L'utilisation de la blockchain pour la sécurité de l'internet des objets.

Khalid Nassiri, El Arbi Abdellaoui Alaoui, Youssef Mejdoub, Youssef Rachdi

L'utilisation de la blockchain pour la sécurité de l'internet des objets.

Khalid NASSIRI[1] , El Arbi ABDELLAOUI ALAOUI[2] , Youssef MEJDOUB[3], Youssef Rachdi[4]
nasskhalid@gmail.com[1], abdellaoui.e@gmail.com[2], ymejdoub@yahoo.fr[3], yousefrachdi@gmail.com[4]

RESUME :

D'ici 2020, l'Institut Gartner, la célèbre compagnie de recherche en technologie de l'information, estime que le nombre des objets connectés sur le marché pourrait atteindre 50 milliards. Les maisons intelligentes, comme une application typique d' IdO, fournissent des dispositifs avec diverses applications pratiques, mais sont confrontés à des problèmes de sécurité et de confidentialité. la technologie Blockchain (BC) a apporté une solution potentielle au problème de la sécurité IdO. L'émergence de cette technologie a provoqué un changement de la gestion décentralisée, fournissant une solution efficace pour la protection de la sécurité du réseau et la confidentialité. Dans cet article, nous proposons une modélisation de la blockchain par la théorie des hypergraphes. Les objectifs de ce modèle sont de réduire la consommation de stockage et de résoudre les problèmes de sécurité supplémentaires.

Mots clés : Internet des objets, hypergraphe. sécurité, stockage, maison intelligente, blockchain, réseaux.

INTRODUCTION

L'Internet des objets (IdO) est un réseau mondial d'objets interconnectés qui, grâce à des programmes, sont capables d'interagir les uns avec les autres et coopérer avec leurs voisins pour atteindre des objectifs communs. L'objectif principal de l'IdO est de partager les informations acquises par des objets dans plusieurs domaines à savoir; la fabrication, le transport, la consommation et d'autres détails de la vie des gens [1 , 2].

L'application la plus populaire pour IdO est la maison intelligente, qui offre une meilleure qualité de vie en introduisant le contrôle de l'appareil automatisé et des services d'assistance. Des dispositifs IdO fonctionnent en collaboration et optimisent le confort de l'utilisateur en utilisant la connaissance du contexte et des contraintes prédéfinies en fonction des conditions de l'environnement domestique. Les maisons intelligentes offrent des services de confort et de sécurité à leurs habitants [3]. Parmi ceux-ci, le plus important est la sécurité, qui fournit non seulement des services d'authentification à l'utilisateur, mais également l'accès limité non autorisé aux dispositifs du ménage [4]. De plus en plus de renseignements personnels sont recueillis et communiqués dans le réseau intelligent à domicile (et peut-être avec d'autres réseaux câblés et sans fil), les questions de sécurité et de confidentialité sont devenues plus prononcées et doivent être sérieusement prises en compte afin d'exploiter tout le bénéfices de l'environnement domestique intelligent.

Dans cet article, nous nous concentrons sur la réduction de la capacité de stockage des appareils IdO et la sécurité et la confidentialité des flux de données dans les systèmes de la maison intelligente.

La technologie Blockchain offre un moyen d'améliorer la sécurité intelligente à domicile en utilisant le grand livre des données transmises d'une maison à une autre maison et prévenir les communications anormales.

2- OUTILS ET ENVIRONNEMENT

2.1- IdO et Maison Intelligente

En tant que champ d'application émergente qui combine plusieurs technologies, IdO et maisons intelligentes se combinent pour réaliser la gestion intelligente de l'environnement de maison moderne en intégrant diverses puces intelligentes dans l'équipement de la maison. Un système intelligent de la maison est un environnement informatique typique omniprésent, mais il y a beaucoup de problèmes qui doivent être résolus.
Chifor et al. [5] a proposé une pile d'autorisation légère pour les applications smart maison IdO et l'architecture est centrée sur l'appareil de l'utilisateur. La recherche récente Dorri [6 , 7] Ont étudié IdO et maisons intelligentes basée sur blockchain et ont présenté une mise en œuvre légère d'une BC particulièrement adaptée pour une utilisation dans IdO.

