ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Group Project / Bachelor Thesis / Semester Thesis / Master Thesis

Breaking a Cryptocurrency

Decentralized cryptocurrencies are used to resist the censorship and monetary control of governments. They are governed by the rules of the software, a principle caught in the catchphrase "code is law". As a consequence design flaws can lead to large cases of fraud in terms of the real world laws, some of the well known ones being the MtGox theft of an equivalent of 500 million Dollar in Bitcoin and the DAO hack in Ethereum which led to the theft of about 3.6 million Ether, worth about 1 billion Dollar at today's price. With the flood of new cryptocurrencies recently entering the market[1] there is likely a large number of unknown vulnerabilities to be haunted.

In this thesis you will explore the market of altcoins (or even have a look at Bitcoin itself) and try to break a cryptocurrency by exploiting design flaws. As the problem may hide in different aspects of the system, a wide variety of skills is helpful.

Requirements: Knowledge of cryptocurrencies, experience with networking and basic cryptography. Good knowledge of C++, Go or Python.

Interested? Please contact us for more details!

Contacts

- Conrad Burchert: bconrad@ethz.ch, ETZ G95

[1] Check e.g. https://coinmarketcap.com/