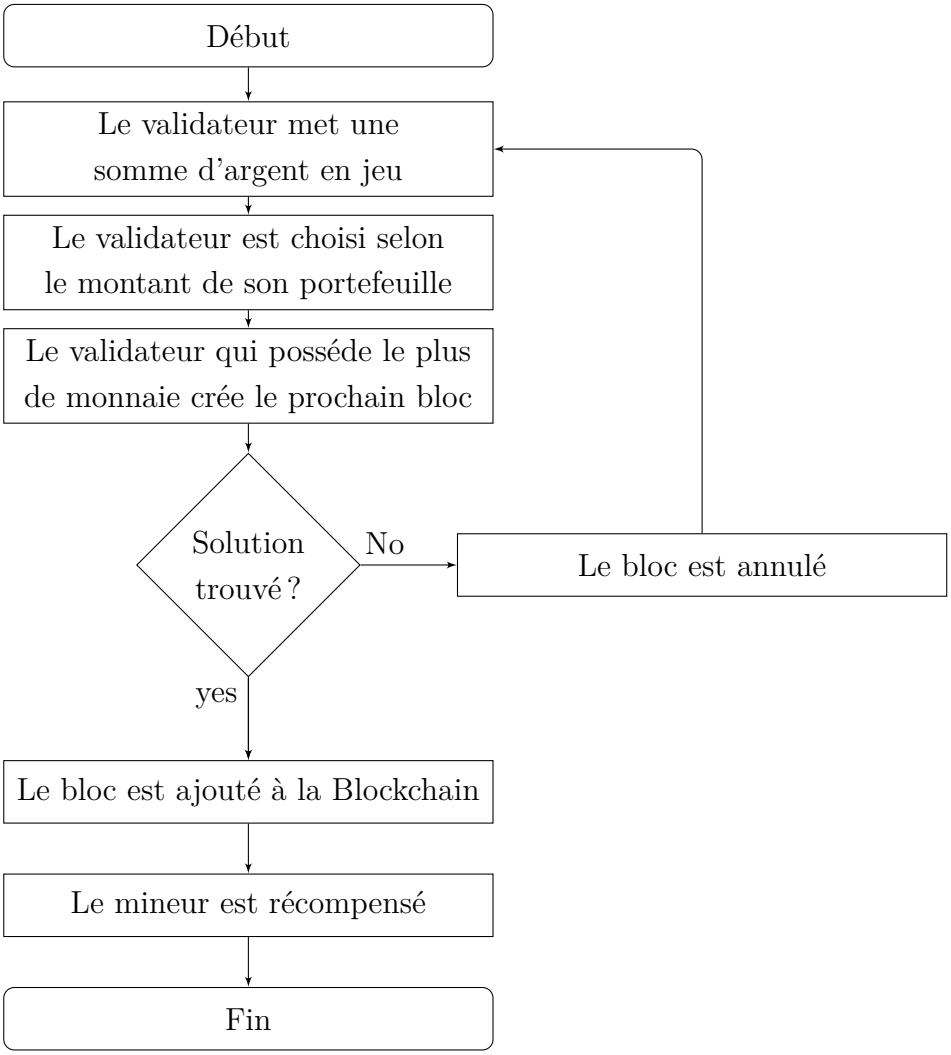

FIGURE 1.10 – La preuve d'enjeu PoS.

1.10.4 Preuve d'enjeu Délégué (DPoS : delegated proof of stake)

Un algorithme de consensus «Delegated proof-of-stake» (preuve d'enjeu déléguée, DPoS) est une variante du protocole de consensus proof-of-stake. Les utilisateurs du réseau sélectionnent un nombre suffisant de délégués (également appelés témoins) pour assurer la décentralisation du réseau, et que leur nœud est toujours opérationnel. Les délégués élus vérifient les transactions et génèrent des blocs. Si un délégué reçoit une récompense globale. Il la partage généralement avec les wallets qui ont voté pour lui et qui ont également un enjeu dans le réseau. Si un nœud élu se

comporte mal ou ne fonctionne pas efficacement, il sera rapidement expulse et remplace par un autre.

Avantages de DPoS :

1. Efficacité d'un point de vue énergétique, et plus rapide qu'un mécanisme de PoW et PoS, il permet de valider les transactions en quelques secondes seulement.
2. Réduit les interactions entre les nœuds .

Inconvénients de DPoS :

1. Risque de centralisation excessive avec des risques de vulnérabilité.
2. Les participants possédant le plus de jetons peuvent voter pour eux-mêmes afin de s'élire vérificateur des transactions.

1.10.5 Preuve du temps écoulé (PoET : Proof of Elapsed Time)

PoET est un algorithme de mécanisme de consensus qui est souvent utilisé sur les réseaux Blockchain autorisés pour décider des droits miniers ou des gagnants de bloc sur le réseau. Les réseaux de Blockchain autorisés sont ceux qui exigent que tout participant potentiel s'identifie avant d'être autorisé à se joindre. Basé sur le principe d'un système de loterie équitable où chaque nœud a la même probabilité d'être gagnant, le mécanisme PoET est basé sur la répartition équitable des chances de gagner entre le plus grand nombre possible de participants au réseau. La minuterie est différente pour chaque nœud. Chaque participant du réseau se voit attribuer un temps d'attente aléatoire, et le premier participant à finir d'attendre peut engager le bloc suivant dans la Blockchain. Semblable à tirer des pailles, mais cette fois, la tige la plus courte de la pile gagne à la loterie.

Le fonctionnement de l'algorithme PoET :

1. Chaque nœud du réseau de chaînes de blocs génère un temps d'attente aléatoire et se met en veille pendant cette durée spécifiée.
2. Celui qui se réveillé en premier c'est-a-dire celui qui a le temps d'attente le plus court se réveillé et valide un nouveau bloc dans la chaîne de blocs, diffusant les informations nécessaires à l'ensemble du réseau de pairs.
3. Le même processus se répète ensuite pour la découverte du bloc suivant.

Le mécanisme de consensus du réseau PoET doit garantir un facteurs importants : les nœuds participants sélectionnent véritablement un temps qui est en effet aléatoire et non une durée plus courte choisie exprès par les participants pour gagner.

Essentiellement, le flux de travail est similaire au mécanisme de consensus suivi par l'algorithme de preuve de travail (PoW) de Bitcoin, mais sans sa consommation d'énergie élevée. Au

lieu d'être gourmande en ressources, elle permet au processeur d'un mineur de dormir et de passer à d'autres taches pendant la durée spécifiée, augmentant ainsi son efficacité.

Le mécanisme d'exécution du code de confiance dans un environnement sécurisé prend également en charge de nombreuses autres nécessites du réseau. Il garantit que le code de confiance s'exécute en effet dans l'environnement sécurisé et n'est modifiable par aucun participant externe. Il garantit également que les résultats sont vérifiables par les participants et entités externes, améliorant ainsi la transparence du consensus du réseau.

Avantage du PoET :

1. Le faible coût de la participation augmente la probabilité que la population de validateurs soit importante, augmentant la robustesse de l'algorithme de consensus.
2. Il est simple pour tous les participants de vérifier que le mineur a été légitimement sélectionné.

Inconvénient du PoET :

1. Même si ça marche, l'utilisateur doit avoir un matériel spécialisé. Il ne peut donc pas être adopté en masse.
2. Ne convient pas aux Blockchain publique.

1.10.6 Preuve d'importance (PoI : proof of importance)

La preuve d'importance est un algorithme de consensus Blockchain qui prend en compte la productivité globale des utilisateurs du réseau.
• Cet algorithme est conçu pour récompenser les utilisateurs très fidèles de la Blockchain. Par conséquent, encourager une plus grande utilisation de la plateforme.
• C'est un algorithme qui dépend de combien d'utilisateurs actifs sur le réseau. Plus ils sont actifs, plus ils reçoivent de récompenses.
• Chaque utilisateur est noté, et plus son score est élevé, plus les récompenses sont importantes.

Avantages de PoI :

Les riches peuvent ne pas continuer à s'enrichir injustement sur la plateforme car le montant d'argent en possession d'un individu n'est pas le seul facteur à prendre en compte lors de la mesure de la réputation d'un compte.

Inconvénients du PoI :

Un problème brûlant avec cette méthode est l'utilisation de transactions fausses qui aurait récompensé les gens pour l'envoi de transactions aller-retour pour tromper l'algorithme.

1.10.7 L'algorithme de Tolérance aux Pannes Byzantines Pratique PBFT

L'algorithme de consensus PBFT (Practical Byzantine Fault Tolerance) permet à un système distribué d'atteindre un consensus même lorsqu'un petit nombre de nœuds démontrent un comportement malveillant (comme la falsification d'informations). Lors de la transmission d'informations, PBFT utilise des algorithmes cryptographiques tels que la signature, la vérification de signature et le hachage pour garantir que tout reste irrévocable, infalsifiable et indiscutable. Il optimise également l'algorithme BFT, réduisant sa complexité d'exponentielle à polynomiale [8].

Principe de fonctionnement de PBFT :

PBFT se concentre sur la fourniture d'une réplication pratique de la machine d'état byzantine qui tolère les erreurs byzantines (c'est-à-dire les nœuds malveillants) en supposant qu'il existe des défaillances de nœuds indépendants et des messages manipulés envoyés via des nœuds spécifiques.

Les nœuds d'un système PBFT sont classés séquentiellement, un nœud étant le leader et les autres étant appelés nœuds de secours. Tous les nœuds du système communiquent entre eux, l'objectif étant que tous les nœuds honnêtes parviennent à un accord sur l'état du système en utilisant une règle de majorité.

La communication entre les nœuds a deux fonctions : les nœuds doivent prouver que les messages proviennent d'un nœud homologue spécifique, et ils doivent vérifier que le message n'a pas été modifié pendant la transmission. Pour que le système PBFT fonctionne, le nombre de nœuds malveillants ne doit pas être égal ou supérieur à un tiers de tous les nœuds du système dans une fenêtre de vulnérabilité donnée. Semblable au mécanisme de consensus de preuve de travail, plus il y a de nœuds dans un réseau PBFT, plus il devient sécurisé.

Les cycles de consensus PBFT sont appelés vues et sont divisés en 4 phases :

1. Un client envoie une requête au nœud leader pour invoquer une opération de service.
2. Le nœud principal diffuse la requête vers les nœuds de secours.
3. Les nœuds exécutent la requête, puis envoient une réponse au client.
4. Le client attend 2f+1 réponses de différents nœuds avec le même résultat, où f représente le nombre maximum de nœuds potentiellement défectueux.
5. Le nœud principal est modifié à chaque vue et peut être remplacé par un protocole appelé changement de vue si un certain laps de temps s'est écoulé sans que le nœud principal ne diffuse la requête. De plus, une super-majorité de nœuds honnêtes peut déterminer quand un leader est défectueux et le remplacer par le prochain leader en ligne.

Avantages PBFT :

1. **Finalité de la transaction :** La nature du PBFT signifie que les transactions peuvent être convenues et finalisées sans avoir besoin de multiples confirmations. Il n'y a pas de période d'attente pour s'assurer qu'une transaction est sécurisée après l'avoir incluse dans un bloc.

2. **Efficacité énergétique :** Contrairement aux mécanismes de consensus de preuve de travail, PBFT peut atteindre un consensus de réseau sans nécessiter de calculs énergivores. Certains systèmes PBFT utilisent la preuve de travail pour empêcher l'attaque Sybil (où un seul adversaire contrôle plusieurs nœuds sur un réseau, prétendant être plusieurs parties), mais seulement après un nombre défini de blocs (c'est-à-dire 100) et non pour chaque bloc.
3. **Faible variance de récompense :** PBFT nécessite une décision collective via le vote sur les enregistrements en signant des messages, contrairement à la preuve de travail où seul le leader propose le bloc suivant. Ainsi, chaque nœud d'un système PBFT peut être incité, ce qui réduit la variance des récompenses pour les mineurs.

Inconvénients du PBFT :

1. **Mise à l'échelle :** PBFT est une solution consensuelle prometteuse lorsque le groupe de nœuds est petit mais devient inefficace pour les grands réseaux. En effet, chaque nœud doit parler à tous les autres nœuds pour assurer la sécurité du réseau, ce qui peut rapidement devenir un coût de communication énorme à mesure que le nombre de nœuds augmente.
2. **Attaques Sybil :** Les modèles PBFT sont sensibles aux attaques sybil, où une seule partie crée ou manipule un grand nombre de nœuds dans le réseau et compromet la sécurité. Cette menace est réduite avec des réseaux de plus grande taille, mais compte tenu du problème d'évolutivité du PBFT, il doit généralement être utilisé en combinaison avec un autre mécanisme de consensus.

1.10.8 La différence entre PoW, PoS, DPoS, PoET et PBFT

	Pow	PoS	DPoS	PoET	PBFT
Matériel spécifique	ASCI|CPU			SGX	
Type de Blockchain	Publique	Publique et Privé	Publique	Publique et Privé	Privé
Débit des transaction	Faible	Elevé	Elevé	Moyen	Elevé
Token nécessaire	Oui	Oui	Oui	Non	Non
Cosommation d'énergie	Oui	Non	Non	Non	Non
Scalabilité de réseau	Elevé	Elevé	Elevé	Elevé	Faible
Modél de confiance	Sans confiance	Sans confiance	Sans confiance	Sans confiance	Semi confiance
Tolerance au fautes byzantines	<=25 %	Dépend d'algorithme spécifique	Dépend d'algorithme spécifique	Inconnu	<=33 %
Niveau de sécurité	Trés elevé	Faible	Elevé	Inconnu	Moyen
Niveau de décentralisation	Moyen	Elevé	Trés elevé	Moyen	Faible

TABLE 1.2 – Comparaison entre les algorithmes de consensus [8].

