The Units of Permissionless Consensus: Towards Mobile and Edge Computing

Eduardo Ribas Brito
eduardo.ribas.brito@ut.ee

***Abstract*—...**

***Index Terms*—IEEE, IEEEtran, journal, LaTeX, paper, template.**

I. Introduction

LONG has been the time when consensus started to be defined as a fundamental problem of distributed systems [1]–[3]. Generally, consensus means reaching an agreement between multiple parties in the potential presence of faulty individuals. As per multi-agent systems, interacting over computer networks, consensus is thought to be the result of a coordination effort such that those parties agree on some value at a given moment. Achieving consensus implies that the system shall be reliable and fault-tolerant. However, the consensus problem has been limited by some assumptions on the networks. The well-known "secure Byzantine-Fault-Tolerant multiparty consensus systems" that have been designed over the years are usually meant to work only with a set of known participants, faulty or not [4]. The other side of the coin is the permissionless consensus challenge, consisting of achieving agreement in an environment where the participants are unknown and untrusted [5], [6]. Plus, there are other intrinsic particularities of this type of networks, for example, their openness, and the lack of any kind of central authority. This adds another layer of complexity to the problem, as the participants are not only unknown and untrusted but can also join or leave the network at any time, freely choosing if they want to participate in the consensus protocol or not. Nevertheless, the problem of permissionless consensus can still be seen as a special case of the more general consensus and can still be formalized in the same way. In this paper, we will focus on consensus in permissionless systems, especially in the context of blockchain networks. We will reason about its meaningfulness, ultimately by trying to identify the units that may underpin consensus. We will also discuss the current state-of-the-art, with a particular interest in the shift of the consensus layer of these distributed networks to mobile and edge computing environments, for which computationally expensive consensus algorithms are impractical and unfair.

II. Related Work

A. Classical Consensus

The establishment of a definition for the problem of reaching agreement in a distributed system was pioneered by Lamport et al. in [1]. The authors defined consensus as the problem of agreeing on a single value among a set of processes, in the presence of faulty entities. The first consensus algorithms were designed for synchronous systems, where the communication between the processes is reliable, and the delay is bounded. However, these initial attempts failed to cover the different types of faulty behaviour. Along with the establishment of the famous Byzantine Generals Problem, the first solutions, not only for dealing with treason, but also for unreliable communication channels, or any other kind of arbitrary byzantine behaviour, were also proposed by Lamport in [2], [3]. The solution was a synchronous mechanism that used a set of leaders to reach consensus. Multiple practical implementations and optimizations to this solution have been proposed in the literature.

B. Asynchronous Byzantine Consensus

The first asynchronous consensus algorithm was later proposed by Castro and Liskov in [4]. And naturally, after that work, many other asynchronous consensus algorithms have appeared. However, all of them are based on the assumption that the number of faulty processes is less than a certain threshold. Additionally, the assumption of a known set of participants is also made. This is a very strong assumption, as it is not always possible to know the participants beforehand as they may, for example, participate anonymously, or dynamically.

C. Permissionless Consensus

The advancements of the internet more than potentiated the revolution and what we now call the permissionless consensus problem was finally born. Without forgetting the previous attempts, the first practical permissionless consensus algorithm was proposed by Nakamoto in [5]. It is a proof-of-work consensus protocol that resembles a "replicated state machine" where the independent participants reach agreement not only about transactional values, but also about their order. "Proof-of-work is essentially one-CPU-one-vote" and this is the novelty introduced by Bitcoin [7], [8]. The focus shifted for decentralized systems and after proof-of-work many other consensus mechanisms have been proposed, based on different consensus units, like proof-of-stake, proof-of-space, proof-of-burn, etc. The chaotic diversity of new consensus protocols gave also room for endless reviews, overviews and comparisons [9]–[14]. The authors of these surveys often put multiple dimensions into comparison, like fault tolerance, scalability, or energy consumption, and, among those, some focused their efforts on mechanisms that may work in resource-constrained networks [15]–[18]. This paper will try to identify the common conclusions from these comparisons, while looking into the

state-of-the-art and novel approaches for running permissionless consensus protocols in mobile and edge devices.

REFERENCES

[1] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)*, 27(2):228–234, 1980.

[2] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency: the works of leslie lamport*, pages 203–226. Springer, 2019.

[3] Leslie Lamport. The weak byzantine generals problem. *Journal of the ACM (JACM)*, 30(3):668–676, 1983.

[4] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OsDI*, pages 173–186, 1999.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[6] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

[7] Rafael Pass and Elaine Shi. Hybrid consensus: Efficient consensus in the permissionless model. *Cryptology ePrint Archive*, 2016.

[8] Rafael Pass and Elaine Shi. Hybrid consensus: Scalable permissionless consensus, 2016.

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

[10] Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, and Alireza Babaei Bondarti. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, 154:113385, 2020.

[11] L. M. Bach, B. Mihaljevic, and M. Zagar. Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1545–1550, 2018.

[12] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7:22328–22370, 2019.

[13] Bahareh Lashkari and Petr Musilek. A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, 9:43620–43652, 2021.

[14] Sarah Bouraga. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications*, 168:114384, 2021.

[15] Aleksandr Ometov, Yulia Bardinova, Alexandra Afanasyeva, Pavel Masek, Konstantin Zhidanov, Sergey Vanurin, Mikhail Sayfullin, Viktoriia Shubina, Mikhail Komarov, and Sergey Bezzateev. An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends. *IEEE Access*, 8:103994–104015, 2020.

[16] Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, 15(6):3680–3689, 2019.

[17] Kimchai Yeow, Abdullah Gani, Raja Wasim Ahmad, Joel J. P. C. Rodrigues, and Kwangman Ko. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access*, 6:1513–1524, 2018.

[18] Mehrdad Salimitari, Mainak Chatterjee, and Yaser P. Fallah. A survey on consensus methods in blockchain for resource-constrained iot networks. *Internet of Things*, 11:100212, 2020.