LAB DAY 3 - PAYMENT CHANNELS

A27 - Fundamentals and Design of Blockchain-based Systems

February 8, 2023

Assignment

Payment channel networks (PCNs) are proposed as a solution to the scalability problem of blockchain. Users in a PCN can make transactions in an off-chain way rather than committing every transaction to the chain. Such a mechanism makes transactions faster and more cost-efficient. In this lab, we will implement some simulations to see how PCNs work.

Implement a payment channel

To open a channel, two parties need to lock some coins in a public address where those locked coins cannot be spent. Then, these parties can make transactions in an off-chain way. In this lab, two parties open a channel using an "open channel transaction". Apart from information included in a normal transaction, this transaction also includes the two parties' signatures, channel ID, and locked funds of each party. At first, one party signs the "open channel transaction" and sends it to the other party. The other party signs it and publishes it on-chain. After the "open channel transaction" is included in the blockchain, they can start to trade with each other.

In a payment channel, two parties only record the newest balance information. So, if one party wants to make a transaction, it calculates the balance of each party after this transaction, signs it, and sends it to the other party. The other party also signs it and sends back its signature. Later, if a party wants to close the channel, it can use these signatures to prove the correctness of its balance.

Requirements for this lab

Correctness: the balance of every party should be correct which means one can not steal money from others.
Performance: you need to consider the throughput, delay, and success rate of implemented PCNs and try to improve them.
Topology: change the topology of the PCN to study the influence of decentralization.

Detail your design in a small report (max. 2 pages).