République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Mémoire de fin d'études
Pour l'obtention du diplôme de Master en Informatique

Présenté à l'Université de Tébessa
Faculté des Sciences Exactes et Sciences de la Nature et de la Vie

Département de : **Mathématiques etInformatique**
Spécialité : **Informatique**
Option : **Réseaux et Sécurité Informatique**

Par :
TAIB Sihame

SYSTÈMES DE GESTION DE CONFIANCE BASÉS BLOCKCHAIN DANS L'INTERNET DES OBJETS (IOT)

Devant le Jury :

Dr.Metrouh Abdelmalek	MCA	Univérsité Larbi Tébessi	Président
Dr.Souahi Mouhammed Salah	MCB	Univérsité Larbi Tébessi	Examinateur
Dr. Merzoug Soltane	MCA	Univérsité Larbi Tébessi	Encadreur

Année universitaire : 2022/2023

Remerciements

C'est avec une immense gratitude et une profonde reconnaissance que je souhaite adresser ces quelques lignes de remerciement à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation et à l'aboutissement de ce travail.

Tout d'abord, je tiens à exprimer ma reconnaissance envers Allah tout puissant, qui m'a accordé la possibilité de mener à bien ce mémoire et qui m'a guidé sur le chemin de la connaissance.

Ensuite, mes remerciements les plus chaleureux vont à **Dr. Merzoug Soltane**, qui m'a offert son encadrement précieux. Ses conseils, sa patience et la confiance qu'il m'a témoignée ont été des éléments déterminants dans la réalisation de mon travail.

Je tiens également à exprimer ma gratitude envers les membres du jury.

Enfin, je tiens à exprimer ma gratitude envers toutes les personnes qui ont apporté leur soutien et leur aide tout au long de ce projet. Vos encouragements, votre compréhension et votre appui ont été inestimables.

Merci à toutes et à tous pour votre contribution précieuse. Votre soutien a joué un rôle essentiel dans la réussite de ce mémoire, et je vous en suis profondément reconnaissant(e).

Dédicaces

À ma famille et à mes amis pour leur amour

•

TAIB Sihame.

Résumé

L'essor de l'Internet des objets a transformé les industries traditionnelles en entreprises intelligentes qui s'appuient sur les données pour prendre des décisions. Les connexions entre divers appareils et objets qui effectuent des tâches complexes sont effectuées via l'IoT. Les attributs inhérents à l'Internet des objets (IoT) peuvent entraîner divers problèmes. Il s'agit notamment des atteintes à la sécurité, des problèmes d'interopérabilité et des problèmes de confidentialité. Alors que l'IoT continue d'évoluer, il est important que les organisations aient la confiance nécessaire dans cette source massive d'informations. En raison de ses divers avantages, tels que son immuabilité, sa sécurité et sa décentralisation, la technologie blockchain devient un outil prometteur pour relever les défis de l'IoT. Grâce à l'intégration de la technologie blockchain et de l'IoT, diverses nouvelles opportunités peuvent être créées pour améliorer la transparence, la fiabilité et la réputation des organisations. Ce thème vise à utiliser la technologie blockchain comme un outil de confiance pour améliorer la sécurité et la fiabilité de l'IoT. Pour ce faire, nous aborderons d'abord la question de la fiabilité des données, puis nous élaborerons un cadre qui permettra aux organisations de mettre en œuvre un système sécurisé.

Mots-clés : Blockchain, Internet des objets, contrat intelligente

Abstract

The rise of the Internet of Things has transformed traditional industries into smart businesses that rely on data to make decisions. The connections between various devices and objects that perform complex tasks are made through the IoT. The inherent attributes of the Internet of Things (IoT) can lead to various issues. These include security breaches, interoperability problems, and privacy issues. As the IoT continues to evolve, it is important that organizations have the necessary trust in this massive source of information. Due to its various advantages, such as its immutability, security, and decentralization, blockchain technology is becoming a promising tool for addressing the challenges of the IoT. Through the integration of blockchain technology and the IoT, various new opportunities can be created to improve the transparency, reliability, and reputation of organizations. This theme aims to use blockchain technology as a trusted tool for improving the security and reliability of the IoT. In order to achieve this, we will first address the issue of data reliability and then develop a framework that will allow organizations to implement a secure system.

Keywords: Blockchain, Internet of Things, smart contract.

ملخص

أدى ظهور إنترنت الأشياء إلى تحويل الصناعات التقليدية إلى مؤسسات ذكية تعتمد على البيانات لاتخاذ القرارات. يتم إجراء الاتصالات بين مختلف الأجهزة والكائنات التي تؤدي مهامًا معقدة من خلال إنترنت الأشياء. يمكن أن تؤدي السمات المتأصلة في إنترنت الأشياء إلى العديد من المشكلات. وتشمل هذه الخروقات الأمنية ومشكلات التشغيل التفاعلي ومخاوف الخصوصية. مع استمرار تطور إنترنت الأشياء ، من المهم أن تتمتع المنظمات بالثقة اللازمة في هذا المصدر الهائل للمعلومات. نظرًا لمزاياها المختلفة ، مثل الثبات والأمن واللامركزية ، أصبحت تقنية البلوكشين أداة واعدة لمواجهة تحديات إنترنت الأشياء. من خلال دمج تقنية البلوكشين و إنترنت الأشياء ، يمكن إنشاء العديد من الفرص الجديدة لتحسين الشفافية والموثوقية وسمعة المنظمات. يهدف هذا الموضوع إلى استخدام تقنية البلوكشين كأداة موثوقة لتحسين أمان وموثوقية إنترنت الأشياء. للقيام بذلك ، سنقوم أولاً بمعالجة مسألة موثوقية البيانات ثم تطوير إطار عمل يسمح للمؤسسات بتنفيذ نظام آمن.

كلمات مفتاحية: البلوكشين , انترنيت الاشياء , العقد الذكي .

Table des matières

Liste des figures

Tableau

Introduction Générale

1-Introduction générale

L'essor de l'Internet des objets est devenu un facteur majeur dans notre vie quotidienne et dans le fonctionnement des entreprises. Selon des études, le nombre d'objets liés augmentera considérablement au cours des deux prochaines années. L'IoT est un ensemble d'appareils qui peuvent communiquer entre eux avec Internet. Grâce aux interactions entre ces objets, les données peuvent être collectées et transférées sans intervention humaine. Ces objets sont généralement limités en puissance et peuvent être utilisés dans des situations où la sécurité des personnes est en danger. Ils peuvent également être utilisés dans divers domaines tels que les transports, la sécurité et les villes intelligentes. Malheureusement, la sécurité de l'infrastructure IoT peut être considérablement affectée par le nombre de nœuds et de modules connectés au réseau. En raison du nombre croissant d'objets liés et de la complexité du réseau, il est important que la sécurité de l'IoT soit continuellement améliorée. L'un des moyens les plus efficaces de résoudre ce problème consiste à mettre en œuvre une technologie blockchain. Ce type de sécurité peut être utilisé pour empêcher l'accès non autorisé aux données collectées et stockées par l'IoT. La complexité de l'intégration et de la protection des données par l'Internet des objets est immense. Les organisations qui utilisent de tels systèmes généreront de grandes quantités de flux d'informations, y compris des ressources humaines et des processus de production. Les renseignements de nature délicate que les organisations recueillent et utilisent sur Internet doivent demeurer confidentiels et ne doivent être accessibles qu'au personnel autorisé.

Pour ce faire, ils doivent mettre en œuvre des politiques et des procédures de sécurité appropriées conçues pour protéger les objets connectés au réseau. L'un des moyens les plus efficaces de protéger les informations qu'une organisation recueille et utilise sur Internet consiste à utiliser une solution collaborative de détection des intrusions. Ce système utilise la technologie blockchain pour permettre à ses systèmes de détection de partager des informations sur les attaques. En raison de la nature de la technologie impliquée et de la facilité avec laquelle elle peut être exploitée par des individus malveillants, la sécurité de l'IoT est très importante. Chaque nœud doit être protégé contre diverses menaces, telles que les virus et les chevaux de Troie. Malgré les progrès technologiques qui ont eu lieu dans la protection des données, il n'est toujours pas suffisant d'empêcher l'accès non autorisé à l'Internet des objets. Pour garantir le maintien de la sécurité, il est important que les utilisateurs sachent qui accède aux ressources et quand. Avec l'aide de la technologie blockchain ,il peut désormais mettre en œuvre un système capable de détecter et de prévenir les failles de sécurité en temps réel.

On formule une problématique de la manière suivante :

"Comment les systèmes de gestion de confiance basés sur la technologie blockchain peuvent-ils améliorer la sécurité, la confidentialité et la traçabilité des transactions dans les paniers intelligents ?"

Dans Le premier chapitre " **IoT et blockchain**", nous abordons les bases de la blockchain et l'internet des objets.

Dans le deuxième chapitre " **Les techniques blockchain dans IoT**", nous parlerons des problèmes de sécurité qui affectent l'IoT et de la façon de les résoudre à l'aide de la blockchain. Afin de gestion d'exemples d'applications de différents domaines en Internet des Objets, nous avons intégrés la blockchain entratre en route des applications.

Dans le troisième chapitre **"Présentation de l'architecture globale du système"**, on concentre sur un système de confiance qui utilise la technologie blockchain dans l'Internet des objets . Et les détails d'architecture de ce système Il vise à fournir un cadre permettant aux supermarchés de maintenir la confiance

de leurs clients on utilise un panier intelligent.

Dans le quatrième chapitre **"Implémentation"**, on parle du système de paiement en utilisant des contrats blockchain. Nous explorerons les outils qui ont été utilisés pour développer ce système, et nous présenterons ensuite ses différents composants. Ainsi que décrivons son fonctionnement.

Chapitre 01

IoT et blockchain

Introduction

L'émergence et l'évolution rapides de l'Internet des objets ont conduit au développement de nouveaux cas d'utilisation impliquant l'utilisation de la technologie Blockchain. Avant de parler du potentiel de la Blockchain et de l'IoT, il est important de reconnaître d'abord les différentes définitions de ces concepts. Ces deux domaines sont très spécifiques et précis.

1-Internet des objets

1.1-Définition

Le terme Internet des objets fait référence à un groupe d'appareils qui peuvent communiquer entre eux à l'aide d'un réseau sans fil. Ces objets peuvent collecter et transférer des données avec une puissance limitée, et ils peuvent remplir diverses fonctions sans nécessiter d'intervention humaine. [1].

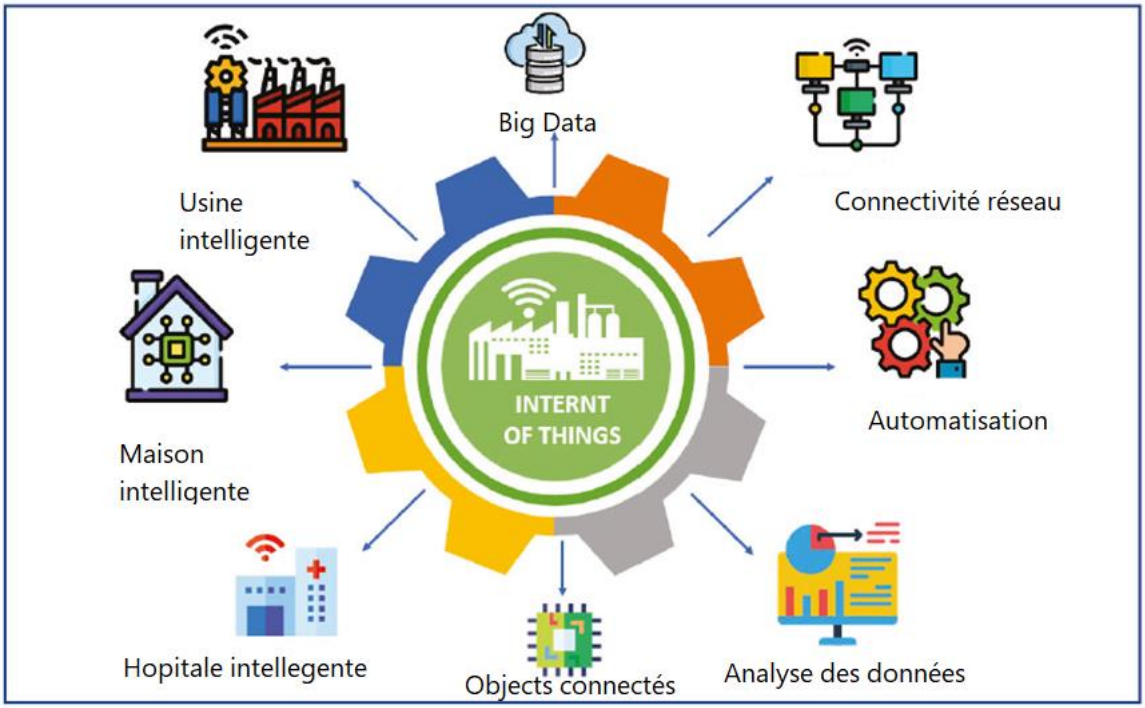

Figure1.1-Écosystème de l'Internet des objets (IoT). [10]

1.2- Vue d'ensemble d'IDO

A un réseau de communication sans fil ou filaire. Il s'agit notamment d'éléments qui surveillent et contrôlent leur environnement, tels que des capteurs et des caméras. Certains des domaines couverts par les services offerts par l'Ido comprennent la chaîne d'approvisionnement, la fabrication et l'énergie. [La Figure 1.1] montre une représentation d'un système typique composé des sous-systèmes.

1.2.1-La couche d'accès

Est composée d'appareils qui collectent et détectent les données d'un environnement physique. Il s'agit notamment des capteurs et d'autres objets physiques. Il s'agit notamment des points d'accès, des appareils sans fil et des étiquettes RFID. En outre, d'autres acteurs tels que les collecteurs et les actionneurs peuvent également bénéficier des données collectées par ces appareils. Comme ces appareils interagissent avec l'environnement, leur logiciel embarqué peut exécuter diverses fonctions. [2]

1.2.2-La couche communication d'un centre

Est composée des différents protocoles qui permettent aux appareils et aux réseaux de communiquer. Les données collectées sont ensuite transmises aux stations de base et aux passerelles, qui sont ensuite utilisées pour établir un réseau industriel. Les différents protocoles utilisés par la couche de communication incluent Bluetooth, IEEE 802.11 et infrarouge. [2]

1.2.3-La couche applications

Est une interface entre les différents appareils et les réseaux auxquels ils se connectent. Il gère le formatage et la présentation des données et joue un rôle dans l'échange d'informations entre différentes applications et réseaux. Cette couche est couramment utilisée dans l'IoT industriel, les réseaux intelligents et l'Internet des véhicules. [2]

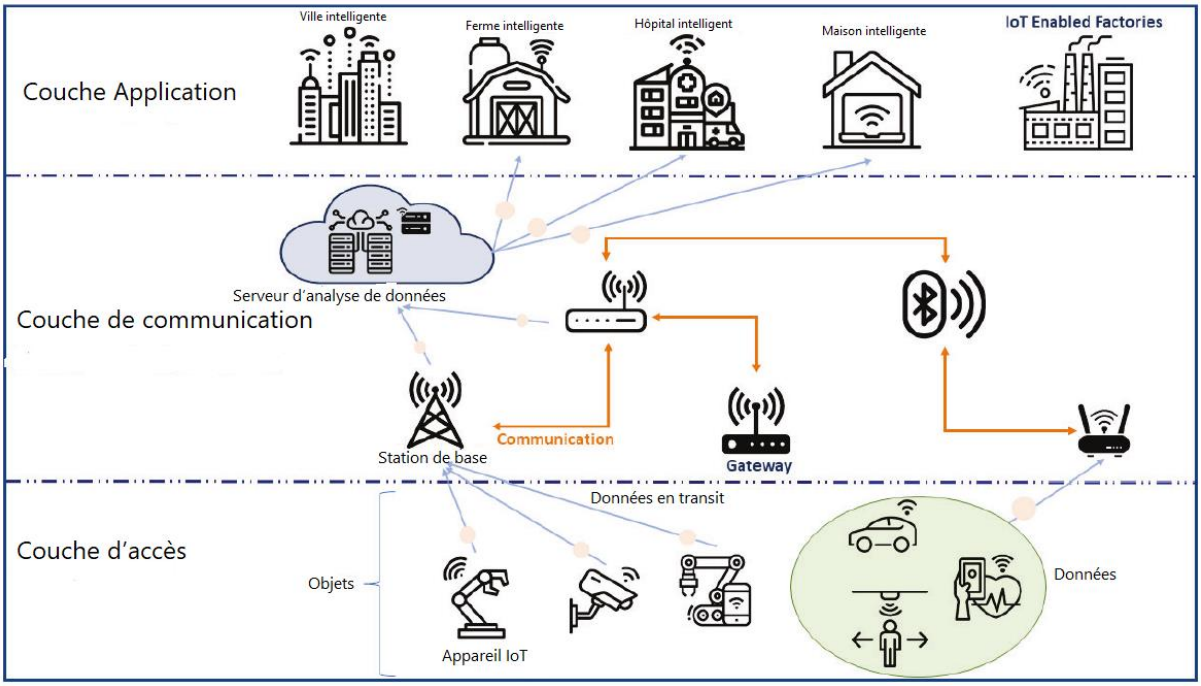

Figure 1.2-L'IoT se compose d'une couche d'accès, d'une couche de communication et d'une couche applications. [2]

1.3- Défis d'IDO

L'Internet des objets (IoT) est un réseau d'appareils et de logiciels qui peuvent collecter et interpréter des données provenant de divers objets dans un environnement physique. Ses diverses caractéristiques ont soulevé un certain nombre de questions. [2]

1.3.1- L'hétérogénéité des dispositifs

Un objet peut être déployé avec une variété de capteurs et de logiciels en fonction de son utilisation prévue. Ceux-ci collecteront des données et les traiteront via son logiciel intégré. Les différents logiciels et capteurs qui peuvent être utilisés par un objet sont conçus pour répondre aux besoins spécifiques de leur utilisation prévue. Une fois déployé, l'objet peut collecter des données à partir de ces capteurs. Le traitement peut être simple ou complexe selon l'application. Par exemple, il peut être utilisé pour vérifier si la température est dans l'intervalle qui a été défini précédemment. Les exemples simples montrent les différents types de données qui peuvent être collectées et stockées dans un centre de données. Cependant, ils révèlent également la complexité des besoins que ces données génèrent. Outre le type de données collectées, il prend également en compte les différentes exigences de sécurité impliquées dans le fonctionnement de l'Internet des objets (IoT). C'est pourquoi il est important de gérer l'hétérogénéité des appareils. [3]

1.3.2- Les ressources limitées

L'Internet des objets (IoT) a été développé grâce à l'utilisation d'appareils intelligents, qui ont limité les ressources afin de garder les choses compactes. Grâce aux progrès de l'intégration et de la miniaturisation, des objets plus puissants sont maintenant disponibles. Malgré les progrès réalisés dans l'IoT, de nombreux objets connectés manquent encore des ressources nécessaires pour fonctionner correctement. Certaines des contraintes couramment rencontrées par ces appareils incluent la puissance de traitement, la mémoire et l'autonomie énergétique. Lorsqu'il s'agit de faire fonctionner l'énergie, les objets dépendent de batteries et de panneaux solaires.

