A Mini Project Report On

Proof of Priority: A Priority based Consensus Algorithm for Blockchain

IT465: Cryptocurrencies and Blockchain Technologies

Submitted to

Dr. Kiran M

Department of Information Technology

National Institute of Technology Karnataka, Surathkal

Submitted by

Yash Dodeja - 16IT149

Bharath Raghunath - 16IT211

Swapnil Chavan - 16IT214

On

22nd November 2019

Methodology

Structures Created :

User - Name,wallet and balance.
Wallet - pair of public and private key generated.
Block - Index,Timestamp,hash,PrevHash,Transactions(2 per block),validator(miner)
Transaction - From ,to,amount,Timestamp

Basic Working of the Consensus Algorithm

This algorithm has two main attributes given to each miner - one is a priority and the other is the number of blocks mined till now. Every time a block is to be mined, all miners are assigned a random priority value. The one with the lowest priority value is given first preference to mine. In case two or more miners have the same priority, the miner with the least blocks mined till then is given the opportunity to mine the block. There may be a case where multiple miners have the same priority and the same number of blocks mined, then any one of the miners is chosen at random.

Transaction Verification

There are two transactions per block. One being the generation transaction which rewards the miner of the block while the other is a dummy transaction of money transfer between two users. Every transaction is signed by the sender(in case of generation transaction, dummy value “bank” is sender) using his RSA private key and then stored in a signed transaction pool that is propagated to all miners. The miners verify these transactions by using the RSA public key and ensures he doesn't spend more than his balance. All valid transactions are only put in the block.

Ensuring Fairness

Proof of Elapsed Time (PoET) is a well known consensus algorithm and is considered to be one of the fairest. Our idea of using priorities instead of making all miners sleep for a random amount of time follows the core concept of PoET and further improvises it by reducing the time taken to pick a winner. Furthermore, adding another parameter for counting blocks mined by every miner and choosing the one with minimum blocks mined in case of priority clash gives fair chance to miners who didn’t get enough chance till now.

Results and Analysis

	50 blocks	100 blocks	150 blocks	200 blocks
Miner 1	5	13	17	26
Miner 2	6	13	19	25
Miner 3	5	12	20	28
Miner 4	5	12	18	21
Miner 5	6	13	21	25
Miner 6	8	13	19	26
Miner 7	6	13	19	26
Miner 8	9	11	17	23
Time taken	~8min 30sec	~17min	~26min	~36min