BlockChain Lab 2018

13 July 2018

Group 4:

Selin Sezer
Hisham Ismail
Patricia Patricia
Yifei Zhang

RWTH AACHEN UNIVERSITY

Consensus Component

Consensus

Main Features

- Mining
  - Kill mining
  - Min, max, average mining time
- Nonce Calculation
  - Initially started with zero nonce then decided to switch to random nonce
- Validation
  - Block is validated based on the current difficulty
  - Merkle tree root, creator id, nonce and difficulty are part of the validated hash
- Difficulty recalculation
  - Difficulty is recalculated before and after each mining or validation operations
  - A Bitcoin like approach for the calculation:
    - A scaled ratio between the number of generated blocks within 2 timestamps

CryptoHelper Component

CryptoHelper

Main Features

- Library & Primitives Used
  - PyCryptodome
  - Elliptic Curve Cryptography (ECDSA for signatures), SHA256
- Sign
  - Signing a payload with a private key
  - Signatures are encoded using UTF-8 format
- Validate
  - Checks if the payload was signed by the intended key pair owner
- Generate Key pairs
  - Generates a private-public key pair over NIST P-256 curve
- Hash
  - Generates a payload's SHA256 hash in Hex Decimal format

Node Dashboard

Node Dashboard

Main Features

- Displays:
  - Min, max, average mining time
  - Number of mined blocks
  - Current Blockchain Length
  - Current Difficulty
- Charts with respect to time :
  - Memory usage of the blockchain
  - Length of blockchain
  - Number of nodes connected to the blockchain
  - Difficulty change of the blockchain
- Mining
  - Option to start and stop mining
- Link to the Block Explorer

- Technology Used
  Node-RED and MQTT

Node Dashboard