ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

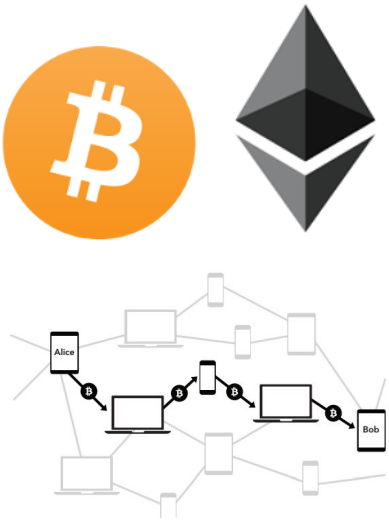
Master Thesis Description

Durations: Aug. '17 - January '18

Implementation of a Blockchain Micropayment Channel Network

Heavily relying on its fully replicated and globally synchronized state, the Bitcoin blockchain is increasingly running at full capacity. Given the limited on-chain scalability of currently available cryptocurrencies, micropayment channel networks have been proposed [1, 2].

A micropayment channel network is essentially an overlay network that can work over any cryptocurrency using three main technologies:



- Multisignature outputs
- Replaceable transactions
- Hash-Timelocked Contracts (HTLC) – forward a promise that can only be unlocked with a secret.

Micropayment channel networks promise to massively increase privacy and anonymity while instantly executing numerous off-chain micropayments. The payments are end-to-end secure (due to HTLCs), as transfers between hops are only performed conditional on the intended recipient receiving its payment. Different versions of micropayment channel networks are currently being developed for both Bitcoin [3] and Ethereum [4].

The goal of this thesis is to simplify the state-of-the-art technologies for micropayment channels and to implement our own version of an off-chain micropayment network.

Supervisor(s):

- Prof. Dr. Roger Wattenhofer: wattenhofer@ethz.ch, ETZ G96
- MSc. Conrad Burchert: bconrad@ethz.ch, ETZ G95

Student:

- Spyros Lalos: laloss@student.ethz.ch

References

[1] Christian Decker, Roger Wattenhofer *A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels* 17th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), 2015

[2] Joseph Poon, Thaddeus Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. January 14, 2016.

[3] The Bitcoin Lightning Network
`lightning.network`

[4] Ethereum's Network (Raiden),
`http://raiden.network/`