ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

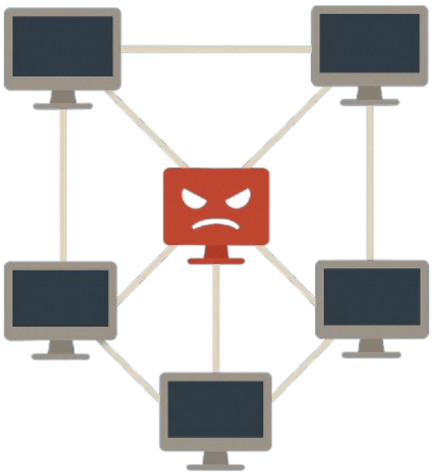
Distributed Computing

Prof. R. Wattenhofer

Attacking P2P networks

One of the crucial aspects of large distributed systems, such as Ethereum, is their promise of safety: no one wants transactions to be lost or funds to be stolen. The mathematical backbone of this safety is the consensus mechanism, which has attracted a tremendous amount of research over the past forty years. However, decentralized systems do not consist of consensus alone. Alongside it sit the *peer-to-peer (P2P) networks*, which have received far less rigorous scholarly attention—if any at all. As the saying goes, "a chain is only as strong as its weakest link," and we still do not know how weak today's P2P protocols may be.

What will you do? Your task will be to investigate modern P2P protocols adopted by major blockchains, formulate attack models, design attacks, and implement them, measuring the decrease of performance or even showing complete crashing.



Why? This project offers a deep dive into the backstage of nowadays distributed systems. You will learn state-of-the-art protocols and how to reason about them. Furthermore, carrying out a successful attack and publishing it may bring the attention of the distributed community to your work and lead to further fruitful collaborations.

Requirements: This project requires a student to be an autonomous programmer. The programming languages used by modern decentralized systems are primarily Rust or Go, so knowledge of **or** a will to learn one of them is a big plus. Further, it's important to understand that it is not just an implementation, but a research project, that encourages curiosity and the ability to lead the discussion by asking fruitful questions.

Interested? Please contact me, attaching your transcript and CV.

Contact

- Anton Paramonov: aparamonov@ethz.ch, ETZ G61.1