Preuve vérifiable pour une blockchain embarquée basse consommation

Quentin Jayet, Christine Hennebert, Yann Kieffer, Vincent Beroulle

Preuve vérifiable pour une blockchain embarquée basse consommation

Quentin JAYET
Univ . Grenoble Alpes
CEA, LETI, DSYS
38000, Grenoble, France
quentin.jayet@cea.fr

Christine HENNEBERT
Univ . Grenoble Alpes
CEA, LETI, DSYS
38000, Grenoble, France
christine.hennebert@cea.fr

Yann KIEFFER
Univ. Grenoble Alpes
Grenoble INP, LCIS
26000 Valence, France
yann.kieffer@lcis.grenoble-inp.fr

Vincent BEROULLE
Univ. Grenoble Alpes
Grenoble INP, LCIS
26000 Valence, France
vincent.beroulle@lcis.grenoble-inp.fr

***Abstract*—Dans la blockchain Bitcoin, la confiance repose sur le protocole de Nakamoto basé sur le mécanisme de preuve de travail. Ce mécanisme permet de garantir qu'au moins un des pairs du réseau sera en mesure de proposer son bloc dans l'intervalle de temps fixé séparant deux blocs consécutifs. Cette garantie est fondamentale pour que le système soit disponible à ses utilisateurs. L'inconvénient de cette solution réside dans la consommation excessive d'énergie qu'elle engendre. Dans ce papier, une autre solution est envisagée, basée sur l'usage de composants de sécurité matérielle pour garantir la confiance à basse consommation.**

***Index Terms*—Cybersécurité, Embarqué, Blockchain, Temps écoulé, Composants de sécurité matérielle, Basse consommation**

I. Introduction

La blockchain forme un historique de transactions authentifiées, ordonnées et horodatées sur lequel tous les noeuds validateurs doivent s'accorder. Chacun des noeuds dispose à son niveau, localement, d'une copie complète de cet historique répliqué de façon instantanée dans le réseau distribué.

Ainsi, la blockchain est un protocole de consensus entre dispositifs physiques asynchrones et indépendants formant un réseau distribué sans autorité de confiance. Le but de ce protocole est de fournir la confiance, si possible par construction, pour permettre l'ajout d'un nouveau bloc de transactions à l'historique, et ceci dans un intervalle de temps déterminé, afin d'assurer la disponibilité du système. La garantie qu'une solution répondant aux critères du consensus sera trouvée dans le temps imparti est appelée la **finalité**. Le terme blockchain fait référence à la structuration des transactions en blocs successifs chainés de façon cryptographique pour protéger l'intégrité de l'historique formant un registre partagé et répliqué.

Chaque bloc de la figure 1 comprend un contenu et une entête. Le contenu se compose de l'ensemble des transactions effectuées par différents utilisateurs du système, a priori depuis la validation du bloc précédent. L'entête inclut plusieurs éléments, chacun assurant une propriété de sécurité à l'ensemble.

Les transactions sont structurées au sein d'un bloc selon un arbre de Merkle. L'empreinte racine figure dans l'entête pour garantir l'intégrité des transactions du bloc. L'empreinte d'un bloc est inscrite dans le bloc suivant pour former la chaine et garantir l'ordonnancement. Chaque bloc est horodaté.

Ce travail est une action de recherche collaborative soutenue par l'Agence Nationale de la Recherche (ANR) dans le cadre du programme « investissements d'avenir » ANR-10-AIRT-05, irtnanoelec

