AAPG 2022	BC4SSI	JCJC
Coordinated by :	Romaric Ludinard	48 months
Axe E.3 / CES 25	Sciences et génie du logiciel - Réseaux de communication multi-usages, infrastructures de hautes performances	

Towards Scalable Public Blockchain

1 Context and Objectives

Bitcoin was the first successful decentralized cryptocurrency and remains the most popular of its kind to this day. Bitcoin circumvents the absence of a global trusted third-party by relying on a blockchain, an append-only data structure, publicly readable and writable, in which all the valid transactions ever issued in the system are progressively appended through the creation of cryptographically linked blocks. In spite of its impressive capability of enabling an unknown and large set of participants to agree on the system state, blockchains suffer from various limitations [1], among which some of them will durably become a major impediment for services leveraging blockchains. In the context of the intership, we will focus on scalability and replication issues.

Sycomore [2] changes the blockchain structure from a linked list to a Directed Acyclic Graph (DAG) to handle transaction scalability issue. Similarly, Kiayias et al. [3] proposed to change the blockchain structure from a linked list to a skip list to handle replication issue, but with constant difficulty.

The objective of this internship is twofold:

- First, leverage the analysis provided by [4, 5] to adapt it to [3].
- Second, adapt the solution [3] to Sycomore [2].

2 Expected skills

Preparing for a Master 2, an engineering degree (5th year) or equivalent in the field of computer science, the candidate should:

- have a strong interest on blockchain technology,
- have good organizational, relational, listening, and receptive skills,
- good skills in mathematics and data structures.

Programming skills (Rust / Python) are definitively a plus.

The internship will last 6 months (full time), based in IMT Atlantique, Rennes Campus, starting on March 2023 within Adopnet Team. This internship will take place in the context of the ANR funded BC4SSI project. Note that, in the context of this project, a PhD grant, starting on September 2023, related to this internship subject, will be funded.

Contacts for more information contact or application:

- Romaric Ludinard: romaric.ludinard@imt-atlantique.fr
- Emmanuelle Anceaume: emmanuelle.anceaume@irisa.fr

3 References related to the project

[1] Direction générale des Entreprises. 2021. Les verrous technologiques des blockchains.

[2] **Anceaume, E.**, Guellier, A., **Ludinard, R.** and Sericola, B. 2018. Sycomore : a Permissionless Distributed Ledger that self-adapts to Transactions Demand. In: *17th IEEE International Symposium on Network Computing and Applications*. NCA.

[3] Kiayias, A., Leonardos, N. and Zindros, D. 2021. Mining in Logarithmic Space. In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. CCS.

[4] Garay, J. A., Kiayias, A. and Leonardos, N. 2015. The Bitcoin Backbone Protocol: Analysis and Applications. In: *34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. EUROCRYPT.

[5] Garay, J. A., Kiayias, A. and Leonardos, N. 2017. The Bitcoin Backbone Protocol with Chains of Variable Difficulty. In: *37th Annual International Cryptology Conference*. CRYPTO.