ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Network-level Attacks Against Ethereum PoS

Ethereum[1] functions as a decentralized blockchain platform that empowers the creation and execution of smart contracts and decentralized applications. Notably, Ethereum has undergone a recent transition in its consensus model, shifting from the energy-intensive Proof-of-Work to the more energy-efficient Proof-of-Stake mechanism. In this transition, Ethereum has embraced the innovative Proposer-Builder-Separation (PBS) scheme. The goals of this scheme include guarding against transaction censorship attacks, re-configuring the economics of Miner Extractable Value (MEV), and laying the groundwork for the implementation of more scalable protocols[2].

Under the PBS framework, the consensus process involves multiple validators collaborating on distinct tasks aimed at generating new blocks. Builders are responsible for crafting blocks and presenting them to proposers. Proposers, in turn, evaluate the potential profitability of the block candidates without having access to their specific contents, thereby promoting fairness and security in the selection process.

While the PBS model holds promise in bolstering various security aspects of Ethereum's consensus mechanism, it does not come without its share of concerns, particularly related to potential centralization issues [Hei+23]. Additionally, prior research has demonstrated vulnerabilities in the communication between blockchain consensus nodes, as exemplified by instances such as BGP hijacks targeting Bitcoin's network [AZV17; SM23; ATV23].

The central objective of this thesis is to thoroughly investigate the viability of network-level attacks against the PBS system and to explore the potential ripple effects of such attacks. By examining the susceptibility of the PBS framework to network-based exploits, we aim to shed light on potential vulnerabilities that could compromise the integrity and security of Ethereum's consensus mechanism. Through rigorous analysis and empirical testing, this study endeavors to provide a comprehensive understanding of the risks associated with network-level attacks on PBS and their possible subsequent repercussions.

Requirements:

- Background: Blockchain/Ethereum, TCP/IP, Basic security understandings
- Programming Languages: Python, Shell, Docker/VMs

Milestones:

- Study the PBS model
- Simulate a simple network of Ethereum validator nodes following the PBS model
- Explore and implement one or more network attacks in the simulations

[1] https://ethereum.org/en/
[2] https://ethereum.org/en/roadmap/pbs/

Interested? Please contact us for more details!

Contact

- Lioba Heimbach: hlioba@ethz.ch, ETZ G95
- Tran Duc Muoi: dutran@ethz.ch, ETZ G87

References

[Hei+23] Lioba Heimbach et al. "Ethereum's Proposer-Builder Separation: Promises and Realities". In: *arXiv preprint arXiv:2305.19037* (2023).

[AZV17] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. "Hijacking bitcoin: Routing attacks on cryptocurrencies". In: *2017 IEEE symposium on security and privacy (SP)*. IEEE. 2017, pp. 375–392.

[SM23] Muhammad Saad and David Mohaisen. "Three birds with one stone: Efficient partitioning attacks on interdependent cryptocurrency networks". In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2023, pp. 111–125.

[ATV23] Theo von Arx, Muoi Tran, and Laurent Vanbever. "Revelio: A Network-Level Privacy Attack in the Lightning Network". In: *8th IEEE European Symposium on Security and Privacy (EuroS&P 2023)*. 2023.