ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

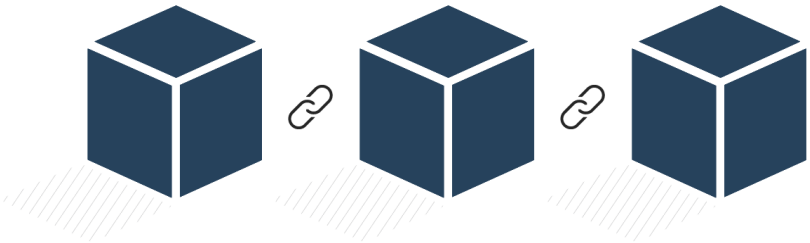
Distributed Computing

Prof. R. Wattenhofer

Analyzing the Properties of Popular Blockchains

The inception of Bitcoin marked the creation of the first fully decentralized cryptocurrency relying on blockchain technology and electrified the world with its potential, namely the ability to securely execute financial transactions without having to rely on a central authority.

In the past decade, we have witnessed the creation of numerous blockchains promising to deliver the same security as Bitcoin, and often making additional promises simultaneously. For example, as every computer participating in Bitcoin's blockchain must exchange, store and verify every transaction, Bitcoin has an infamously low transaction throughput of seven transactions per second. Thus, newer blockchains often improve the transaction throughput by, for instance, adapting the consensus mechanism. Another example is the support for smart contracts, as introduced by Ethereum. Smart contracts allow blockchains to build decentralized applications and handle complex financial transactions. Thus, many of these blockchains supporting smart contracts have become popular alternatives but their (security) properties are not well understood.



In this thesis, we want to analyze the crypto protocols of popular blockchains, describe their properties under specific models, and discover potential flaws, both in their designs and implementations. Thus, as part of this thesis, you will analyze the crypto protocols of one or more blockchains in depth.

Requirements: 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
- Quentin Kniep: qkniep@ethz.ch, ETZ G95
- Jakub Sliwinski: sljakub@ethz.ch, ETZ G95