1.11 La sécurité dans la Blockchain

Le système ouvert de la Blockchain n'est pas synonyme de système non sécurisé. La technologie utilisée est protégée contre la falsification ou la modification par des nœuds de stockage. Chaque bloc est connecté à tous les blocs avant et après. Cela rend difficile sa falsification.

Les enregistrements sur une Blockchain sont sécurisés par cryptographie. Les participants au réseau ont leurs propres clés privées qui sont affectées aux transactions qu'ils effectuent et agissent comme une signature numérique personnelle. Si un enregistrement est modifié, la signature deviendra invalide. Donc le rajout de nouvelles transactions n'est possible qu'après la validation de plusieurs participants du réseau.

Les chaînes de blocs sont décentralisées et distribuées. De ce fait toute modification frauduleuse nécessiterait des quantités massives de puissance de calcul pour accéder à chaque instance (ou au moins une majorité de 51 %) de la Blockchain.

Quelques types d'attaques :

• **Attaques à 51 % :** L'attaque de 51 % sur un réseau de Blockchain fait référence à un mineur ou à un groupe de mineurs qui essaient de contrôler plus de 51 % de calcul ou de minage. Dans cette attaque, l'attaquant peut empêcher de nouvelles transactions d'avoir lieu ou d'être confirmées. Ils sont également en mesure d'annuler des transactions qui ont déjà été confirmées alors qu'ils contrôlaient le réseau, ce qui entraîne un problème de double dépense [23].

• **Les attaques DOS :** Cette attaque vise à rendre inaccessible un serveur grâce à l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation de faille de sécurité à fin de provoquer une panne ou un fonctionnement dégradé du service.

1.12 Exemple de plateformes Blockchain

1.12.1 Ethereum

Ethereum est une plateforme décentralisée qui utilise la technologie de la Blockchain.
Le réseau Ethereum est la base d'un nouveau type d'Internet. Il fonctionne comme une plateforme sur laquelle des applications décentralisées (DAPP) et des contrats intelligents peuvent être lancés. Par rapport aux applications Internet centralisées actuelles, ces DAPP offrent des niveaux de sécurité et de confidentialité plus élevés. Quand nous parlons d'Ethereum, nous entendons également de l'ether. L'ether est la monnaie utilisé par le réseau Ethereum.

• **Les contrats intelligents :** Les contrats intelligents (Smart Contract) sont des programmes informatiques qui s'appuient sur la technologie Blockchain. Ils sont équivalents aux contrats papiers. Durant l'exécution de ces contrats, toutes les étapes de validations sont enregistré dans la Blockchain ce qui permet de sécuriser l'ensemble des données.

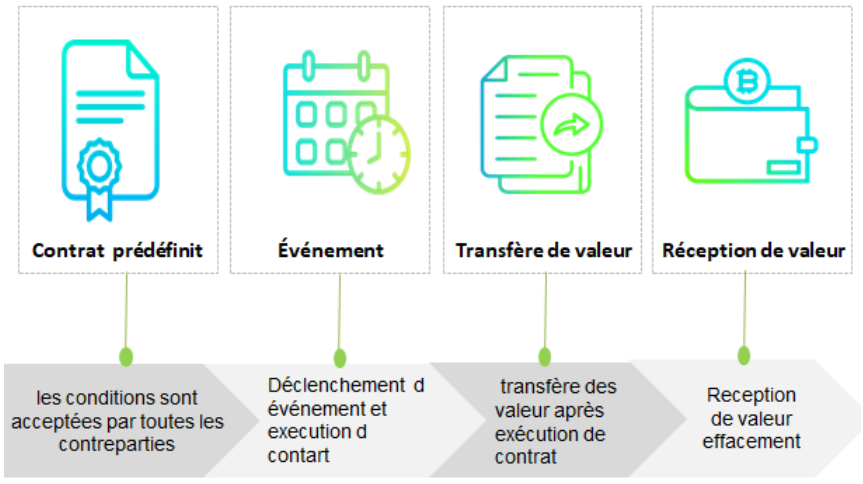

FIGURE 1.11 – Smart Contract.

1.12.2 Hyperledger Fabric

Hyperledger Fabric est un ensemble d'outils qui permettent de créer des applications Blockchain. Soutenu par la Fondation Linux, il a été conçu dès le départ pour répondre aux besoins des entreprises en matière de registres distribués [24].

1.13 Domaines d'utilisations de la Blockchain

1.13.1 L'assurance

Le secteur de l'assurance peut également utiliser la démarche Blockchain Comme approche efficace pour traiter les dossiers, vérifier la réalité d'un événement (par exemple, un accident) et proposer au client une indemnisation équitable et rapide.

1.13.2 Le vote électronique

Le développement de la Blockchain vient bouleverser ce secteur, puisque elle est transparente, est infalsifiable ce qui empêche la modification des voix tout en suivant chaque opération effectuée lors du vote.

1.13.3 Paiements de redevances

Les musiciens, les créateurs de jeux vidéo et les artistes en général ont souvent du mal à obtenir le salaire qu'ils méritent en raison du piratage numérique, des relations inéquitables avec des agences intermédiaires ou simplement du fait qu'ils ne reçoivent pas les redevances dues. La technologie Blockchain peut être utilisée pour créer une plate-forme où les talents créatifs ont une trace immuable et transparente de ceux qui louent, achètent et / ou utilisent leur contenu. Une telle plate-forme peut également faciliter les paiements via des contrats intelligents.

1.13.4 L'E-paiement

Pour l'envoi d'argent dans le monde entier, la technologie Blockchain s'est déjà révélée très efficace. Envoyer des cryptomonnaie à des amis, de la famille ou à d'autres personnes dans le monde coûte déjà moins cher et se fait plus rapidement que ce que proposent les banques centralisées et les solutions de paiement classiques.

1.13.5 La santé

Le secteur de la santé fait face à de nombreux problèmes que certaines entreprises cherchent aujourd'hui à résoudre les principaux : défis concernent le besoin de systèmes plus efficaces et sécurisés pour pouvoir gérer les dossiers médicaux des patients, la traçabilité des médicaments, les suivis et la surveillance des patients, etc. [25].

— **Les dossiers médicaux des patients :** Plusieurs acteurs de la santé s'intéressent de près à la création d'un registre patient distribué, pouvant par exemple s'appuyer sur une architecture Blockchain. Actuellement, l'information n'est pas partagée entre les différents médecins mais ils sont stockés aux siens de Cloud central, et le patient doit lui-même reporter les comptes rendus de ses précédentes consultations auprès de chaque nouveau spécialiste. Pour lutter contre ce problème, certains projets commencent à voir le jour. C'est notamment le cas de PassCare.

1.13.6 Internet des objets (IoT)

L'Internet des Objets, en anglais the Internet of Things (IoT) est de plus en plus présent dans notre vie courante ainsi dans plusieurs domaines ce qui la rend face à plusieurs cyberattaques. La sécurité de l'IoT est primordiale, chaque « nœud » doit être protégé contre les logiciels espions et malveillants, les chevaux de Troie, et toutes les intrusions menaçant la vie privée, cependant, il ne suffit pas d'empêcher ou d'autoriser les accès pour garantir la sécurité. Il faut surveiller qui accède à quelle ressource et surtout quand. Afin d'éviter des failles de sécurité dramatiques (L'usurpation d'identité, le vol d'information et la modification des données), l'union de la Blockchain avec l'iot presente une solution.
La technologie Blockchain dans le domaine de l'IoT permet le stockage des données, le transfert, la traçabilité ...etc en garantissant la sécurité[26].

1.14 Les limites de la Blockchain

Même avec ses caractéristiques innovantes, la technologie Blockchain n'est pas l'abri de certains problèmes notamment :

— **Le coût de traitement :** Ces dernièrs années, à mesure que le nombre de transactions de cryptomonnaie augmentait, le temps et les frais pour effectuer ces transactions augmentaient également.

— **La technologie de Blockchain reste énergivore :** Actuellement, Bitcoin est la Blockchain la plus critiquée, car il consomme le plus d'énergie. Sa consommation énergétique représente un problème notamment parce qu'elle augmente proportionnellement aux nombres de participants sur le réseau. Pour autant, les nouvelles générations de Blockchain sont aujourd'hui 2,5 fois plus efficaces en consommation énergétique, et le choix du type de consensus utilisé pour la validation des blocs fait énormément varier leurs besoins en énergie.

1.15 Conclusion

Dans ce chapitre, nous avons présenté la Blockchain à travers ses caractéristiques et ses principes, son modèle de fonctionnement, son utilité, ses types, ainsi ses domaines d'application et ses plateformes.

Cette technique s'impose aujourd'hui dans plusieurs domaines où les avantages de son utilisation sont considérables et pourraient être d'une grande utilité pour le monde futur qui comprend à la fois des modèles centralisés et décentralisés tel que le Fog computing.

CHAPITRE 2

LE FOG COMPUTING

2.1 Introduction

L'IoT est une infrastructure qui sert à connecter tout objet à Internet, tels que des capteurs, des dispositifs portables (Wearables), des smartphones, des appareils photos, des appareils électroménagers et des véhicules.
Au cours des dernières années, le nombre d'objets connectés n'a cessé d'augmenter ce qui implique une grande masse de données à traiter et à stocker dans des infrastructures distantes tels que le Cloud qui offre la flexibilité et la puissance de calcul et de stockage, cependant le fait de ne compter que sur des infrastructures distantes présente également plusieurs inconvénients. Par exemple, le transfert de données vers le Cloud peut induire des retards non négligeables et ralentir le traitement de données ou la prise de décision. De plus, les applications qui dépendent exclusivement de services distants peuvent se bloquer si la connexion réseau est instable ou défaillante ce qui pourrait dégrader la qualité de service (QoS) requise pour certaines applications.
Du fait des problèmes de latence et de trafic réseau générés par le Cloud, le paradigme de Fog computing a émergé. Le Fog permet de décentraliser les services traditionnellement fournis par le Cloud sur l'ensemble des équipements réseaux. Par conséquent le traitement et les applications sont déployés dans les dispositifs à la périphérie du réseau plutôt qu'entièrement dans le Cloud.
Dans ce chapitre, l'accent sera mis sur le concept du Fog computing y-compris son architecture, ses caractéristiques ainsi que ses avantages pour les applications distribués.

2.2 Le Cloud computing

Traditionnellement, une entreprise utilisait sa propre infrastructure pour héberger ses services. Elle achetait ses propres serveurs, et assurait le développement et la maintenance des systèmes nécessaires à son fonctionnement. Par opposition, le Cloud computing (L'informatique en nuage) fournit des services ou des applications informatiques en ligne, accessibles partout, à tout moment, et de n'importe quel terminal (Smartphone, PC, tablette). Pour être plus précis, le Cloud computing permet de partager chez un fournisseur d'offres Cloud une infrastructure, une solution applicative ou encore une plateforme à tout utilisateur qui en fait la demande via un simple site internet (appelé aussi portail) en libre-service applicative, sans se soucier du reste [27][28].

Le Cloud computing propose généralement trois types de services :

— **Application (SaaS, Software as a Service) :** Permet aux consommateurs d'utiliser des applications qui se trouve dans le Cloud. Les applications sont accessibles depuis n'importe quel appareil connecté à internet.
De cette façon, l'utilisateur final n'a plus besoin d'installer tous les logiciels existant sur sa machine de travail. Cela réduit également la maintenance en supprimant le besoin de mettre à jour les applications. Ce type de modèle transforme les budgets logiciels en dépenses variables et non plus fixes et il n'est plus nécessaire d'acquérir une version du logiciel pour chaque personne au sein de l'entreprise [29].

— **Platform (PaaS, Platform as a Service) :** Les services fournis sur la couche PaaS sont destinés développeurs. Ces services sont des environnements de programmation ou d'exécution où un logiciel (programme) propriétaire écrit dans un langage de programmation spécifique peut être exécuté. Dans ce modèle, L'utilisateur n'a pas de contrôle sur l'infrastructure [30].

— **Infrastructure (IaaS, Infrastructure as a Service) :** Ce modèle donne aux utilisateurs une vue abstraite sur le matériel, processeurs, mémoire, systèmes de stockage, réseaux. Il permet aux utilisateurs d'avoir le contrôle sur l'ensemble des ressources allouées, exemple : création et suppression des instances de machine, démarrage et arrêt des OS, définition des topologies réseaux.

