Conception et Implémentation d'une Blockchain Légère

Proposition de sujet de stage recherche, niveau M2
Année universitaire 2023 – 2024

Contacts	arthur.baudet@lcis.grenoble-inp.fr
Encadrement	Arthur Baudet, Oum-El-Kheir Aktouf, Annabelle Mercier
Lieu	Laboratoire de Conception et d'Intégration des Systèmes (lcis.fr) à Valence
Mots clefs	Blockchain, Implémentation, Algorithme de consensus, Optimisation taille mémoire

Description

Ce stage porte sur la conception et l'implémentation d'une Blockchain pouvant être utilisée dans des réseaux de systèmes embarqués. Dans le cas de travaux de thèse portant sur la sécurisation de réseaux décentralisés de systèmes embarqués autonomes [1] réalisés au LCIS, la question de l'utilisation d'une Blockchain a été soulevée pour le partage d'informations critiques. Or, la décentralisation et l'autonomie de ses systèmes empêchent l'utilisation des Blockchains existantes (Bitcoin, Ethereum, etc.) ainsi que l'utilisation de tiers pour le maintien de la Blockchain. Il devient donc nécessaire de déployer une Blockchain *décentralisée* et *légère* capable d'être maintenue directement par ses participants à ressources limitées (calcul, mémoire et énergie). Une implémentation incluant un algorithme de consensus léger a été réalisée mais une recherche plus approfondie quant à la consommation de mémoire et de stockage est nécessaire. Certains travaux industriels [2] et académiques [3] s'intéressent déjà à cette problématique, il est donc question de se les approprier et de fournir une solution s'en inspirant.

Cahier des charges

Le ou la stagiaire aura la charge de proposer, puis d'implémenter, une architecture de Blockchain adaptée aux contraintes des systèmes embarqués : limite de puissance de calcul, d'espace mémoire et de stockage, et d'énergie. Cette architecture pourra notamment comprendre :

- Un algorithme de consensus pour l'addition de blocs ;
- Une structure de données pour la Blockchain ;
- Un algorithme de consensus pour la résolution de forks ;
- Un algorithme d'optimisation de la taille de la structure de données pour prévenir la croissance infinie de Blockchain (telle qu'on la voit dans les Blockchains classiques).

Ce thème étant vaste, une focalisation sur un point précis sera nécessaire.

Livrables

Il sera attendu du ou de la stagiaire de fournir :

- Un rapport faisant état des technologies liées aux Blockchains (Veille technologique) ;
- Une proposition d'architecture de Blockchain ;
- Une preuve de concept de l'architecture définie en début de stage.

Bibliographie

[1] Arthur BAUDET et al. « MAKI : A Multi-Agent Public Key Infrastructure ». In : *15th International Conference on Agents and Artificial Intelligence*. T. 3. 2023, p. 177-184. DOI : 10.5220/0011631800003393.

[2] J.D. BRUCE. *The Mini-Blockchain Scheme*. Whitepaper. Cryptonite, 2017. URL : https://cryptonite.info/files/mbc-scheme-rev3.pdf (visité le 21/09/2023).

[3] Emanuel PALM, Olov SCHELÉN et Ulf BODIN. « Selective Blockchain Transaction Pruning and State Derivability ». In : *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 2018, p. 31-40. DOI : 10.1109/CVCBT.2018.00009.

Intégration dans les travaux du LCIS

Ce sujet s'intègre dans la thématique transverse concernant la confiance dans les systèmes décentralisés et autonomes et, se focalise sur un aspect sécurité issu des perspectives de la thèse d'Arthur Baudet soutenu par le Cybersecurity Institute de l'UGA.

L'obtention d'un financement de stage permettra de renforcer les résultats de cette thématique et apportera des arguments tangibles pour les réponses aux appels à projets. Dans un premier temps, l'équipe d'encadrement projette de soumettre un projet sur cette thématique dans le cadre de l'appel IRGA 2024 de l'Université Grenoble Alpes pour poursuivre les travaux. Dans un second temps, un sujet de thèse pourra être proposé dans le cadre de l'appel à sujet MSTII si la procédure est renouvelée comme en 2023.

Les résultats obtenus durant le stage seront communiqués dans un workshop ou une conférence internationale.

Cet encadrement de stage permettra de soutenir l'activité de recherche d'Annabelle Mercier après une période de charge administrative significative effectuée à l'IUT de Valence.

Diffusion du sujet pour le recrutement de l'étudiant

Un projet PX511 sur ce thème a été proposé aux étudiants 5A IR&C et a été retenu par un groupe. Le sujet de stage sera proposé aux étudiants du projet et de la promotion IR&C.

Le sujet sera diffusé via les listes de diffusion et le réseau des encadrants.