ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

MA:

Detecting DDoS Attacks on Ethereum Validators

Ethereum's consensus protocol change from Proof-of-Work to Proof-of-Stake fundamentally changes how Ethereum's block production is structured. Since the launch of the Beacon Chain in 2020, upcoming block proposers have been known in advance. It has been shown that linking validators to their respective IP address is possible [1]. This opens up the door for precisely timed DDoS attacks on individual Ethereum validators. However, besides a short lived network performance degradation and the monetary loss for the attacked validator, an attacker had no incentive for such a behaviour.

The Ethereum Merge in 2022 introduced execution layer transactions to the Beacon Chain. The time varying value associated with transactions, namely transaction fees and MEV (Maximal Extractable Value), change the incentives for discussed DDoS attacks. Under the right conditions such attacks might be highly profitable and might entail negative consequences not only for the attacked validator but also for the network as a whole.

We want to investigate the newly formed incentives structures for such attacks. Furthermore, we want to develop methods for detecting possible DDoS attacks on Ethereum validators and if present, further investigate performed attacks.

Requirements: This project will involve programming in a language of your choice, preferably Python. An interest and experience with blockchain is a plus. We will have weekly meetings to discuss open questions and determine the next steps.

Interested? Please contact us for more details!

Contact

- Lioba Heimbach: hlioba@ethz.ch, ETZ G95

References

[1] Bürgel Sebastian. "Proof-of-Stake Validator Sniping Research". In: 2022. URL: https://medium.com/hoprnet/proof-of-stake-validator-sniping-research-8670c4a88a1c.