2.2- Blockchain

La technologie Blockchain est apparue au début de 2009 avec le crypto-devise Bitcoin (BTC). les utilisateurs Bitcoin utilisent une clé publique variable (PK) pour générer des informations sur les transactions et la diffuser au réseau pour le transfert de fonds. Les informations de transaction sont stockées par tous les utilisateurs dans son propre bloc. Une fois que le bloc est plein, un processus d'exploration de réseau est effectué; la valeur de hachage du bloc est calculée, et les informations chiffrées et les blocs sont ajoutées à la blockchain. Pour exploiter la valeur de hachage cryptographique d'un bloc, certains nœuds du réseau, connus sous le nom des mineurs, en concurrence pour résoudre une preuve de travail appelée casse-tête cryptographique de la consommation des ressources (POW) [8]. Le nœud qui permet de résoudre d'abord le casse-tête et obtient l'approbation de tout le monde est considéré comme ayant exploité le bloc. Cela est dû au fait que la technologie blockchain conserve tous les comptes de

données de transaction parmi tous les membres, et que tous les membres mettent à jour les comptes simultanément pour maintenir l'exhaustivité lorsque de nouvelles transactions se produisent. Internet et les technologies de cryptage sont les technologies sous-jacentes qui permettent à tous les membres de vérifier la fiabilité de chaque transaction afin de résoudre un point de défaillance unique provoqué par une transaction autorisée par un tiers traditionnel. La blockchain a la caractéristique d'être exempte de courtier (P2P), de sorte que la transaction élimine les coûts non autorisés pour le tiers. Puisque tout le monde maintient les informations de transaction synchronisées, l'effet de piratage des enregistrements en mode point unique devient très limité et ne fonctionne souvent pas. En outre, les utilisateurs d'un système blockchain peuvent ouvertement avoir accès aux enregistrements de transaction et de réduire les coûts de surveillance des transactions. Étant donné que la valeur de hachage stockée dans chaque homologue du bloc est affectée par la valeur du bloc précédent, la falsification et la modification des données nécessitent la modification de la chaîne entière et la quantité de calcul en un point est loin derrière le calcul de l'ensemble du réseau. En conséquence, la contrefaçon est presque impossible.

Le réseau de blockchains est constitué de nombreux périphériques intelligents. Chaque périphérique est considéré comme un nœud. Le nœud blockchain contient une liaison de données comme représenté sur la figure 1. Chaque liaison de données comprend plusieurs blocs de données qui contiennent la valeur de hachage du bloc précédent et des informations de transaction en tant que données de bloc.

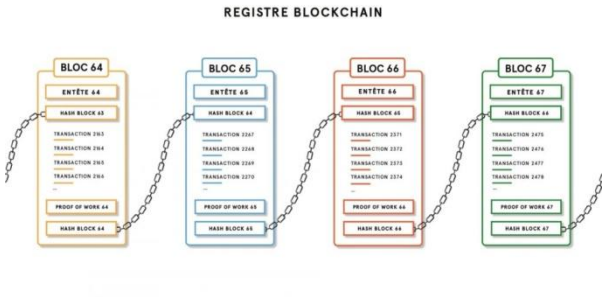

fig1

2.3- Hypergraphe

Au cours des dernières décennies, la théorie de l'hypergraphe s'est révélée utile pour résoudre des problèmes du monde réel. En tant qu'outil mathématique, les hypergraphes peuvent être utilisés pour simuler des réseaux informatiques, des réseaux biologiques, des structures de données, des ordonnancements de processus et divers autres systèmes. Les objets du système et les relations complexes qui les unissent peuvent souvent être cartographiés par des hypergraphes, de manière à rechercher une solution efficace à divers problèmes complexes [9]. Pour des applications dans l'IoT, Jung et al. ont proposé une structure multidimensionnelle basée sur l'hypergraphe pour modéliser l'IoT afin de permettre une gestion et une découverte efficaces des objets IoT [10].

Un hypergraph *H* noté par *H(E;V)* sur un ensemble fini *V*. $E(e_i)_{i\epsilon I}$, où I est un ensemble d'indices finis, est un sous-ensemble de *V* appelé hyperarête. généralement, *V* est un ensemble de sommets notée *V (H)* et *E* notée par *E (H).* Si deux sommets sont dans une hyperarête, ils sont appelés adjacents. La cardinalité d'une hyperarête notée $|e_i|$ est le nombre de sommets dans l' hyperarête. Le rang de *H* noté $r(H) = max_{i\epsilon I}|e_i|$ est la cardinalité maximale des hyperarête dans l'hypergraphe; la cardinalité minimale des hyperarête appelée le co-rang de *H* est notée $cr(H) = min_{i\epsilon I}|e_i|$. Deux hyperarêtes dans un hypergraphe sont adjacents si leur intersection n'est pas vide. Le degré d'un sommet est le nombre d'hyperarêtes qui l'incluent. Et le degré maximum est défini comme le degré du graphe.

