PROPOSITION SUJETS DE THESES

CONTRATS DOCTORAUX 2020-2023

Appel ciblé (merci de cocher la case correspondante):

☒ **Contrat doctoral ministériel ED 536**

☐ **Contrat doctoral ministériel ED 537**

Directeur de thèse : Abderrahim BENSLIMANE

Co-directeur éventuel :

Co-encadrant éventuel :

Titre en français : Contribution à la sécurité et la vie privée dans l'Internet des Objets basée sur BlockChain : Robustesse, fiabilité et passage à l'échelle.

Titre en anglais : Contribution to security and privacy in the Internet of Things based on Blockchain: Robustness, reliability and scalability.

Mots-clés : Sécurité, Cryptographie, Algorithmique Distribué, Réseaux informatique, outils mathématiques (méta heuristiques, programmation linéaire, Federated Machine Learning).

Co tutelle : Oui - Non **Pays :**

Opportunités de mobilité à l'international du doctorant dans le cadre de sa thèse : oui

Profil du candidat : Master Informatique

Objectifs

Ce sujet concerne la sécurité de l'Internet des Objets (IoT) basée sur la BlockChain.

Notre objectif est de concevoir un système, avec des méthodes et outils, robuste basé sur la Block-Chain pour sécuriser les réseaux IoT en leur permettant de supporter les fonctions dédiées à la sécurité (telles que cryptographie, gestion des clés, contrôle d'accès et identification) et de palier aux pro-blèmes de stockage, tout en les gérant (accès et contrôle) de façon distribuée.

Une implémentation d'un prototype basé sur FPGA est programmée.

Les verrous à lever portent principalement sur les performances du système et les coûts de la mise en place. Une étude sera donc menée dans ce sens pour étudier les apports de notre solution ainsi que ses limites.

Contexte

Plus de soixante-quinze milliards d'appareils dans le monde devraient être connectés les uns aux autres d'ici 2025, ce qui représente un défi majeur pour la nouvelle ère de la technologie numérique que le monde est sur le point d'entrer. En raison de ce grand nombre croissant d'appareils connectés à Internet, de leur grande connectivité, de leur diversité, de leur hétérogénéité, et du fait que ces appareils sont incapables de supporter des protocoles de sécurité complexes et lourds, un certain nombre de défis en matière de sécurité et de protection des renseignements personnels se posent.

Pour répondre à ces défis, nous proposons d'introduire le concept de la BlockChain pour sécuriser les systèmes IoT.

La convergence BlockChain/IoT apportera beaucoup d'avantages ; cependant, ils restent encore beaucoup de défis concernant la sécurité, le stockage et la vie privée à résoudre. Par conséquent, ce travail de recherche, à la fois exploratoire et testbed, a pour objectif principal de proposer une nouvelle architecture IoT pour fournir une sécurité robuste avec une capacité de stockage illimitée qui peut être adapté aux contraintes de ressources IoT en introduisant un nouveau composant de gestion de sécurité et de stockage dans la BlockChain.

La BlockChain s'appuie sur une méthode de consensus pour valider toute nouvelle donnée. La plus part des méthodes de consensus de différents cryptocurrencies demande une puissance de calcul très élevée et alors ne sont pas adéquats pour des systèmes à ressources contraintes.

Ainsi, nous discuterons les mesures possibles qui peuvent être prises pour réduire la puissance de calcul et le temps de convergence pour les méthodes de consensus.

