ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Analysis of Bitcoin Lightning

The Bitcoin Lightning Network is a decentralized system that builds on top of Bitcoin and makes cheap, fast and secure Bitcoin transactions possible. As a layer 2 payment protocol it can handle transactions off-chain and only rarely necessitates on-chain transactions, lowering the overall cost. The Lightning Network consists of a bidirectional payment channels between nodes running the Lightning protocol.

In this thesis, we want to gain insights into and explore security and privacy loopholes in the Lightning Network. For instance, utilizing the IP addresses of the network's members, we want to map the members to geographic locations. Understanding the geographic distribution of the members can reveal issues in the Lightning Network regarding centralization. Additionally, we want to analyze what proportion of the network an attacker would have to control to de-anonymize transaction routes in the network and use other signals from historic data to gain insights on the dynamics of the network.

Requirements: Strong motivation, programming experience, knowledge of blockchain technologies 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

- Florian Grötschla: fgroetschla@ethz.ch, ETZ G 93
- Lioba Heimbach: hlioba@ethz.ch, ETZ G 95