LAB DAY 1 - THE BASICS

A27 - Fundamentals and Design of Blockchain-based Systems

February 6, 2023

Assignment

For the first lab day, we expect you to implement the preliminaries towards a functioning blockchain. For this, you will be using the IPv8 simulator. Carefully read through the explanation of the simulator setup. This first day can be split up into three parts.

Communication

Design a community with full visibility. There should be support for two different types of nodes: full nodes and light nodes. Full nodes store all of the blockchain's data and participate in block validation, whilst light nodes simply interact with the blockchain (e.g., by creating transactions). Design different types of messaging within the network. More specifically, create functionalities for direct peer-to-peer messages, multi-casting and broadcasting. Also, design a method for gossiping information to other clients. *Hint: use additional communities to differentiate between full and light nodes.*

Transactions

In this second part, you will be implementing your very own cryptocurrency. To achieve this, you will be designing a balance-based system. Full nodes store, locally, the balance of each client that they are aware of. You may initialize this system with a set amount of currency for each node in the network. When a node initiates a transaction of cryptocurrency from its address to another's, they do so by broadcasting it to a single (random) full node or validator. This validator validates the validity of the transaction (e.g., by checking signatures and balances) and then executes it by mutating its local storage accordingly. Next, it gossips these changes to a random set of other validators, which also run this gossip routine.

Experimentation & Validation

In this final part, you will play around with your rudimentary payment system. See what happens when differing the network size, the ratio between full and light nodes and the number of clients validators gossip towards. How long does it take for all validators to be notified of a transaction? Do all validators reach a consistent state? Write a small report (max. two pages) detailing your implementation and the performance of your system.