universität wien

Private Blockchain System

Samuel Mitterrutzner

universität wien

Outline

1. Blockchains in general
2. Private vs. public blockchain
3. Proof of Authority
4. Aura Protocol
5. Demo
6. Architecture
7. Block mining

universität wien

Blockchains in general

- Blockchain: A distributed database that is maintained by different nodes
- They consist of 3 main building blocks:
  - The ledger consisting of a series of blocks
  - The nodes that maintain the ledger by mining and validating new blocks
  - The consensus algorithm that specifies how the nodes make decisions
- Main benefits:
  - Immutability
  - Decentralisation
  - No trusted third-party

universität wien

Private vs public Blockchain

- **Participation**
  - Nodes in private blockchains are usually controlled by one or a few organisations
  - In public blockchains everyone can join and participate
- **Performance**
  - Private blockchains are much faster
  - Public blockchains are slower because everyone can participate
- **Cryptocurrency**
  - Private blockchains usually do not have a cryptocurrency
  - Public blockchains have cryptocurrencies to support the miners

universität wien

Proof of Authority

- Originally proposed by Gavin Wood the co-founder of Ethereum in 2015
- Relies on 2 assumptions:
  - There exists a set of *N* nodes that can be identified by a unique id
  - At least *N/2 + 1* of those nodes can be trusted
- How it works
  1. In a fixed time interval a primary node is selected to propose a new block
  2. The primary node then sends the proposed block to all the other nodes
  3. The other nodes validate the proposed block
  4. Once N/2 + 1 nodes consider the proposed block as valid it will be added to the ledger

Aura Protocol

- Implementation of Parity Ethereum Client
- 2 rounds are needed before a block is added to ledger
- Nodes need to be synchronized within the same UNIX time t
- The primary node is selected as follows:

$$l = s \mod N \quad (1)$$

$$s = \frac{t}{step\_duration} \quad (2)$$

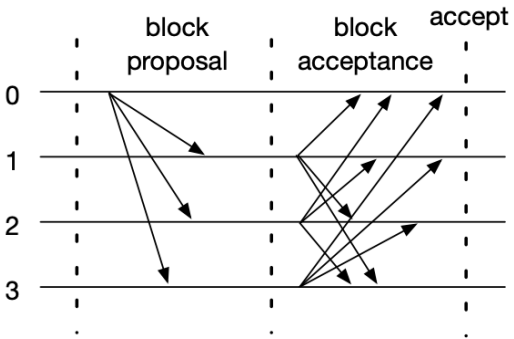
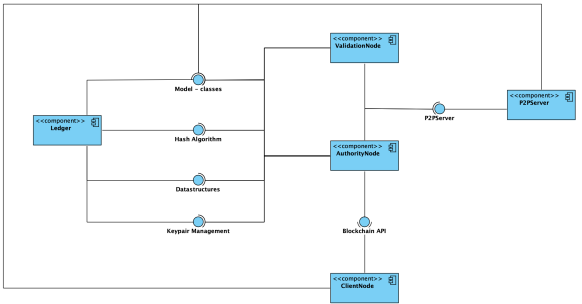


Figure from: https://eprints.soton.ac.uk/415083

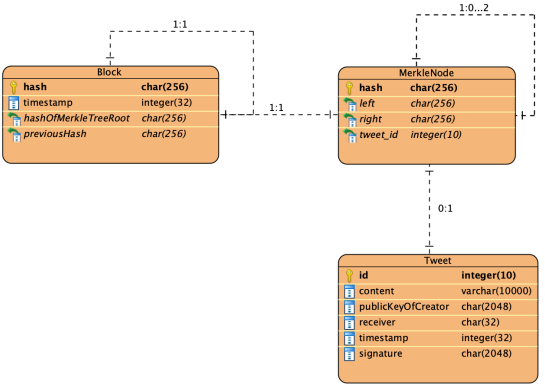
Architecture

- Component based architecture:
  - **Ledger**: data structures, model classes, hash algorithms, cryptography
  - **P2P-Server**: handles the communication between the different validation-nodes.
  - **Authority-Node**: rest-api, primary node selection
  - **Validation-Node**: block mining, block validation
  - **Client-Node**: CLI to interact with the blockchain



Ledger

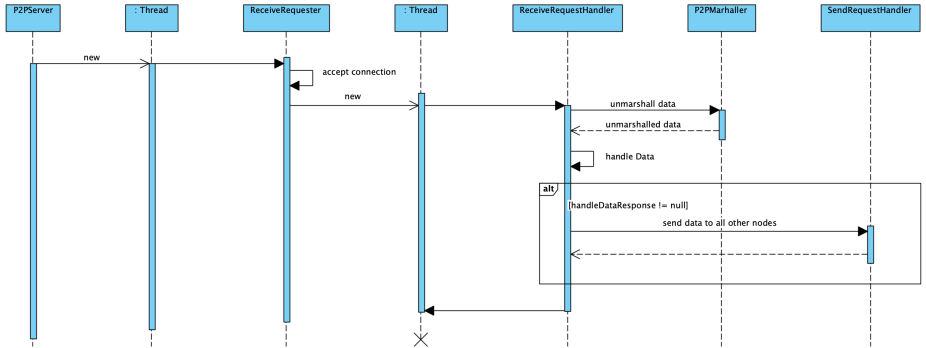
- Merkle Tree:
  - Perfectly balanced binary tree
  - Only leaves contain data
  - The parent only contains the following value: *SHA256(left.hash, right.hash)*
- Hash algorithm: SHA256 with Base64 encoding
- Asymmetric encryption algorithm: RSA



ER-Diagram of the model classes

universität wien

P2PServer



universität wien

Authority Node

- Provides Rest API that can be accessed by client applications
  - Posting and fetching tweets
  - Login and register
- Handles the selection of the primary node
  - The authority selects the primary node by using round robin

universität wien

Validation Node

- This is the component that actually maintains the blockchain
- Block validation and Block mining is done by the validation node
- When is a block considered valid?
  - All tweets are valid: Check if signatures are correct.
  - Valid Merkle Root: Is the Merkle root the same as the one a node gets when it creates a new Merkle tree with the same tweets?
  - Known previous Hash: Check if the previous hash of the proposed block is equal to the hash of the last added block.

universität wien

Block Mining