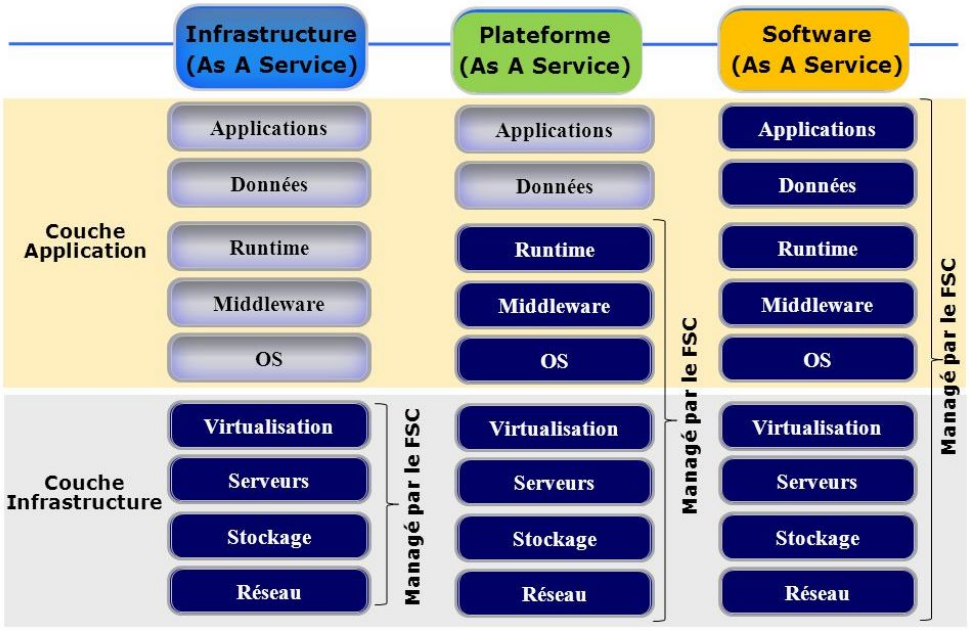

FIGURE 2.1 – Les types de service du Cloud computing [6].

Le tableau ci-dessous regroupe quelques avantages et inconvénients de ces trois types de services :

	Avantages	Inconvénients
SaaS	+Pas d'installation +Pas de license +Migration +Accessible via un abonnement	-Logiciel limité -Sécurité -Dépendance des prestatires
PaaS	+Pas d'infrastructure nécessaire +Pas d'installation +Environnement hétérogène.	-Limitation des langages -Pas de personalisation dans la configuration des machines virtuelles
IaaS	+Administration. +Personalisation +Fléxibilité d'utilisation +Capacité de stockage infini	-Sécurité. -Besion d'un administrateur systéme

TABLE 2.1 – Différences entre les modèles des services Cloud.

2.3 Le Fog computing

2.3.1 Défnition

Fog computing ou (l'informatique en brouillard) est un paradigme proposé par Cisco en 2012 essentiellement pour faire face aux problématiques des latences élevées et du trafic réseau important causé par l'utilisation du Cloud. Il est considéré comme une extension locale du Cloud. Le Fog permet de décentraliser les services traditionnellement fournis par le Cloud sur l'ensemble des équipements réseaux. Il permet d'utiliser les ressources de calcul et de stockage des équipements réseaux tels que les routeurs et les switchs localisés entre les objets connectés et les centres de données du Cloud.
Le Fog permet le filtrage, l'agrégation et le traitement des données à la périphérie du réseau, offrant une réduction de la latence, la préservation de la bande passante du réseau et l'amélioration de la qualité de service (QoS). Le Fog présente une infrastructure informatique géo-distribuée à grande échelle. Les composants du Fog, également appelés nœuds de Fog, sont hétérogènes en termes de performances de traitement, de capacité de stockage et de latence d'accès pour les objets et les utilisateurs. Les nœuds ayant des ressources limités sont plutôt situés en périphérie du réseau et fournissent une latence d'accès faible (de quelques millisecondes), tandis que les nœuds riches en ressources sont situés au cœur du réseau et fournissent un temps de latence d'accès plus élevée (de plusieurs secondes) [31].

2.3.2 Caractéristique du Fog

Les caractéristiques du Fog computing peuvent être résumées comme suit :

— **Distribution géographique :** Contrairement aux cloud centralisés, les services et applications fournis par Fog sont distribués et peuvent être déployés n'importe où [32].

— **Interactions en temps réel :** Les applications de calcul du Fog fournissent des interactions en temps réel entre les nœuds du Fog plutôt que le traitement par lots utilisé dans le Cloud [32].

— **L'hétérogénéité :** Les nœuds Fog se présentent sous diffèrents formes et sont déployés dans une variété d'environnement distribués [7].

— **Support de la mobilité :** Un aspect important des applications du Fog est la capacité de communiquer directement avec les appareils mobiles et donc d'activer des méthodes de navigation, telles que le LISP (Locator ID Separation Protocol) qui nécessite un système d'annuaire distribué [33].

2.3.3 Architecture du Fog computing

L'architecture du Fog computing est implémentée généralement en un seul modèle, le modèle d'architecture hiérarchique [7].

Modèle d'architecture hiérarchique :

1. **Terminaux connectés :** La couche inférieure qui déploie différents types de dispositifs de traitement intelligents, tels que des capteurs (locaux ou globaux), les machines connectées, les robots, les interfaces homme-machine ..., sont capables de communiquer avec la couche intermédiaire, pour assurer un traitement rapide des données.
2. **La couche Edge :** Cette deuxième couche est très proche des nœuds terminaux. Elle est composée de nœuds Edge, qui forment une passerelle entre les nœuds terminaux et les serveurs Fog pour acheminer les données et couvrir les appareils mobiles.
3. **La couche Fog :** La troisième couche regroupe différents nœuds de Fog tels que les serveurs, les routeurs, les passerelles et les commutateurs, qui sont capables d'extraire les connaissances des données puis de les transmettre aux serveurs Cloud computing. La couche Fog diffère d'une utilisation à l'autre, elle peut être une combinaison de plusieurs sous-couches Fog ou inclure différents modes de calcul selon les besoins de l'application. Chaque sous-couche traite localement les données communiquées et si elle ne supporte pas la quantité de données ou le routage, les données seront prises en charge par une autre sous-couche Fog pour les calculer et les router rapidement.
4. **Les Passerelles :** Ce sont des dispositifs qui relient les serveurs Fog au serveurs Cloud. Cette couche est souvent confondue ou attribuée à la couche Cloud.
5. **La couche Cloud :** C'est la couche supérieure, qui est composée des serveurs d'autorité pouvant être mis à jour avec les dernières informations fournies par les serveurs Fog et permettant l'analyse des données et des prises de décisions [29].

Remarque : Il convient de noter que certaines architectures considèrent que les deux couches Edge et Fog sont similaires et représentent la même couche.

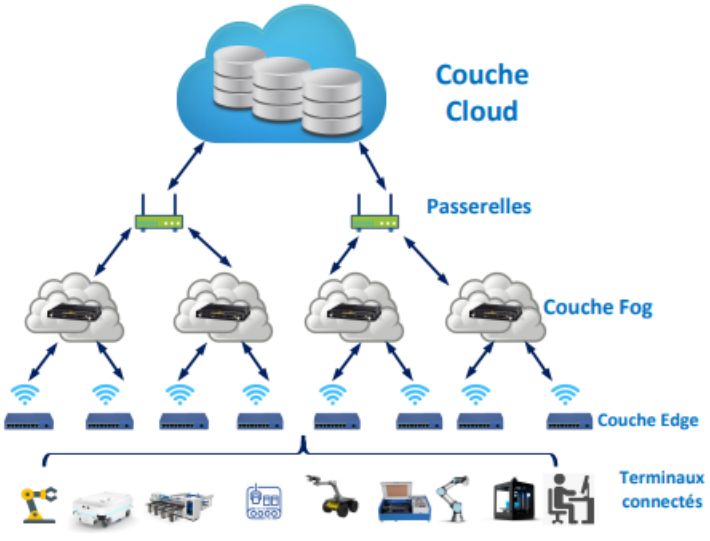

FIGURE 2.2 – Les couches de l'architecture basée sur le Fog Computing [7]

2.4 Cloud vs Fog

2.4.1 Les différences

La principale différence entre le Fog computing et le Cloud computing est que le Cloud est un système centralisé, tandis que le Fog est une infrastructure décentralisée. C'est un médiateur entre le matériel et les serveurs distants. Il régule quelles informations doivent être envoyées au serveur et lesquellles peuvent être traitées localement. De cette façon, le Fog computing est une passerelle intelligente qui décharge les Clouds en permettant un stockage, un traitement et une analyse des données plus efficaces.

Il convient de noter que le Fog n'est pas une architecture distincte et qu'il ne remplace pas le Cloud computing mais plutôt le complète, on se rapprochant le plus possible de la source d'information [34].

2.4.2 Les similarités

Le Cloud computing est connu pour sa capacité puissante d'analyse, de stockage et de calcul. Le Fog fournit également ce type de services et ajoute de nouvelles applications aux utilisateurs finaux, ce qui distribue l'exploitation dynamique des ressources du Cloud computing. Par conséquent, cette nouvelle couche de Fog est une amélioration de la couche Cloud computing, qui offre des services locaux plus raffinés. Il fournit des flux de haute qualité vers les nœuds et il est particulièrement adapté aux applications à faible latence, au lieu de le faire dans un centre Cloud distant. Le Fog transmet la partie profonde de l'analyse au Cloud computing. Il orchestrent d'une façon autonome un grand nombre de dispositifs. De plus, le Cloud computing se caractérise par sa localisation au sein d'Internet, qui coordonne un grand nombre de réseaux, clients, fournisseurs, environnements et ressources hétérogènes. Le Fog partage la même caractéristique de supporter des ressources hétérogènes et des nœuds déployés dans une grande variété d'environnements avec des formes et des utilisations différentes, qui peuvent être déployés d'une manière hiérarchique.

Fonctionnalité	Cloud computing	Fog computing
Latence	Le Cloud computing a une latence élevée par rapport au Fog computing	Le Fog Computing a une faible latence
Capacité	Le Cloud Computing ne fournit aucune réduction des données lors de l'envoi ou de la transformation des données	Le Fog Computing réduit la quantité de données envoyées au Cloud computing
Réactivité	Le temps de réponse du système est élevé	Le temps de réponse du système est quasi réel.
Sécurité	Moins sécurisé que le Fog Computing	Haute sécurité.
La vitesse	La vitesse d'accès est élevée en fonction de la connectivité de la machine virtuelle.	Élevé encore plus par rapport au Cloud Computing.
Mobilité	Mobilité limitée.	La mobilité est prise en charge.
Nombre de nœuds de serveur	Peu de nœuds de serveur.	Grand nombre de nœuds de serveur.
Distribution géographique	Centralisé.	Décentralisé et distribué.

Table 2.2 – Cloud Vs Fog

2.4.3 Fonctionnement du Fog computing

Le Fog computing fonctionne en utilisant des dispositifs locaux appelés nœuds ainsi que des dispositifs de périphérie. A titre d'exemple, les données collectées par des capteurs IoT, sont envoyées au noeud le plus proche directement ou via des passerelles. Ces données sont ensuite analysées localement, filtrées, puis envoyées vers le Cloud pour un stockage à long terme si nécessaire ou pour une analyse massive qui nécessite plus de ressources [35].

2.4.4 Le Fog et le Edge computing

Le Fog computing et le Edge computing offrent des fonctionnalités similaires en termes de distribution des ressources et du stockage. Ces deux technologies exploitent la puissance, des capacités de calcul au sein d'un réseau local pour effectuer des tâches de calcul. En fait, la philosophie du Fog et du Edge computing est de déplacer l'activité de traitement plus près du réseau pour accélérer le service. Bien qu'ils aient tous deux l'intention de réduire la latence et la congestion du réseau, elles diffèrent considérablement dans la façon dont elles traitent réellement les données. Dans ce contexte, la principale différence entre le Edge computing et le Fog computing

réside dans l'endroit où l'intelligence et la puissance de calcul se placent. Dans le Edge computing, les données sont traitées directement sur les sources de données telles que les capteurs, les appareils IoT, ou sur les appareils auxquels les capteurs sont connectés.
D'autre part, le Fog computing transfère les tâches de calcul vers une passerelle IoT ou des nœuds situés dans le réseau LAN [36].

2.4.5 Avantages du Fog computing

— **Le temps de latence :** Les applications d'aujourd'hui exigent un temps de réponse très réduit(dans l'ordre de quelques millisecondes). Dans ce contexte, le Fog computing élimine le besoin d'envoyer des données pour un traitement dans le Cloud. Par conséquent, le calcul s'effectue plus rapidement et le réseau de Fog peut traiter de gros volumes de données avec un délai minimal. Autrement dit, la latence entre l'entrée et la réponse est minimisée. L'objectif est de fournir une réactivité en périphérie du réseau, permettant le traitement des données en temps quasi réel [36].

— **Conservation de la bande passante du réseau :** Le transfert de données entre la périphérie du réseau vers un serveur Cloud nécessite beaucoup de bande passante. Exemple dans le cas où il ya des milliers d'appareils et chaqu'un d'eux génère 100 GO de données par jours. Ce qui amène à une surchage de la bande passante du réseau. En fait le Fog computing traite ces données localement et il conserve au maximum la bande passante du réseau [36].

— **Passage à l'échelle :** La distribution géographique des nœuds de Fog et leur proximité avec les utilisateurs finaux permettent de gérer un grand nombre d'objets connectés (la répartition de la charge de travail). Les nœuds de Fog sont de nature hétérogène avec des performances et des coûts différents. Ce deuxième point permet de déployer, selon le besoin de nouveaux nœuds de manière simple et moins coûteuse (en comparaison avec le Cloud) [31].

— **Réduction du trafic réseau :** Le Fog computing permet d'exécuter des fonctions de traitement, de filtrage et d'agrégation de données tout au long du chemin du réseau. En effet, la pertinence de l'envoi de données est examinée à chaque étape de la transmission permettant une réduction importante du trafic réseau [31].

— **Disponibilité hors ligne :** Les appareils IoT sont également disponibles hors ligne quand ils sont intégrés dans une architecture de Fog computing.

