Blockchain **

Zhivko Stoimchev

February 2024

Blockchain technology is a very promising innovation. While ideas of digital cash have existed decades before, Bitcoin was the first implementation that was able to address all issues previous systems had. A key building block of blockchain networks is the ability for a completely decentralized network of peers to reach consensus. One of many consensus algorithms, also used by Bitcoin is proof of work.

The goal of this project is to implement a fully working blockchain with very basic algorithms for peer discovery, block propagation, and a simple consensus protocol. Usually, proof of work is the easiest to implement. However, other consensus algorithms such as practical Byzantine fault tolerance or Paxos are welcome. The blockchain must be able to process transactions into blocks and protect against double spend attacks using a UTXO transaction model.

Optimization is not key. Hence, implementation specific tasks will be easier. The protocol does not have to be efficient and using JSON or any other structured data format is encouraged. Additionally, using java built in crypto utility functions for creating public-private key pairs are sufficient. Hashing must be based on SHA256.

For bootstrapping a test-net, docker containers should be used. The network protocol must be fault tolerant handling disconnects and reconnects. For simplification a trusted setup can be used, where a trusted node is used to boot up the network.