Can we make permissionless blockchains scalable ? How ?

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

Keywords permissionless blockchains, scalability, adversarial attacks

Context 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. Despite the benefits of its blockchain, Bitcoin still faces serious scalability issues, most importantly its ever-increasing blockchain size.

Internship The overall objective of this internship is to address the following two questions: *(a)* how to extend existing blockchain systems with pruning capabilities and *(b)* how to do so in a secure and trustworthy manner, that is, despite the presence of adversarial strategies.

To answer both questions, the master student will first survey approaches to reducing blockchain size, e.g [1, 2], and will focus on their capability to be efficient, secure, and deployable in an open environment. The second step of this internship will be to combine existing approaches or to propose a new one that allows to significantly reduce the storage requirements of bitcoin.

Required skills Knowledge on distributed algorithms and cryptography.

References

[1] R. Matzutt, B. Kalde, J. Pennekamp, A. Arthur Drichel, M. Henze, and K. Wehrle. How to securely prune bitcoins blockchain. https://arxiv.org/pdf/2004.06911.pdf, 2020.

[2] H. Schoenfeld and A. Molina. Pascal: An infinitely scalable cryptocurrency. https://www.pascalcoin.org/storage/whitepapers/PascalWhitePaperV5.pdf, 2019.