Abstract of the Thesis Titled: “Capabilities and Limitations of Payment Channel Networks for Blockchain Scalability”

Marco Conoscenti

Bitcoin and other blockchain-based cryptocurrency do not scale, because the blockchain limits transaction throughput. Payment channel networks are the most promising solution to address scalability, as they enable off-blockchain payments that are not subject to the blockchain throughput limit. The Lightning Network (LN) is the mainstream payment channel network, built on top of the Bitcoin blockchain. The LN leverages the Hashed Timelock Contract (HTLC) to transfer off-chain payments in a trustless and secure way. However, the Lightning Network and HTLC-based payment channel networks present critical features that might undermine their correct functioning and therefore need to be investigated. Some examples of these critical features are channel economic capacity, which limits payment amounts, channel unbalancing, which makes payment channels unusable in one direction, and uncooperative behavior of nodes, which causes increased payment time and failures.

This work presents CLoTH, a simulator for HTLC payment networks. CLoTH is an original payment network simulator, as it constitutes a precise mapping of the LN code functions. As input, it takes parameters defining a payment channel network (e.g., number of channels per node, average channel capacity) and parameters defining payments (e.g., payment amounts and payment rate). It simulates the input-defined payments on the input-defined HTLC payment network. It produces performance measures in terms of payment-related statistics, such as probability of payment failure and time to complete payments. CLoTH is a valuable tool to identify issues, analyze solutions and steer future developments of payment channel networks.

This work discusses three groups of simulations conducted using the CLoTH simulator. In the first group a snapshot of the Lightning Network was given as input to the simulator. The goal of these simulations was to find configurations in which a payment is more likely to fail than to succeed in the LN. Simulations of the second group were conducted on synthetic networks, i.e., payment networks generated by the simulator using their statistical description. The goal of these simulations was to study the impact of each simulator input parameter on payment network performance. The third group of simulations aimed to analyze the effects of network and protocol modifications in the Lightning Network, like for instance the removal of network hubs and channel rebalancing approaches.

Simulation results prove that the current most relevant issues of the Lightning Network are limited channel capacities and channel unbalancing, which both cause payment failures. A rebalancing approach designed and simulated in this work effectively addresses channel unbalancing. At the same time, the simulations performed prove that the Lightning Network is resilient to the removal of the most connected network hubs and can support a contained level of node uncooperativeness.

This work is one of the first attempts to thoroughly examine capabilities and limitations of payment channel networks, and to provide viable solutions. The CLoTH simulator is a valid and useful tool for systematically studying payment channel networks and assisting their development.