Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

BA/MA:

Secure Payment Channels

Blockchain systems face a scalability problem. Due to the consensus mechanisms these systems use, they suffer from a limitation on the transaction throughput in order to guarantee security. The most prominent solution to this problem is payment channels, that allow users to move the transaction load off-chain securely. However, payment channels have a major shortcoming, since they demand users to be constantly online and run a full node of the underlying blockchain to maintain the security of the transactions. To address this issue, third parties were introduced to act on behalf of the users of the channel. These third-parties are service providers and thus have to be rewarded as such.

In this thesis, you will delve into the core design of payment channels and understand what can (or cannot) be done with Bitcoin Script. The main goal of the thesis will be to design a reward mechanism for the service providers that is incentive compatible, thus securing the underlying payment channel construction. Your main focus will be on the Lightning Network, which is the payment network operating on top of the Bitcoin network.

Requirements: Knowledge of Bitcoin Script would be an advantage.

Interested? Please contact us for more details!

Contacts

- Zeta Avarikioti: zetavar@ethz.ch, ETZ G95
- Tejaswi Nadahalli: tejaswin@ethz.ch, ETZ G93