Équipe Réseaux **Sujet de Thèse 2023-2026**

Better Algorithms for Secure and Efficient Blockchains

Algorithmes de consensus efficaces pour les Blockchains (version française en page 3)

Location	Team Réseaux, ICube (UMR CNRS 7357)
Supervision	Quentin Bramas (bramas@unistra.fr)
Duration	3 years

Keywords

Distributed Ledger Technologies ; Blockchain ; Consensus

Context

Blockchain [1] is a technology allowing independent entities to maintain a consistent state of a database. Although the entities do not necessarily know and trust each other (some may be malicious), the correct entities must agree on the current state of the database. This technology is based on a theoretical problem of distributed algorithms : the consensus. A major difficulty arises when the network is open, i.e., any entity can participate in the protocol. Existing solutions do not scale, which is why alternatives exist allowing for example to have a subset of the entities to collaborate "outside" the blockchain, while maintaining the same security [3].

Scientific Objectives

This thesis subject proposes to theoretically analyze the consensus algorithms used within blockchains. The analysis concerns aspects of complexity in time, in memory and the associated security guarantees, for example :

- how to reduce the amount of information needed to check the current state of the blockchain [2].
- how interactions between entities can be used to elect the entity responsible for writing to the blockchain [4].
- how the structure of the blockchain impacts the applications that use it.
- how to model the notion of "Blockchain level 2", i.e., how to model an algorithm that uses the blockchain as an external tool [3].

Several problems come down to mathematical analyzes of functions (proofs of convergence, equivalence, probabilistic analysis).

Skills

The expected skills are :

- Excellent programming skills (in C or other languages) ;
- Distributed algorithms ;
- Applicants should possess good verbal and written English skills. French is not a requirement ;
- Holding an MSc in Computer Science (CS) or Mathematics.

Application

Please send an email to `reseaux-pos-2023@icube.unistra.fr` comprising :

— a detailed CV ;
— your possible list of publications if applicable ;
— the grades for the last three years, with your position after the final exams ;
— a cover letter.

Références

[1] Satoshi Nakamoto. Bitcoin : un système de paiement électronique pair-à-pair. Traduction Française par Arnaud-François Fausse. https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf

[2] Aggelos Kiayias, Nikos Leonardos, and Dionysis Zindros. Mining in Logarithmic Space. https://eprint.iacr.org/2021/623.pdf

[3] Poon, J., & Dryja, T. (2016). The bitcoin lightning network : Scalable off-chain instant payments. https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf

[4] Jean-Philippe Abegg, Quentin Bramas, and Thomas Noël. Blockchain using Proof-of-Interaction. https://arxiv.org/pdf/2002.07763.pdf

Version Française

Équipe Réseaux **Sujet de Thèse 2023-2026**

Algorithmes de consensus efficaces pour les Blockchains

Mots clés

Livre de compte distribué ; Blockchain ; Consensus

Contexte

La Blockchain [1] est une technologie permettant à des entités indépendantes de maintenir un état cohérent d'une base de données. Bien que les entités ne se connaissent pas forcément et ne se font pas confiance (certaines peuvent être malicieuses), les entités correctes doivent se mettre d'accord sur l'état courant de la base de données. Cette technologie repose sur un problème théorique d'algorithmique distribuée : le consensus. Une difficulté majeure intervient lorsque le réseau est ouvert, c'est-à-dire que n'importe quelle entité peut participer au protocole. Les solutions existantes ne passe pas à l'échelle, c'est pour cela que des alternatives permettant par exemple de faire collaborer un sous-ensemble d'entités "en dehors" de la blockchain, tout en conservant la même sécurité [3].

Objectifs

Ce sujet de thèse propose d'analyser de manière théorique les algorithmes de consensus utilisés au sein des blockchains. L'analyse concerne les aspects de complexité en temps, en mémoire et les garanties de sécurité associées, par exemple :

- comment réduire la quantité d'information nécessaire à la vérification de l'état courant de la blockchain [2].
- comment les interactions entre les entités peuvent servir à élire l'entité responsable d'écrire sur la blockchain [4].
- comment la structure de la blockchain impacte les applications qui l'utilisent.
- comment modéliser la notion de "Blockchain niveau 2", c'est-à-dire comment modéliser un algorithme qui utilise la blockchain comme un outils externe [3].

Plusieurs problèmes se ramènent à des analyses mathématiques de fonctions (preuves de convergence, d'équivalence, analyse probabiliste).

Compétences

Les compétences requises sont :

- Excellentes compétences en programmation (en C ou dans d'autres langages) ;
- Algorithmes distribués ;
- Les candidats doivent posséder de bonnes compétences en anglais à l'oral et à l'écrit. Le français n'est pas requis ;
- Posséder un Master en Informatique (CS) ou en Mathématiques.

Candidature

Veuillez envoyer un e-mail à l'adresse `reseaux-pos-2023@icube.unistra.fr` comprenant :

- un CV détaillé ;
- votre liste éventuelle de publications, le cas échéant ;
- les notes des trois dernières années, avec votre position après les examens finaux ;
- une lettre de motivation.

Références

[1] Satoshi Nakamoto. Bitcoin : un système de paiement électronique pair-à-pair. Traduction Française par Arnaud-François Fausse. https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf

[2] Aggelos Kiayias, Nikos Leonardos, and Dionysis Zindros. Mining in Logarithmic Space. https://eprint.iacr.org/2021/623.pdf

[3] Poon, J., & Dryja, T. (2016). The bitcoin lightning network : Scalable off-chain instant payments. https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf

[4] Jean-Philippe Abegg, Quentin Bramas, and Thomas Noël. Blockchain using Proof-of-Interaction. https://arxiv.org/pdf/2002.07763.pdf