ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

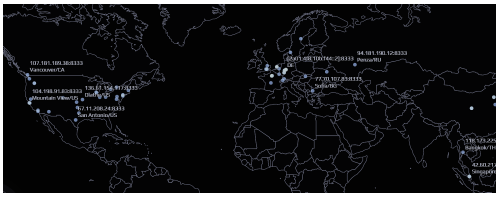
Prof. R. Wattenhofer

BA/SA:

Simulating Bitcoin's Network Topology

Bitcoin is a decentralized dynamic peer-to-peer network. The security of the transactions is dependent on the information propagation time, hence the network topology is important for Bitcoin' s operation. The protocol implements a specific way of connecting new peers to the existing network to ensure the graph structure resembles that of a random graph while obfuscating the network topology to protect against various attacks (e.g. eclipse attack).

In this thesis, we will have a close look at the connection strategy of the bitcoin network and evaluate its fairness properties regarding the interests of all bitcoin miners. Our goal is to identify weaknesses in the running system and propose a more robust solution.



Requirements: The nature of this project is mostly practical; hence, programming experience is an advantage. There will be weekly meetings with your supervisors to discuss progress and open questions.

Interested? Please contact us for more details!

Contacts

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

Detailed Project Outline

We denote the following primary tasks mandatory (on the right side you find a rough estimate for the time that we allocate to the respective task):

- understand bitcoin's connection strategy in detail ($\star\star$)
- defining metrics for simulation ($\star\star$)
- evaluate how to implement the simulation best ($\star$)
- write simulation of the broadcasting algorithm used by bitcoin ($\star\star\star\star$)
- compare simulation to real data as far as one finds any ($\star\star\star$)
- come up with a different connection strategy "X" ($\star\star\star\star$)
- implement connection strategy in simulation ($\star\star$)
- compare connection strategy with bitcoin's current broadcasting algorithm on fairness and efficency ($\star\star$)
- report and presentation ($\star\star$)

Extensions

Apart from these requirements, we can think of plenty of ways to extend the *bitcoins broadcasting algorithm* with cool features. Of course, you may add your own ideas to this non-exhaustive enumeration:

- realtime simulation plots
- simulate multiple different broadcasting algorithms