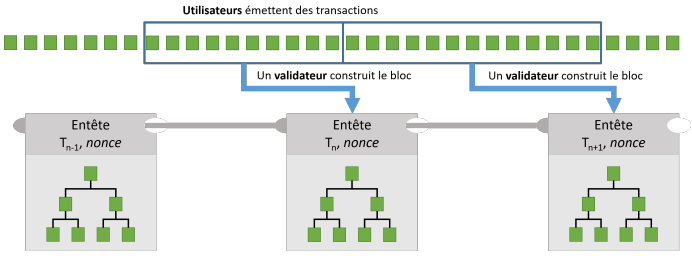

Fig. 1. Ordonnancement des transactions dans une blockchain

A ce stade, l'élément de l'entête qui retient notre attention est la *preuve*, qui permet de garantir la propriété de finalité et désigner le noeud validateur légitime pour ajouter *son* bloc. Dans la blockchain Bitcoin, cet élément est un *nonce* permettant à ses pairs de vérifier que le noeud légitime a bien effectué la preuve de travail (*Proof-of-Work*, PoW). Ce mécanisme garantit la finalité en assurant statistiquement qu'un *nonce* sera trouvé comme solution au challenge cryptographique donné, et ceci dans l'intervalle de temps entre deux blocs successifs. Mais, la PoW assure la finalité au détriment d'une consommation excessive d'énergie, le challenge requérant des calculs s'apparentant à de la brute force cryptographique. Pour résoudre ce problème, des solutions se basant sur une preuve de temps écoulé et des composants matériels de sécurité ont ainsi émergé.

Dans la suite de ces travaux, nous présenterons l'état de l'art ainsi que notre approche pour adresser la problématique de construction d'une preuve vérifiable d'un temps écoulé en embarqué qui réponde aux exigences de sécurité et de basse consommation pour garantir la finalité.

II. État de l'art

A. Consensus basé sur le temps écoulé

L'idée d'utiliser des composants de sécurité matérielle pour garantir un intervalle de temps, au lieu d'effectuer un très grand nombre de calcul cryptographique, a émergé en 2016 avec le papier [5] dans lequel Milutinovic présente la preuve de chance (*Proof of Luck*, PoL).

Dans la suite, Intel a proposé une implémentation avec la preuve de temps écoulé (*Proof of Elapsed Time*, PoET)[1]

[1]https://www.hyperledger.org/blog/2016/11/02/meet-sawtooth-lake

lors du déploiement d'Hyperledger Sawtooth[2]. Cette preuve se base sur l'enclave sécurisée SGX d'Intel, qui fournit une zone de confiance (*Trusted Execution Environnement*, TEE) pour l'exécution d'un code informatique. Mais cette implémentation n'est pas adaptée au contexte embarqué car il nécessite des processeurs présents au sein d'ordinateurs.

Dans PoET, les noeuds validateurs génèrent un temps d'attente aléatoire au sein d'un TEE. Chaque noeud validateur se met en veille pour la durée tirée au sort. Le premier qui se réveille est légitime pour ajouter son bloc à la blockchain. En 2017, Chen dans [4] a démontré que l'implémentation du protocole PoET dans Hyperledger Sawtooth est vulnérable lorsqu'une faible proportion des validateurs est compromise.

Bowman dans [2] démontre formellement qu'un protocole de consensus basé sur un temps écoulé peut être robuste. Pour cela, l'auteur décrit une version simplifiée de PoL et PoET basée sur l'usage de TEE.

B. Attestation basée sur des composants de sécurité matérielle

Dans [1], Salimitari propose une étude sur les différentes blockchains utilisables dans un contexte IoT. Trois protocoles de consensus sont mis en avant : PoET, Tangle et PBFT. Le protocole PBFT requière un grand nombre de communications dans un réseau de noeuds synchrones, ce qui rend délicat son passage à l'échelle. Avec Tangle, les transactions sont validées *à l'unité* pour diminuer la consommation énergétique. Mais les validateurs ne disposent pas d'une copie complète de l'historique et dépendent d'un coordinateur central. Le protocole PoET est mieux adapté dans un contexte distribué, mais la nécessité d'utiliser SGX restreint son usage.

Dans [3], Ankergård propose de lier le principe d'auto-attestation à distance avec le temps d'attente de PoET. Il crée ainsi une blockchain permettant d'attester un ensemble de dispositifs IoT prédéfini à l'initialisation du système mais ne pouvant évoluer avec l'ajout de nouveaux dispositifs.

