Designing a Dynamic Micropayment Channel Network
Bachelor Thesis - Corsin Gutkowski

Problem description

Since the introduction of Bitcoin in 2008 by Satoshi Nakamoto [5] cryptocurrency systems are ever growing. New participants are joining the network every day thereby increasing the number of transactions on the blockchain constantly. This development yields new challenges as the Bitcoin system is by far not perfect. Especially scalability to a larger user base and transaction speed are critical. As the processed amount of transactions in a block of the blockchain is limited a backlog of transactions is created, thus further increasing the time for a transaction to be confirmed. With just increasing the size of the blocks other issues are introduced and the existing problem is not solved [1, 3].

One way to reduce the transactions on the blockchain drastically is the usage of micro-payment channels first described by Hearn [4] and further improved by Decker et al [2]. A channel originates from a contract between two nodes in the network. The main advantage of these contracts is that they only require an on-chain transaction when created, dissolved or on disagreement. By linking together nodes which belong to more than one contract, whole payment chains can be built without opening new channels. Sending a transaction over such a chain can pay a small fee for each link used. This is more cost effective than just creating a new contract which would require an expensive on-chain transaction.

Objectives

The thesis will focus on some of the following aspects:

- Provide and analyze a strategy for making payment channels and updating fees between nodes
- Realize the strategy in a centralized system
- Analyze the reaction of the network to crashes

Organization

Duration: 6 months
Professor: Roger Wattenhofer
Supervisor: Conrad Burchert

References

[1] Kyle Croman et al. "On Scaling Decentralized Blockchains". In: *3rd Workshop on Bitcoin Research (BITCOIN), Barbados*. Feb. 2016.

[2] Christian Decker and Roger Wattenhofer. "A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels". In: *17th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), Edmonton, Canada*. Aug. 2015.

[3] Christian Decker and Roger Wattenhofer. "Information Propagation in the Bitcoin Network". In: *13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy*. Sept. 2013.

[4] Mike Hearn. *Bitcoin contracts*. [Online; accessed June 2017]. URL: `https://en.bitcoin.it/wiki/Contract`.

[5] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (). [Online; accessed June 2017]. URL: `https://bitcoin.org/bitcoin.pdf`.