A Modular Approach for the Analysis of Blockchain Consensus Protocol Under Churn

Floris Ciprian Dinu ✉
Department of Computer, Control, and Management Engineering Antonio Ruberti,
University of Rome La Sapienza, Italy

Silvia Bonomi ✉
Department of Computer, Control, and Management Engineering Antonio Ruberti,
University of Rome La Sapienza, Italy

Abstract

Blockchain is an emerging technology that gained a lot of attention in the last years. Many different consensus protocols have been proposed to improve both the scalability and the resilience of existing blockchain. However, all these solutions have been defined for rather static settings. We propose a modular approach for analysing and comparing different consensus protocols used in blockchain under churn.

2012 ACM Subject Classification Computer systems organization → Reliability; Information systems → Distributed storage

Keywords and phrases Blockchain Dependability, Dynamic Distributed Systems, Simulation

Digital Object Identifier 10.4230/OASIcs.FAB.2022.8

Category Poster

Introduction. In the last 10 years, Blockchain became one of the most widespread technology used to store transactions in a distributed system characterized by full decentralization, transparency, immutability and non-repudiation of data. Blockchain represents an example of emerging technology that first consolidated its development and only recently started to investigate the theoretical foundations behind them. As a consequence, many different algorithmic solutions have been defined trying to improve as much as possible the scalability and the resilience to Byzantine processes. However, most of the existing solutions lack a solid theoretical analysis proving their formal correctness and the evaluation is carried out by considering rather static environments where the system does not change or changes very slowly mainly due to failures. However, real networks (especially those underlining public permissionless blockchain) are not static and are subject to a progressive refreshment of the peers participating in the system. Such phenomenon is also known as *churn* and if not properly analysed and managed may have a strong impact on both correctness and performance of the blockchain. To the best of our knowledge, currently there do not exist results showing the impact of churn over the blockchain. We took a first step in this direction by defining a framework that can be used to evaluate how existing consensus protocols for blockchains respond to churn.

Reviewing and analysing the state of the art on consensus protocols for blockchain [6], we observed that every blockchain protocol can be seen as the composition and orchestration of the following main distributed building blocks:

- an *Overlay Management Protocol* (OMP) responsible for connecting replicas into a logical overlay network and preserve the connectivity of the overlay network graph;
- a *Communication Layer* implementing one-to-one, one-to-many and many-to-many communication primitives that allow the dissemination of transactions and blocks to all interested replicas and

© Floris Ciprian Dinu and Silvia Bonomi;
licensed under Creative Commons License CC-BY 4.0

5th International Symposium on Foundations and Applications of Blockchain 2022 (FAB 2022).
Editors: Sara Tucci-Piergiovanni and Natacha Crooks; Article No. 8; pp. 8:1–8:2
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- an *Agreement* primitive (e.g., a consensus, a leader election, a committee-based voting) that is used to select, validate and attach blocks to the blockchain consistently with other replicas in the system.

Let us note that such primitives are not independent of each other but they rather work in synergy. As a consequence, when the system becomes dynamic the effect of the churn does not impact only the overlay network and the OMP but it also impacts all the other layers built on top of it.

Research Direction and Contribution. Our research is aimed to define a framework that can be used to analyse different blockchain solutions in dynamic settings and to compare their characteristics. Our proposed framework is composed of four main elements:

- a *distributed building blocks composition model* that allows to define a blockchain protocol as composition of existing distributed building blocks.
- a *churn* model that allows to characterize the dynamic of the system and to describe the arrival and departure distribution of processes from the system (and in particular at the OMP level).
- a *load* model that allows to characterize the how transactions are generated by clients
- a set of *metrics* that allows to analyse every blockchain protocol and to perform a comparison between different protocols.

To create our composition model, we selected consensus protocols from the state of the art (e.g., SCP [4], Tendermint [1], XRP [3], PBFT [2]) and we analysed them to identify the set of assumptions concerning (i) the overlay network (ii) the communication primitives used and (iii) the type of agreement implemented on top of them. Almost every algorithm either assumes a fully connected overlay network (e.g., PBFT, Tendermint) or an overlay network having the characteristics of a random graph (e.g., SCP). Concerning the communication primitives, almost all the papers consider a reliable communication system without specifying any further detail about its implementation. Then we analysed the state of the art concerning OMPs and protocols implementing a reliable communication primitive. While from the correctness point of view the many available solutions can be considered equivalent each other, from the performance, dependability and robustness point of view they are not. Thus, we implemented in OMNeT++ [5] a composition model that allows to define a blockchain as a composition of (i) one OMP, (ii) one (or more) communication primitive(s) and (iii) an agreement primitive and we are currently implementing several algorithms, exposing the same interface, for any required building block.

References

1 Ethan Buchman, Jae Kwon, and Zarko Milosevic. The latest gossip on BFT consensus. *CoRR*, abs/1807.04938, 2018. `arXiv:1807.04938`.

2 Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, pages 173–186, USA, 1999. USENIX Association.

3 Brad Chase and Ethan MacBrough. Analysis of the XRP ledger consensus protocol. *CoRR*, abs/1802.07242, 2018. `arXiv:1802.07242`.

4 David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.

5 OMNeT++. Home page, 2022. URL: `https://omnetpp.org`.

6 Yang Xiao, Ning Zhang, Wenjing Lou, and Y Thomas Hou. A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, 22(2):1432–1465, 2020.