ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Adversarial Attack on Decentralized Financial System

Decentralized finance is one of the most promising blockchain-based applications. It does not rely on centralized financial systems such as brokerages, exchanges, or banks and instead utilizes smart contracts on blockchains, the most common being Ethereum. Financial transactions occur on decentralized exchanges (DEX) instead of centralized exchange infrastructures. However, the design flaw of centralized exchange infrastructures threatens the underlying blockchain security through different attacks such as oracle manipulations and liquidity pool manipulations.

In the thesis, we first aim to understand the mechanisms behind different adversarial attacks. Then we will instigate how to design more robust decentralized exchange protocols by discovering more vulnerabilities of current protocols. In particular, we will investigate how machine learning can help discover the vulnerabilities of current protocols and design more advanced protocols.

Prerequisite:

- The candidate should have basic knowledge of blockchains, smart contract, and fundamental knowledge of machine learning. The candidate should be interested in financial models and applications.
- Required programming skills: basic knowledge of Solidity, Go, and Python.

Interested? Please contact us for more details!

Contact

- Zhao Meng: zhmeng@ethz.ch, ETZ G61.3
- Yunpu Ma: cognitive.yunpu@gmail.com