Improving Blockchain Resilience to Network Partitioning by Sharding

Juncheng Fang
University of California, Irvine, CA, United States

Farzad Habibi
University of California, Irvine, CA, United States

Kevin Bruhwiler
University of California, Irvine, CA, United States

Fayzah Alshammari
University of California, Irvine, CA, United States

Faisal Nawab
University of California, Irvine, CA, United States

Abstract

Blockchain plays a significant role in cryptocurrencies and growing applications like smart contracts. However, prior blockchain algorithms did not consider large-scale network partitioning a considerable concern while relying heavily on a reliable global network. Previous works have shown a possibility of a massive disruption on the Internet. The author in [2] discusses the case of Internet disorder due to solar superstorms, which can disconnect different geographical regions from each other for months. Partitioning attacks are also notable concerns that should be considered, in which their goal is to cut connections between a set of nodes and the rest of the network.

In the case of network partitioning, the main chain will fork into branches, and miners in different disconnected regions will create multiple blocks in parallel. The longest chain rule in current blockchain systems accepts only one of the branches after the network is recovered, and because of that, all blocks in other branches will be pruned. Losing a considerable number of mined blocks is not tolerable and significantly impacts the reliability of the ledger and miners' benefit.

In this work, we aim to improve blockchain resilience by designing a partition-tolerance blockchain system that: (1) split into branches when network partition happens. (2) merge existing branches into one when the network goes back to normal. (3) ensure the safety and integrity of the blockchain.

Newly mined blocks will be collectively signed by a group of miners with a BFT protocol similar to ByzCoin[1], where the consensus group is formed by the miners of the previous w blocks. When a network partition happens, only part of the consensus group can be reached; thus the number of signers w_b of the new block will be less than w. If a block with w_b signers is published, every node in the partition learns that they are now in a branch with around w_b/w of the total hashing power, and it can be identified by the signature of the block. After the network recovers, miners will receive multiple branches, and they mine on a merging block which points to the last block of each branch as the parent blocks. The consensus group will be selected from each branch according to the branch size. Transactions in each partition are preserved after merging.

2012 ACM Subject Classification Computer systems organization → Reliability

Keywords and phrases resilience, partitioning, blockchain, collective signing

Digital Object Identifier 10.4230/OASIcs.FAB.2022.9

Category Poster

References

1 Kogias et al. Enhancing bitcoin security and performance with strong consistency via collective signing. In *25th usenix security symposium (usenix security 16)*, pages 279–296, 2016.

2 Sangeetha Abdu Jyothi. Solar superstorms: planning for an internet apocalypse. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, pages 692–704, 2021.