— **Géolocalisation et support de la mobilité :** La distribution géographique des nœuds de Fog aide à localiser les objets. De plus, la latence existante entre des nœuds de Fog voisins est courte. Cela aide à migrer des tâches (ex. à base de conteneurs) d'un nœud à un autre de manière transparente, afin de supporter la mobilité des objets. Élimination de la dimension centralisée de l'environnement informatique, réduisant, ainsi les points de blocage et de défaillance.

2.4.6 Défis de Fog computing

Bien que le paradigme du Fog computing offre de nombreux avantages pour différentes applications IoT, il est confronté à de nombreux défis qui font obstacle à son déploiement réussi. Ces défis sont l'évolutivité, la complexité, la dynamité, l'hétérogénéité, la latence et la sécurité.

— **Évolutivité :** Le nombre de dispositifs IoT est de l'ordre de milliards, ce qui génère une énorme quantité de données et nécessite une énorme quantité de ressources telles que la puissance de traitement et le stockage. Par conséquent, les serveurs du Fog devraient être en mesure de prendre en charge tous ces appareils avec des ressources adéquates. Le véritable défi sera la capacité à répondre à la croissance rapide des dispositifs et applications IoT.

— Complexité : Comme il existe de nombreux appareils et capteurs IoT conçus par différents fabricants, le choix des composants optimaux devient très compliqué, notamment en raison des différentes configurations logicielles et matérielles et des exigences personnelles. En outre, certaines applications ayant des exigences de sécurité élevées nécessitent un matériel et des protocoles spécifiques pour fonctionner, ce qui augmente la difficulté d'opération [33].

— **Dynamisme :** L'une des caractéristiques importantes des dispositifs IoT est leur capacité à évoluer et à modifier dynamiquement la composition de leur flux de travail. Ce défi va modifier les propriétés internes et les performances des dispositifs IoT. En outre, les appareils portables souffrent du vieillissement des logiciels et du matériel, ce qui entrainera une modification du comportement du flux de travail et des propriétés des appareils. Par conséquent, les nœuds de Brouillard auront besoin d'une reconfiguration automatique et intelligente de la structure topologique et des ressources attribué.

— **Hétérogénéité :** Aujourd'hui, il existe de nombreux appareils et capteurs IoT qui sont conçus par différents fabricants. Ces appareils ont des capacités diverses en matière de radios de communication, de capteurs, puissance de calcul de stockage, etc. La gestion et la coordination des réseaux de ces dispositifs IoT hétérogènes et la sélection des ressources appropriées deviendront un grand défi.

— **Application temps réel :** Le Fog computing a été proposé principalement pour lutter contre les latences élevées du Cloud. Le Fog est utilisé pour déployer des applications sensibles aux latences comme l'Internet des véhicules, la santé et l'industrie 4.0. Afin de réduire la latence, il est important d'étudier comment les données et leurs traitements sont placés dans l'infrastructure. Par exemple, un nœud de Fog peut avoir besoin de traiter des données distribuées dans plusieurs nœuds éloignés. Le calcul ne peut être démarré qu'après avoir récupéré toutes les données requises, ce qui ajoute de la latence au service.

— **La fiabilité :** Comme le Fog computing est réalisé par l'intégration d'un grand nombre d'équipements répartis géographiquement, la fiabilité est l'un des principaux défis à considérer lors de la conception d'un tel système. La fiabilité peut être améliorée grâce à une vérification périodique pour reprendre après un échec, à un ré-ordonnancement des tâches échouées ou à une réplication pour exploiter le traitement en parallèle. Toutefois, les points de contrôle et d'ordonnancement ne peuvent pas s'adapter à l'environnement hautement

dynamique du Fog à cause des latences. La réplication semble plus prometteuse, mais elle repose sur le fonctionnement synchronisé de plusieurs nœuds de Fog [31].

2.4.7 Cas d'utilisation

La ville intelligente :

Prenons l'exemple d'une ville intelligente. Les centres de données ne sont pas conçus pour répondre aux demandes des applications de ville intelligente. La quantité toujours croissante de données transmises, stockées et accessibles depuis tous les appareils IoT d'une ville nécessitera un nouveau type d'infrastructure pour gérer ce volume. Ce sont ces applications qui ont besoin du fog computing pour offrir toute la valeur que l'IoT leur apportera.

La santé :

Dans le domaine de la santé on utilise le Fog dans la surveillance médicale. L'idée est que des capteurs mesurent différents paramètres de la personne, Transmettre cette grande quantité de mesures sur une plateforme de Cloud Computing pour l'analyser est très coûteux. L'idée proposée est d'introduire L'infrastructure de Fog pour détecter des motifs dans les données qui signifient que la personne est en danger. L'objectif est de pouvoir être alerté le plus rapidement possible sans attendre que le calcul soit traité sur une plateforme de Cloud [37].

Robotique et industrie du futur :

Dans les usines du futur, le Fog peut être utilisé pour analyser les données issues de capteurs mais également pour contrôler la production de façon centralisée. Des machines virtuelles sont alors automatiquement déployées pour en contrôler le bon fonctionnement mais aussi pour les commander. Une infrastructure de Fog peut être utilisée pour produire des marchandises personnalisées selon les besoins de l'utilisateur. Par exemple, l'utilisateur donne les caractéristiques du produit qu'il souhaite sur le site web de l'entreprise puis le système de production est re-paramatré afin que les machines fabriquent ce qui a été demandé.

Fonctions de virtualisation réseau :

L'approche consiste à virtualiser les équipements qui composent les réseaux informatiques (pare-feu, serveurs, routeurs, commutateurs) au sein des sites de Fog. Il n'est donc plus question d'aller déployer un pare-feu physique à tel ou tel endroit du réseau mais d'installer une machine virtuelle ayant ce rôle dans le site de Fog correspondant. Cette approche permet de créer des réseaux flexibles, reconfigurables et adaptés aux besoins des utilisateurs tout en garantissant une latence pour l'accès aux différents services.

2.5 Conclusion

Le Fog computing apparaît comme une solution intéressante au problème du traitement des données dans l'IoT. Il s'appuie sur des appareils à la périphérie du réseau qui ont plus de puissance de traitement que les appareils finaux et sont plus proches de ces appareils que les ressources Cloud, réduisant ainsi la latence des applications. Dans le chapitre suivant, nous allons étudier l'approche d'intégration entre le paradigme Fog computing et Blockchain.

CHAPITRE 3

INTÉGRATION IOT-BLOCKCHAIN

3.1 Introduction

Avec le développement rapide des technologies de communication, l'IoT atteint sa pleine maturité, et tend à se développer de manière explosive, des milliards de dispositifs IoT interagissent les uns avec les autres et avec d'autres entités telles que les êtres humains et les différentes plateformes. Une telle interaction nécessite donc d'être sécurisée et protégée.

La plupart des architectures IoT sont hautement centralisées, ayant par conséquent plusieurs limitations techniques telles que le problème du point de défaillance unique.

Pour faire face à ce type de problèmes, la Blockchain est proposée comme étant une solution prometteuse pour plusieurs approches d'intégration avec l'IoT.

Dans ce contexte, ce chapitre met l'accent sur l'approche d'intégration entre la Blockchain et le Fog computing afin d'apporter certaines solutions aux problèmes et défis qui font face aux applications IoT. L'objectif de cette intégration est d'assurer la sécurité de données et de communications tout en préservant la traçabilité, la transparence et la fiabilité dans les réseaux IoT. Ainsi, l'utilisation de la Blockchain peut transformer l'industrie de l'IoT vers un nouvel horizon.

3.2 La convergence Blockchain-IoT

Au cours de ces dernières années, l'IoT crée des défis fondamentaux dans plusieurs aspects tels que la sécurité, la confidentialité, l'évolutivité et la maintenabilité. Les dispositifs IoT doivent fonctionner sur une architecture efficace même pour effectuer des tâches simples telles que la détection, le traitement, la collecte de données et la communication. La nature décentralisée de la Blockchain et ses caractéristiques offrent un mécanisme utile pour relever les défis de l'IoT [38]. Les applications IoT peuvent généralement utiliser Blockchain pour accéder à des objets et stocker des données. Les utilisateurs doivent pouvoir accéder aux données à distance depuis n'importe quel endroit en utilisant un moyen sécurisé et en garantissant la confidentialité de ces données dans le réseau.

3.2.1 Quelques travaux connexes

Dans cette section, nous survolons quelques travaux de la littérature traitant la Blockchain et l'IoT. Les acteurs de ces travaux ont étudié comment utiliser la technologie Blockchain pour résoudre les problèmes liés à IoT en investiguant les manières d'adaptation de la Blockchain aux besoins spécifiques de l'IoT pour développer des applications basées sur cette intégration (BC-IoT).

Chen et al [39] ont proposé un schéma d'authentification géolocalisée utilisant des contrats intelligents pour garantir que les appareils IoT peuvent effectuer en toute sécurité l'authentification du réseau Wi-Fi. Ainsi selon une enquête de Gartner [40] ,d'ici 2025, les problèmes confrontés par les industries de l'IoT seront résolus par la technologie Blockchain.

En 2017, une brève recherche examinant les critères nécessaires pour développer un systéme de cryptomonnaie qui intègre les systèmes d'interface neuronale (SIN), l'IA, la Blockchain et le Fog computing [41].
En 2018, R. Almadhoun et M. Kadadha [42] ont proposé un schéma d'authentification BC-Fog sans TTP (Trusted Third Party) en utilisant la plate-forme Ethereum, pour contrôler l'accès à distance aux objets dans les systèmes IoT. Ainsi, X.Zhang et R.Li ont proposé une architecture VANET décentralisée multicouche basée sur la Blockchain.

En 2020, MA Bouras et Q. Lu[43] ont étudié les systèmes de gestion d'identité décentralisés basés sur la Blockchain et les scénarios possibles d'adoption de tels systèmes pour améliorer les applications de soins de santé. Ainsi, Alli et M. Fahadi [44] ont présenté les concepts de base de l'IoT, du Fog computing, et de la Blockchain, dans le cadre de déploiement général Fog-Blockchain, ainsi les opportunités et les défis associés. Ils ont clarifié comment la propriété de décentralisation de Blockchain peut être appliquée au niveau des périphériques, au niveau du Fog computing ou au niveau du Cloud, en discutant certains algorithmes de consensus les plus répandu. Cependant, malgré un accord croissant sur le potentiel de l'intégration de la Blockchain et l'IoT, la principale question concernant l'endroit où la Blockchain serait déployée reste un sujet discutable.

Dans ce qui suit, nous présentons trois approches d'intégration, à savoir l'intégration au niveau Cloud, l'intégration au niveau de Fog et l'intégration au niveau de périphériques.

3.2.2 L'approche Cloud- Blockchain

La contrainte des ressources limitées des appareils IoT, impose la délégation de certaines tâches applicatives de l'IoT au Cloud computing, qui donne naissance au paradigme de Cloud of Things (CoT). Le CoT fournit un environnement de Cloud computing flexible et robuste pour le traitement et la gestion des services IoT, montrant un grand potentiel pour améliorer les performances du système et l'efficacité de la prestation de services. Cependant, les infrastructures CoT conventionnelles ont tendance à être inefficaces en raison des plusieurs défis [45].

Premièrement, les solutions CoT conventionnelles se sont principalement appuyées sur des modèles de communication centralisés pour exécuter les services IoT, ce qui rend difficile la mise à l'échelle des réseaux IoT.

De plus, la plupart des systèmes CoT actuels exigent de faire confiance à un tiers, par exemple un fournisseur de Cloud, pour le traitement des données IoT, ce qui soulève des problèmes de sécurité et de confidentialité de données.

Enfin, l'infrastructure centralisée du réseau entraîne une latence de communication et une consommation d'énergie plus élevées pour les appareils IoT en raison de la langue distance de transmission de données.

Dans ce contexte, le concept de convergence entre la Blockchain et le Cloud se propose comme étant un solution qui relève plusieurs caractéristiques intéressantes telles que :

— **Sécurité :** Les serveurs Cloud sont des cibles au potentiels attaques ce qui signifie qu'une défaillance à un certain point affectera l'ensemble de l'écosystème. Mais, dans la Blockchain, ce risque est diminué à cause de la distribution des nœuds de la Blockchain.

— **Évolutivité :** Sur les applications Blockchain à grande échelle, le nombre de transactions peut être énorme. Il est donc très important de disposer de services de traitement de données puissants pour une exécution efficace des transactions afin de permettre des services de blockchain évolutifs. Par conséquent, le Cloud peut fournir des ressources de calcul à la demande pour les opérations Blockchain. Ainsi, la combinaison du Cloud computing et de la Blockchain peut fournir un système intégré hautement évolutif.

— **Décentralisation :** Dans l'IoT et le Cloud computing, un problème majeur est la dépendance à un serveur centralisé dans le but de gérer les données et de prendre des décisions. Des problèmes comme une défaillance du serveur central peuvent perturber l'ensemble du système, entraînant également la perte de données stockées sur un serveur central. De plus, ce dernier est susceptible d'être une cible de plusieurs types d'attaques. La Blockchain peut fournir une solution à ce problème car plusieurs copies des mêmes données sont stockées sur plusieurs nœuds, ce qui élimine la possibilité d'une défaillance globale du système en cas de défaillance d'un serveur.

Cependant, il convient de noter que malgré que le Cloud soit doté d'une puissance de calcul et d'une capacité de stockage immenses, cette approche n'est pas toujours adaptée pour principalement deux raisons :

— La latence très importante.

— La consommation d'énergie qui pose déjà un problème avec les centres de données au niveau du Cloud.