Dans la suite, notre approche consiste à construire une preuve de temps écoulé se basant sur des composants de sécurité matérielle standardisés intégrés dans un System-on-Module (SoM) comprenant plusieurs microcontrôleurs, un TPM (*Trusted Platform Module*) et un TEE (*ARM TrustZone*).

III. Cadre expérimental

A. Objectif

L'objectif est de créer une preuve vérifiable d'un temps écoulé afin de garantir la finalité au sein d'un réseau distribué de dispositifs IoT ou Edge asynchrones et contraints.

La mesure d'un intervalle de temps par le système numérique doit être cohérente avec la grandeur physique du temps qui passe et la vérification doit être simple et efficace.

B. Preuve de concept

Pour cela, le déploiement d'une preuve de concept est envisagée selon l'architecture présentée sur la figure 2.

Cette architecture va permettre de modéliser, d'implémenter et d'expérimenter différents types de preuves de temps écoulé,

[2]https://sawtooth.hyperledger.org/

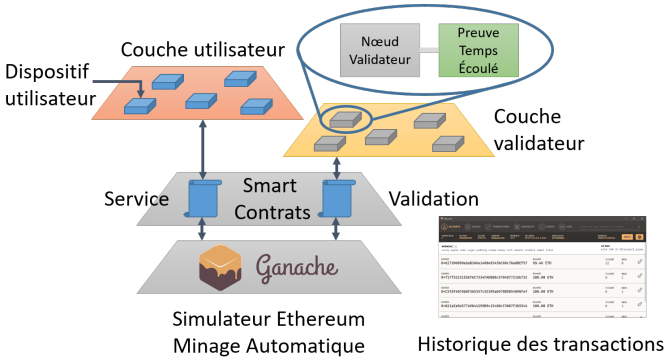

Fig. 2. Première architecture d'une preuve de concept

depuis celles existantes telles que la PoL ou PoET, jusqu'à celles que nous allons concevoir.

Sur la couche utilisateur, des clients envoient des transactions vers la blockchain. A intervalle de temps réguliers, un bloc doit être ajouté à la chaine. Ce sont les dispositifs validateurs figurant sur la couche validateur qui assurent ce rôle. Ces dispositifs pourront être simulés ou physiques avec le développement de SoM dédiés. L'usage de smart contracts, codés dans un langage turing-complet, exécutés sur le simulateur Ethereum Ganache va permettre de bénéficier de souplesse pour modéliser et implémenter le protocole de consensus et observer son comportement.

IV. Conclusion

Dans ce papier, nous posons les fondements qui motivent l'intérêt du sujet de la construction d'une preuve vérifiable permettant de garantir la finalité à basse consommation dans un réseau de dispositifs IoT asynchrones. Grâce au travail effectué par Bowman dans [2], nous défendons la thèse qu'une implémentation sécurisée, basée sur l'usage de composants de sécurité matérielle, est envisageable. Aussi, nous proposons une architecture permettant d'explorer la question et d'interpréter les résultats à venir.

References

[1] Salimitari, M., & Chatterjee, M. (2018). A survey on consensus protocols in blockchain for IoT networks. arXiv preprint arXiv:1809.05613.

[2] Bowman, M., Das, D., Mandal, A., & Montgomery, H. (2021). On elapsed time consensus protocols. In Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22 (pp. 559-583). Springer International Publishing.

[3] Ankergård, S. F. J. J., Dushku, E., & Dragoni, N. (2022, June). PERMANENT: Publicly Verifiable Remote Attestation for Internet of Things Through Blockchain. In Foundations and Practice of Security: 14th International Symposium, FPS 2021, Paris, France, December 7–10, 2021, Revised Selected Papers (pp. 218-234). Cham: Springer International Publishing.

[4] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (poet). In Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19 (pp. 282-297). Springer International Publishing.

[5] Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016, December). Proof of luck: An efficient blockchain consensus protocol. In Proceedings of the 1st Workshop on System Software for Trusted Execution (pp. 1-6).