ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

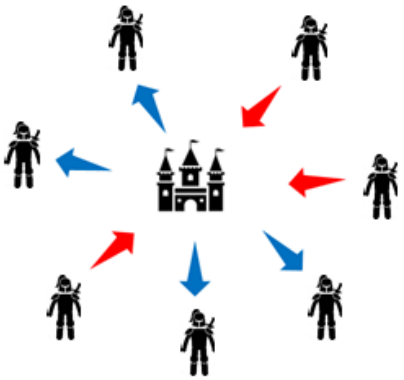
Distributed Computing

Prof. R. Wattenhofer

Partially-Synchronous Scalable Consensus

With the rise of cryptocurrencies and blockchain technology, a traditional problem in distributed computing – known as *byzantine consensus* – has regained traction recently. To reach consensus, multiple players have to agree on a common value despite the participation of malicious actors. Although consensus is considered a fundamental problem and multiple protocols exist in literature, they all either make strong assumptions concerning the network (synchrony), the adversary, the protocol randomness, etc., or do not scale to reasonably large systems that are used in practice. However, scalability is an essential requirement for blockchain protocols that are meant to be deployed in real-life applications and hence cannot afford to make unrealistic assumptions.

In this thesis, you will delve into the fundamentals of distributed computing, and understand the bounds and limitations of byzantine consensus with a focus on modern permissioned blockchain systems. Your goal will be to design a *provably secure and scalable* consensus protocol in the partially-synchronous setting, robust against an adaptive but computationally-bounded adversary that controls a constant fraction of the players. You will assume that standard cryptographic tools such as signatures, asymmetric encryption schemes and hash functions, do exist. However, you will aim to alleviate all unrealistic assumptions such as the existence of random beacons, common coins, or trusted setup.



Requirements: The expected outcome of this project is of theoretic nature; hence, you should be comfortable to formalize both theorems and proofs independently. Progress, open problems and new ideas will be discussed in collaborative (at least) weekly meetings throughout the project!

Contacts

- Zeta Avarikioti: zetavar@ethz.ch, ETZ G95
- Roland Schmid: roschmi@ethz.ch, ETZ G94