3- LA BLOCKCHAIN BASEE SUR L'HYPERGRAPHE

3.1- Positionnement du problème

Nous concevons un modèle de blockchain amélioré afin de réaliser la solution précédente. Dans ce modèle, les nœuds du réseau de blockchain sont divisés en plusieurs clusters, chacun avec la même chaîne d'enregistrement de transaction. En même temps, en raison de la nature dynamique du réseau de blockchain, comme dans l'environnement IoT, il n'est pas possible de formuler de manière statique les clusters de nœuds enregistrant les transactions. Pour des raisons de sécurité et de confidentialité, les nœuds qui enregistrent les transactions apparaissent dans le réseau de blockchain de manière aussi anonyme que possible. La théorie de l'hypergraphe nous fournit un modèle mathématique de la conception structurelle.

- *Nœuds* : un nœud est un périphérique avec une capacité de stockage dans un réseau blockchain. La route est accessible dans le réseau et la communication normale peut être effectuée. Chaque nœud du réseau appartient à au moins une hyperarête et peut appartenir à plusieurs hyperarête en même temps.
- *Mineurs* **:** les mineurs sont des dispositifs permettant de calculer les clés de chiffrement de hachage de bloc dans le réseau blockchain, qui n'est pas très différent des mineurs ordinaires.
- *Hyperarête* : Une hyperarête est un ensemble de nœuds. Tous les nœuds du même hyperarête ont le même vecteur qui est indépendant des autres quantifications, et ils ont synchronie lors de l'enregistrement des données de transaction.

3.2- Paramètres du réseau

Dans l'architecture conçue, les nœuds peuvent appartenir à plusieurs hyperarêtes en même temps, et les nœuds dans la même hyperarête sont synchronisés dans le processus de stockage d'enregistrement de transaction, ce qui conduira à la mémorisation simultanée de plusieurs nœuds dans plusieurs hyperarêtes. Afin de rendre la distribution de stockage des enregistrements de transaction plus équilibrée et éviter l'effet Matthew (c'est-à-dire que certains nœuds de la plupart des hyperarêtes stockent de grandes quantités de données, mais que d'autres sont tout au contraire), le degré de chaque nœud du réseau spécifié doit être N, ce qui peut être considéré comme un paramètre de réseau. Selon cette idée, un enregistrement de transaction est enregistré par certains nœuds du réseau blockchain.

Par conséquent, dans l'architecture conçue, un enregistrement de transaction est enregistré par les nœuds dans une hyperarête. Étant donné que le nombre de nœuds dans l'hyperarête peut être déséquilibré, les limites inférieure et supérieure du nombre de nœuds indiqué par le co-rang et le rang doivent être spécifiées. Les nœuds nouvellement ajoutés au réseau doivent être ajoutés simultanément à N hyperarêtes. Si le nombre de nœuds sur une hyperarête a atteint la limite supérieure, l'hyperarête doit être scindé en deux hyperarête.

3.3- Nœud Blockchain

Sur la base de l'architecture proposée, l'ensemble du mécanisme de travail du réseau de chaînes de blocs est différent de celui d'origine. Ainsi, la structure de données du nœud dans l'hypergraphe et la fonction de stockage doivent être redéfinies.

Étant donné qu'un nœud appartiendra simultanément à plusieurs hyperarêtes en même temps et que les nœuds de chaque hyperarêtes nécessitent une synchronisation de stockage, ils doivent également stocker les informations de transaction synchronisées dans différents hyperarête. Dans ce cas, si la structure originale de la blockchain est adoptée, les blocs de données dans les nœuds ne seront plus les mêmes. Lorsque le bloc en cours est plein et doit être chiffré, les valeurs de hachage calculées par chaque nœud sont toujours différentes. Cela conduit à la défaillance de l'ensemble du réseau.

