Project Presentation: Proof Of Work Consensus

12/03/2018

Group 5- Proof of Work Consensus

Arun Swaminathan, Hardik S Negi, Shubham Jindal

- Problem: Achieving consensus in a system with Distributed Nodes (eg Blockchain)

- Proposed Solution: Proof Of Work Consensus Algorithm

Solution Implementation

- Understood the Proof Of Work consensus algorithm.
- Understood the nuances of Blockchain system like blocks, Merkle Tree, transactions, nodes, miners and coinbase etc.
- Implemented the proof of work consensus algorithm in blockchain system using the DistAlgo framework.
- Fixed multiple design flaws in existing Python based implementation like added asynchronous operations, Merkle tree implementation etc.
- Performed correctness testing of the blockchain generated.

```
[592] miner.Miner<Miner:a9c09>:OUTPUT: Accepted block 0031e669f0db5a61e069161ffbcb031e0a8b51f6b5e498e1ca08d628af3fcdfc
Block received is valid
[593] miner.Miner<Miner:a9c0a>:OUTPUT: New block with proof of work has been computed
[594] miner.Miner<Miner:a9c0b>:OUTPUT: Rejected block 0031e669f0db5a61e069161ffbcb031e0a8b51f6b5e498e1ca08d628af3fcdfc
[594] miner.Miner<Miner:a9c09>:OUTPUT: Rejected block 0031e669f0db5a61e069161ffbcb031e0a8b51f6b5e498e1ca08d628af3fcdfc
[596] miner.Miner<Miner:a9c0b>:OUTPUT: Rejected block 003615d0014be33ff1f8c1258f79c864d6b17ea686ce623feec3345e85ad5b64
Blockchain of node <Miner:a9c0a>:
Chain Length: 4

        Block: {
    "version": "0.1",
    "index": 0,
    "previous_hash": "0",
    "timestamp": 141385154705,
    "difficulty_bits": 10,
    "nonce": 1,
    "blockhash": "d31504ee49203e6910482b8eab898336b8c0dcb9545da9b55acb47fce89f12ee",
    "merkleroot": "1751bd9aa5541bf0a8a00f7e6cf28906db5b323e5bf7e59c84beaf83402c51ca"
}

        Block: {
    "version": "0.1",
    "index": 1,
    "previous_hash": "d31504ee49203e6910482b8eab898336b8c0dcb9545da9b55acb47fce89f12ee",
    "timestamp": "1543799019",
    "difficulty_bits": 10,
    "nonce": 32,
    "blockhash": "002f499cbdae27235a4283a0eefa721d64fa9456aef305d26d37137a0dfbc2fb",
    "merkleroot": "d6ecdec231f7e64d586793efba37e0e00f87d8f9f1f0bb87f5838226df8b1f9e"
}

        Block: {
    "version": "0.1",
    "index": 2,
    "previous_hash": "002f499cbdae27235a4283a0eefa721d64fa9456aef305d26d37137a0dfbc2fb",
    "timestamp": "1543799020",
    "difficulty_bits": 10,
    "nonce": 568,
    "blockhash": "002a1b33adfb1c1d117275d9d6ad9f957ec08484adc1b792dec19e2bdd259432",
    "merkleroot": "3c2b6dee074bf6c71ea9da00547fd136ea2be303e075843e2610f7048d737a67"
}

        Block: {
    "version": "0.1",
    "index": 3,
    "previous_hash": "002a1b33adfb1c1d117275d9d6ad9f957ec08484adc1b792dec19e2bdd259432",
    "timestamp": "1543799020",
    "difficulty_bits": 10,
    "nonce": 1134,
    "blockhash": "003615d0014be33ff1f8c1258f79c864d6b17ea686ce623feec3345e85ad5b64",
    "merkleroot": "e4ecfdb8327f45e5c266d21afebd46894f344290158a5b23c59a60ec9899a93a"
}



MINER DEAD
```