3.2.3 L'approche Fog-Blockchain

Le Fog computing est un système distribué qui vise à rendre les services du Cloud computing plus proche et plus accessible en créant des hubs ou des mini-centres de données déployés à la périphérie du réseau. Fondamentalement, le Fog computing accomplie plusieurs tâches d'une manière moins exigeante et réduit la communication entre le Cloud et l'utilisateur final [38]. Cependant, des défis majeurs sont restés ouverts même lorsque le Fog computing est intégré à l'IoT tels que le besoin de système de gestion de données et les problèmes de sécurité. Donc une telle intégration entre le Fog et la Blockchain peut fournir une gestion de données fiable, immuable et entièrement décentralisée.

La Blockchain peut être une technologie utile pour répondre aux problèmes de sécurité et de confidentialité mentionnés ci-dessus dans les systèmes FC-IoT. La Blockchain garantit la sécurité, l'authentification et l'intégrité des données transmises par les appareils IoT pour qu'elles soient vérifiées par chiffrement et attribuées par l'expéditeur authentique. Comme le Fog computing possède un environnement informatique distribué, la technologie Blockchain peut offrir de bonnes solutions de confiance et de sécurité décentralisées. La Blockchain peut détecter et isoler le nœud défectueux pour protéger l'ensemble du système de toute faille de sécurité. Cela fournit une capacité d'autoréparation aux systèmes IoT compatibles Fog. Le système de sécurité équipé d'une sécurité basée sur Blockchain répond à la plupart des exigences des systèmes IoT compatibles Fog en améliorant le fonctionnement indépendant entre tous les nœuds connectés.

Lors que la Blockchain est déployer dans les nœuds Fog, une transaction est demandé par un appareil IoT qui sera ensuite intégrées dans un bloc après avoir été vérifié et validé par l'ensemble de nœuds du réseau puis ajouté à la Blockchain ce que montre la Figure 3.1.

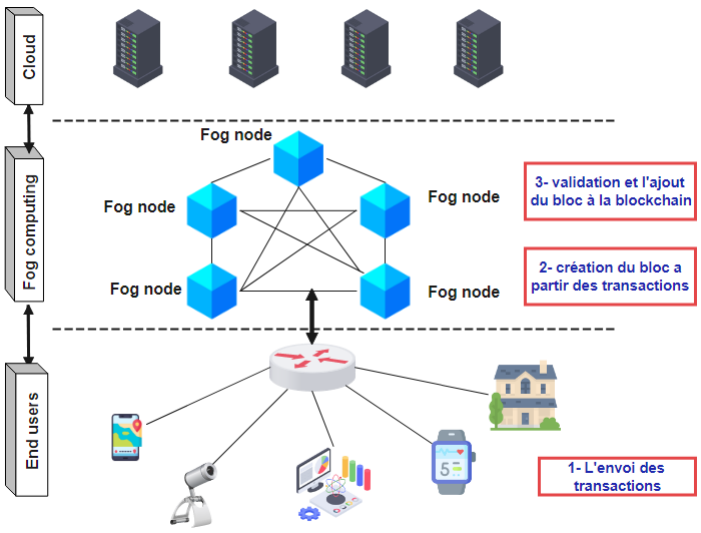

FIGURE 3.1 – Approche Fog-Blockchain

3.2.4 L'approche périphériques-Blockchain

Cette approche consiste à déployer la Blockchain directement dans les objets connectés, où chaque objet est constitué un nœud de la Blockchain autrement dit, chaque nœud dispose d'une copie de la Blockchain. Il convient de noter qu'Ethereum et ses implémentations sont l'exemple populaire d'intégration au niveau de l'appareil. Plusieurs cartes de circuits intégrés ont été introduites pour créer des dispositifs intelligents basés sur la Blockchain tels que Edison Arduino afin de présenter le déploiement de la Blockchain au niveau de l'appareil. Cette approche est bonne si nous disposons d'un ordinateur puissant et d'une capacité de stockage suffisante au niveau de l'appareil, car avec le temps, la taille de la Blockchain augmente également. La contrainte des ressources limitées des dispositifs IoT constitue un réel problème et rend potentiellement cette approche inutilisable a long terme [46].

Donc, il est clair que l'utilisation de la Blockchain pourrait ajouter à l'IoT une certaine couche de sécurité et de confidentialité, ainsi que d'une transparence et de visibilité accrues. D'autre part, d'autres problèmes persistent tels que la latence et les contraintes liées à l'infrastructure du réseau sous-jacent. Donc le Fog computing, proposé initialement pour améliorer les performances de l'IoT et minimiser certaines limitations existantes, peut constituer une plateforme convenable pour une telle intégration avec la Blockchain [26].

En outre, nous avons constaté que les principales observations suivantes peuvent être faites :

— La plupart des solutions d'intégration BC-FC ont été proposées pour l'IoT et les applications associées, telles que les applications IoV (Internet of Vehicles), IIoT (Industrial Internet of Things) et eHealth. Ainsi, le déploiement de la Blockchain à des fins de gestion de données, est conçu comme une alternative plus fiable à une base de données classique.

— La grande majorité des approches d'intégration BC-FC utilisaient des algorithmes basés sur la preuve. Pour être plus précis, la plupart des solutions ont déployé une variante de l'algorithme de consensus basé sur PoW, malgré le fait que les BC basés sur PoW sont les plus énergivores par rapport aux autres algorithmes.

— La Blockchain est déployée dans la couche Cloud lorsqu'elle est utilisée à des fins de paiement/trading. Suivant cette hypothèse, la plupart des solutions d'intégration BC-FC ont déployé le BC dans la couche Cloud.

3.3 Conclusion

Les systèmes IoT se développent énormément en termes de types d'applications et de nombre d'appareils. Cela a créé de nombreux défis qui nécessitent des solutions urgentes pour permettre d'exploiter pleinement le potentiel de l'IoT à l'avenir. D'autre part, la Blockchain est apparue comme une technologie distribuée, immuable, transparente, décentralisée et sécurisée qui a un rôle prometteur dans de nombreux secteurs. Les caractéristiques et la structure de la Blockchain en font un candidat solide pour résoudre les problèmes et les défis des systèmes IoT. Le rapprochement de ces deux paradigmes a attiré l'attention de nombreux chercheurs qui ont proposé différentes approches d'intégration, parmi lesquelles l'intégration Fog-Blockchain.

Cependant, une telle intégration est encore nouvelle, car aucune des solutions proposées n'était capable de résoudre la plupart des défis ni d'explorer tout le potentiel de la Blockchain pour en bénéficier dans le paradigme IoT. Dans ce chapitre nous avons essayé de mettre en relief cette intégration afin de résoudre certains problémes, notament la sécurité dans l'IoT. Ainsi, nous avons survolé quelques travaux connexes et les différentes approches d'intégration existantes. Le prochain chapitre est consacré à l'implémentation d'une approche d'intégration Fc-Bc utilisant les algorithmes de consensus PBFT et PoET.

CHAPITRE 4

IMPLÉMENTATION

4.1 Introduction

Ce chapitre décrit l'intégration de la Blockchain et le Fog computing à travers une étude de simulation. Dans ce qui suit, nous décrivons l'environnement de simulation, les protocoles utilisés, ainsi qu'une étude de cas.

4.2 L'environnement de simulation

Le simulateur Fobsim est un outil de simulation des environnements intégrés de type BC-Fog. Il est utilisé dans cette étude pour simuler l'approche d'intégration étudiée sachant qu'il est capable de simuler différents scénarios d'intégration, c'est-à-dire que BC peut être placée dans la couche Fog, la couche utilisateur final ou la couche Cloud [47].

4.2.1 L'architecture de Fobsim

Fobsim offre tous les modules nécessaires pour une simulation fiable d'une telle intégration tel qu'il est illustré dans la figure suivante :

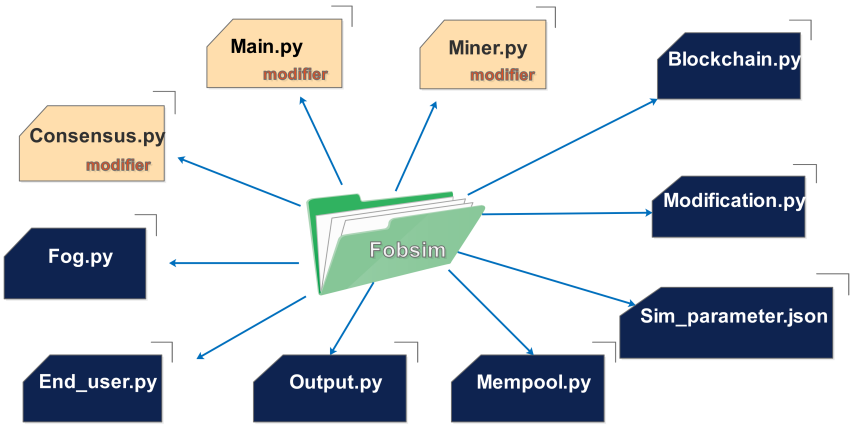

FIGURE 4.1 – Architecture de FobSim

Mempool.py : Dans ce module les transaction sont accumulés dans une file d'attente de multi-traitement qui permet aux différents processus d'ajouter et d'obtenir des transactions de manière synchrone.

Fog.py : Ce module permet de créer des nœuds fog qui reçoivent des tâches à exécuter (End user tasks)puis les envoient au mempool afin d'être stockées temporairement.

End user.py : Ce module génère des tâches selon la fonctionnalité de Blockchain choisie par l'utilisateur puis l'envoie au Fog correspondant sinon au cloud.

Output.py : Contient des informations sur les paramètres de fonctions telles que l'emplacement, les types de consensus, les données des blocs, les messages d'erreur, etc.

Blockchain.py : Ce module contient les fonctions suivantes :
• generate_new_block : qui permet de créer un bloc puis l'hacher on utilisant la fonction hashing_function.
• Report_a_successful_addition : incrémente le nombre de votes si les données d'un bloc ne sont pas modifiées .
• Fork_analysis : cette fonction est appelée en cas d'utilisation du consensus de PoW pour vérifier s'il y a un fork en hachant la chaine local de chaque nœud, le hach est ajouté à une liste s'il n'existe pas puis on test si la longueur de chaine est supérieure à 1.

Miner.py : Le mineur peut concevoir un bloc après l'accumulation des transactions dans le memepool à l'aide de la fonction build_block selon le type du consensus choisi. Après la génération du nouveau bloc, il le transfert vers ses voisins, ensuite à tous les nœuds de réseau par la fonction receive_new_block pour qu'ils puissent les valider et les ajouter, s'il est valide la chaine globale est confirmée en appliquant la méthode global_chain_isconfirmed_by_ majority.

Sim_parameters.json : C'est un fichier json qui contient les paramètres de simulation à savoir le nombre des noeuds Fog,le nombre des End User, nombre des transaction par bloc, délai entre les noeuds Fog et les utilisateurs finaux et le délai entre les noeuds Fog .

Modification.py : Ce module permet l'initialisation des fichiers json, la lecture, l'écriture et la modification du fichier.

Consensus.py : Il existe trois algorithmes de consensus disponibles à être utilisés dans différents scénarios de simulation a savoir PoW, PoS, PoA qui seront ensuite décrits individuellement . Les méthodes de chaque module de FoBSim sont décrites dans la Figure 4.2.

