

LAB DAY 2 - CONSENSUS

A27 - Fundamentals and Design of Blockchain-based Systems

February 7, 2023

Assignment

For this second day, you will implement a consensus mechanism for your preliminary blockchain. More specifically, you will create your own **Proof of Stake** (PoS) blockchain. You can start by defining a data structure for **blocks**. These must be able to store a set number of transactions and contain a **pointer** to a previous block.

Also, you must create a **mempool**. Have validators first validate a transaction and then broadcast it to all other nodes. In order to simplify the assignment, you may use a single validator that acts as an **oracle**. This oracle randomly picks a validator out of the **weighted** set of validators. The weight is the balance of the validator. This ensures that validators with a high balance are more likely to be picked. The picked validator is then allowed to craft the next block. It does so by removing transactions from the mempool and broadcasting the next block across the network. This node is rewarded with a set amount of cryptocurrency.

As an outcome, play with different stake weights and see how this affects the consensus mechanism. For example, what happens if a validator has 10x more cryptocurrency than the other validators? Discuss your solution in a small report (max 2 pages).