On Scalability and Performance of Permissioned Blockchain Systems

Chrysoula Stathakopoulou
IBM Research - Zürich
Departement of Computer Science - ETH Zürich
tat@zurich.ibm.com

ABSTRACT

Blockchain systems have emerged as the backbone of the Bitcoin cryptocurrency. Even though considerable research has been made towards Proof of Work based blockchain systems, the scalability of systems based on Byzantine Fault Tolerance (BFT) protocols is still limited. This work aims to suggest BFT consensus protocols for scalable blockchain systems that allow reconfiguration. At the same time the participants of the system are considered rational and incentive mechanisms are adopted in the blockchain ecosystem.

1 INTRODUCTION

Blockchain systems have emerged as the backbone of the Bitcoin cryptocurrency, introduced in 2008 [14]. A blockchain system consists of a distributed append-only ledger of blocks of transactions. The participants of the cryptocurrency system need to maintain a synchronized view of the ledger and, therefore, a consensus protocol is required. Bitcoin introduced a Proof of Work (PoW) consensus mechanism where, essentially, each participant votes with its computing power.

In 2014 Ethereum Project [17], a new cryptocurrency, redefined blockchain systems introducing smart contracts, which are custom application code that enforces properties among the blockchain participants. A cryptocurrency exchange is a special case of a smart contract. The concept of smart contracts decoupled the currency logic from the distributed ledger infrastructure and opened the way to general purpose blockchain systems. This resulted in the conception of private or enterprise blockchain systems, such as Hyperledger Fabric [5], Tendermint [3], Chain [1], and Quorum [2]. Unlike Ethereum, Bitcoin and other cryptocurrencies, where anyone can participate, enterprise blockchain systems enforce access control to the participants and, hence, we call such a blockchain system permissioned, whereas public systems like Bitcoin are called permissionless.

2 MOTIVATION

Enterprise blockchain systems have different properties and requirements. Proof of Work mechanisms are not sustainable as they waste exorbitant amounts of energy. More recent protocols [10] [11] move to Proof of Stake consensus mechanisms to tackle the energy inefficiency. However, both mechanisms suffer from low throughput and high latency, as a result of the probabilistic agreement, which makes them unsuitable for an enterprise ecosystem. On the other hand, while open membership systems are prone to Sybil attacks [8], the access control in permissioned systems allows us to move towards Byzantine Fault Tolerant (BFT) algorithms [12] that have been studied for decades now with respect to the machine state replication problem. Practical BFT protocols, introduced by Castro and Liskov [6] allow a large throughput. Their high message complexity, though, limits their scalability. As Vukolić analyzes [16], numerous protocols have been proposed as improvements to both PoW and BFT and there exist efforts to combine the best of both worlds.

3 RESEARCH PLAN

So far, considerable research has been conducted in the performance and security of permissionless blockchain systems. Decker and Wattenhofer [7] study the time needed for the propagation of a transaction block in the Bitcoin network and they associate the delay with the size of the block. Gervais et al. [9] developed a framework to evaluate and compare Bitcoin with Litecoin, Dogecoin, Bitcoin's most important forks, as well as with Ethereum.

However, the recently conceptualized permissioned blockchain systems have not been studied until now in depth. Therefore, the proposed research project aims to explore this area. As a first step, existing consensus protocols must be deployed in the context of a blockchain system and in the scale of a wide area network so that network parameters such as latency, throughput, availability and scalability can be evaluated. Taking into account the results of this study, the goal is to suggest an optimal protocol according to a set of requirements (security assumptions, number of nodes, network topology, transaction and block size, etc.) that correspond to a realistic enterprise blockchain ecosystem. Looking into enterprise blockchain proof-of-concepts and prototypes, already reveals a wide variety of requirements and therefore the suggested protocol should be highly configurable.

More specifically, regarding the scalability parameter, despite the extended aforementioned research in Byzantine Fault Tolerance, defining and evaluating a practical protocol that scales up to thousand nodes, a realistic number of stakeholders in an enterprise blockchain setup, is still an open problem. This research work aims to explore this problem.

Considering the configuration of the system, in a realistic scenario the set of participants should be able to change without compromising security. However, unlike PoW consensus BFT protocols require a static set of known participants. To this direction, Martin and Alvisi [13] and later Rodrigues et al. [15] have suggested automatic reconfiguration protocols for reliable distributed storage systems. This work aims to further explore dynamic consensus protocols and evaluate them in the context of a permissioned blockchain system. Hyperledger Fabric [5] has already decoupled ordering from execution and validation of transactions. As a next step, we envision a public yet permissioned distributed ordering service, where participants can offer resources for the ordering and receive payment for their services in the form of transaction

fees. The dynamic reconfigurable protocol is required to serve this scenario.

Finally, in a blockchain ecosystem the participants of the consensus protocol can belong to different organisations with opposing interests, unlike in a traditional distributed system. In such an environment, each participant is expected to be rational, i.e. try to optimize its own state. Therefore, the participants must be given incentives to comply with the protocol. Moreover, if we consider a public ordering service, the participants should be incentivised to actively participate in the protocol, despite their negative utility i.e. the cost of the resources they dedicate. Solidus [4] is a recent proposal for incentive-compatible Proof of Work consensus in a public blockchain, while Ouroboros [11] studies rational participants with respect to a Proof of Stake Protocol. This research project aims to study how to adopt Game Theory mechanisms in a BFT protocol.

4 SUMMARY

To summarize, this research work will focus on the performance and scalability of distributed fault tolerant protocols with application to blockchain systems, targeting the following key points:

(1) Analysis and large scale evaluation of the performance, scalability and security of consensus mechanisms. Suggestion of optimal protocols with respect to required network and security parameters.
(2) Suggestion and evaluation of dynamic consensus mechanisms that allow the reconfiguration of the network without compromising the security properties of the system, while allowing a public ordering service.
(3) Incentive compatible BFT protocols.

REFERENCES

[1] Chain. http://chain.com.
[2] Quorum. http://www.jpmorgan.com/global/Quorum.
[3] Tendermint. http://tendermint.com.
[4] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman. Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus. *arXiv preprint arXiv:1612.02916*, 2016.
[5] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *EuroSys 2018: Thirteenth EuroSys Conference*. ACM, 2018.
[6] M. Castro, B. Liskov, et al. Practical Byzantine fault tolerance. In *Proc. Third USENIX Symposium on Operating Systems Design and Implementation (OSDI), New Orleans, Louisiana, USA, February 22-25, 1999*, pages 173–186. USENIX Association, 1999.
[7] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pages 1–10. IEEE, 2013.
[8] J. R. Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.
[9] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16. ACM, 2016.
[10] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68. ACM, 2017.
[11] A. Kiayias, A. Russell, B. David, and R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.
[12] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.
[13] J.-P. Martin and L. Alvisi. A framework for dynamic byzantine storage. In *Dependable Systems and Networks, 2004 International Conference on*, pages 325–334. IEEE, 2004.
[14] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.
[15] R. Rodrigues, B. Liskov, K. Chen, M. Liskov, and D. Schultz. Automatic reconfiguration for large-scale reliable storage systems. *IEEE Transactions on Dependable and Secure Computing*, 9(2):145–158, 2012.
[16] M. Vukolić. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In *International Workshop on Open Problems in Network Security*, pages 112–125. Springer, 2015.
[17] G. Wood. Ethereum: A secure decentralised generalised transaction ledger. http://gavwood.com/paper.pdf, 2014.