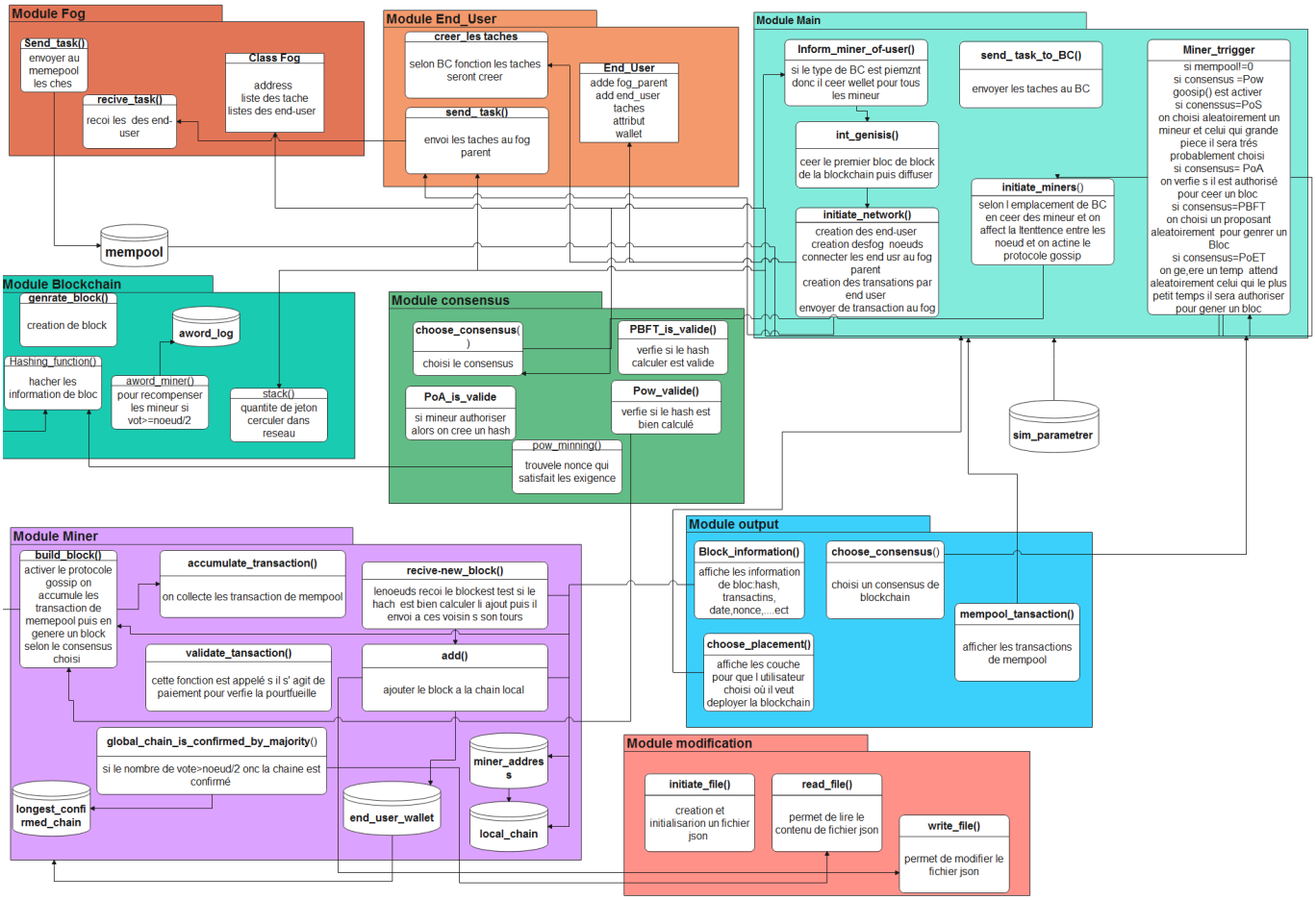

FIGURE 4.2 – Les modules de FobSim

4.2.2 Le protocole Gossip

Le protocole Gossip est un protocole de communication qui permet le partage d'état dans les systèmes distribués (peer-to-peer), afin de garder une trace de tous les nœuds et savoir si un nœud est en panne ou non tel que les nœuds de la Blockchain où chaque noeud l'utilise pour partager les blocs de la Blockchain [48]. Le fonctionnement de ce protocole est basé sur un concept simple qui consiste à distribuer et à propager des informations sur un réseau. Dans ce protocole, pour qu'un nœud distribue des informations, il lui suffit de se coupler avec d'autres nœuds au hasard. Une fois que cela se produit, il est possible d'échanger des informations reçues avec lesdits nœuds, qui à leur tour distribueront ces informations avec d'autres nœuds auxquels ils sont connectés, formant ainsi une chaîne de diffusion des informations sur tout le réseau de manière opportune et efficace. De plus, la manière dont les informations sont propagées au sein d'un réseau peer-to-peer via le protocole Gossip se produit rapidement et en toute sécurité tant que les nœuds impliqués peuvent garantir la propagation et la divulgation des informations sans discriminer ni exclure aucune des parties dans leur propre réseau.

Ce protocole permet de diffuser les données de la blockchain sur tous les paires de réseau ce qui garantit la synchronisation des données ,d'identifier les nœuds qui sont connecter et détecter ceux qui sont déconnectés ou malveillant et mettre à niveau les pairs nouvellement connectées

4.2.3 Les algorithmes de consensus

Le simulateur FobSim dispose de trois algorithmes de consensus :

— **Le consensus PoW :**
les mineurs collectent les TX(les transactions) du mempool (qui est une file d'attente partagée dans FoBSim) et les accumulent dans des blocs. Le mineur le plus rapide qui produit un hach inférieur à l'hach cible et qui est accepté par tous les nœuds, pourra l'ajouter dans la Blockchain. Pour que les mineurs puissent travailler en parallèle, on doit déployer le package de multitraitement(multiprocessing) de Python.

Algorithm 1 PoW

```
for i in range (expected_chain_length) do
    mineur= random.choice transaction = accumulate_transaction(num_de_tx_block,mempol,
    block_chain_function, obj.address )
    if blockchain = paiment then transaction =mineur.validation(transaction)
  end if
  if gossip = active then
      gossip()
      while true do
      bloc[hahs] = hashing_function(bloc[nonce],bloc[transaction],bloc[hash_precedent])
      if int(bloc[hash],16)>target then
        bloc[nonce]+=1
      else
        Break
      end if
    end while
  end if
  for elem in mineur_list do
    if elem.add in self.neighbours then
    elem.receive_new_bloc(bloc, type, consensus, bloc_function,expected_chain_length)
    end if
  end for
end for
```

— **Le consensus POS :**
Les mineurs disposent des pièces numériques dans leur portefeuille. Le réseau choisit au hasard un mineur. Une fois qu'un mineur est choisi, il est le seul autorisé, à générer et à diffuser le bloc suivant.

Algorithm 2 PoS

for conter in rang(excepted_chain_length) **do**
x = int(rond((len(miner_list)/2), 0) **for** *i* in range x **do**
Aliétoire_mineur.append(random.choice(the_miners_list))
plus_grand_jeton=0
Choisir quelques mineurs parmis les noeuds de réseau
end for
for mineur_choisi in Aliétoire_mineur **do**
if mineur_choisi.[wallet]> plus_grand_jeton **then**
plus_grand_jeton=mineur_choisi.[wallet]
finel_choice_mineur=mineur_choisi.[address] Broadcast (finel_choice_mineur)
end if
end **for**mempool.size() != 0 : transaction = accumulate_transaction(num_de_tx_block,mempol, block_chain_function, obj.address)

if blockchain = paiment **then**
transaction =mineur.validation(transaction)
end if new_block[hash] = hashing_function(new_block[nonce], new_block[transactions], new_block[generation_id], new_block[privious_hash])
for *elem* in mineur_list **do**
if elem.add in self.neighbours **then**
elem.receive_new_bloc(bloc, type, consensus, bloc_function,expected$_c hain_l ength$)
end if
end for
end for

— **Le consensus PoA :**
Seules les entités réseau autorisées sont capables de créer des nouveaux blocs.

Algorithm 3 PoA

```
for i in rang(len(the_miner_list)) do
  the_miner_list[i].isAutorized = true
  liste_ofAutorized_miner.append(the_miner_list[i])
end for
for counter in rang(excepted_chain_length) do
  for obj in miner_list do
    if mempol.qsize() != 0 then
      transactions =accumulate_transactions(num_de_tx_block,mempol,
      block_chain_function, obj.address )
    end if
    if Function_blockchain = 3 then
      transaction =obj.validate_transaction(transaction, generateur)
    end if
    new_block[hash] = hashing_function(new_block[nonce], new_block[transactions],
    new_block[generation_id], new_block[privious_hash])

    for elem in mineur_list do
      if elem.add in self.neighbours then
      elem.receive_new_bloc(bloc, type, consensus, bloc_function,expected_chain_length)
      end if
    end for
  end for
end for
```

4.3 Contribution réalisée

Notre contribution dans ce travail consiste en intégration et implémentation de deux algorithmes de consensus, à savoir l'algorithme PBFT et l'algorithme PoET. Dans ce qui suit, nous décrivons le principe de fonctionnement de ces deux algorithmes, ensuite nous présentons le résultat d'une étude de cas réalisée sous FobSim.

4.3.1 Le consensus PBFT :

Comme il a été mentionné précédemment dans la section 1.10 (chapitre 1), plusieurs types de consensus existent pour la Blockchain. Parmis lesquels, trios sont implémentés dans Fobsim (PoW, PoS, PoA).

Dans notre cas, nous avons choisi d'appliquer le protocole PBFT vu qu'il possède quelques caractéristiques intéressante puisqu'il n'effectue pas des calculs mathématiques, il n y pas de fork ou de réorganisation de la chaine, ainsi il fonctionne même s'il existe des noeuds défaillants c'est à dire qu'il est tolérant aux pannes (le nombre de nœuds malveillants ne dépasse un tiers de tous les nœuds du système).

Fonctionnement du PBFT :

Les nœuds d'un système distribué PBFT sont classés de manière séquentielle, un nœud étant le nœud principal et les autres appelés secondaires (ou les nœuds de secours).Il convient de noter tout nœud éligible du système peut devenir principal. Le cycle du fonctionnement PBFT est comme suit [49] :

Un nœud principal est élu à tour de rôle. Il collecte les transactions à partir du pool de transactions, puis il crée et diffuse le bloc a tous les nœuds secondaires.

Les nœuds secondaires reçoivent le bloc et vérifient la proposition, puis diffusent un message PREPARE aux autres validateurs.

Les validateurs attendent les 2F+1 messages de validation, puis entrent dans l'état COMMITTED

Lorsque le nœud principal reçoit des réponses « 2F+1 » de différents nœuds du réseau avec le même résultat, il ajoute le bloc dans la blockchain. Ainsi que tous les nœuds l'inséré dans leur chaîne local.

Enfin, Un nouveau tour est lancé avec l'élection d'un nouveau proposant.

Le diagramme suivant présente le fonctionnement du PBFT oú un noeud défectueux ne retoune aucun résultat :

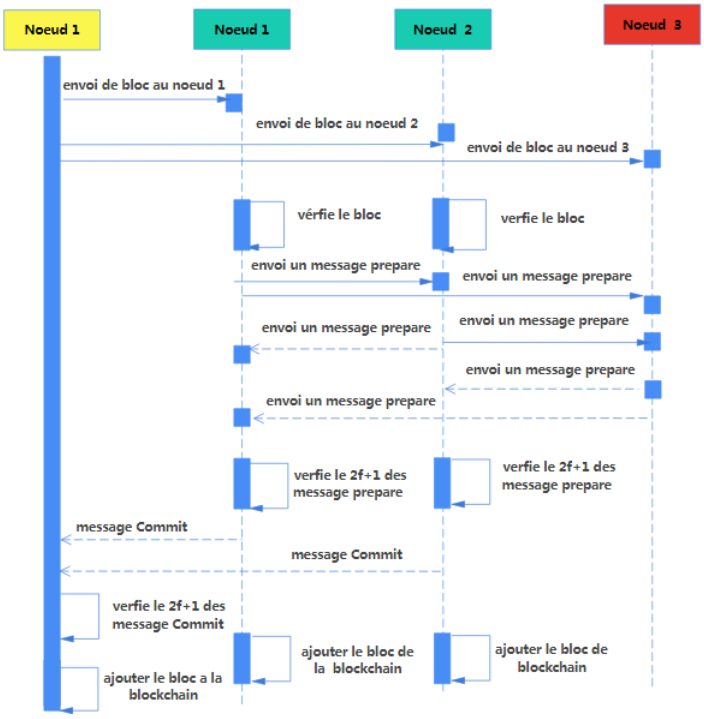

FIGURE 4.3 – Diagramme de séquence d'algorithme PBFT

le cas contraire :
L'échec prise en compte dans un scénario de PBFT est la défaillance d'un nœud arbitraire. C'est a dire : le non-retour d'un résultat, répondre avec un résultat incorrect, répondre avec un résultat différent aux différentes parties du système

Algorithm 4 PBFT

```
for counter in rang (excepted_chain_length) do
  proposant = random.choice(the_miner_list)
  accumulate_transaction(num_de_tx_block,mempol, block_chain_function, obj.address )
end fornew_block[hash] = hashing_function(new_block[nonce], new_block[transactions],
new_block[generation_id], new_block[privious_hash])
for elem in the_miner_list do
  for k in the_miner_list do
    if elem[address] != k[address] then
        cond = pbft_block_isValid(nouveau_block, nouveau_block[hash]) if cond= true
        then Diffuse preper a l'ensemble de réseau
      end if
    end if
  end for
  if len(preper_pool)>=(2*f+1) then
    for elem in the_miner_list do
      for k in the_miner_list do
        if elem[address] != k[address] then
          Envoyer message commit au pool
        end if
        if len(commit_pool)>=2*f+1 then
          Ajouter le block à la blockchain
        end if
      end for
    end for
  end if
end for
```

4.3.2 Le consensus PoET

Le mécanisme PoET attribue une durée à chaque nœud du réseau de manière aléatoire grâce a la fonction generate_random_time . Le nœud doit se mettre enveille ou effectuer une autre tâche pendant ce temps d'attente aléatoire. Le nœud qui obtient le temps d'attente le plus court se réveille et crée un nouveau bloc qui sera ensuite vérifie par les autres nœuds afin qu'ils puissent l'ajouter à la Blockchain.

Algorithm 5 POET

```
for obj in the_miers_list do
  objt[temps_attent]= generate_random_time(excepted_chain_length,poet_block,obj[address])
end forpetit_temps=poet_block
for obj in the_miners_list do
  if obj[temps_attent]<petit_temps then
    petit_temps=obj[temps_attent]
  end if
end for
for obj in the_miers_list  do
  if obj[temps_attent]==petit_temps then
    address_miner.append(obj[address])
  end if
end for
time.sleep(petit_temps)
if parallel_pow_mining then
  for obj in the_miers_list  do
    if obj[address] in address_miner  then
      transaction=accumulate_transaction(num_de_tx_block,mempol,
      block_chain_function, obj.address )
    end if
  end for
  process=Process(target=obj.build_block, args(num_of_tx_per_block, mempool.Mempool,
  the_miner_list, type_of_consensus, blockchain_Function ,excepted_chain_length))
  process.start() the_mining_processes .append(process)
  for process in the_mining_processes  do
    process.join()
  end for
else
  for obj in the_miner_list  do
    obj.build_block(num_of_tx_per_block, mempool.Mempool, the_miner_list,
    type_of_consensus, blockchain_Function ,excepted_chain_length)
  end for
end if
```

4.3.3 Étude de cas

Le processus de simulation est illustré dans la figure qui suit sachant que plusieurs scénarios peuvent être considérés dans Fobsim. Dans notre cas d'étude, nous avons opté pour un scénario d'emplacement au niveau de la couche Fog en comparant les deux algorithmes implémentés avec ceux déjà disponibles sur Fobsim.