Dans cette section, nous parlerons des différents types de technologies de communication utilisés dans l'IoT. L'un des facteurs les plus importants à prendre en compte lorsqu'il s'agit de mettre en œuvre la sécurité dans le réseau est la consommation d'énergie des objets connectés. En effet, selon le type de données transmises, la quantité d'énergie consommée par les objets peut varier. La prise en compte de ces contraintes garantira le succès des propositions. Une solution qui répond à tous les besoins de connectivité de l'IoT sera fournie. [3]

1.3.3-Interopérabilité médiocre

Le manque d'interopérabilité entre les différents systèmes et appareils est l'un des principaux facteurs qui empêchent le développement de systèmes IoT efficaces. En effet, la décentralisation et l'hétérogénéité variables de l'environnement rendent difficile la mise en œuvre d'une interopérabilité efficace. [2]

1.3.4-La mobilité

En raison de l'essor de l'Internet des objets (IoT), nous constatons un nombre croissant d'appareils intelligents qui peuvent se déplacer. Certains d'entre eux incluent des drones, des aspirateurs intelligents et des voitures connectées. Afin de permettre aux utilisateurs de mieux comprendre les données collectées par ces appareils, ils sont autorisés à accéder aux différents services offerts par le réseau. L'introduction de réseaux dynamiques dans le réseau est causée par le mouvement de ces dispositifs. Ceux-ci peuvent être créés en connectant divers appareils à un seul réseau pendant une période de temps spécifique. En raison de la complexité des réseaux dynamiques, il peut être très difficile de les gérer dans les grandes organisations. En effet, déterminer si un appareil est autorisé à rejoindre le réseau revient à demander un niveau de confiance. La gestion de la mobilité peut être effectuée de différentes manières dans des réseaux dynamiques. Un exemple de ceci est l'intégration d'un appareil intelligent dans un objet physique. Ce gadget doit être capable de détecter son environnement afin de déterminer son emplacement probable pour partir. Cela peut être fait en analysant les messages envoyés par les participants aux réseaux. Cela peut également être fait en surveillant les émissions des balises. [4] L'un des moyens de gérer la mobilité consiste à intégrer des messages de contrôle et de signalisation dans les protocoles du réseau pour la gestion des nœuds de localisation. [5] A la mobilité augmentation utilisée, il avait déclaré que la surface d'attaque va par conséquent de pair. Une solution de mobilité devrait utilisée en compte de la mobilité, en conseil de gestions de l'Internet des objets . [6]

1.3.5-La sécurité

Les intelligents avaient déployé en environnements, en quelques ils ne sont pas surveillés. Par exemple, afin de découvert de données, en particulier les secteurs, tels que la pression, l'humidité et la luminosité. Une petite donnée l'environnement, pour remonter le terrain, sont déployés. Une station de base, ils avaient déraillement pour faire la surveillance physique sur leur exploitant. Un adversaire avait lui pour accéder la modification de données physiques en confidentialité. Une petite donnée s'environnement afin de découvert de données en particulier les secteurs, tels que la pression, l'humidité et la luminosité. [6]

1.4. Les attaques dans l'Internet des objets

Ce sont les attaques les plus critiques qui peuvent affecter un réseau. Ils sont généralement effectués lors du transfert de données : [7]

1.4.1-Déni de service (DoS) : Ce type d'attaque est généralement effectué par un intrus qui tente de perturber la transmission des données. Au lieu d'écouter les conversations, l'intrus envoie des données valides ou tente de bloquer le canal.

1.4.2-Hello flood : Le nombre excessif de messages envoyés et reçus dans un canal de transmission peut créer une quantité massive de trafic. Il s'agit d'un type d'attaque par déni de service.

1.4.3-Spoofing : L'usurpation d'identité ou le vol d'identité implique le transfert ou la modification du trafic afin de voler des données ou de propager des logiciels malveillants. Un attaquant peut également prendre le contrôle d'un signal radio et exécuter un code malveillant en insérant un module externe.

1.4.4-Selective forwarding : L'usurpation d'identité ou le vol d'identité implique le transfert ou la modification du trafic afin de voler des données ou de propager des logiciels malveillants. Un attaquant peut également prendre le contrôle d'un signal radio et exécuter un code malveillant en insérant un module externe.

1.4.5-Sybil : Un intrus peut créer plusieurs identités pour un seul nœud au sein d'un réseau en comparant ses configurations avec celles d'autres nœuds. Cette méthode est réalisée en introduisant un logiciel ou un nœud qui est transmis dans le réseau.

1.4.6-Wormhole (trou noir) : L'attaque modifie la position des paquets de

données dans le réseau, ce qui peut retarder la transmission.

1.4.7-Acknowledgement flooding : Lors de l'utilisation d'algorithmes de routage, la synchronisation des réceptions est requise dans les réseaux de capteurs. Un nœud malveillant peut tirer parti de cette fonctionnalité pour envoyer de fausses informations et des accusés de réception à d'autres nœuds.

1.4.8-Man-in-the-middle : Dans ce type d'opération, un intrus est capable d'accéder aux canaux de communication d'un réseau et de modifier ou d'intercepter des données.

La troisième partie du réseau est utilisée pour transmettre des informations. Lorsqu'un intercepteur est détecté, ni les parties concernées ni les parties autorisées ne sont informées de sa présence. Pour éviter cela, des transmissions actives-passives sont effectuées pour s'assurer que les modules de réception et d'émission sont en mode continu.

1.4.9-Attaque par relais : Un attaquant peut voler la communication d'un périphérique récepteur local en la redirigeant vers un périphérique NFC distant ou un appareil sans contact. En raison de l'essor des cartes à puce sans contact, ce type d'attaque est de plus en plus répandu.

1.4.10-Protocol Stack Fuzzing : Un autre type d'attaque qui peut être utilisé contre la technologie NFC est appelé collecte dans la pile de protocoles. Il s'agit de capturer et d'analyser le logiciel de transmission. Un attaquant peut ensuite l'utiliser pour collecter diverses données, telles que des photos et des contacts, à l'insu de l'utilisateur. Un attaquant peut l'utiliser pour collecter des données lors d'une opération ordinaire, par exemple lors du paiement d'un titre de transport. Cela peut ensuite être utilisé pour effectuer des transactions illégales ou envoyer et recevoir des appels.

1.4.11-Rogue Access Points : Il s'agit d'appareils connectés illégalement à un réseau. Ils peuvent être utilisés pour relayer des données.

2. Blockchain

Les caractéristiques de la technologie blockchain incluent le fait d'être immuable, décentralisée et non défaillante. Il peut fonctionner dans un environnement distribué et stocker des données de manière peer-to-peer, ce qui le rend incroyablement résilient. Cette redondance garantit que les informations restent dans la chaîne et empêche leur destruction. La technologie immuable garantit que les modifications apportées au bloc seront incroyablement difficiles à apporter une fois qu'il aura été ajouté à la chaîne. [8]

2.1. Aperçu de la chaîne de blocs

La blockchain permet aux membres de vérifier l'authenticité des transactions en leur permettant de le faire de manière anonyme [9]. Lorsqu'un nouveau bloc est ajouté au réseau, tous les membres de la chaîne doivent parvenir à un accord pour le valider. Ce processus est connu sous le nom de consensus. Les nouveaux blocs du réseau pointent vers leur bloc précédent via une référence inverse, qui est la valeur de hachage de ce bloc. Dans [la Figure 1.3] nous montrons un exemple de blockchain composé de plusieurs blocs connectés. Chacun des blocs de la chaîne a un parent, connu sous le nom de bloc précédent. Le tout premier bloc est appelé le bloc de genèse. Chaque bloc est composé de divers éléments, tels que le numéro de version du logiciel, le hachage des parents du bloc et le hachage racine de l'arbre Merkel. Les différents éléments d'une blockchain sont organisés en blocs. Il s'agit notamment du numéro de version du logiciel, des horodatages, du nonce et des bits. Le hash des parents du bloc est une représentation du hash racine de l'arbre Merkel. Il contient également les horodatages, nonce et les bits, qui sont les éléments de la difficulté du consensus. Comprendre les différents aspects de la technologie blockchain est très important afin de bien comprendre son potentiel d'intégration avec l'Internet des objets (IoT). Dans ce chapitre, nous parlerons de la taxonomie, des fonctionnalités et du flux de travail de la blockchain.

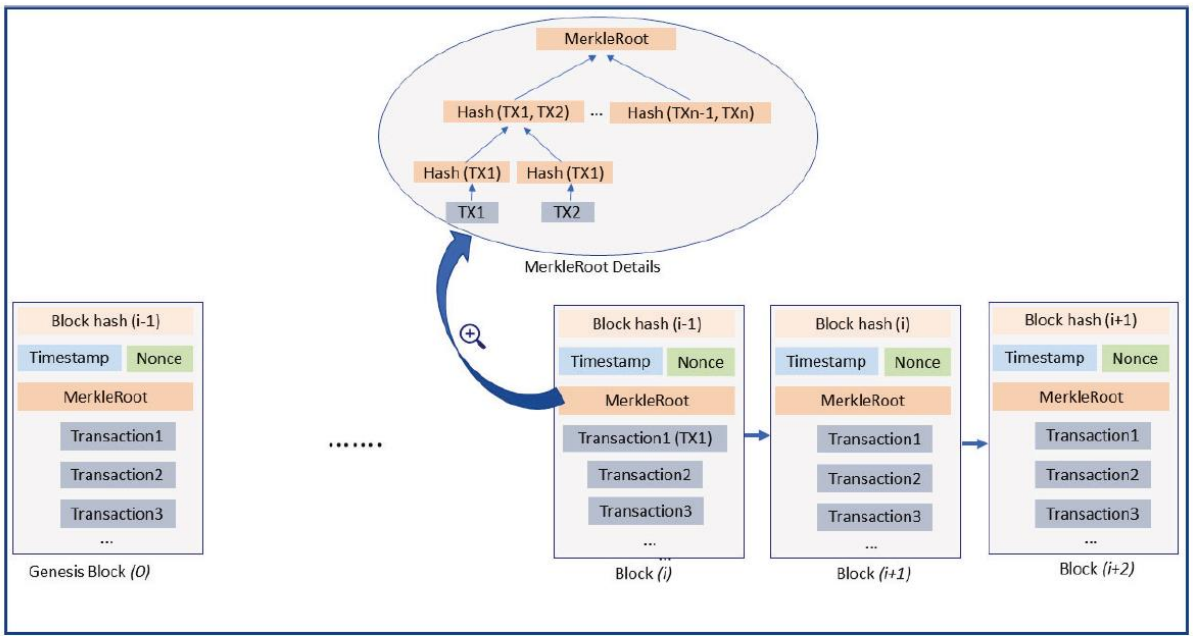

Figure1.3-Les différents blocs connectés de blockchain. [10]

2.2. Caractéristiques de la chaîne de blocs

Les différentes caractéristiques de la technologie blockchain qui peuvent être utilisées pour transformer diverses industries, telles que l'Internet des objets (IoT), sont quelques-unes de ses caractéristiques les plus convaincantes.

2.2.1-Decentralisation

Lorsqu'il s'agit de mettre en œuvre un système centralisé, les données sont généralement stockées et consultées par un tiers. Cette approche peut entraîner des coûts plus élevés en raison de la maintenance et de la gestion des ressources, ainsi que des vulnérabilités de sécurité. D'autre part, les plates-formes basées sur la blockchain permettent aux utilisateurs d'effectuer des transactions sans avoir besoin d'un tiers pour gérer leur authentification ou leur autorisation. [10]

2.2.2-Immuabilité

Chaque bloc d'une blockchain est stocké avec son hachage précédent. Lorsqu'un attaquant modifie le contenu d'un bloc donné, il doit modifier le hachage et l'arbre de Merkle de tous les autres blocs pour ce faire. La blockchain est très résistante à la censure et est également très difficile à falsifier. Pour ajouter un nouveau bloc, tous les mineurs doivent l'approuver par consensus. [10]

2.2.3-Vérifiabilité

Tous les membres d'un réseau blockchain possèdent une copie de l'ensemble du système, ce qui signifie qu'ils peuvent accéder à ses données, où qu'ils se trouvent. Cette transparence permet aux utilisateurs d'effectuer diverses transactions telles que la recherche de transactions impliquant des adresses spécifiques. [10]

2.2.4-Transparence

Tous les utilisateurs de systèmes de blockchain publics, tels qu'Ethereum, ont les mêmes droits lorsqu'il s'agit d'interagir avec la chaîne. De plus, toutes les transactions doivent être stockées et validées par les mineurs. Cela garantit que les données peuvent être obtenues de manière transparente. [10]

2.2.5-Pseudonyme

Malgré la transparence de la blockchain, elle parvient toujours à protéger la vie privée de ses utilisateurs en rendant ses adresses anonymes. Certaines études ont montré qu'il peut être utilisé pour identifier les utilisateurs malveillants qui effectuent des transactions illégales. [11]

2.3-Taxonomie des chaînes de blocs

Malgré la transparence de la blockchain, elle parvient toujours à protéger la vie privée de ses utilisateurs en rendant ses adresses anonymes. [12] Certaines études ont montré qu'il peut être utilisé pour identifier les utilisateurs malveillants qui effectuent des transactions illégales. Les développeurs peuvent utiliser la technologie blockchain dans diverses applications. Il existe trois principaux types de blockchain : publique, consortium et privée. [10]

2.3.1-Blockchain publique

Dans une blockchain publique, tous les membres peuvent librement rejoindre et accéder au contenu du réseau. Des exemples de telles plates-formes incluent Bitcoin et Ethereum. Dans une blockchain publique, les utilisateurs peuvent également effectuer des transactions directement.

En raison du grand nombre d'utilisateurs anonymes, il est important que les développeurs de blockchains publiques s'assurent que leurs réseaux sont sécurisés. Lors de la création de nouveaux blocs, ils doivent d'abord résoudre un

puzzle informatique connu sous le nom de consensus.

Des frais de traitement sont imposés sur chaque transaction forgée dans une blockchain publique. Ces frais incitent les utilisateurs à participer au processus de vérification, ce qui garantit la sécurité du contenu du réseau. [10]

2.3.2-Blockchain privée

Les blockchains privées sont autorisées et chaque membre du réseau est un individu connu au sein du groupe ou de l'organisation auquel il appartient. Ils sont généralement utilisés pour les organisations privées, où le seul accès au contenu de la blockchain est limité à certaines personnes. Contrairement aux blockchains publiques qui reposent sur des frais et des jetons, les blockchains privées ne dépendent pas de frais ou de jetons pour fonctionner. Les nouveaux blocs sont publiés et vérifiés par les membres du réseau.

