# Some Insights on Open Problems in Blockchains: Explorative Tracks for Tezos

**Sylvain Conchon** ✉
Laboratoire Méthodes Formelles, Université Paris-Saclay, CNRS, ENS Paris-Saclay,
91190 Gif-sur-Yvette, France

## Abstract

Blockchain is an emerging field that started with the advent of Bitcoin, the first cryptocurrency launched in 2008. Since then, new distributed applications (DApps) based on blockchain have emerged, such as non-fungible tokens (NFT) or decentralized finance (DeFi). All this contributes to an ever-increasing use of blockchains and poses many technological and scientific challenges.

The first challenge is related to *scalability*, usually measured by the number of transactions per second (TPS) that a blockchain can process. Recent solutions, such as Rollups, implement the concept of Layer 2, a secondary framework built on top of an existing blockchain that allows transactions to be managed off-chain for efficiency. The primary blockchain is used to secure the exchanges of the second layer by regularly recording its exchanges and its current state. A first experiment of Optimistic Rollups has been implemented in the Blockchain Tezos. The TORUs (Transaction Optimistic Rollups) allow efficient financial assets exchanges in the form of Michelson tickets. A generalization to Smart contracts Optimistic Rollups (SCORU) is currently under development.

Another challenge is to improve the *efficiency* of the data structures used in blockchain implementations. The main explorative tracks are to reduce and improve disk usage (compact representations, serialization of big data, sharing, ...), increase the speed of access operations (efficient caching strategies, asynchronous I/O, ...). For example, recent improvements to the storage layer of Octez, Tezos' most popular node implementation, have shown that it is possible to significantly speed up transactions, stabilize average transaction latency, and significantly reduce memory usage.

The *security* issues associated with blockchains also raise many challenges. Indeed, the economic protocols or consensus algorithms implemented in blockchains use incentive mechanisms to discourage nodes from engaging in bad behavior or in launching attacks. A fine tuning of these incentives is difficult in situations where decision makers interact. Game theory can be used to develop incentives, in particular its integration into verification tools (model-checkers, proof assistants, deductive program verification) or machine-learning tools could be very promising.

Finally, given the financial amounts managed by blockchains, it is essential to have a very precise specification of the algorithms, protocols and data structures used in blockchain implementations in order to guarantee the *reliability* of these very complex software. Whether it is for the programming of smart contracts, consensus algorithms or the P2P layer, the introduction of formal methods in the development cycle of blockchains is a major challenge in this domain. A lot of work in formal methods has been done for the Tezos blockchain. Among others, the formalization in TLA+ of Tenderbake, a PBFT-style consensus algorithm which offers deterministic finality to Tezos.

**Author Bio.** Sylvain Conchon is Professor in Computer Science at University Paris-Saclay since 2013. He is a member of LMF (Formal Methods Laboratory) and his research focuses on automatic deduction and model-checking, using techniques based on SMT (Satisfiabilty Modulo Theories) solvers. He is one of the designers of the SMT solver Alt-Ergo and the model-checker Cubicle. In collaboration with Nomadic-Labs, he is currently working on the use of formal methods to design and verify several aspects related to the blockchain Tezos, such as Michelson smart contracts or the Tenderbake consensus algorithm.

**2012 ACM Subject Classification** Software and its engineering

**Keywords and phrases** Blockchain, Tezos, Scalability, Efficiency, Security, Reliability

**Digital Object Identifier** 10.4230/OASIcs.FAB.2022.2

**Category** Invited Talk



5th International Symposium on Foundations and Applications of Blockchain 2022 (FAB 2022).
Editors: Sara Tucci-Piergiovanni and Natacha Crooks; Article No. 2; pp. 2:1–2:1

OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany