Sycomore: A permissionless distributed ledger that self-adapts to transactions demand

Advisers
Emmanuelle Anceaume, emmanuelle.anceaume@irisa.fr
Bruno Sericola, bruno.sericola@inria.fr
Romaric Ludinard, romaric.ludinard@imt-atlantique.fr

Context The goal of decentralized cryptocurrency systems is to offer a medium of exchange secured by cryptography, without the need of a centralized banking authority. An increasing number of distributed cryptocurrencies systems are emerging, and among them Bitcoin, which is often designated as the pioneer of this kind of systems. 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. One of the main drawbacks of chains of blocks is their performance issues. Bitcoin cannot confirm more than 7 transactions/s in average.

We propose a new way to organise both transactions and blocks in a distributed ledger to address the performance issues of permissionless ledgers. In contrast to most of the existing solutions in which the ledger is a chain of blocks extracted from a tree or a graph of chains (e.g., HashGraph [2], ByteBall [3], Iota [4], Ghost [6] and Spectre [5]), we have proposed Sycomore [1], a distributed ledger whose structure is a balanced directed acyclic graph of blocks. This specific graph, that we have called a SYC-DAG allows us to keep all the remarkable properties of the Bitcoin blockchain in terms of security, immutability, and transparency, while enjoying higher throughput and self-adaptivity to transactions demand. Note that to the best of our knowledge, such a design has never been proposed so far.

Internship The first goal of this internship is to study other cryptocurrency systems that propose to organise transactions or blocks within a graph, acyclic or not. The second goal of the internship is to analytically and possibly experimentally evaluate the performance of Sycomore. We already have some theoretical results that we would like to extend. This will require some nice background on graph and probabilities. In case, the student will also be motivated by experiments on Sycomore, this will require to plunge in the existing code, and to rewrite some functionalities in order to run Sycomore in the testing network of Bitcoin.

References

[1] E. Anceaume, A. Guellier, R. Ludinard, and B. Sericola. Sycomore : a permissionless distributed ledger that self-adapts to transactions demand. In *Proceedings of the International IEEE conference on Network Computing and Applications (NCA)*, `https://www.youtube.com/watch?v=YLW-iHjsWoO`, 2018.

[2] L. Baird. The SWIRLDS Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance. `http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf`, 2016.

[3] A. Churyumov. ByteBall : A Decentralized System for Storage and Transfer of Value. `https://byteball.org/Byteball.pdf`, 2017.

[4] S. Popov. The Tangle. `https://iota.org/IOTA_Whitepaper.pdf`, 2017.

[5] Y. Sompolinsky, Y. Lewenberg, and A. Zohar. SPECTRE: A fast and scalable cryptocurrency protocol. *IACR Cryptology ePrint Archive*, 2016, 2016.

[6] Y. Sompolinsky and A. Zohar. Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains. *IACR Cryptology ePrint Archive*, 2013, 2013.