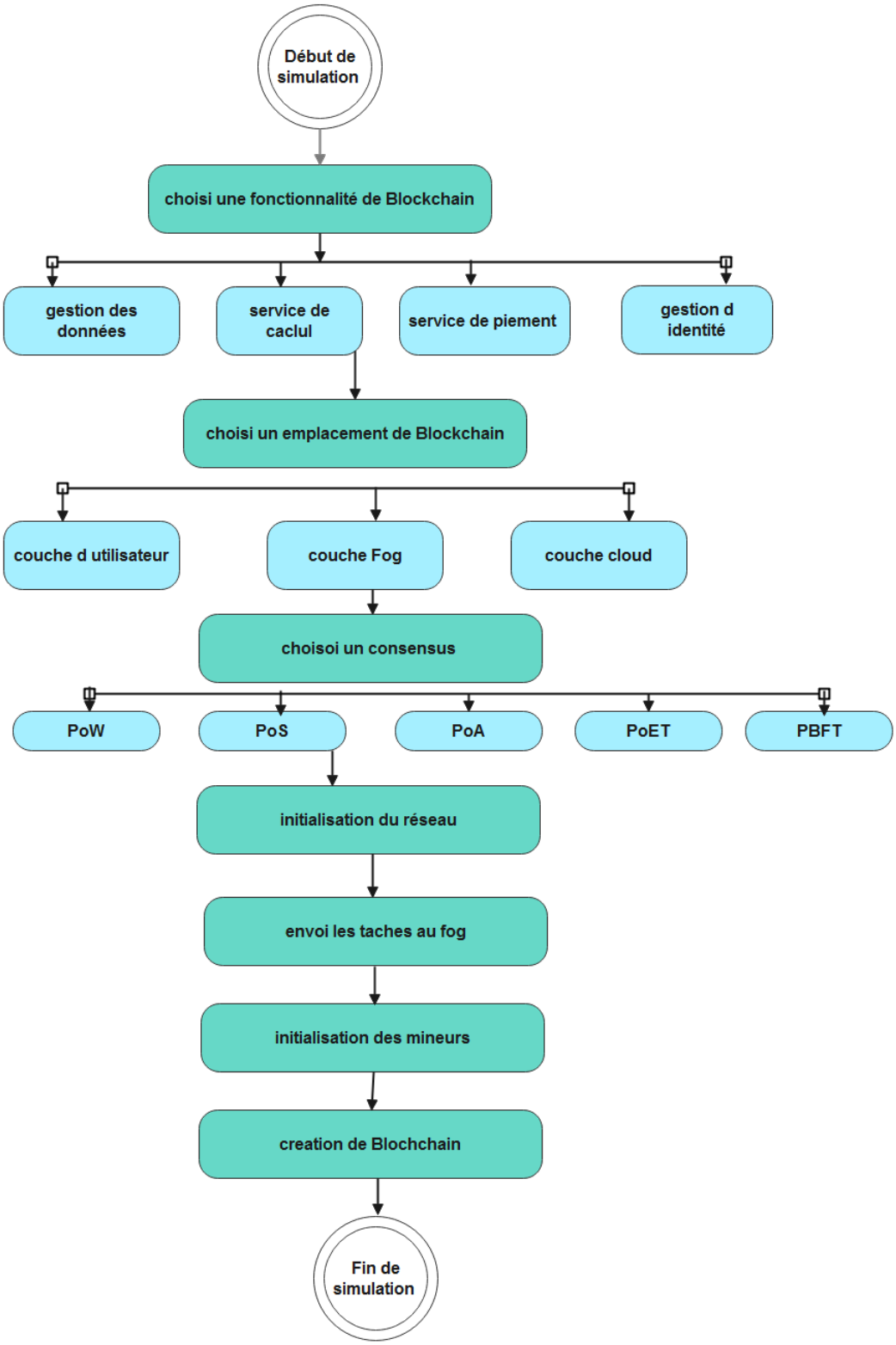

FIGURE 4.4 – Simulation Fobsim

4.4 Processus de simulation

Le tableau suivant présente les paramètres initiaux du Fobsim :

Paramètres initiaux	
Nombre des nœuds Fog	5
Nombre d'utilisateur par Fog	2
Nombre des taches par utilisateur	1
Nombre des mineurs	5
Nombre des voisins de Fog	2
Nombre des transactions par block	5
Difficulté de PoW	5
Temps de PoET	2
Délai entre nœud Fog	12
Délai entre utilisateur et nœud Fog	150

TABLE 4.1 – Etat intial.

Dans Table 4.2 nous avons comparé PoW, PoS et PoA en termes de temps d'exécution et celà dans le cas initial avant notre contribution, PoW devrait présenter la consommation de temps la plus élevée. Cela est dû à l'énigme mathématique que chaque mineur doit résoudre afin de prouver son illisibilité pour frapper le bloc suivant. Dans PoS, en revanche, le choix du prochain mineur est au hasard. L'algorithme PoA est cependant le plus délicat. En effet, tous les mineurs autorisés créent de nouveaux blocs, vérifient les blocs nouvellement frappés. Donc PoA est le meilleur en terme de consommation d'énergie.

Consensus	Temps d'exécution (s)
PoW	0.66 S
PoS	0.058 S
PoA	0.056 S

TABLE 4.2 – Etat intial

Les résultats de simulation sont représentés dans le tableau suivant, dans lesquels nous avons effectuer différentes simulation avec différents algorithmes de consensus dans des conditions similaires(Table 4.1), et a chaque exécutions on augmente le nombre des mineurs.

Le critère d'évaluation sera le temps que doit prendre chauque consensus a fin d'ajouter un bloc à la Blockchain et celà, à partir du moment où un mineur a créé un nouveau bloc, jusqu'à ce que ce dernier soit confirmé par tous les mineurs afin d'être inséré dans la Blockchain.

Pour mesurer avec précision cette moyenne, nous avons ajouté des variables contenant l'heure de début et le temps écoulé, exactement avant d'appeler la fonction generate_new_block et

juste après qu'un bloc est confirmé et ajouté à la blockchain après l'appel de la fonction recive_new_bloc.

Consensus	50 Mineurs	100 Mineurs	150 Mineurs	200 Mineurs
PoS	0.96 s	2.21 s	3.5 s	4 s
PoA	0.8 s	1.71 s	3.4 s	3.5 s
PoET	0.3 s	1.61 s	2.26 s	3.5 s
PBFT	1.2 s	4.1 s	6.46 s	7.71 s
PoW diff=5	2.3 s	4.3 s	6.3 s	8.4 s
PoW diff=10	4.1 s	7.09 s	11.1 s	14.6 s
PoW diff=20	73.5 s	77 s	80.5 s	84s
PoW diff=25	117.63 s	170.79 s	171.63 s	172.42 s

TABLE 4.3 – Les temps d'exécution des différents consensus

Selon les résultats obtenu à partir des simulations, nous pouvons remarquer que la Blockchain basé sur PoW prend beaucoup de temps par rapport au PoA, PoS, PoET et PBFT ce qui est conforme aux études théorique, de plus PBFT dépend de la taille du réseau c'est à dire plus le réseau évolue, plus le PBFT devient lent à cause des échanges de message entre chaque nœud de réseau pour arriver à un accord, sachant que dans notre cas le délai pour qu'un message arrive à un nœud est 12 ms. Tandis que PoET est plus rapide que les autres algorithmes ce qui signifie que le temps de réponse à l'utilisateur est très court.

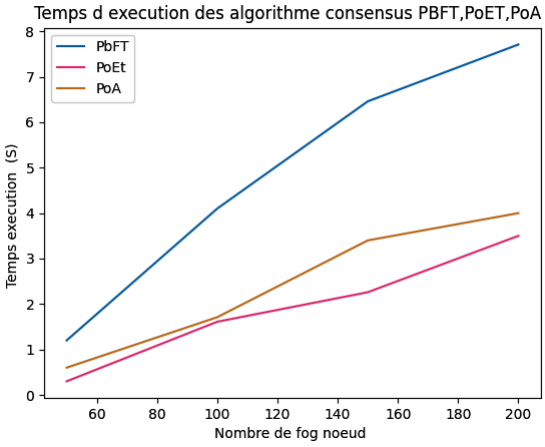

FIGURE 4.5 – A

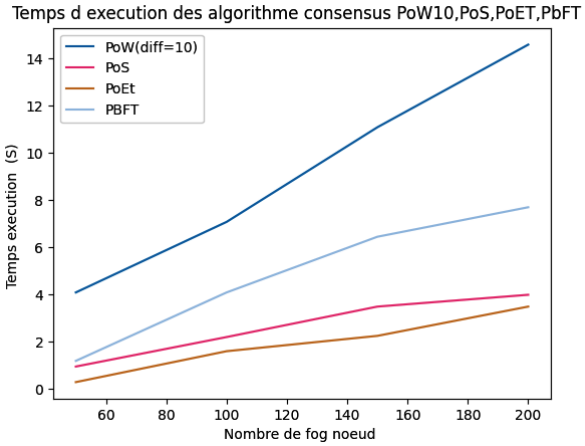

FIGURE 4.6 – B

FIGURE 4.7 – A : Le temps d'exécution des algorithmes PBFT, PoET, PoA.
B : Le temps d'exécution des algorithmes consensus PoW, PoS, PoET, PBFT

4.5 Conclusion

Dans ce chapitre, nous avons présenté une étude sur l'intégration de deux technologies importantes, notamment la Blockchain et Fog computing, nous avons motivé notre travail par un survol de quelques travaux de la littérature qui discutent les avancées récentes de cette intégration. Ensuite, nous avons implémenté dans le simulateur FobSim deux nouveaux consensus : PBFT et POET qui sont plus adaptés aux applications IoT en raison de leurs avantages en matière de sécurité, évolutivité et de temps de confirmation de bloc.

En dernier lieu, nous avons illustré le résultat par une étude de cas en comparant les différent protocoles PoW, PoS, PoA, PBFT, PoET en terme de temps de validation et ajout de bloc où nous avons conclu que le modèle de consensus PBFT ne fonctionne efficacement que lorsque le nombre de nœuds dans le réseau distribué est faible en raison de la surcharge de communication élevée qui s'augmente de façon exponentielle avec le nombre des nœuds du réseau tandis que PoET n'est pas affecté par la taille de réseau.

CONCLUSION GÉNÉRALE

Avec la croissance des réseaux IoT et l'explosion du nombre d'objets connectés, les aspects de sécurité, de transparence et d'intégrité de données, sont devenus des facteurs critiques. A titre d'exemple, les dispositifs IoT sont aujourd'hui vulnérables aux différents types de menaces et d'attaques en matière de sécurité, ceci est dû essentiellement au manque de conceptions matérielles et logicielles adéquates. Dans cette étude, l'accent est mis sur les défis potentiels observés en matière de sécurité et de confidentialité dans la littérature sur l'IoT.

Ce mémoire aborde la Blockchain en tant qu'une solution émergente de sécurité et de confidentialité pour le domaine de l'IoT et du Fog computing. Il donne également un aperçu de la façon dont la Blockchain peut atténuer la plupart de ces défis. Les caractéristiques inhérentes à la Blockchain telles que la décentralisation et la traçabilité, peuvent fournir un mécanisme qui améliore la sécurité, l'authentification et l'intégrité des données générées par les appareils IoT.

Cependant, malgré les caractéristiques et les avantages de la BC et le Fog, certains mécanismes de consensus ne sont pas bien adaptés aux applications de type Fog. Par exemple, la preuve de travail (PoW) ne peut pas être hébergée sur des appareils Fog car elle nécessite d'énormes ressources de calcul telles que la puissance pour exécuter et valider des transactions. De plus, la BC impose une latence importante, le processus de validation des transactions, ce qui n'en fait pas le meilleur choix pour les applications en temps réel. De plus, en raison de l'énorme taux de croissance du nombre d'appareils IoT, la BC peut être confrontée à un problème d'évolutivité.

Donc, notre travail repose sur une simulation d'intégration des deux technologies Fog computing et Blockchain. Nous avons implémenté deux algorithmes de consensus, a savoir PBFT et POET pour augmenter la sécurité, minimiser la consomation d'énergie et être plus adaptable aux contraintes des objets connéctés. Un résultat de simulations est présenté pour démontrer la fiabilité et la faisabilité des algorithmes de consensus implémentés en termes de temps de réponse et de scalabilité.

Comme perspective de ce travail, nous proposons d'explorer de nouvelles techniques pour améliorer et apporter plus d'efficacité au fonctionnement de la Blockchain dans le contexte de l'IoT et du Fog computing.

BIBLIOGRAPHIE

[1] BakhAoum Ana. La blockchain pour la sécurisation des e-livrets scolaires . Mémoire Master . Université ASSANE SECK DE ZIGUINCHOR . 2019.

[2] Tara Salman, Raj Jain, and Lav Gupta. Probabilistic blockchains : A blockchain paradigm for collaborative decision-making. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 457–465.

[3] Signature numérique (signature digitale). `https://www.lemagit.fr/definition/Signature-numerique-signature-electronique-ou-e-signature` Consulté le :06/01/2022.