Le Proof Of Work (Proof of Capacity, Proof of Elapsed Time) ou Proof of Stake (Delegated, Leased, Importance, Activity, Casper, Burn) ou tout autre algorithme de consensus qui est utilisé dans le minning de BlockChain pour trouver le bon hachage et pour préserver l'intégrité du réseau, dépense beaucoup de temps, d'énergie et de ressources. En consacrant ces ressources à la maintenance du réseau et à l'ajout de blocs à la BlockChain, les mineurs sont récompensés par l'actif cryptographique pour lequel ils calculaient les hachages. Pour IoT, il n'en est pas claire comment ces récompenses peuvent être gérées.
La BlockChain avec sa nature décentralisée, sécurisée, cryptée et transparente est considérée comme le meilleur système à utiliser dans différents aspects. Cependant, La Blockchain fait toujours face à plusieurs problèmes ; la BlockChain n'a pas été conçue pour transporter des données volumineuses, les transactions dans la BlockChain doivent être publiques pour que les mineurs puissent les valider ce qui entraîne un manque important de confidentialité et aussi la croissance rapide de Blockchain qui af-

fecte les appareils de IoT (Internet of Things) qui ont des ressources limitées en stockage, énergie, calcul, etc.

Ainsi, la Blockchain a été évaluée pour être le meilleur système à utiliser avec les dispositifs IoT puisque que toutes les données et les transactions des dispositifs IoT seront stockées dans un environnement sécurisé et bénéficiera d'un registre distribué « distributed ledger ». Par ailleurs, la convergence IoT-Blockchain a soulevé divers défis. La Blockchain sera copiée dans chaque appareil IoT. Comme la Blockchain croît très rapidement et les dispositifs IoT sont limités en ressources, ce défi peut créer un gros problème de stockage dans les dispositifs IoT. En outre, la Blockchain n'a pas été conçu pour transporter des données massives et les transactions dans la Blockchain doivent être publiques aux mineurs pour les valider, alors ce processus conduit à un grand manque de confidentialité.

Etat de l'art

Concernant les architectures IoT/BlockChain

Les auteurs dans [1] ont proposé une gestion décentralisée des données IoT en utilisant le concept de Blockchain et un environnement d'exécution fiable « Intel SGX », pour assurer la sécurité des données et la confidentialité du système. Cependant, l'inconvénient de l'utilisation de SGX est sa mémoire limitée. SGX est un ensemble d'extensions de processeur à la conception x86 d'Intel qui permet la création d'environnements d'exécution isolés appelés enclaves, et ces enclaves résident dans une zone de mémoire protégée appelée Enclave Page Cache (EPC). EPC est actuellement limitée à 128 Mo [2]. En outre, la solution proposée ne résout pas le problème d'évolutivité, de sorte que leur système peut être appliqué seulement si les données ne sont pas nécessaires immédiatement ; les fonctions sont exécutées à un moment ultérieur dans la Blockchain. En outre, les passerelles IoT sont ceux qui stockent le hachage des données dans la Blockchain et les données principales dans SGX. Ainsi, c'est comme si les données sont envoyées à partir des dispositifs IoT au SGX sans passer par la BlockChain.

Hossein et al. [2] présentent pour les applications IoT-Blockchain, un cadre de stockage de données distribué, qui garantit que la propriété des données IoT reste entre les mains des intervenants. Dorri et al. [3] présentent les lacunes des méthodes actuelles de sécurité et de protection de la vie privée, et contribuent avec LSB, a Lightweight Scalable BlockChain for IoT Security and Privacy, qui est une chaîne de blocs évolutive et légère pour l'IoT, en ce qui concerne la sécurité et à la protection de la vie privée. Ces protocoles LSB légers réduisent la bande passante et les coûts de calcul.
Cependant, dans les deux articles [2] et [3], les détails architecturaux et les répercussions sur la performance ne sont pas abordés en particulier, pour ce qui est de la contrainte des ressources des plateformes de IoT.

Les auteurs de [4] ont proposé une nouvelle architecture de cloud BlockChain distribuée qui est basée sur BlockChain, Fog et SDN. Elle fournit une solution efficace pour gérer les données qui sont produites

par les appareils IoT dans le nuage distribué et aussi à la bordure du réseau. Cependant, le modèle ne propose aucun schéma pour réduire la consommation énergétique.

