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 DAG-based Public Blockchain

1 Context and Objectives

Blockchain technology is proposed as the panacea for developing decentralised applications and the underlying technology that powers decentralised finance. However, the long-term feasibility of blockchain technology is hindered by the inability of existing protocols to prune the data leading to constantly growing storing requirements [6, 9]. Researchers have proposed Non-Interactive-Proofs-of-Proof-of-Work (NIPoPoWs) [1, 2, 7] as a mechanism to reduce the storage and communication complexity of totally ordered blockchains to $\mathcal{O}(\text{polylog}(n))$, where n is the number of blocks before the compression. However, current NIPoPoWs designs only address blockchains whose structure is a totally ordered sequence of blocks, where blocks are created at constant rate and thus do not address the actual blockchains whose structure is a graph of blocks [3, 4, 5, 8].

The objective of this internship is to address the following open question: How to design a Non-Interactive-Proofs-of-Proof-of-Work (NIPoPoWs) compliant with dynamic graph based blockchains [4, 5]. If a $\mathcal{O}(\text{polylog}(n))$ construction is feasible, this will prove that one can securely compress a DAG of blocks whose structure self-adapts to the observed transaction submission rate.

2 Expected skills

The candidate should have nice interest on blockchain technology, good skills in distributed algorithms, data structures, programming and mathematics. (Rust) Programming skills are not mandatory but are definitively a plus. The internship will last 6 months (full time), based in IMT Atlantique, Rennes Campus, starting on **January, 29th 2024** within Sotern[1] Team. This internship will take place in the context of the ANR funded BC4SSI[2] project. Note that, in the context of this project, **a PhD grant, starting on September 2024, 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] Jain, A., **Anceaume, E.** and Gujar, S. 2022. Extending The Boundaries and Exploring The Limits Of Blockchain Compression. working paper or preprint.

[2] 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.

[3] Rocket, T., Yin, M., Sekniqi, K., van Renesse, R. and Sirer, E. G. 2019. Scalable and Probabilistic Leaderless BFT Consensus through Metastability. *CoRR* abs/1906.08936.

[4] **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.

[5] Churyumov, A. 2017. ByteBall : A Decentralized System for Storage and Transfer of Value.

[6] 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.

[7] Kiayias, A., Miller, A. and Zindros, D. 2017. Non-Interactive Proofs of Proof-of-Work. Cryptology ePrint Archive, Paper 2017/963. https://eprint.iacr.org/2017/963.

[8] Popov, S. 2017. The tangle.

[9] 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.

[1] https://www-sotern.irisa.fr/

[2] https://hub.imt-atlantique.fr/bc4ssi/