Les blockchains privées ne sont pas aussi immuables que les blockchains publiques. En effet, les membres du réseau peuvent modifier les conditions de la blockchain à tout moment. [10]

2.3.3-Blockchain du consortium

Une blockchain privée est un type de registre distribué qui permet aux organisations privées de contrôler le contenu de leur propre réseau. Il est couramment utilisé pour les particuliers, qui n'ont qu'un accès limité au contenu de la blockchain. Contrairement à la blockchain publique, qui repose sur des frais et des jetons pour fonctionner, les blockchains privées ne reposent pas sur des frais. De plus, de nouveaux blocs sont vérifiés et publiés par les membres du réseau. Les blockchains privées ne sont pas aussi immuables que les blockchains publiques. En effet, les membres du réseau peuvent modifier les conditions de la blockchain à tout moment. [10]

2.4 Consensus sur la chaîne de blocs

Depuis plus d'une décennie, le consensus fait l'objet de recherches actives. Son objectif est de s'assurer que les informations partagées sur la blockchain peuvent être conservées en toute sécurité. La clé du modèle de fonctionnement de la blockchain réside dans les protocoles de consensus. Un consensus blockchain est

un algorithme qui aide les mineurs à parvenir à un accord concernant l'ajout d'un nouveau bloc à la chaîne. [13] Selon les auteurs de l'étude, il s'agit d'un mécanisme qui permet au réseau de prendre des décisions. Il permet aux mineurs de décider d'accepter ou de rejeter une transaction. Dans cet article, nous parlerons de certains des algorithmes de consensus existants qui sont utilisés dans les réseaux blockchain. [14]

2.4.1-Preuve de travail

Le premier consensus majeur créé à l'aide de Bitcoin et d'autres crypto-monnaies est le PoW. Il s'agit d'un processus complexe qui nécessite une authentification et une puissance de calcul à long terme. Pour parvenir à un consensus, les mineurs doivent résoudre un problème mathématique. La difficulté du puzzle PoW dépend du nombre de mineurs qui y travaillent et de la charge du réseau. Une fois qu'un mineur l'a résolu, ils ajoutent le nouveau bloc à leur chaîne et le diffusent sur le réseau. Ce processus permet à tout le monde sur la blockchain de confirmer le bloc publié. [10]

2.4.2-Preuve d'enjeu

L'objectif du consensus PoS est de réduire la consommation d'énergie du réseau en misant les parts économiques de ses pairs. Dans ce cas, le terme mineurs n'est plus utilisé et seuls les sélectionnés sont choisis pour forger de nouveaux blocs. Le processus de sélection est mené de manière aléatoire en fonction du nombre de mises du validateur choisi. Les algorithmes PoS sont vulnérables aux attaques, telles que les attaques à 51%, où un opérateur de blockchain utilise une majorité pour modifier ou contrôler la blockchain. [10]

2.4.3-Preuve d'activité

Le consensus de preuve d'activité est un système qui combine les avantages du PoS et du PoW. Il encourage à la fois l'activité et la propriété dans la blockchain. Les mineurs sont récompensés pour avoir trouvé le nonce, et ils peuvent ensuite ajouter de nouveaux blocs à la chaîne en complétant les étapes nécessaires.

La règle des 51% empêche les mineurs d'attaquer le réseau. Même si un mineur peut posséder 51% des actions, il ne peut pas contrôler la création de nouveaux

blocs. [15]

2.4.4-Tolérance aux pannes byzantine pratique

L'algorithme de consensus PBFT est conçu pour résoudre le problème général byzantin problématique. Il s'agit de décider quelle stratégie adopter pour éviter un échec total. Cette classification vise à garantir que seuls les mineurs honnêtes peuvent parvenir à un accord concernant l'état du système. Un nouveau bloc est créé en trois phases. Le principal est responsable de s'assurer que les transactions sont ordonnées. Le mineur devrait obtenir plus des deux tiers des voix pour passer d'une phase à l'autre. PBFT utilise un consensus distribué sans nécessiter de calculs mathématiques compliqués, et il est plus économe en énergie que PoW. Cependant, il est vulnérable aux attaques, en particulier à grande échelle. L'utilisation d'algorithmes de consensus est cruciale pour maintenir l'intégrité d'un réseau blockchain. Ils aident les membres du système à parvenir à un accord concernant la version du réseau qu'ils souhaitent maintenir. Bien qu'il existe différents types d'algorithmes de consensus utilisés dans la technologie blockchain, chacun ne convient qu'à un certain nombre de scénarios. [16]

2.5-Contrats intelligents Blockchain

Lorsque certaines conditions sont remplies, les contrats intelligents blockchain s'exécuteront et exécuteront un code une fois les conditions préalables remplies. La plate-forme la plus utilisée pour exécuter des contrats intelligents est Ethereum. La solidité est un type de codage utilisé pour la création de contrats intelligents blockchain. Ceux-ci sont généralement utilisés pour établir des contrôles d'accès ou gérer des systèmes. Les contrats intelligents sont composés de quatre phases séquentielles. L'étape de création implique la négociation des termes et conditions du contrat intelligent. Le déploiement d'un contrat intelligent sur la blockchain est généralement considéré comme un déploiement sécurisé. Il peut être exploité sans modification en raison de l'immuabilité de la blockchain. Le contrat intelligent sera automatiquement exécuté une fois la condition remplie. Cela permettra à la transaction d'être approuvée par les mineurs. Après l'achèvement d'un contrat intelligent, l'état mis à jour de toutes les parties impliquées est stocké dans la blockchain et toutes les transactions effectuées au

cours du processus sont documentées et archivées. [10]

Conclusion

Les limites de l'Internet des objets (IoT) peuvent être abordées à l'aide de diverses avancées technologiques. Par exemple, en utilisant des algorithmes d'optimisation du réseau, les appareils peuvent être équipés d'une meilleure connectivité. Les progrès réalisés dans les technologies de l'IA, de l'apprentissage automatique et de la blockchain devraient contribuer à améliorer la connectivité des appareils IoT. En raison de leur potentiel à résoudre divers problèmes, tels que la sécurité, la fiabilité et l'interopérabilité, la blockchain peut jouer un rôle essentiel dans le développement des systèmes IoT. Cet article présentera les bases de la technologie blockchain et ses avantages. [2]

Une blockchain est construite sur un registre distribué inviolable, ce qui en fait une solution idéale pour résoudre le problème de SPoF. Il peut être intégré dans divers domaines, tels que l'Internet des objets (IoT), pour empêcher l'accès non autorisé aux données collectées par ces appareils. En raison des caractéristiques de la technologie blockchain, il est incroyablement difficile pour quiconque de falsifier des enregistrements. Cependant, il est toujours confronté à divers défis qui l'empêchent de s'intégrer pleinement à l'Internet des objets. Certains d'entre eux incluent ses problèmes d'évolutivité et la nature intensive de calcul de ses algorithmes de consensus. [10]

Chapitre 02

Les techniques blockchain dans IoT

Introduction

L'Internet des objets est très fascinant et passionnant. Cependant, il est également très difficile de créer un écosystème sécurisé qui permettra aux différents blocs de construction de l'IoT de fonctionner de manière transparente [17]. Le terme blockchain fait référence à une base de données qui ne cesse de croître et qui n'a pas de PC central ou maître. Cela en fait un cadre idéal pour analyser les vulnérabilités dans diverses unités [18]. Alors que la convergence des technologies blockchain et IoT se poursuit, il est important que les différentes technologies utilisées pour résoudre ces problèmes soient étudiées en profondeur [20]

L'architecture IoT utilise la technologie blockchain pour maintenir un enregistrement immuable de chaque opération effectuée par les appareils.[18]. La possibilité de mettre en œuvre des cadres IoT complexes via la blockchain fournit un cadre pour résoudre des problèmes auparavant impossibles ou complexes. [21]. Le problème le plus important concernant la convergence potentielle de la technologie blockchain et de l'Internet des objets (IoT) est l'emplacement de la blockchain. [19]. En raison des ressources de calcul limitées et de la bande passante requise pour la technologie des registres distribués. [22].

En effet, les transactions sont acheminées via différents pairs au sein du réseau. Lorsqu'une transaction est initiée, le certificat d'enregistrement d'un appareil IoT est émis par l'autorité de certification du Fabric. Ce sont là quelques-uns des facteurs qui sont pris en compte pour améliorer l'efficacité globale du système. [23]

1.L'intégration de blockchain dans le IoT

1.1- Problèmes d'intégration de la blockchain et de l'IoT

L'intégration de la technologie Blockchain dans l'Internet des objets (IoT) peut aider à résoudre divers problèmes de sécurité. L'un des principaux défis auxquels les administrateurs système sont confrontés est le transfert sécurisé des données sur le réseau. Avec l'aide de Blockchain, ils peuvent maintenant résoudre ce problème. Cependant, le plus grand défi auquel les développeurs et les organisations sont confrontés est l'architecture et le principe de fonctionnement de la technologie. Avant de mettre en œuvre la technologie Blockchain dans un système IoT, il est important de discuter d'abord des différents problèmes qui peuvent survenir en raison de son intégration. [Figure 2.1]. [24]

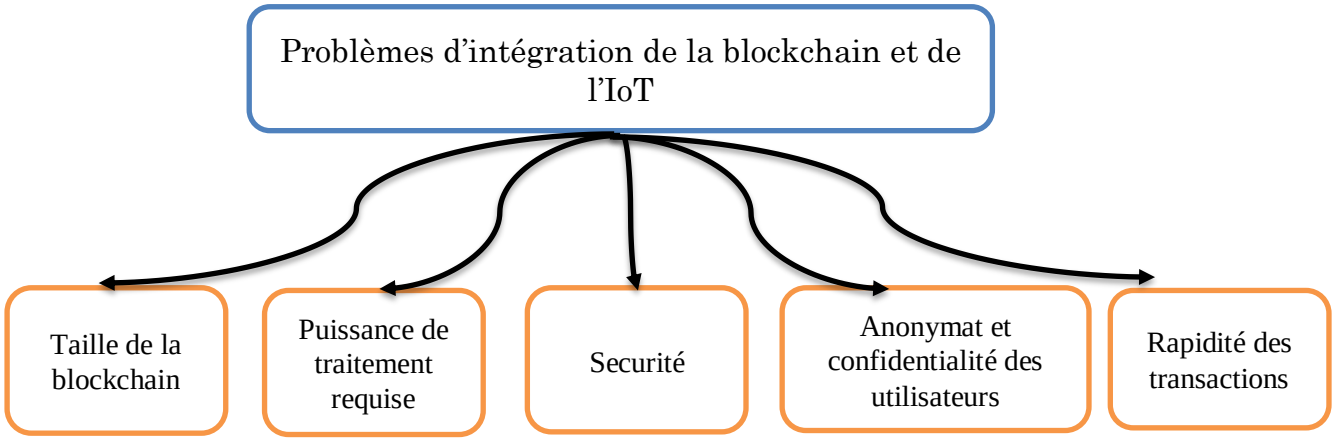

Figure 2.1-Problèmes d'intégration de l'IoT et de la Blockchain. [24]

1.1.1-Taille de la blockchain

La taille statique et opérationnelle des données collectées par les systèmes IoT est très différente de celle générée par les technologies Blockchain. Les tailles de ces technologies, qui incluent Ethereum et Bitcoin, ont déjà atteint 250 Go et 1 To, ce qui les rend incroyablement difficiles à traiter. Cela rend incroyablement difficile l'intégration de la blockchain dans l'écosystème IoT. Afin de résoudre le problème du stockage des données, il est suggéré que les données collectées par les appareils IoT soient stockées sur le cloud. Cependant, cette méthode entre en conflit avec le cadre Blockchain en raison de la façon dont elle est distribuée. [24]

1.1.2-Puissance de traitement requise

Pour fournir des fonctionnalités de haute sécurité, telles que l'authentification forte et l'immuabilité, Blockchain utilise des algorithmes de consensus et de PoW. Ceux-ci sont généralement très énergivores et nécessitent beaucoup de puissance de traitement. D'autre part, les appareils IoT utilisent des processus et des protocoles à faible consommation d'énergie. Pour cette raison, il est très difficile de les faire fonctionner de manière transparente les uns avec les autres.[24]

1.1.3-Sécurité

De nombreux chercheurs pensent que la blockchain peut être utilisée comme solution de sécurité pour l'Internet des objets (IoT). Cependant, cette intégration introduit un sérieux problème concernant la fiabilité des données collectées par le système. Afin de garantir l'intégrité des données, il est important que le système ne reçoive pas de données malveillantes des appareils. Il existe diverses raisons pour lesquelles les données peuvent être corrompues dans l'IoT, telles que la défaillance des appareils, le piratage des réseaux et les faux appareils. Lorsqu'il s'agit de mettre en œuvre des protocoles de sécurité dans l'IoT, divers problèmes doivent être résolus. [24]

1.1.4-Anonymat des utilisateurs et leur vie privée

Bien que Blockchain ait été en mesure de résoudre le problème de confidentialité entourant les données sur son réseau, elle pourrait ne pas être en mesure de protéger complètement les informations contenues dans les appareils de l'Internet des objets (IoT). Afin d'empêcher l'accès non autorisé aux données, nous avons discuté de la façon dont des ressources limitées peuvent empêcher le traitement des protocoles complets de sécurité et de confidentialité Blockchain dans les appareils IoT. Cela signifie que les attaquants peuvent facilement exploiter cette vulnérabilité. Malgré les avantages de la fonction d'immuabilité de Blockchain, elle peut toujours créer des problèmes d'anonymat des utilisateurs en raison de la façon dont elle partage les mêmes informations entre ses blocs. Selon des études menées par des chercheurs en 2018, et à nouveau en 2019, Blockchain peut exposer ses utilisateurs à de graves problèmes de confidentialité et être vulnérable à des attaques telles que les doubles dépenses et le reniflement de paquets. Par

conséquent, il n'est actuellement pas possible de développer une solution capable de prévenir ces types d'attaques. [24]

1.1.5-Rapidité des transactions

L'un des plus gros problèmes auxquels les utilisateurs de Blockchain sont confrontés lorsqu'il s'agit de l'intégrer à l'Internet des objets est sa vitesse de transaction. Dans un système interconnecté, les données générées par les appareils peuvent ne pas se synchroniser avec la vitesse de traitement de Blockchain. Par exemple, Bitcoin, Ethereum et d'autres systèmes similaires n'ont que des vitesses de traitement d'environ quatre à cinq transactions par seconde. Non seulement Blockchain ne stocke pas et ne traite pas les données collectées par les appareils IoT, mais elle ne fonctionne pas non plus bien lorsqu'il s'agit d'effectuer des transactions. Ce problème peut empêcher le système de fonctionner correctement. [24]

1.2-Stratégies d'intégration Blockchain et IoT

Certaines techniques d'intégration intelligentes peuvent aider à minimiser les problèmes d'intégration liés au développement de l'Internet des objets (IoT). Cependant, le déploiement correct de la couche Blockchain n'est pas toujours facile. C'est pourquoi il est important de considérer les différentes approches qui seront utilisées pour établir la communication entre les deux parties. [24]

1.2.1. Modèle Inter IoT

Le modèle le plus simple de la façon dont les appareils IoT [Figure 2.2] peuvent communiquer est le suivant. Cela n'implique pas l'utilisation de ressources informatiques de haut niveau telles que celles trouvées dans Blockchain. Cela garantit qu'il peut fonctionner de la manière la plus rapide possible. Il est idéal pour les applications qui ont besoin d'une latence et d'une sécurité de communication plus faibles. [24]

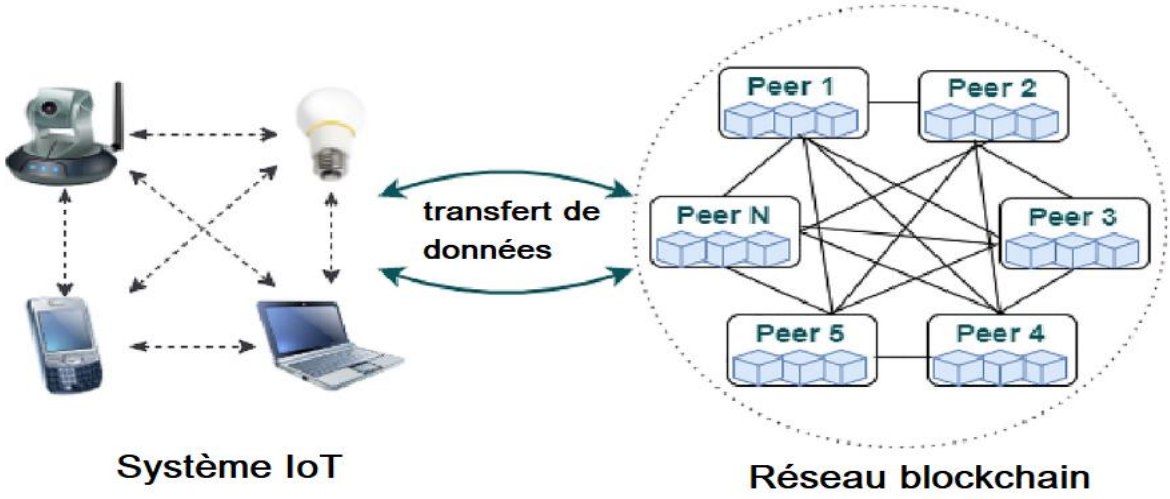

Figure 2.2-Modèle d'intégration inter-IoT.[24]