La structure de stockage dans chaque nœud est conçue en deux parties: la tête de chaîne et les sous-chaînes. La tête de blockchain est construite par une matrice d'indépendance linéaire, un vecteur et une liste de blockchain. La matrice d'indépendance linéaire est une matrice entière d'ordre N composée de N vecteurs linéairement indépendants, chacun d'eux mappant sur une hyperarête comme caractéristique. N représente le nombre d'hyperarêtes dans le réseau. Cela signifie que pour chaque hyperarête du réseau blockchain, un vecteur à N dimensions est associé. Le vecteur peut être considéré comme l'identifiant de l'hyperarête. La raison pour laquelle nous utilisons une matrice d'indépendance linéaire est que, lorsque le réseau évolue, il est difficile de générer un nouvel ID pour une nouvelle hyperarête de manière synchrone, mais il est facile de générer un vecteur d'indépendance linéaire à partir d'une matrice d'indépendance linéaire.

La blockchain-list contient plusieurs index de blockchains. Chaque index pointe vers une sous-chaîne. Le nombre de sous-chaînes est égal au degré du nœud. Une subblockchain est une sorte de chaîne de chaînes avec une tête dans laquelle se trouve un vecteur à N dimensions en tant que caractéristique d'hyperge. Chacune des sbublockchain stocke des enregistrements de transaction synchrones séparément dans l'hyperarête, dont le vecteur de caractéristiques est identique au vecteur de la tête de sous-chaîne. Par conséquent, les nœuds d'une même hyperarête doivent avoir une même sous-chaîne de blocs (subblockchain).

4-MECANISME DE TRAVAIL

Lorsqu'une transaction est effectuée, le nœud source construit un enregistrement qui comprend les informations suivantes: horodatage, le vecteur indépendamment linéaire sélectionné (un vecteur entier à N dimensions) et les informations communes, telles que les parties à la transaction, le contenu de la transaction, nécessaires à la sauvegarde. Ce qui nécessite une attention particulière est que le nœud source trouve de manière aléatoire un vecteur différent du vecteur d'indépendance linéaire dans sa propre tête de sous-chaîne de la matrice d'indépendance linéaire. Et ajouter ce vecteur à l'enregistrement en tant que fonction d'enregistrement.

Tout d'abord, lorsqu'une transaction se produit, tous les nœuds du réseau reçoivent la déclaration et la recherche sur les enregistrements relatifs à leurs subblockchains. Les nœuds qui ont stocké les dernières informations de transaction du nœud source obtiennent le droit d'arbitrage. Les nœuds d'arbitrage vérifient la déclaration. Si c'est légal, les nœuds d'arbitrage envoient un message indiquant que la transaction est légale pour le réseau; sinon, un message indiquant que la transaction est illégale sera envoyé. Il est différent du mécanisme de la blockchain d'origine dans lequel chaque nœud possède l'enregistrement complet et peut vérifier la déclaration par lui-même. Dans notre modèle, la vérification est effectuée par certains des nœuds, qui envoient le résultat à d'autres.

Après avoir reçu les messages de vérification, les nœuds du réseau peuvent juger de la légitimité des transactions en fonction du rapport entre la cardinalité

moyenne et le nombre de messages reçus, ainsi que du rapport entre le certificat légal et le nombre de certifications illégales. Simplement, pour un seuil donné, si le nombre de messages légaux dépasse le seuil, la transaction est considérée comme légale. La sécurité des messages est garantie par un système à clé secrète.

Lorsqu'une transaction se produit, les nœuds du réseau blockchain comparent le vecteur caractéristique enregistré avec les vecteurs dans sa propre tête de subblockchain. Si correspondance et la transaction est vérifiée pour être légal, l'enregistrement est ajouté au bloc actuel subblockchain correspondant.

Lorsque le bloc actuel d'une certaine sous-chaîne d'un certain nœud est plein, conformément au principe de fonctionnement de la blockchain, des données du bloc complet en cours, de la valeur de hachage du bloc précédent et d'autres informations seront publiées sur le réseau. Tous les mineurs recevront ces données et calculeront une valeur de hachage de cryptage de manière compétitive. Lorsqu'un mineur résout le casse-tête, il le publie sur le réseau et les nœuds qui acquièrent ce prisonnier de guerre vérifient facilement le résultat. Si le résultat est acceptable, le bloc sera chiffré et stocké, sinon le résultat sera abandonné et le calcul se poursuivra.