Par conséquent, notre travail se veut de proposer une architecture différente puisque notre travail de recherche envoie les données à la Blockchain et le nouveau composant qui réside dans la BlockChain est celui qui gère et stocke, de façon sécurisée, les données dans le cloud avec un espace de stockage illimité.

A notre connaissance, nous sommes les premiers à vouloir proposer une telle architecture IoT sécurisée avec la BlockChain, robuste et permettant le passage à l'échelle. L'idée elle-même ainsi qu'une conception embryonnaire a été publiée dans une conférence internationale IEEE Globecom en Décembre 2019, Hawaii, USA [5]. Un brevet a aussi été déposé en France est en cours de validation.

Méthodologie

Nous proposons une nouvelle architecture IoT BlockChain, où nous introduirons un nouveau composant gestionnaire de sécurité et de stockage qui permet d'offrir une sécurité puissante qui optimise à la fois le problème du stockage des données dans la BlockChain et le problème de la confidentialité et de la sécurité. Le concept repose à la fois sur le cryptage des données principales qui seront stockées dans des blocs verrouillés et dispersés sur l'internet (cloud) et le stockage de juste quelques données utiles dans la BlockChain.

Selon des modes particuliers de réalisation et en fonction des contraintes particulières sur les ressources, nous proposons les tâches suivantes :

- Tâche 1 : Après étude et comparaison des différentes architectures de IoT/BlockChain, nous proposerons un nouveau module pour traiter et stocker les données reçu. De nature, la BlockChain est complexe surtout lorsqu'elle est complétement distribuée ; l'enjeu est d'adapter la BlockChain pour une utilisation légère dans IoT à cause de la limitation des ressources.

- Tâche 2 : Après étude de la complexité (tout en tenant compte du caractère ressource limité) et comparaison des différents algorithmes de cryptographie (exemple : ECC (Elliptic-Curve Cryptography) ou AES (Advanced Encryption Standard), etc.), nous proposerons d'intégrer un hachage des données en utilisant une fonction de hachage adéquate pour créer une signature numérique des données. Le problème est la complexité ainsi, l'enjeu majeur ici est de minimiser la consommation d'énergie.

- Tâche 3 : Nous concevons un contrat intelligent « smart contract » pour permettre à la Blockchain de gérer l'accès aux données de l'IoT de manière décentralisée. En d'autre terme, le contrat intelligent vérifiera la politique d'accès à la BlockChain, définira qui a le droit d'écrire et de lire dans la BlockChain.

- Tâche 4 : Après étude et comparaison des différents consensus existants utilisés la BlockChain en général et appliqués à IoT en particulier, nous souhaitons proposer un nouveau algorithme de consensus auquel nous avons pensé récemment. C'est une technique nouvelle à laquelle nous pensons et que nous souhaitons étudier plus théoriquement et implémenter dans le cadre de projet. La plus part des méthodes de consensus demandent une puissance de calcul très élevée et alors ne sont pas adéquats pour des systèmes à ressources contraintes.

Références bibliographiques

1. G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment", IEEE International Conference on Information Reuse and Integration (IRI), 6-9 July 2018.
2. Ben A Fisch, Dhinakaran Vinayagamurthy, Dan Boneh , and Sergey Gorbunov, "Iron: Functional Encryption using Intel SGX", ACM SIGSAC Conference on Computer and Communications Security, October 2017.
3. H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards BlockChain-based Auditable Storage and Sharing of IoT Data," *NSDI 2017 - 14th USENIX Symposium* on *Networked Systems Design* and. *Implementation*, Mar *2017*, Boston, USA.
4. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," IEEE Symposium on Security and Privacy, 2017.
5. S. Benouar, A. Benslimane, "Robust Blockchain for IoT Security", IEEE Globecom 2019, CISS - Communication & Information Systems Security Symposium, IEEE Global Communications Conference, 9-13 December 2019, Waikoloa, HI, USA.

Les sujets devront être adressés à

secretariat-ed@univ-avignon.fr

avant le 8 avril 2020