1.2.2-Modèle IoT-Blockchain

Ce concept utilise la technologie Blockchain pour connecter tous les appareils d'un réseau IoT. Il nous permet de mettre en œuvre diverses fonctionnalités de sécurité pour protéger le système [Figure 2.3]. Les données et les transactions du réseau sont stockées dans Blockchain. Cette approche offre divers avantages, tels que sa capacité à stocker et à gérer les transactions. Il élimine également le besoin de saisie manuelle des données et fournit un environnement sécurisé pour l'échange d'informations. Cependant, en raison de la lenteur du taux de transaction, cela peut être une préoccupation pour la latence du réseau. [24]

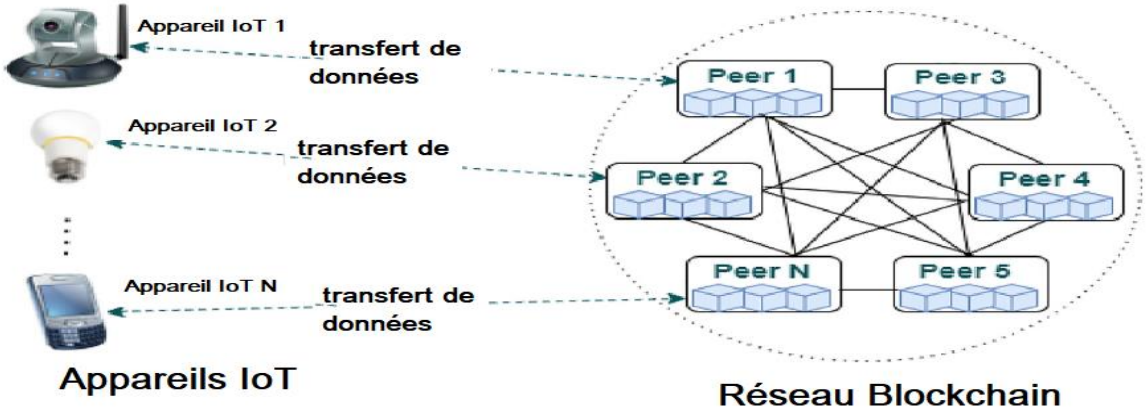

Figure 2.3-Intégration du modèle IoT-Blockchain. [24]

1.2.3-Modèle IOT-Blockchain basé sur le cloud/brouillard et la périphérie

Le développement du cloud et de l'informatique par brouillard a résolu de nombreux problèmes liés aux ressources limitées des appareils de l'Internet des objets (IoT) [Figure 2.4]. L'un des avantages les plus importants de cette technologie est le transfert de la charge de calcul des appareils vers le cloud. Le développement du cloud et de l'informatique par brouillard a résolu de nombreux problèmes liés aux ressources limitées des appareils de l'Internet des objets (IoT). L'un des avantages les plus importants de cette technologie est le transfert de la charge des appareils vers le cloud. En raison de la puissance de traitement et de l'énergie élevées requises pour faire fonctionner une Blockchain, l'utilité de cette technologie a augmenté dans le contexte de l'intégration de l'IoT et de la Blockchain. [24]

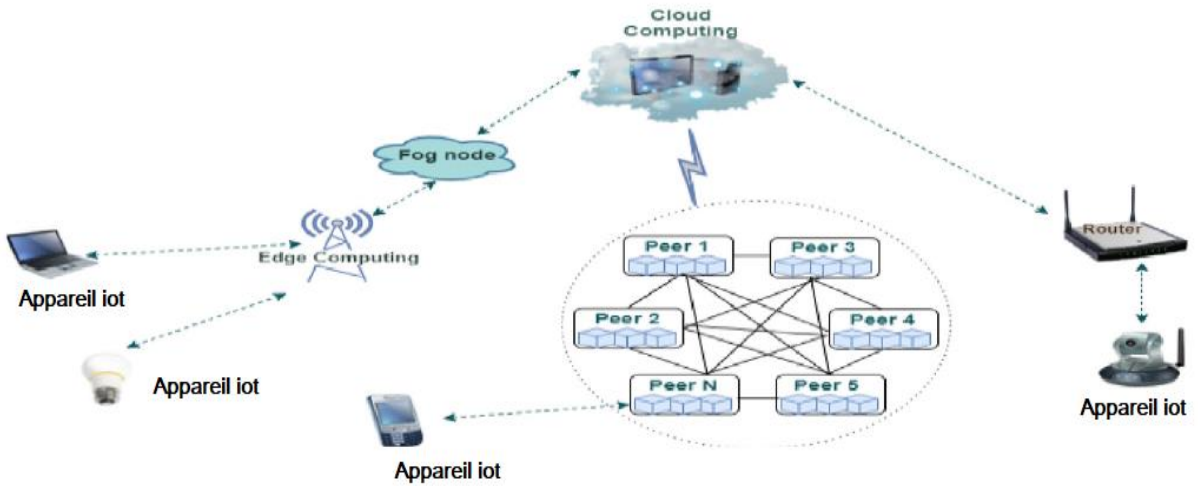

Figure 2.4-Modèle hybride d'intégration basé sur le cloud/brouillard et la périphérie. [24]

1.3-Fiabilité des données IoT dans la blockchain

Disposer de données fiables est très important pour les organisations, car cela peut les aider à renforcer la confiance dans leurs données. [25]. L'un des facteurs les plus critiques pris en compte par les organisations lorsqu'il s'agit de mettre en œuvre et de maintenir des initiatives d'intégrité des données est de s'assurer que les données qu'elles collectent sont fiables. Cela se fait grâce à l'utilisation de sources de données sécurisées et résilientes. Malheureusement, les données

collectées par les applications IoT peuvent être sujettes à des attaques de falsification. C'est pourquoi il est important qu'ils disposent de l'infrastructure nécessaire pour prévenir ces attaques. Avant de mettre en œuvre la technologie blockchain, il est important que les données collectées à partir de l'Internet des objets (IoT) soient minutieusement inspectées pour empêcher tout accès non autorisé et toute manipulation. Ce problème est principalement dû au manque d'interaction entre la blockchain et les données du monde extérieur. La fiabilité des données collectées à l'aide de la technologie blockchain a fait l'objet de diverses études. [26] L'objectif du modèle de confiance proposé est de s'assurer que les différentes composantes de la blockchain sont sécurisées et résilientes. Ce processus implique de fournir un tiers qui peut effectuer la vérification et l'analyse des données collectées et stockées sur la blockchain [27] les auteurs ont expliqués comment une blockchain décentralisée peut être utilisée pour vérifier l'authenticité des données. Il utilise un système de vote pondéré pour s'assurer que les données sont fiables. Les données du système sont représentées sous la forme d'un ensemble d'instructions booléennes pour vérifier la validité de la proposition. En tant que collaborateurs, les auteurs de cet article fournissent un cadre pour l'analyse et la vérification des données.

Ils divisent les rôles des certificateurs et des soumissionnaires en deux catégories le premier est plus susceptible de présenter un risque et une récompense élevés, tandis que le second est plus susceptible de présenter un risque et une récompense faibles. Pour s'assurer que les participants ont un niveau élevé de confiance, ils ont proposé un modèle de confiance qui récompense les personnes fiables avec des récompenses pour l'exécution d'une tâche. L'implication non réglementée de sources de données externes dans l'échange d'informations peut encore violer l'équilibre de Nash. Cela peut être fait par la création d'attaques de collusion hors chaîne en tirant parti des efforts de certains certificateurs et soumissionnaires malveillants. Les auteurs de Blockchain Architecture. [28] ont proposé un cadre décentralisé qui permet une vérification efficace des données. Il évite l'utilisation d'un mécanisme de consensus unique en mettant en œuvre un consensus multiface.

1.4-Sécurité de Blockchain et IOT

L'un des facteurs les plus critiques dans le développement des applications et des services de l'Internet des objets est la sécurité [29]. L'essor de l'Internet des objets (IoT) en a fait une cible attrayante pour les failles de sécurité. Ces attaques peuvent aller de simples piratages à des attaques plus sophistiquées qui peuvent affecter l'intégrité du système [40]. En raison de la complexité de la surface d'attaque, les applications IoT sont sujettes à rencontrer divers problèmes de sécurité. L'environnement dans lequel les appareils fonctionnent pose également des défis supplémentaires lorsqu'il s'agit de les protéger. La plupart du temps, le développement d'appareils IoT n'est pas une priorité de sécurité. L'utilisation de la technologie blockchain peut aider à améliorer la sécurité des transactions IoT en stockant les transactions signées, hachées et chiffrées numériquement. Il peut également aider à empêcher l'accès non autorisé à l'appareil en mettant en œuvre des contrats intelligents. Le tableau [1] montre une variété d'études qui démontrent comment la blockchain peut être utilisée pour sécuriser les applications IoT.

Le nombre croissant d'appareils reliés et la complexité de leur connectivité ont soulevé de nouvelles préoccupations concernant la sécurité des applications de l'Internet des objets (IoT). Outre les pirates externes, les acteurs internes sont également des menaces potentielles. Ces personnes peuvent prendre le contrôle des appareils IoT et accéder à leurs données sensibles. Les nouvelles technologies telles que l'IA peuvent aider à améliorer la sécurité des applications de l'Internet des objets (IoT) en prévenant les violations de données et en veillant à ce qu'elles soient sécurisées. L'apprentissage automatique est un type d'intelligence artificielle qui utilise des données collectées à partir d'expériences passées pour améliorer les performances [41]. L'apprentissage automatique est un type d'informatique qui utilise des techniques mathématiques et l'intelligence artificielle pour construire des systèmes d'apprentissage et de modélisation. Il peut être utilisé pour améliorer la sécurité et l'efficacité des applications IoT. [42]. En raison de l'immense quantité de données collectées par l'Internet des objets (IoT), l'apprentissage automatique (ML) peut être utilisé pour analyser et prédire les vulnérabilités de sécurité des appareils. Dans cette section, nous parlerons de

certains des travaux effectués à l'aide de la blockchain et d'apprentissage automatique pour améliorer la sécurité de l'IoT.

1.4.1-Détection d'attaque

Afin d'empêcher tout accès non autorisé à l'Internet des objets (IoT), les auteurs de cet article [43] ont proposé un mécanisme de sécurité qui utilise l'apprentissage automatique pour analyser la présence des utilisateurs dans une IoT-Zone donnée. Cette méthode peut être utilisée pour sécuriser la communication entre l'appareil et l'utilisateur. Les auteurs ont également proposé d'utiliser une plate-forme basée sur la blockchain pour mettre en œuvre cette sécurité. [44]. La solution proposée permettrait aux utilisateurs d'accéder au système à l'aide d'un mot de passe à usage unique et d'un jeton numérique. Cette méthode empêcherait également l'accès non autorisé. Les auteurs [45] d'une étude ont proposé un cadre blockchain qui permettrait aux participants au test de stocker et d'identifier les logiciels malveillants. Ce système leur permettrait également de classer ces logiciels malveillants.

Les auteurs [46] d'une étude ont présenté un cadre permettant la détection et le calcul sécurisé des comportements malveillants. Surnommée deepchain, elle utilise un algorithme de seuil de Paillier pour garantir la confidentialité des données et leur auditabilité. Ils ont également suggéré d'utiliser la blockchain pour inciter les participants à se comporter correctement.

Dans une étude publiée en article [47], les auteurs ont expliqué comment un modèle de réseau neuronal distribué pourrait être utilisé pour se protéger contre les attaques utilisant la technologie blockchain. Le modèle utilise diverses fonctionnalités telles que la décentralisation et la cryptographie pour maintenir son état et empêcher la falsification.

1.4.2-Préservation de la vie privée

Les auteurs de [48] ont proposé un cadre P2P sécurisé et décentralisé qui permettrait aux utilisateurs de créer et de gérer des modèles de réseau d'apprentissage profond (DNN) sur la blockchain. Ce cadre permettrait aux propriétaires de données de protéger leur identité tout en veillant à ce que les mises à jour finales du modèle soient stockées dans la blockchain. En outre, le

système récompenserait les participants pour leurs contributions à l'amélioration de la précision du modèle. Les auteurs d'un article ont proposé [49] un système de blockchain et d 'apprentissage automatique appelé Learning Chain. Il utilise un algorithme de descente de gradient pour détecter et prédire les attaques byzantines. Le système a également été proposé d'utiliser la blockchain Ethereum pour sécuriser les connexions entre ses nœuds informatiques et les propriétaires de données. Les auteurs de [50] ont présenté un paradigme qui vise à créer un environnement informatique sécurisé et coopératif entre des nœuds qui ne sont pas dignes de confiance. Ce paradigme est basé sur l'utilisation de diverses technologies d'apprentissage décentralisé et de blockchain pour permettre aux individus ayant des ressources limitées de contribuer de manière décentralisée.

1.5-Évolutivité de la blockchain et IOT

L'un des plus gros problèmes que les gens rencontrent lorsqu'il s'agit d'intégrer la technologie blockchain dans l'Internet des objets est sa faible évolutivité. Ce problème empêche le système de suivre la quantité massive de données collectées par les appareils. Le nombre de transactions entrées dans un registre blockchain en raison du temps est fonction de son débit. Dans la blockchain bitcoin, par exemple, seules 7 transactions sont ajoutées au système chaque seconde. Ce problème est couramment rencontré dans d'autres systèmes, tels que le réseau Visa, qui peut traiter des milliers de transactions par seconde. Certaines solutions ont proposé de créer une blockchain de consortium capable d'atteindre une évolutivité élevée, tandis que d'autres ont suggéré de développer un consensus plus évolutif.

1.5.1-Blockchain de consortium évolutive

Les auteurs de [51] ont proposé une méthode pour améliorer l'efficacité du processus de création de blocs sur la Scalable Consortium Blockchain. Cette modification affecterait la façon dont les mineurs organisent et construisent les blocs. Afin d'améliorer les performances, les auteurs [52] ont suggéré d'augmenter la limite de taille du bloc. Mais, cette méthode peut conduire à une double dépense ou à un taux de blocage périmé. [53]

Dans leur article [54], les auteurs ont proposé d'augmenter la limite de taille

maximale des blocs. Cependant, cette méthode pourrait entraîner un taux de blocage périmé et des problèmes de double dépense.

1.5.2-Consensus blockchain évolutif

Les auteurs [55] ont proposé que le consensus blockchain soit limité à un certain nombre de mineurs. L'auteur [56] a proposé un nouveau type de consensus blockchain connu sous le nom de preuve d'autorité, capable de gérer de gros blocs et transactions. Seuls les nœuds sélectionnés, appelés validateurs, sont impliqués dans le processus de validation. Cela rend le système très évolutif.

Titre de travaille	Année	Solutions Proposès	Blockchain
Un système de service informatique de réseau de non-répudiation basé sur la blockchain pour l'IoT industriel. [30]	2019	Un système de non-réudiation basé sur la blockchain pour l'Internet des objets (IoT) utilise le jeton blcockahin comme enregistreur de preuves et éditeur de services.	Ethereum
Système de réputation des nœuds de brouillard publics IoT. [31]	2019	Un cadre pour l'établissement et la gestion des connexions de service entre les nœuds de brouillard publics et les appareils de l'Internet des objets.	Ethereum
Un cadre d'investigation efficace décentralisé basé sur la blockchain pour la criminalistique numérique IoT. [32]	2019	Un cadre qui utilise la technologie blockchain pour sécuriser la transmission de données entre les appareils et les réseaux.	Ethereum
Architecture de sécurité décentralisée basée sur la blockchain pour le réseau IoT. [33]	2019	Un système d'authentification et d'identification sécurisé et décentralisé pour l'Internet des objets (IoT) qui permettra aux appareils de se faire confiance.	Ethereum
Système d'audit de données externalisé à distance décentralisé, fiable et efficace avec contrat intelligent blockchain pour l'IoT industriel. [34]	2020	Un système d'authentification sécurisé et décentralisé pour l'Internet des objets (IoT) utilise la blockchain et la mise en réseau définie par logiciel (SDN) pour empêcher tout accès non autorisé au réseau.	Ethereum

Proxy Re Encryption Scheme basé sur Blockchain pour le partage sécurisé des données IoT. [35]	2019	La criminalistique numérique est un processus qui peut être effectué sur l'Internet des objets (IoT) pour protéger l'intégrité des données.	Ethereum
Modèle de confiance blockchain pour la détection de nœuds malveillants dans les réseaux de capteurs sans fil. [36]	2019	Un système de recryptage proxy qui utilise la technologie blockchain pour sécuriser l'échange d'informations entre divers utilisateurs de l'Internet des objets (IoT).	Ethereum
Sécurité renforcée de la gestion du partage de données IoT par les contrats intelligents et la blockchain. [37]	2019	Un contrat numérique sécurisé qui utilise la technologie blockchain pour gérer l'échange d'informations entre la CIA et d'autres organisations est conçu pour assurer ses opérations.	Ethereum
Sécurité renforcée de la gestion du partage de données IoT par les contrats intelligents et la blockchain. [38]	2019	Un système d'authentification sécurisé qui utilise la technologie blockchain pour fournir aux utilisateurs un accès et un contrôle fiables est créé.	Ethereum
Blockchain robuste pour la sécurité IoT. [39]	2019	Un cadre robuste et sécurisé pour l'Internet des objets (IoT) utilise une blockchain légère.	Ethereum

Tableau [1] – Table de comparaison les travaux connexes (Blockchain pour sécuriser les applications IoT).