[4] PIGNEL Marion and STOKKINK Denis. La technologie blockchain une opportunité pour l'économie sociale ? Economie sociale, 2019.

[5] Fourchettes blockchain. `https://hackernoon.com/blockchain-forks-b0dca84db0b0` Consulté le :04/02/2022.

[6] Exemple d'application le cloud computing. `https://slideplayer.fr/slide/3311097/` Consulté le :04/02/2022.

[7] Bouzarkouna Imen. *Implémentation industrielle du" Fog Manufacturing" : défis et applications à la logistique interne dans le contexte de l'industrie du futur*. PhD thesis, Normandie, 2021.

[8] Zabat Anis et al. *Combinaison de blockchain et biométrie pour la gestion des identités*. PhD thesis, University Mohamed Seddik Benyahia of Jijel. 85 pages, 2020.

[9] 30 statistiques sur l'internet des objets (iot) 2022 - sources fiables. `https://yoomweb.com/blogue/hi-tec/statistiques-internet-objets-iot.html` Consulté le :01/06/2022.

[10] Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[11] Amarpreet Singh. Distributed ledger vs blockchain technology : Do you know the difference ?. edison : Brandlitic. `https://medium.com/brandlitic/difference-between-distributed-ledger-and-blockchain-vs-dlt-7969f3837ded`, January 2021.

[12] Mancer Mohamed. Conception et réalisation d'un modèle de blockchain intelligent. Université Mohamed Khider – BISKRA. Mémoire master. page 61.

[13] L'histoire de la blockchain. `https://academy.binance.com/fr/articles/history-of-blockchain`, Consulté le :20/03/2022,.

[14] Hamidache Nesrine et al. *Déanonymisation de clients dans le réseau Bitcoin à l'aide de l'apprentissage automatique.* PhD thesis, Université Mouloud Mammeri, 2020.

[15] Dellys Sabrina Benbouabdellah Sofia . Applications de la technologie blockchain. Mémoire de master. Université Akli Mohand Oulhadj de Bouira. 2020.

[16] Ayadi Oussama Abderraouf. Chapitre iii : État de l'art de la blockchain. Mémoire de master. Université Constantine Abdelhmid Mehri. 2019.

[17] Parizo Christine. What are the 4 different types of blockchain technology ? `https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology`, year= 2021 Consulté le :12/02/2022,.

[18] Combien de types de blockchain existe-t-il. `https://academy.bit2me.com/fr/combien-de-types-de-blockchain-existe-t-il/`, year = 2015 Consulté le :05/03/2022,.

[19] Sid Aissa Ikram .Keddar Souria . Proposition d'un système à base de blockchain pour la gestion des opérations sur les véhicules au niveau national. Mémoire master Université Abou Bekr Belkaid. juin 2018.

[20] Présentation de l'algorithme sha-256. `https://www.n-able.com/blog/sha-256-encryption#:~:text=SHA%2D256%20is%20a%20patented,as%20long%20as%20when%20unencrypted` Consulté le :03/15/2022.

[21] L'arbre de merkle : la colonne vertébrale de la blockchain. `https://medium.com/@BlockchainsExp/larbre-de-merkle-la-colonne-vert%C3%A9brale-de-la-blockchain-4939a37711ef`Consulté le :05/20/2022.

[22] Desdous Mohammed, Bouketta Chanez, Meriama MAHAMDIOUA, et al. *Analyse de quelques algorithmes de consensus dans la blockchain.* PhD thesis, University of Jijel, 2020.

[23] Zouaoui Rania. Blockchain pour gestion des données médicales. Mémoire master. Université Mohamed Khider – BISKRA. 2021.

[24] 8 meilleures plateformes de blockchain pour créer des applications financières modernes. `https://geekflare.com/fr/finance/blockchain-platforms-for-finance-applications/` Consulté le :05/04/2022.

[25] Rahmani Rokia. Les dossiers médicaux sur blockchain . Mémoire master. Université Mohamed Khider – BISKRA. page 56, 2021.

[26] Atef Ballouche. La sécurité de l'internet des objets (i o t) a l'aide d'un cids et de la blockchain. Mémoire de mastére. 2021.

[27] Probst Thibaut. *Évaluation et analyse des mécanismes de sécurité des réseaux dans les infrastructures virtuelles de cloud computing.* PhD thesis, INP Toulouse, 2015.

[28] Akbi khalil Zehri, mohammed. Etude et mise en place d'une solution cloudcomputing privé au sein de l'université deouargla. Mémoire MASTER ACADEMIQUE. page 58, 2013.

[29] Benkoudir Sahraoui Soufyane Mansouri Yasmine. Etude de sécurité d'une extension cloud. Mémoire de fin de cycle. Université AMira de Béjaia. page 29, juin 2017.

[30] REGUIEG Hicham. Cloud computing : services informatiques dynamiques basés sur le web-concepts et notions de base. University of Science and Technology of Oran. 2020.

[31] Naas Mohammed Islam. *Placement des données de l'internet des objets dans une infrastructure de fog*. PhD thesis, Université de Bretagne occidentale-Brest, 2019.

[32] Mededjel Mansour Belalem Ghalem Neki Abdelkader. *Internet physique au service de la logistique : interconnectée, intelligente et durable : Application à un secteur économique Algérien. Université d'Oran1 Ahmed Ben Bella*. PhD thesis, 2020.

[33] Hany F. Atlam Robert J. Walters Gary B. Wills. Fog computing and the internet of things. Big Data and Cognitive Computing. page 18, 8 April 2018.

[34] What is fog computing ? `https://www.techtarget.com/iotagenda/definition/fog-computing-fogging` Consulté le :15/05/2022.

[35] Architecture du fog computing : tout ce que vous devez savoir. `https://wisdomplexus.com/blogs/fog-computing-architecture/` Consulté le : 15/05/2022.

[36] Fog computing : guide complet sur ce concept. `https://www.lebigdata.fr/fog-computing-guide-complet`Consulté le : 17/05/2022.

[37] Bastien Confais. *Conception d'un système de partage de données adapté à un environnement de Fog Computing*. PhD thesis, Université de Nantes, 2018.

[38] M Mohammad A Reza B mozaffari tazekand. On the convergence of blockchain and internet of things (iot) technologies. 2019.

[39] Gang Liu Jinsong Wu Ting Wang. Blockchain-enabled fog resource access and granting. 2021.

[40] L Wallin L Walker, N Jones. How to address the top five iot challenges with enterprise architecture. *Gartner. Inc, Online*, 2016.

[41] NN Pokrovskaia. Mécanismes de régulation fiscale, financière et sociale dans l'économie de la connaissance. algorithmes blockchain et calcul du brouillard pour une régulation efficace. *dans Proc. 20e IEEE Int. Conf. Calcul doux. Mes. (SCM), mai 2017*, 88 :709 —- 712.

[42] R. Almadhoun M. Kadadha M. Alhemeiri M. Alshehhi K. Salah. «un schéma d'authentification d'utilisateur d'appareils iot utilisant des nœuds de brouillard activés par la blockchain». *dans Proc. IEEE/ ACS 15e Int. Conf. Calcul. Syst. Pomme.*

[43] F. Zhang Y. Wan T. Zhang et H. Ning MA Bouras, Q. Lu. Distributed ledger technology for ehealth identity privacy : State of the art and future perspective. *Systèmes informatiques de la génération future*, 20 :483.

[44] AA Alli M. Fahadi. Chapitre quatre blockchain et calcul de brouillard : Concept de brouillardblockchain, opportunités et défis. *Blockchain in Data Analytics. Newcastle, Royaume-Uni : Cambridge Scholars Publishing*, 88 :75.

[45] C.Dinh Nguyen N.Pubudu Pathirana M.Ding Aruna. Integration of blockchain and cloud of things : Architecture, applications and challenges.

[46] Dualfog-iot : couche de brouillard supplémentaire pour résoudre le problème d'intégration de la blockchain dans l'internet des objets. *Accès IEEE*, 7 :169073–169093.

[47] Baniata Hamza and Kertesz Attila. A survey on blockchain-fog integration approaches. *IEEE Access*, 8 :102657–102668, 2020.

[48] Adnan Abbas. What is gossip protocol ? `https://www.educative.io/edpresso/what-is-gossip-protocol` Consulté le :06/01/2022.

[49] Tolérance de panne byzantine pratique (pbft). `https://fr.acervolima.com/tolerance-de-panne-byzantine-pratique-pbft/`Consulté le :20/05/2022.

polyglossia french arabic

Résumé

L'adoption de l'Internet des objets (IoT) connaît une croissance importante et réussie dans de nombreux domaines. Néanmoins, la demande croissante d'appareils connectés entraîne le besoin d'architectures IoT évolutives qui sont capables de rapprocher le traitement, la communication et le stockage des appareils et des utilisateurs finaux tout en mutualisant les ressources locales. Ainsi, le Fog Computing (FC) peut être utilisé comme plate-forme intermédiaire entre les appareils IoT et le cloud traditionnel pour répondre aux exigences des applications sensibles à la latence en réduisant le temps de traitement et la quantité de données à transférer vers le cloud. La Blockchain (BC) fait partie des technologies révolutionnaires qui pourraient influencer de nombreux domaines. Un tel déploiement de cette technologie offrirait des moyens plus efficaces d'effectuer des tâches de manière décentralisée (peer-to-peer) en fournissant une gestion des données fiable, immuable et sécurisée. Ces critères peuvent être d'une grande importance pour l'IoT et le Fog computing. Par conséquent, l'intégration de ces deux technologies (BC-FC) pourrait aider à résoudre de nombreux problèmes auxquels sont confrontés les environnements IoT, tels que le stockage des données, la sécurité, la gestion des identités et la réduction des coûts. A travers ce projet de fin d'étude, nous avons simulé cette intégration en implémentant deux algorithmes de consensus, à savoir PBFT et PoET pour augmenter la sécurité, minimiser la consommation d'énergie et être plus adaptable aux contraintes des objets connectés. L'étude menée a démontré la fiabilité et la faisabilité des algorithmes de consensus mis en œuvre en termes de temps de réponse.

Mots clés : Blockchain, Fog computing, Internet des objets, Consensus.

Abstract

The adoption of the Internet of Things (IoT) is experiencing significant and successful growth in many areas. Nevertheless, the increasing demand for connected devices is driving the need for scalable IoT architectures that can bring processing, communication and storage closer to devices and end users while pooling local resources. Thus, Fog Computing (FC) can be used as an intermediate platform between IoT devices and the traditional cloud to meet the requirements of latency-sensitive applications by reducing the processing time and amount of data that needs to be transferred to the cloud. Blockchain (BC) is one of the revolutionary technologies that could influence many fields. Such a deployment of this technology would offer more efficient ways to perform tasks in a decentralized way (peer-to-peer) by providing a reliable, immutable, and secure data management. These criteria can be of great importance to IoT and Fog computing. Therefore, integrating these two technologies (BC-FC) could help to solve many problems facing IoT environments, such as data storage, security, identity management and cost reduction. Through this end-of-study project we simulated this integration by implementing two consensus algorithms, namely PBFT and PoET to increase security, minimize energy consumption and be more adaptable to the constraints of connected objects. The study conducted demonstrated the reliability and feasibility of the implemented consensus algorithms in terms of response time.

Keywords : Blockchain, Fog computing, Internet of Things, Consensus.

ملخص : يتزايد اعتماد إنترنت الأشياء بشكل كبير وينجح في العديد من المجالات المختلفة. ومع ذلك ، فإن الطلب المتزايد باستمرار على المزيد من الأجهزة المتصلة يدفع الحاجة إلى بنى إنترنت الأشياء القابلة للتطوير والتي يمكن أن تجعل المعالجة والتواصل والتخزين أقرب إلى الأجهزة والمستخدمين النهائيين ، مع تجميع الموارد المحلية. وبالتالي ، من خلال تقليل زمن الوصول وكمية البيانات التي سيتم نقلها إلى السحابة ، توفر حوسبة الضباب فعليًا منصة وسيطة بين الأجهزة السحابية التقليدية وأجهزة إنترنت الأشياء التي يمكنها تلبية متطلبات التطبيقات في الوقت الفعلي والحساسة للوقت. وقت الاجابة. اليوم ، تعد البلوك تشين واحدة من التقنيات الثورية التي يمكن أن تؤثر على العديد من المجالات. وفر هذا النشر لهذه التقنية طرقًا أسهل لأداء المهام بطريقة لامركزية (نظير إلى نظير) من خلال توفير إدارة بيانات موثوقة وغير قابلة للتغيير وآمنة. يمكن أن تكون هذه المعايير ذات أهمية كبيرة لإنترنت الأشياء وحوسبة الضباب. لذلك ، يمكن استخدام تكامل هاتين التقنيتين لحل أكثر من مشكلة تواجهها بيئات إنترنت الأشياء ، مثل تخزين البيانات ، والأمن ، وإدارة الهوية ، وخفض التكلفة وبروتوكول الامتثال. من خلال مشروع نهاية الدراسة هذا ، نقوم بمحاكاة هذا التكامل من خلال تنفيذ خوارزميتي الإجماع ، PBFT و POET لزيادة الأمان وتقليل استهلاك الطاقة وتكون أكثر قابلية للتكيف مع قيود الكائنات المتصلة ، ثم يتعين على الدراسة إثبات الموثوقية و جدوى خوارزميات الإجماع المنفذة من حيث زمن الاستجابة.

الكلمات الدالة :

بلوك تشين ، حوسبة الضباب ، إنترنت الأشياء ، الإجماع.