ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Oracle Manipulation Attacks

We sometimes need external data in blockchain systems - say, the weather report, Bitcoin's price in USD, whether Switzerland won the FIFA World Cup or not, etc. This data is given by external entities called "oracles". Many smart contracts rely on these oracles to drive critical functionalities - like setting the daily external exchange rate in Ampleforth, a popular on-chain stablecoin. Bad actors can compromise or manipulate an oracle to serve "wrong" data, and try to profit it through the smart contract.

In this project, we look at such oracle manipulation attacks that have happened in the past, and generalize them into categories. We look at popular solutions to the oracle manipulation problem, like chain.link, and see whether they actually work - and under what conditions they can fail.

Requirements: This project involves understanding Ethereum, smart contract design, popular smart contracts like Uniswap, Chain.Link, Ampleforth, etc., and being able to understand and program in Solidity.

Interested? Please contact us for more details!

Contact: Tejaswi Nadahalli: tejaswin@ethz.ch, ETZ G97