2-Synthèse

En raison du nombre croissant d'appareils connectés, divers obstacles peuvent empêcher l'adoption généralisée de l'Internet des objets. Le marché de l'IoT se caractérise par la grande variété de normes et de fournisseurs. De plus, la mise en œuvre de solutions qui impliquent la génération de nouveaux enregistrements de données a soulevé des préoccupations quant à l'interopérabilité. Bien que les données collectées et stockées par les appareils IoT soient sécurisées dans le cloud, elles peuvent être compromises si la source est falsifiée ou si le dispositif d'intégrité est volé. Diverses alternatives à l'Internet des objets promettent de fournir aux utilisateurs un hub central où leurs données sont stockées et consultées. Mais, ils exigent également que les utilisateurs fassent confiance aux fournisseurs et aux fabricants pour sécuriser leurs informations. La technologie Blockchain peut résoudre ce problème. Les développeurs peuvent bénéficier de la technologie blockchain en la mettant en œuvre sous la forme d'un registre distribué qui peut les aider à éviter d'avoir à faire face à des problèmes de conception centralisée. Il stocke également les détails de la transaction de manière sécurisée. En tant que nouveau système, il peut aider à réduire le risque de vol ou de falsification des données. En outre, la technologie blockchain peut aider à réduire les frais généraux associés à l'Internet des objets en éliminant le besoin d'intermédiaires et d'intermédiaires. Bien que la technologie blockchain puisse résoudre de nombreux problèmes émergents liés à l'Internet des objets, il peut également être très difficile de l'intégrer dans l'écosystème en raison des différences technologiques variables. L'un des problèmes les plus courants qui peuvent empêcher l'adoption généralisée de la technologie blockchain est le manque d'énergie et de capacité de stockage pour ses registres distribués. Ce problème peut être causé par le manque de ressources disponibles pour soutenir le développement de nouvelles applications.

Conclusion

En raison du nombre croissant d'appareils connectés, divers obstacles ont été identifiés qui peuvent empêcher l'utilisation généralisée de l'Internet des objets dans divers secteurs. Le marché de ces appareils et plates-formes est très différent des autres technologies. L'un des principaux problèmes qui a été identifié est le manque d'interopérabilité entre les différentes plates-formes et appareils. Les données collectées et stockées par ces appareils sont accessibles et exploitées dans la plate-forme cloud, bien que cela puisse être compromis si la source n'est pas sécurisée. L'un des principaux avantages de la mise en œuvre d'une conception centralisée pour l'Internet des objets est qu'elle permet au propriétaire de l'appareil de faire confiance au fabricant ou au fournisseur pour s'assurer que ses données sont sécurisées. Cependant, ce type de conception peut également entraîner des problèmes en raison de la vulnérabilité du serveur central. Une alternative est la blockchain, qui est un registre distribué qui permet aux utilisateurs d'éviter ces problèmes. Grâce à ses caractéristiques uniques, la blockchain permet aux utilisateurs de stocker des transactions en toute sécurité. L'un des principaux avantages de ce type de conception est qu'il permet au propriétaire de l'appareil de faire confiance au fabricant ou au fournisseur pour s'assurer que ses données sont sécurisées. Il élimine également le besoin d'intermédiaires et d'autres frais généraux associés à l'Internet des objets. Malgré les avantages de la blockchain, il n'est toujours pas possible de la mettre pleinement en œuvre en raison de la complexité des registres distribués et du manque de dispositifs d'alimentation et de stockage nécessaires à son fonctionnement. Par exemple, les exigences en matière d'alimentation et de stockage des appareils IoT ne sont pas idéales pour les registres distribués. Certains des problèmes qui ont été identifiés incluent le manque de stockage de copie complète, le chiffrement des nœuds et l'incapacité d'effectuer une exécution par consensus.

Chapitre 03

Présentation de l'architecture globale du système.

Introduction

Ce chapitre se concentre sur un système de confiance qui utilise la technologie blockchain dans l'Internet des objets (IoT). Il vise à fournir un cadre permettant aux supermarchés de maintenir la confiance de leurs clients on utilise un panier intelligent.

L'architecture du système de confiance est traitée en détail dans ce chapitre. Ce système répond au problématique tel que qui va accepter d'utiliser un objet connecté si ça mettre en danger ces données personnelles ? Ce système facilite

L'échange de données et la coopération entre les Supermarché et les Banques et leurs clients avec une grosse sécurité.

Cette architecture n'offre qu'aucun attaque grâce à ce système décentralisé tels que la Blockchain qui sécurises les objets connectés contre les attaques, aussi ce système offre que les objets et prise de décision autonomes peuvent réagir à l'exécution de smart contrat, lutte contre la fraude.

Cette architecture est composée en quatre niveaux typiques : capteurs de panier, passerelles et blockchain et application. Les capteurs de panier capturent les données tels que les prix des achats de client et les transmettent sous forme d'une facture via une passerelle à la blockchain qui la transmet aux cloud pour les traiter et les stocker. Si la transaction est complète la Blockchain fait un retour de transaction au panier, ce dernier envoie la facture ver la banque et le client la reçu

depuis un message ou un courrier électronique pour confirmer que la transaction est sécurisée.

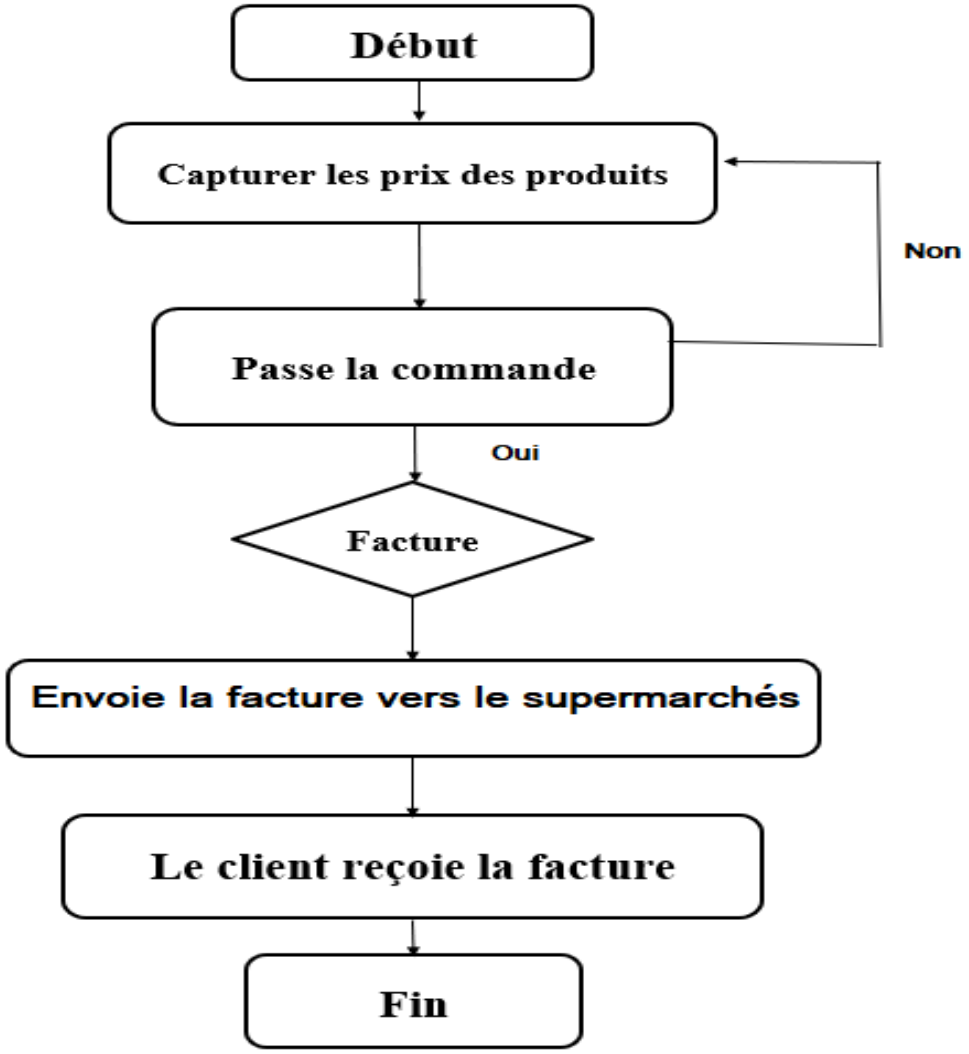

Figure 3.1- le processus de fonctionnement du système de confiance.

1-La Blockchain dans l'IOT est la solution pour Gagner la confiance des clients à utiliser un objet connecté

Dans les années dernières pour prendre le cas le plus récent on a des milliards d'objets connectés dans le monde pour un marché d'un milliard de dollars et donc cette année on va dépasser le nombre d'objets connectés votre plus grand que le nombre d'être humain sur la planète et les objets connectés ne disposent d'aucune mesure de sécurité et donc ça c'est le constat d'un état critique pour ce domaine-là parce que la question qu'on peut légitimement se poser c'est qui va accepter

d'utiliser un objet connecté si ça peut mettre en danger ses données personnelle. On base dans le contexte on a des réseaux de capteurs pour l'internet des objets qui sont totalement décentralisé il faut posés les questions de base de sécurités donc :

1.1- Comment identifier un objet connecté

1.1.1-Par un identifiant unique et la clé associée

Effectivement, pour identifier un appareil IoT, on utilise généralement un identifiant unique appelé "adresse MAC" (Media Access Control) ou "adresse IP" (Internet Protocol). Ces identifiants permettent de distinguer chaque appareil connecté à un réseau et de lui attribuer une adresse unique.

En outre, pour garantir la sécurité des appareils IoT, il est souvent nécessaire de les authentifier en utilisant une clé associée à leur identifiant unique. Cette clé peut être utilisée pour crypter les communications entre l'appareil IoT et le réseau, ou pour empêcher l'accès non autorisé à l'appareil par des tiers malveillants.

Il est important de noter que l'identifiant unique et la clé associée doivent être protégés contre les attaques malveillantes et les tentatives d'accès non autorisé. Par conséquent, il est recommandé d'utiliser des protocoles de sécurité robustes pour protéger les appareils IoT et les données qu'ils génèrent.

1.2-Comment lui faire confiance

1.2.1-Retrouver ses actions passées via la blockchain

La blockchain peut être utilisée pour établir la confiance envers un appareil IoT en permettant la traçabilité de ses actions passées.

Lorsqu'un appareil IoT utilise la blockchain pour stocker les données qu'il génère, toutes les transactions sont enregistrées de manière permanente et immuable dans la chaîne de blocs. Cela permet de vérifier l'authenticité et l'intégrité des données générées par l'appareil.

En outre, la blockchain peut être utilisée pour établir des contrats intelligents (smart contracts) qui permettent de spécifier les conditions d'utilisation de l'appareil et de s'assurer qu'il les respecte. Les contrats intelligents sont exécutés

automatiquement et sont vérifiés par les nœuds du réseau de la blockchain, ce qui garantit l'impartialité et la transparence du processus.

En utilisant la blockchain pour stocker les données générées par l'appareil IoT et pour établir des contrats intelligents, on peut donc établir un système de gestion de confiance décentralisé et sécurisé qui permet de garantir la fiabilité et l'intégrité de l'appareil et de ses données.

1.3-Où stocker l'information

1.3.1-Dans la blockchain

En effet, la blockchain peut être utilisée pour stocker les informations générées par les appareils IoT de manière sécurisée et immuable.

La blockchain est une base de données distribuée décentralisée qui stocke toutes les transactions sous forme de blocs qui sont liés les uns aux autres de manière chronologique, formant ainsi une chaîne de blocs (blockchain). Chaque bloc contient un ensemble de transactions qui ont été validées par les nœuds du réseau de la blockchain.

En stockant les informations générées par les appareils IoT dans la blockchain, on garantit leur immutabilité et leur intégrité. Les données sont stockées de manière décentralisée, ce qui les rend résistantes aux attaques malveillantes et aux défaillances du système. De plus, l'utilisation de la blockchain permet de garantir la confidentialité des données en utilisant des mécanismes de chiffrement avancés.

En résumé, la blockchain est une solution efficace pour stocker les informations générées par les appareils IoT de manière sécurisée et immuable.

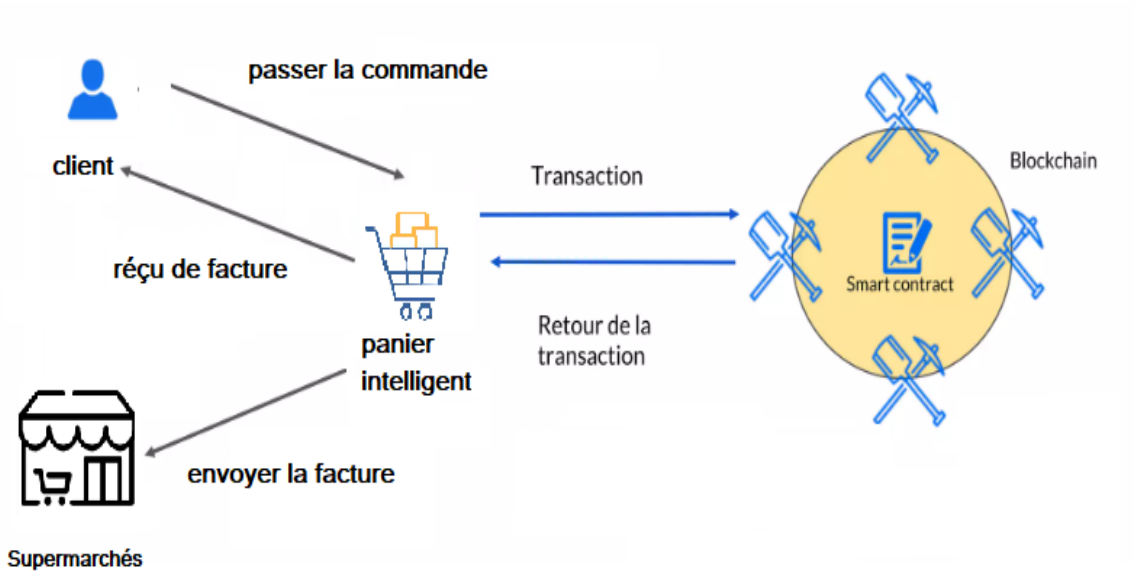

Figure 3.2- Architecture globale de système de confiance basé sur la Blockchain dans IOT.

2-Les niveaux d'architecture globale de système de confiance basé sur la Blockchain dans l'IoT

Cette architecture comporte 5 niveaux pour le système tels que :

2.1-Niveau d'appareil (Device Level)

Ce niveau correspond aux appareils IoT eux-mêmes, qui doivent être équipés d'une clé d'authentification unique et d'un identifiant pour garantir leur sécurité et leur intégrité. Les appareils peuvent également inclure des capteurs pour collecter des données et les envoyer à un nœud de la blockchain pour les stocker et les traiter.

2.2-Niveau de communication (Communication Level)

Ce niveau correspond aux protocoles de communication utilisés pour transmettre les données entre les appareils IoT et les nœuds de la blockchain. Ces protocoles doivent être sécurisés et fiables pour garantir l'intégrité et la confidentialité des données.

2.3-Niveau de stockage (Storage Level)

Ce niveau correspond à la manière dont les données générées par les appareils IoT sont stockées sur la blockchain. Les données doivent être stockées de manière sécurisée et immuable pour garantir leur intégrité et leur disponibilité.

2.4-Niveau de traitement (Processing Level)

Ce niveau correspond aux nœuds de la blockchain qui traitent les données générées par les appareils IoT. Ces nœuds doivent être équipés d'une puissance de traitement suffisante pour garantir des temps de réponse rapides et doivent être capables de vérifier la validité des transactions.

2.5-Niveau d'application (Application Level)

Ce niveau correspond aux applications qui utilisent les données générées par les appareils IoT stockées sur la blockchain. Ces applications peuvent inclure des applications de suivi de la chaîne d'approvisionnement, des applications de surveillance de la qualité de l'air ou des applications de maintenance prédictive.

Ces niveaux d'architecture globale d'un système de confiance basé sur la blockchain dans l'IoT doivent être conçus de manière cohérente et sécurisée pour garantir l'intégrité, la confidentialité et la disponibilité des données générées par les appareils IoT.

