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	

How scalable are current solutions to scalability issues ?

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 design and deploy an experimental testbed in order to measure and quantify improvements provided by [2, 3]. A large code basis written in Rust (with Tokio[1] and nom[2]) is already developped to implement Bitcoin protocol.

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,
- good organizational, relational, listening, and receptive skills,
- good ability to interact with the borrow checker,
- good skills in mathematics and data structures.

Rust Programming skills are definitively a plus.

The internship will last 6 months (full time), based in IMT Atlantique, Rennes Campus, starting on March 2023 within Sotern Team. This internship will take place in the context of the ANR funded BC4SSI project.

Please contact Romaric Ludinard: romaric.ludinard@imt-atlantique.fr for more information contact or application.

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.

[1] https://tokio.rs/

[2] https://github.com/Geal/nom