Comme mentionné dans notre modèle, les enregistrements sont stockés séparément et presque personne ne possède la copie complète des recodages, ce qui est différent du stockage distribué comme [11], qui utilise un schéma de codage pour réduire la capacité de stockage et assurer la totalité des enregistrements intégrité dans chaque nœud. Cela entraîne les risques de sécurité supplémentaires suivants:

- Les attaques sur les nœuds de stockage peuvent être plus faciles que dans le réseau original de la blockchain;
- Une attaque de vérification tentera de forger le message juridique et d'augmenter le ratio légal;
- Des attaques peuvent être provoquées par la création d'une nouvelle hyperarête et la modification des enregistrements enregistrés par celle-ci.

5- Application de la domotique

nous appliquons le modèle de blockchain basé sur l'hypergraphe proposé au système de maison intelligente. La recherche sur les systèmes de maison intelligente se divise principalement en deux catégories : les interactions entre les appareils de la maison et les interactions entre les maisons en tant que nœuds indépendants. Dans l'environnement domestique intelligent, le nombre d'appareils internes est généralement maintenu à un ordre de grandeur inférieur et le système de blockchain ne peut pas être pleinement utilisé. Les réseaux domestiques intelligents à domicile couvrent souvent plus de nœuds, offrant un environnement approprié pour les applications en chaîne. Par conséquent, le modèle proposé dans cet article s'applique principalement aux réseaux de maisons intelligentes avec des maisons en tant que nœuds indépendants (la passerelle de la maison peut être considérée comme un accès de connexion). Dans l'étude de cas d'utilisation, chaque domicile est considéré comme un nœud, les communications et les accès distants entre eux sont mappés en tant que transactions. Dans un système de maison intelligente, les gestionnaires de maison intelligente peuvent être considérés comme des passerelles et des gestionnaires de maison. De même, ils sont traités comme des nœuds dans le réseau de chaînes de maisons. Ces nœuds stockent non seulement des données mais peuvent également être des mineurs. Voici les études de cas pour discuter des avantages du modèle : La communication et l'accès.

CONCLUSION

Nous avons modélisé le réseau de blockchain par un hypergraphe. Nous avons considéré chaque maison comme un nœud du graphe et avons utilisé la théorie de l'hypergraphe pour actualiser le stockage du réseau pour les enregistrements. Le modèle de blockchain basé sur l'hypergraphe proposé dans le présent document peut être appliqué aux maisons intelligentes et peut faciliter le maintien des exigences de sécurité et de protection de la vie privée.

Bibliographie

[1] Tao, M.; Zuo, J.; Liu, Z.; Castiglione, A.; Palmieri, F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Gener. Comput. Syst. 2018.

[2] Li, H.; Tian, Y.; Liu, Y.; Li, T. UAI-IOT framework: A method of uniform interfaces to acquire information from heterogeneous enterprise information systems. In Proceedings of the IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 724–730.

[3] Tao, M.; Ota, K.; Dong, M. Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes. Future Gener. Comput. Syst. 2017, 76, 528–539.

[4] Chen, Z.H.; Zhang, F.G.; Zhang, P.; Liu, J.K.; Huang, J.W.; Zhao, H.B.; Shen, J. Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control. Future Gener. Comput. Syst. 2018, 87, 712–724.

[5] Chifor, B.C.; Bica, I.; Patriciu, V.V.; Pop, F. A security authorization scheme for smart home internet of things devices. Future Gener. Comput. Syst. 2018, 86, 740–749.

[6] Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[7] Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. In Proceedings of the International Conference on Internet-Of-Things Design and Implementation, Pittsburgh, PA, USA, 18–20 April 2017; pp. 173–178.
[8] Gervais, A.; Karame, G.O.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the ACM SigsacConference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 3–16.
[9] Bretto, A. Hypergraph Theory; Springer: Cham, Switzerlands, 2013.
[10] Jung, J.; Chun, S.; Lee, K.H. Hypergraph-based overlay network model for the internet of things. In Proceedings of the IEEE World Forum on Internet of Things, Milan, Italy, 14–16 December 2015; pp. 104–109.
[11] Raman, R.K.; Varshney, L.R. Dynamic distributed storage for scaling blockchains. arXiv 2017, arXiv:1711.07617.