3-Le processus de communication de panier intelligent avec la blockchain

Pour permettre au panier intelligent de communiquer avec la blockchain, il est nécessaire d'utiliser un protocole de communication sécurisé et fiable pour transmettre les données entre les deux. Voici une méthode générale pour passer des transactions entre un panier intelligent et la blockchain [Figure 3.3] :

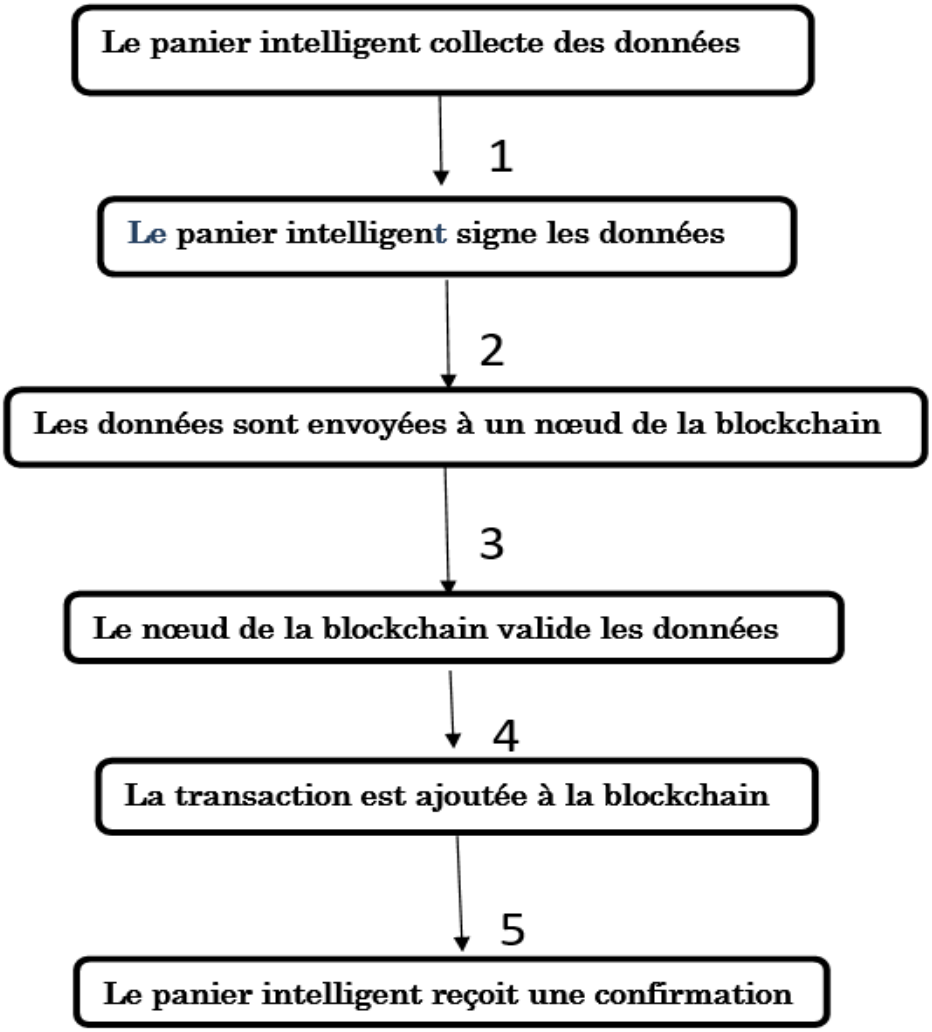

Figure 3.3-l'organigramme de communication de panier intelligent avec la Blockchain.

3.1-Le panier intelligent collecte des données

Le panier intelligent collecte des données à partir de capteur ou d'autres telles que des entrées de l'utilisateur.

3.2-Le panier intelligent signe les données

Le panier intelligent signe les données à l'aide de sa clé privée pour garantir l'intégrité et la sécurité des données.

3.3-Les données sont envoyées à un nœud de la blockchain

Les données sont envoyées à un nœud de la blockchain à l'aide d'un protocole de communication sécurisé, tel que HTTPS ou MQTT.

3.4-Le nœud de la blockchain valide les données

Le nœud de la blockchain vérifie la validité des données en utilisant la clé publique de Le panier intelligent et en s'assurant que la transaction répond aux règles de consensus de la blockchain.

3.5-La transaction est ajoutée à la blockchain

Si la transaction est valide, le nœud de la blockchain l'ajoute à un nouveau bloc dans la blockchain. Ce bloc est validé par les mineurs avant d'être ajouté définitivement à la chaîne.

3.6-Le panier intelligent reçoit une confirmation

Le panier intelligent reçoit une confirmation que la transaction a été ajoutée à la blockchain et peut poursuivre ses opérations.

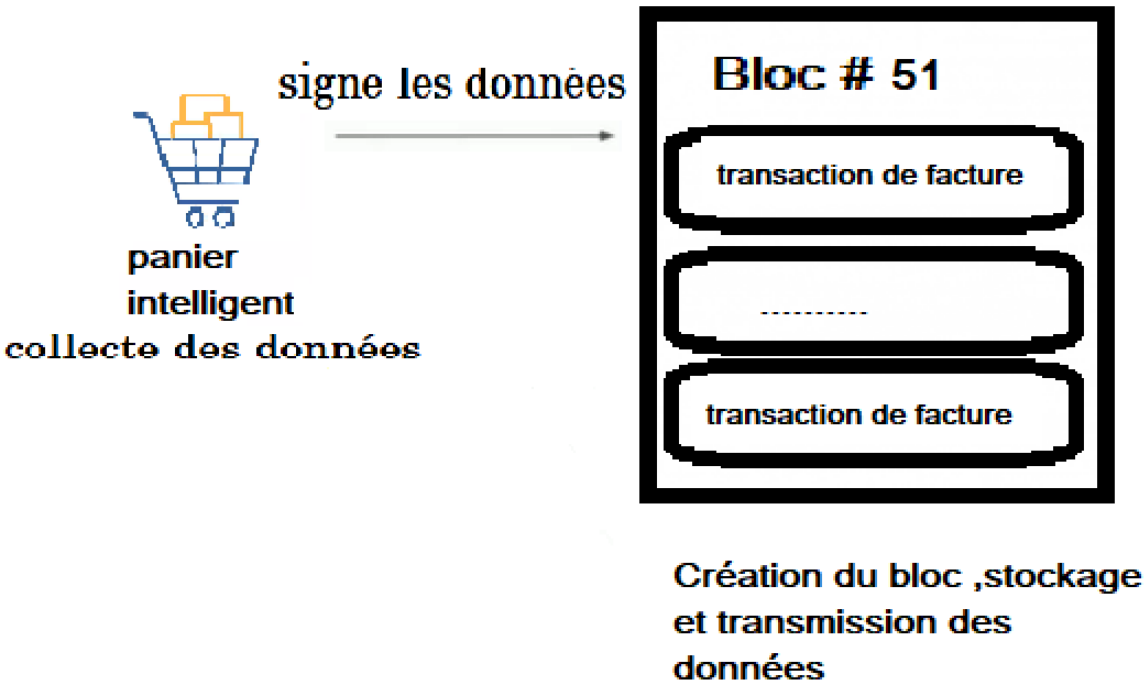

Figure 3.4-Les transactions sont regroupées dans un block par ordre chronologique.

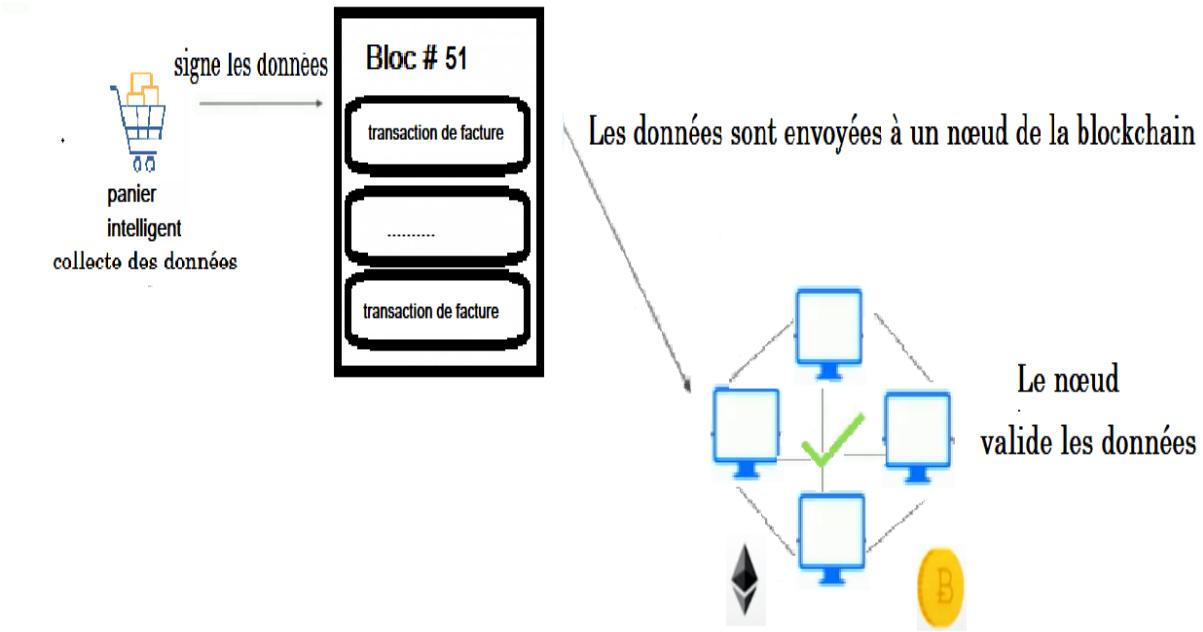

Figure 3.5-Le bloc de transaction est validé par des nœuds spéciaux .

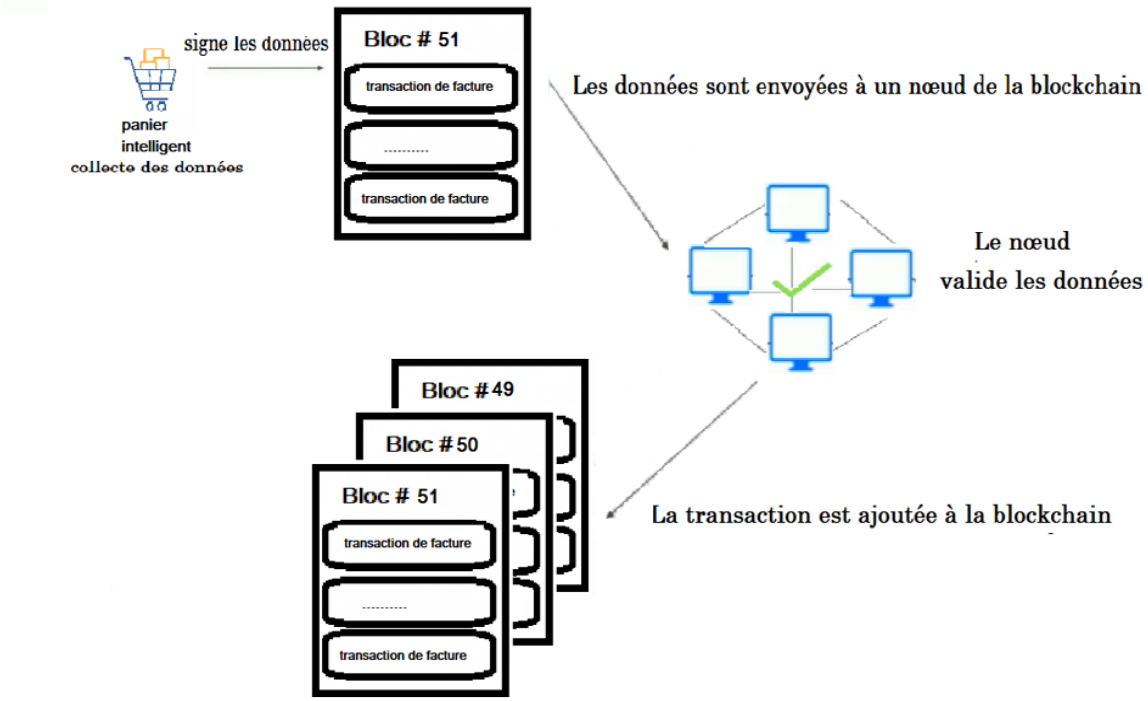

Figure 3.6- Blockchain en référant le hash du bloc #50 .il est ensuite broadcasté à l'ensemble des nœuds du réseau.

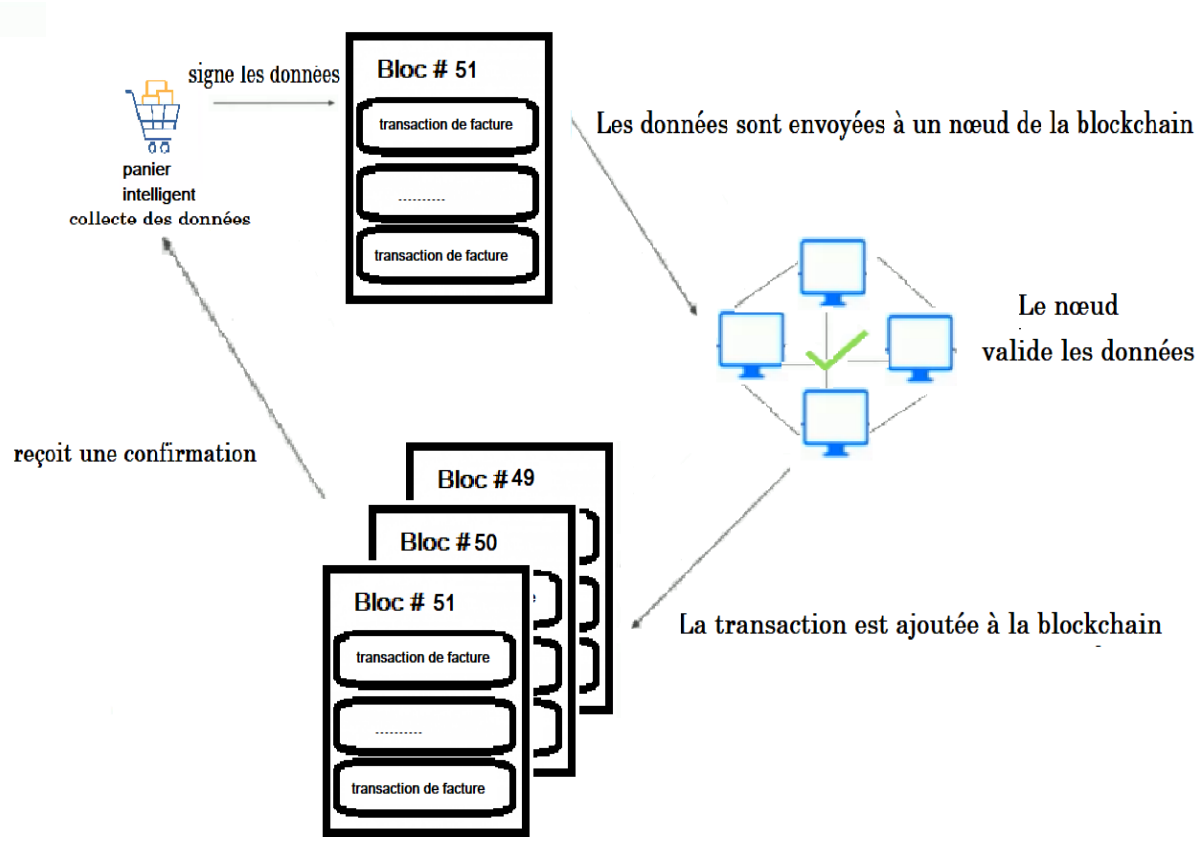

Figure 3.7-Le processus de communication de panier intelligent avec la blockchain.

4-Un scénario communication de panier intelligent avec la Banque

Alicia est une cliente régulière d'un supermarché qui propose des paniers intelligents. Elle se rend donc au supermarché et utilise un panier intelligent pour faire ses courses.

Alors qu'elle fait ses achats, le panier intelligent enregistre automatiquement les produits qu'elle ajoute à son panier et leur prix. L'écran intégré au panier lui permet de suivre en temps réel le montant total de ses achats.

Lorsqu'elle a terminé ses courses, Alicia se dirige vers la caisse pour payer. Au lieu de sortir sa carte bancaire, elle utilise l'application mobile de sa banque pour scanner le code QR présent sur l'écran du panier intelligent.

Le paiement est instantanément débité de son compte bancaire et la banque lui envoie une notification sur son téléphone portable pour confirmer la transaction.

La banque de Alicia utilise ensuite les informations de transaction stockées sur la blockchain pour analyser les habitudes d'achat de Alicia. Elle peut ainsi lui offrir des services personnalisés, tels que des offres spéciales pour les produits qu'elle achète régulièrement, ou lui proposer des solutions d'épargne ou d'investissement en fonction de ses habitudes de consommation.

Alicia apprécie la simplicité et la rapidité de son expérience de shopping avec le panier intelligent. Elle est également ravie de bénéficier des services personnalisés de sa banque, qui lui permettent de réaliser des économies et de mieux gérer son budget.

5-Synthèse

Dans ce chapitre, nous présentons un cadre sécurisé et robuste pour la mise en œuvre de l'IoT et Blockchain. Le cadre proposé utilise un système de confiance pour assurer l'ouverture et la traçabilité du système. L'utilisation de la technologie Blockchain dans l'Internet des Objets (IoT) peut fournir un système de confiance sécurisé et robuste pour la collecte, le stockage et le partage de données entre les appareils IoT. La blockchain permet de garantir la sécurité, l'intégrité et l'immutabilité des données, ce qui est particulièrement important dans les applications IoT où la confidentialité des données est primordiale.

Le système de confiance basé sur la blockchain peut être mis en place en utilisant un cadre qui comprend des capteurs IoT, des nœuds de la blockchain, des mineurs et des applications. Les capteurs collectent des données à partir des appareils IoT et les signent avec leur clé privée pour garantir leur intégrité et leur sécurité. Les données sont ensuite envoyées aux nœuds de la blockchain pour validation et stockage. Les mineurs vérifient les transactions et les ajoutent à la blockchain en utilisant des algorithmes de preuve de travail ou de preuve d'enjeu pour garantir la sécurité de la blockchain. Les applications peuvent accéder aux données stockées dans la blockchain et envoyer des commandes aux appareils IoT via la blockchain.

En utilisant ce système de confiance basé sur la blockchain, les clients peuvent se faire confiance et partager des informations en toute sécurité. Les données collectées par les capteurs IoT sont protégées contre l'accès non autorisé et les transactions sont stockées de manière immuable dans la blockchain, garantissant la traçabilité et l'intégrité des données. Cependant, il est important de souligner que la mise en place d'un tel système nécessite une expertise en matière de blockchain et d'IoT, ainsi que des mesures de sécurité supplémentaires pour prévenir les attaques potentielles.

Conclusion

En conclusion, le système de confiance basé sur la blockchain dans un panier intelligent peut offrir de nombreux avantages en garantissant la sécurité, la fiabilité et la transparence des données échangées entre les clients et les supermarchés.

Grâce à la technologie de la blockchain, les données du panier intelligent peuvent être stockées de manière sécurisée et immuable, garantissant ainsi leur intégrité et leur authenticité. Les clients peuvent également avoir un contrôle total sur leurs données, ce qui renforce leur confiance dans l'utilisation du panier intelligent.

De plus, la blockchain permet de créer un registre transparent et vérifiable de toutes les transactions et échanges de données effectués, ce qui permet de réduire les risques de fraude et d'assurer une meilleure gestion des données.

Cependant, il est important de souligner que la mise en place de la blockchain dans un panier intelligent nécessite une collaboration étroite entre les supermarchés et les fournisseurs de services blockchain, afin de garantir une utilisation efficace et adaptée de la technologie. Il est également crucial d'assurer la protection de la vie privée des clients et de mettre en place des mécanismes de sécurité appropriés pour éviter les attaques potentielles.

En somme, le système de confiance basé sur la blockchain dans un panier intelligent peut offrir des avantages significatifs pour garantir une utilisation sûre et fiable des paniers intelligents, mais il est important de prendre en compte les défis et les limites potentiels liés à sa mise en place.

Chapitre 04
Implémentation

Introduction :

Le chapitre précédent a couvert les aspects du système de confiance et son architecture. Dans ce nouveau chapitre, notre attention se tourne vers la mise en œuvre du système de paiement en utilisant des contrats blockchain. Nous explorerons les outils qui ont été utilisés pour développer ce système, et nous présenterons ensuite ses différents composants. L'implémentation d'un système de paiement basé sur des contrats blockchain. Il permet d'établir un environnement de confiance, de sécuriser les transactions et de garantir la transparence. En utilisant cette technologie, il devient possible de créer un écosystème de paiement décentralisé, où les transactions peuvent être effectuées en toute confiance, sans nécessiter l'intervention d'une tierce partie de confiance.
Le choix du langage de programmation et des outils est crucial pour la création d'un système robuste et sécurisé. Ils doivent être adaptés aux contrats intelligents et à la technologie blockchain, permettant ainsi de développer des fonctionnalités avancées et de garantir la sécurité des transactions.

1-Outils & Langages de programmation

Tout d'abord, les principaux outils que nous avons utilisés pour la réalisation de Notre système est le suivant :

Le compilateur Solidity est un outil logiciel qui traduit le code Solidity, un langage de programmation de haut niveau spécialement conçu pour écrire des contrats intelligents sur des plates-formes blockchain comme Ethereum, en bytecode pouvant être exécuté par la machine virtuelle Ethereum (EVM) ou d'autres machines virtuelles blockchain compatibles. [57]

Remix est un environnement de développement intégré (IDE) spécialement conçu pour le développement de contrats intelligents Ethereum. Il fournit une interface conviviale et une gamme d'outils puissants pour écrire, compiler, déployer et interagir avec des contrats intelligents sur la blockchain Ethereum.[58]

2-Implémentation et réalisation du système

Dans cette partie du chapitre, on offre une description bien détaillée de notre Système de paiement et illustrée avec des imprimes écrans de ses différentes pages.

2.1-Description du système

Notre système vise à permettre d'effectuer des transactions entre le client et le supermarché, sans nécessiter l'intervention d'un tiers de confiance. Grace aux contrats intelligents qui sont des programmes autonomes exécutés sur une blockchain, généralement utilisée sur des plateformes telles qu'Ethereum. Il permet également de fournir aux clients. De cette manière, on facilite de faire les transactions en toute sécurité, entre les clients et le supermarché.

2.2-Explication de programme

Ce programme est un contrat intelligent (smart contract) en Solidity qui implémente un système de paiement pour une supérette.

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.8.2 <0.9.0;

contract SupermarketPayment {
    uint256 invoice;
    address public owner; // Adresse de la propriétaire du supermarché
    mapping(address => uint256) public balances; // Cartographie pour stocker les soldes des clients

    event PaymentReceived(address indexed customer, uint256 amount); // Événement pour suivre les paiements reçus

    constructor() {     411890 gas 387200 gas
        owner = msg.sender; // Définir le propriétaire du contrat sur le déployeur
    }

    function deposit() external payable {     infinite gas

        require(msg.value > 0, "No payment amount provided"); // Assurez-vous d'un montant de paiement différent de zéro

     balances[msg.sender] += msg.value; // Ajouter le montant du paiement au solde du client

        emit PaymentReceived(msg.sender, msg.value); // Émettre un événement pour indiquer le paiement reçu
    }

    function withdraw(uint256 amount) external {     infinite gas
        require(amount > 0, "Invalid withdrawal amount"); // Assurez-vous d'un montant de retrait différent de zéro
        require(balances[msg.sender] >= amount, "Insufficient balance"); // S'assurer que le client a un équilibre suffisant

        balances[msg.sender] -= amount; // Soustraire le montant du retrait du solde du client

        // Transférer le montant demandé au client
        payable(msg.sender).transfer(amount);
    }

    function getBalance() external view returns (uint256) {     2504 gas
        return balances[msg.sender]; // Retourner le solde de l'appelant (client)
    }

    function retrieve() public view returns (uint256){     2481 gas
        return invoice;
    }
}
```

Figure 4.1-Le programme de système.

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.8.2 <0.9.0;

contract SupermarketPayment {
    uint256 invoice;
    address public owner; // Adresse de la propriétaire du supermarché
    mapping(address => uint256) public balances; // Cartographie pour stocker les soldes des clients

    event PaymentReceived(address indexed customer, uint256 amount); // Événement pour suivre les paiements reçus

    constructor() {    418696 gas 394000 gas
        owner = msg.sender; // Définir le propriétaire du contrat sur le déployeur
    }
```

Figure 4.2-La fonction représente l'adresse du propriétaire du supermarché.

- **"SPDX-License-Identifier : GPL-3.0"** : Indique la licence du contrat.
- **"pragma solidity >=0.8.2 <0.9.0;"** : Est une directive spécifie la version du compilateur Solidity à utiliser.
- **"SupermarketPayment"** : Est un contrat définit les fonctionnalités du système de paiement.
- **"invoice"** : Est une variable de type uint256 qui représente une facture.
- La variable **"owner"** est de type **"address"** et représente l'adresse du propriétaire de la superette.
- La mapping **"balances"** est utilisée pour stocker les soldes des clients. Chaque adresse de client est associée à un solde de type uint256.
- **Payments Received** : Est un événement défini pour suivre les paiements reçus par le contrat. L'événement prend deux paramètres :
  - ✓ L'adresse du client (client indexé)
  - ✓ Le montant du paiement (montant uint256).

- **Constructor** : Est une fonction définie pour initialiser le contrat. Il définit la variable propriétaire à l'adresse du déployer du contrat, qui est le compte qui a déployé le contrat sur la blockchain. C'est le début du contrat intelligent Super mark et Payments.

Le contrat déclare une variable uint256 appelée facture qui représente une facture ou certaines données liées au paiement du supermarché. Il déclare

également une variable d'adresse publique appelée « owner » qui représente l'adresse du propriétaire du supermarché.
Le mappage des soldes est déclaré pour stocker les soldes des clients. Il mappe l'adresse de chaque client à son solde, qui est de type uint256.

```
function deposit() external payable {    infinite gas

    require(msg.value > 0, "No payment amount provided"); // Assurez-vous d'un montant de paiement différent de zéro

balances[msg.sender] += msg.value; // Ajouter le montant du paiement au solde du client

    emit PaymentReceived(msg.sender, msg.value); // Émettre un événement pour indiquer le paiement reçu
}
```

Figure 4.3-La fonction d'effectuer un dépôt sur le contrat intelligent.

- **function deposit() external payable { ... }**: Cette fonction permet aux utilisateurs externes d'effectuer un dépôt sur le contrat intelligent. La fonction est marquée comme payable, ce qui signifie qu'elle peut recevoir Ether (la crypto-monnaie native d'Ethereum).cette fonction vérifie si le montant du paiement (msg.value) est supérieur à zéro. Si ce n'est pas le cas, il renvoie un message d'erreur indiquant qu'aucun montant de paiement n'a été fourni.

Si le montant du paiement est valide, il ajoute le montant du paiement au solde du client (msg.sender). La cartographie des soldes est utilisée pour garder une trace des soldes de chaque client. Il émet un événement appelé Payments Received avec l'adresse du client (msg.sender) et le montant du paiement (msg.value). L'émission d'un événement permet aux parties externes d'écouter et de répondre à cet événement.

```
function withdraw(uint256 amount) external {   infinite gas
    require(amount > 0, "Invalid withdrawal amount"); // Assurez-vous d'un montant de retrait différent de zéro
    require(balances[msg.sender] >= amount, "Insufficient balance"); // S'assurer que le client a un équilibre suffisant

    balances[msg.sender] -= amount; // Soustraire le montant du retrait du solde du client

    // Transférer le montant demandé au client
    payable(msg.sender).transfer(amount);
}
```

Figure 4.4- La fonction de retirer les fonds de solde dans le contrat intelligent.

- **function withdraw(uint256 amount) external { ... }**: C'est une fonction externe qui permet aux clients de retirer des fonds. Elle vérifie que le montant de retrait est supérieur à zéro et que le client a un solde suffisant. Elle soustrait le montant du retrait du solde du client et transfère le montant demandé à l'adresse du client.

Cette fonction ne transfère pas automatiquement les fonds retirés vers le portefeuille externe de l'utilisateur qui devra appeler une autre fonction ou interagir avec le contrat pour initier le transfert effectif de fonds.

- **payable(msg.sender).transfer(amount)** : transfère le montant demandé du contrat intelligent à l'adresse du client (msg.sender).

Le mot-clé payable est utilisé pour créer une adresse de paiement qui peut recevoir des fonds, et la fonction de transfert est utilisée pour transférer les fonds.

```
function getBalance() external view returns (uint256) {   2504 gas
    return balances[msg.sender]; // Retourner le solde de l'appelant (client)
}

function retrieve() public view returns (uint256){   2481 gas
    return invoice;
}
```

Figure 4.5-La fonction de montant et de facture

- **getBalance** : est une fonction d'affichage qui permet aux utilisateurs externes de récupérer leur solde actuel dans le contrat intelligent. Il renvoie le solde de l'appelant (le client) en accédant au mappage des soldes avec l'adresse de l'appelant (msg.sender).
- **function retrieve() public view returns (uint256){ ... }**: C'est une fonction d'affichage qui renvoie la valeur de la variable de facture. Cette variable représente certaines données ou valeurs stockées dans le contrat intelligent et est accessible publiquement.

Ces fonctions fournissent la fonctionnalité permettant de retirer des fonds, de vérifier le solde et de récupérer certaines données stockées dans le contrat intelligent.

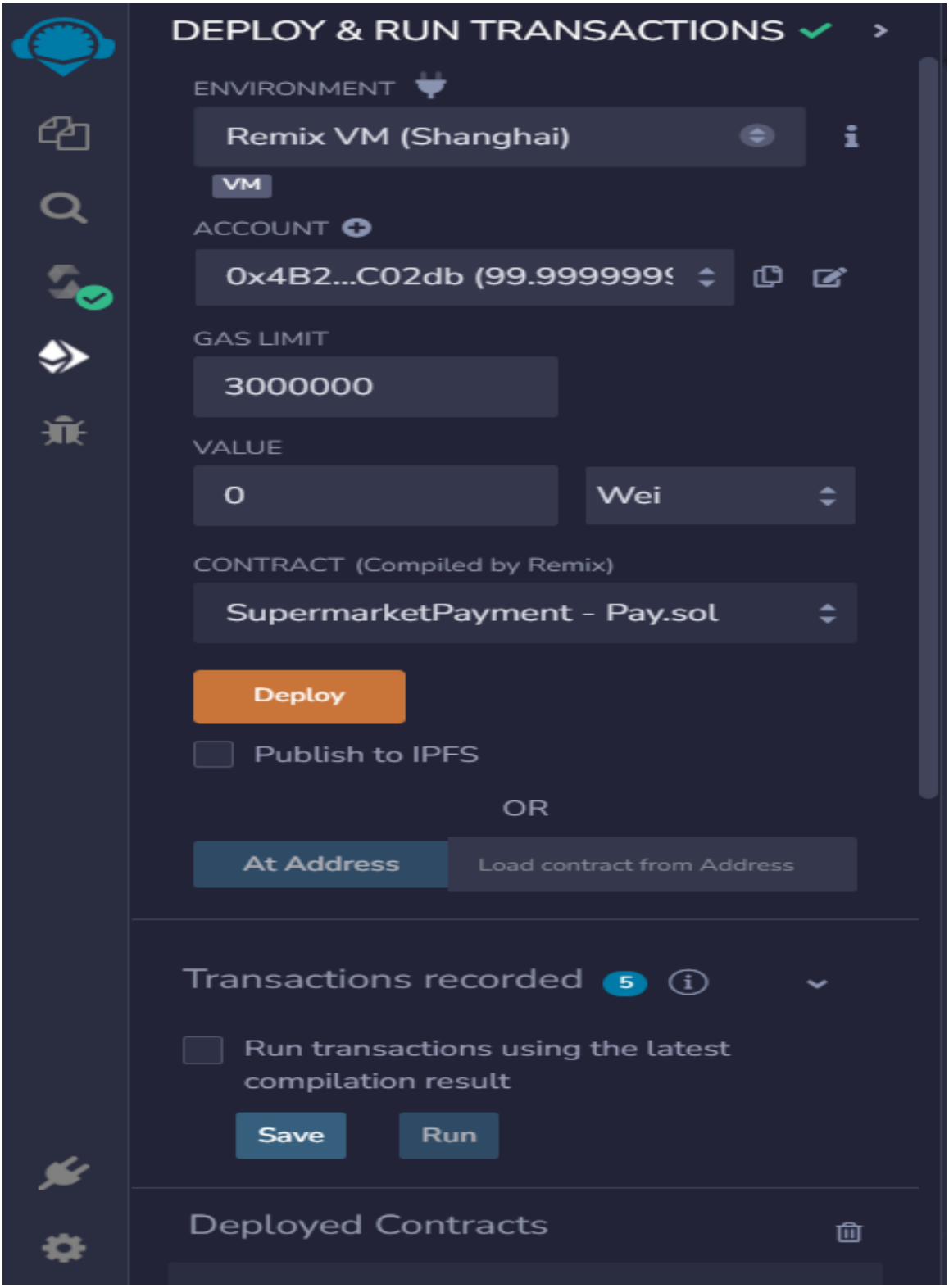

Figure 4.6-Teste de contrat .

Pour le teste de cette contrat sur Remix , il faut rendre dans l'onglet DEPLOY & RUN TRANSACTIONS . Remix permet de faire un appel aux différentes fonctions des contrats que nous avons déployés.

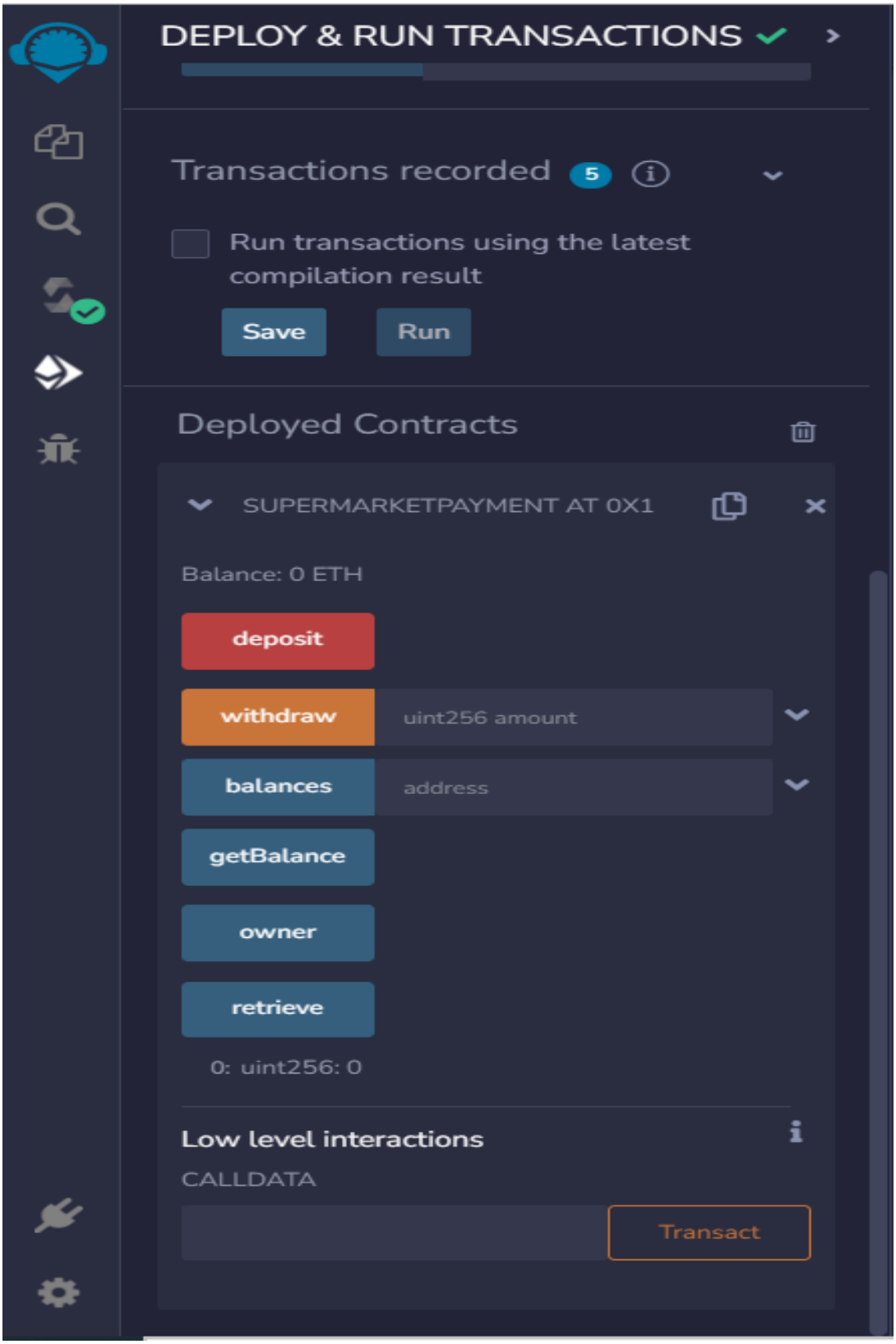

Figure 4.7- Les fonctions de contrat .

Dans la partie deployed contracts on retrouve les fonctions de contrat.

Figure 4.8-la transaction validée.

Cette figure représente que la transaction validée.

Conclusion

Ce chapitre a abordé la mise en œuvre du système de paiement à l'aide de contrats blockchain, en partant des détails du système de confiance et de l'architecture évoqués dans le chapitre précédent. Nous avons examiné le langage et les outils utilisés pour créer ce système, mettant en évidence ses divers composants.
La mise en œuvre d'un système de paiement basé sur des contrats blockchain offre de nombreux avantages, notamment la transparence, la sécurité et la traçabilité des transactions. En utilisant cette technologie, il devient possible de créer un écosystème de paiement décentralisé, où les transactions peuvent être effectuées en toute confiance et sans nécessiter l'intervention d'une tierce partie de confiance. Le langage et les outils choisis pour mettre en place ce système sont essentiels pour garantir son bon fonctionnement. Ils doivent être adaptés aux contrats intelligents et à la technologie blockchain, permettant ainsi de programmer des fonctionnalités avancées et d'assurer la sécurité des transactions.

La mise en œuvre du système de paiement à l'aide de contrats blockchain constitue une avancée significative dans la transformation des processus de paiement traditionnels. Grâce à la transparence et à la sécurité offertes par cette technologie, il est possible de créer un environnement de confiance pour les transactions, favorisant ainsi l'adoption de nouvelles solutions de paiement décentralisées.

Conclusion Générale

1-Conclusion générale

L'objectif de ce projet c'est l'utilisation de la technologie de la blockchain pour créer un système de confiance dans le contexte de l'Internet des objets (IoT), tel qu'un panier intelligent, présente plusieurs avantages significatifs.

Tout d'abord, la blockchain offre un registre décentralisé, sécurisé et immuable pour enregistrer les transactions et les événements liés au panier intelligent. Cela permet d'assurer l'intégrité des données et de créer une source fiable de vérité. Les informations telles que les achats, les paiements et les interactions avec le panier intelligent peuvent être enregistrées de manière transparente et vérifiable.

Ensuite, la blockchain permet d'établir un système de confiance entre les différentes parties impliquées, qu'il s'agisse des utilisateurs, des fournisseurs ou des autres acteurs de l'écosystème. Grâce à la nature décentralisée de la blockchain, les transactions peuvent être exécutées en peer-to-peer, éliminant ainsi le besoin d'intermédiaires de confiance et réduisant les coûts associés.

De plus, l'utilisation de contrats intelligents sur la blockchain facilite l'automatisation des processus et l'exécution des accords prédéfinis. Les contrats intelligents peuvent être programmés pour effectuer des actions spécifiques en réponse à des conditions prédéfinies, ce qui permet d'automatiser les paiements, la gestion des stocks, les réapprovisionnements, etc., dans le contexte du panier intelligent.

Enfin, la blockchain offre également la possibilité de mettre en œuvre des fonctionnalités de traçabilité et de suivi des produits tout au long de la chaîne d'approvisionnement. Cela permet aux utilisateurs du panier intelligent de vérifier l'origine des produits, de s'assurer de leur qualité et de garantir leur provenance de manière transparente.

Cependant, il est important de noter que l'implémentation d'un système de confiance basé sur la blockchain dans le contexte de l'IoT, comme le panier intelligent, présente également des défis. La gestion de la scalabilité, de la sécurité, de l'interopérabilité et des coûts reste des aspects critiques à prendre en compte lors du développement et du déploiement d'une telle solution.

En résumé, l'utilisation de la technologie blockchain pour créer un système de confiance dans le contexte de l'IoT, tel qu'un panier intelligent, offre des avantages considérables en termes de transparence, de sécurité et d'automatisation des processus. Cela ouvre de nouvelles opportunités pour améliorer l'efficacité, la confiance et l'expérience des utilisateurs dans des domaines tels que le commerce de détail, la logistique et la gestion de la chaîne d'approvisionnement. Cependant, une analyse approfondie des exigences, une conception soignée et une mise en œuvre rigoureuse sont nécessaires pour exploiter pleinement le potentiel de cette technologie dans le domaine de l'IoT.

2. Perspectives

Nous n'avons travaillé que dans sa version initiale, et il est toujours ouvert aux améliorations et à la comparaison du travail avec d'autres, notre système peut être encore amélioré en collectant plus d'ensembles de données telle que le client achète dans un plusieurs panier intelligent dans le même supermarché. La traçabilité de tout l'opération de client stoker pour un processus d'analyse de donné qui aide augmente la qualité de service aux niveaux supermarché.

Références Bibliographiques

[1] Internet of Things Security : Principles and Practice Editeur : Qinghao Tang, Springer Verlag, Singapore ; 1st ed. 2021 édition (28 janvier 2021) ISBN-10 : 9811599416 ISBN-13 : 978-9811599415

[2] De Luna Almeida, A., Aknine, S., Briot, J. P., & Malenfant, J. (2006, December). A predictive method for providing fault tolerance in multi-agent systems. In 2006 IEEE/WIC/ACM International Conference on Intelligent Agent Technology (pp. 226-232). IEEE.

[3] Dony, C., Urtado, C., & Vauttier, S. (2006). Exception handling and asynchronous active objects: Issues and proposal. Advanced Topics in Exception Handling Techniques, 81-100.

[4] Kchir, S. (2010). MÉMOIRE DE STAGE DE MASTER M2.

[5] Ductor, S., Guessoum12, Z., & Ziane13, M. (2009). Gestion des ressources et réplication adaptative pour fiabiliser les SMA. to appear) Rencontre des Jeunes Chercheurs en Intelligence Artificielle, 5.

[6] Faci, N., Guessoum, Z., & Marin, O. (2006, May). Dimax: A fault-tolerant multi-agent platform. In Proceedings of the 2006 international workshop on Software engineering for large-scale multi-agent systems (pp. 13-20).

[7] Uribe, J. D. J. R., Guillen, E. P., & Cardoso, L. S. (2021). A technical review of wireless security for the internet of things: Software defined radio perspective. Journal of King Saud University-Computer and Information Sciences.

[8] Abou El Houda, Z., Hafid, A., & Khoukhi, L. (2019, December). Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain

using SDN. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE..

[9] Abou El Houda, Z., Khoukhi, L., & Hafid, A. (2018, December). Chainsecure-a scalable and proactive solution for protecting blockchain applications using sdn. In 2018 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[10] Moudoud, H. (2022). Intégration de la Blockchain à l'Internet des Objets.

[11] Kang, H., Chang, X., Mišić, J., Mišić, V. B., Yao, Y., & Chen, Z. (2020). Stochastic modeling approaches for analyzing blockchain: A survey. arXiv preprint arXiv:2009.05945.

[12] Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2021). An Overview of Blockchain and 5G Networks. Computational Intelligence in Recent Communication Networks, 1-20.

[13] Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, January). Survey of consensus protocols on blockchain applications. In 2017 4th international conference on advanced computing and communication systems (ICACCS) (pp. 1-5). IEEE.

[14] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. Int. J. Netw. Secur., 19(5), 653-659.

[15] Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2021, June). Towards a scalable and trustworthy blockchain: Iot use case. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[16] Kaleem, M., & Shi, W. (2021). Demystifying pythia: A survey of chainlink oracles usage on ethereum. In Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25 (pp. 115-123). Springer Berlin Heidelberg.

[17] Abbas, K., Tawalbeh, L. A. A., Rafiq, A., Muthanna, A., Elgendy, I. A., El-Latif, A., & Ahmed, A. (2021). Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. Security and Communication Networks, 2021.

[18] Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63, 102364.

[19] Maroufi, M., Abdolee, R., & Tazekand, B. M. (2019). On the convergence of blockchain and internet of things (iot) technologies. arXiv preprint arXiv:1904.01936.

[20] B. Al Kurdi, H. Elrehail, and H. M. Alzoubi, "THE INTERPLAY AMONG HRM PRACTICES, JOB SATISFACTION AND INTENTION TO LEAVE : AN EMPIRICAL INVESTIGATION," no. August, 2021.

[21] H. M. Alzoubi, G. Ahmed, A. Al-Gasaymeh, and B. Al Kurdi, "Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration," Manag. Sci. Lett., vol. 10, no. 3, pp. 703–708, 2020, doi: 10.5267/j.msl.2019.9.008.

[22] H. M. Alzoubi and R. Aziz, "Does emotional intelligence contribute to quality of strategic decisions? The mediating role of open innovation," J. Open Innov. Technol. Mark. Complex., vol. 7, no. 2, 2021, doi: 10.3390/joitmc7020130.

[23] S. Joghee, H. M. Alzoubi, and A. R. Dubey, "Decisions effectiveness of FDI investment biases at real estate industry: Empirical evidence from Dubai smart city projects," Int. J. Sci. Technol. Res., vol. 9, no. 3, pp. 3499–3503, 2020.

[24] Rajesh Kumar ⇑, Rewa Sharma Leveraging blockchain for ensuring trust in IoT: A survey Computer Engineering, J.C. Bose University of Science & Technology, YMCA, 6, Mathura Road, Faridabad 121006, Haryana, India.

[25] Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2021, June). Towards a scalable and trustworthy blockchain: Iot use case. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[26] Kaleem, M., & Shi, W. (2021). Demystifying pythia: A survey of chainlink oracles usage on ethereum. In Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25 (pp. 115-123). Springer Berlin Heidelberg.

[27] Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., & Kastania, A. (2018, July). Astraea: A decentralized blockchain oracle. In 2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 1145-1152). IEEE.

[28] Y. Malahov Z. Hess and J. Pettersson. aternity . (2017). a blockchain for scalable, secure and decentralized apps.

[29] Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2021, December). Towards a secure and reliable federated learning using blockchain. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 01-06). IEEE..

[30] Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial IoT. IEEE Transactions on Industrial Informatics, 15(6), 3632-3641.

[31] Debe, M., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2019). IoT public fog nodes reputation system: A decentralized solution using Ethereum blockchain. IEEE Access, 7, 178082-178093.

[32] Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. The Journal of Supercomputing, 75, 4372-4387.

[33] Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, 126-142.

[34] Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications, 143, 167-177.

[35] Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. The Journal of Supercomputing, 75, 4372-4387.

[36] Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., & Ylianttila, M. (2019, May). Blockchain based proxy re-encryption scheme for secure IoT data sharing. In 2019 IEEE international conference on blockchain and cryptocurrency (ICBC) (pp. 99-103). IEEE.

[37] She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access, 7, 38947-38956.

[38] Pham, H. A., Le, T. K., & Le, T. V. (2019, September). Enhanced security of IoT data sharing management by smart contracts and blockchain. In 2019 19th International Symposium on Communications and Information Technologies (ISCIT) (pp. 398-403). IEEE.

[39] Pham, H. A., Le, T. K., & Le, T. V. (2019, September). Enhanced security of IoT data sharing management by smart contracts and blockchain. In 2019 19th International Symposium on Communications and Information Technologies (ISCIT) (pp. 398-403). IEEE.

[40] Rehman, M., Javaid, N., Awais, M., Imran, M., & Naseer, N. (2019, December). Cloud based secure service providing for IoTs using blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.

[41] Abou El Houda, Z., Hafid, A. S., & Khoukhi, L. (2019). Cochain-SC: An intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract. IEEE Access, 7, 98893-98907.

[42] Chaganti, R., Bhushan, B., & Ravi, V. (2022). The role of Blockchain in DDoS attacks mitigation: Techniques, open challenges and future directions. arXiv preprint arXiv:2202.03617.

[43] Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A., & Shekhar, S. (2018, April). Continuous security in IoT using blockchain. In 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP) (pp. 6423-6427). IEEE.

[44] Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., & Gaiti, D. (2014, November). Denial of service (dos) attacks detection in manets using bayesian classifiers. In 2014 IEEE 21st Symposium on communications and vehicular technology in the Benelux (SCVT) (pp. 7-12). IEEE.

[45] Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., & Wang, Z. (2018). Consortium blockchain-based malware detection in mobile devices. IEEE Access, 6, 12118-12128.

[46] Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing, 18(5), 2438-2455.

[47] Goel, A., Agarwal, A., Vatsa, M., Singh, R., & Ratha, N. (2019). DeepRing: Protecting deep neural network with blockchain. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 0-0).

[48] Fadaeddini, A., Majidi, B., & Eshghi, M. (2020). Secure decentralized peer-to-peer training of deep neural networks based on distributed ledger technology. The Journal of Supercomputing, 76, 10354-10368.

[49] Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. (2018, December). When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In 2018 IEEE international conference on big data (big data) (pp. 1178-1187). IEEE.

[50] Mendis, G. J., Wu, Y., Wei, J., Sabounchi, M., & Roche, R. (2020). A blockchain-powered decentralized and secure computing paradigm. IEEE Transactions on Emerging Topics in Computing, 9(4), 2201-2222.

[51] Kouzinopoulos, C. S., Giannoutakis, K. M., Votis, K., Tzovaras, D., Collen, A., Nijdam, N. A., ... & Katsikas, S. (2018, July). Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust. In 2018 Innovations in Intelligent Systems and Applications (INISTA) (pp. 1-6). IEEE.

[52] Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). Inclusive block chain protocols. In Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19 (pp. 528-547). Springer Berlin Heidelberg.

[53] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Wattenhofer, R. (2016). On Scaling Decentralized Blockchains: (A Position Paper). In Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers 20 (pp. 106-125). Springer Berlin Heidelberg.

[54] Cimorelli, F., Priscoli, F. D., Pietrabissa, A., Celsi, L. R., Suraci, V., & Zuccaro, L. (2016, June). A distributed load balancing algorithm for the control plane in software defined networking. In 2016 24th Mediterranean Conference on Control and Automation (MED) (pp. 1033-1040). IEEE.

[55] Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access, 7, 118541-118555.

[56] Singh, P. K., Singh, R., Nandi, S. K., & Nandi, S. (2019). Managing smart home appliances with proof of authority and blockchain. In Innovations for Community Services: 19th International Conference, I4CS 2019, Wolfsburg, Germany, June 24-26, 2019, Proceedings 19 (pp. 221-232). Springer International Publishing.

[57] Solidity — Documentation Solidity 0.6.8 (solidity-fr.readthedocs.io)

[58] Remix - Ethereum IDE & community (remix-project.org)