Simulation of a P2P Cryptocurrency Network with Selfish Miners : Design Document

Input :
n: number of peers in the network
h1: hash value of selfish miner 1
h2: hash value of selfish miner 2
ttx: mean inter-arrival time between transactions
I: average time taken to mine a block

Initialize Honest & Selfish Peers, Connected Graph Add initial Transaction_Gen, Block_Gen Events for each Peer

Clear the Event List. Populate Transactions and visualize Blockchain, Results

Create a new Block by adding feasible txns from pending_txns, add coinbase txn, and update balances at the Block Update pending_txns, pushed_txns, long_Block from Blockchain and bcTree Add Next Block_Gen Event into EventList sendBlockNeighbors

simulate

Simulation Done

Until simulation is complete (# Blocks in BlockChain < blockLimit)

Block_Gen

Peer_Type

Honest_Peer

If already received: return Else, then push into pending_txns Add Transaction_Rec Event into its EventList by computing the Latency

Transaction_Rec

Event Type

Selfish Peer

Create a new Block by adding feasible txns from pending_txns, add coinbase txn, and update balances at the Block Update pending_txns, pushed_txns, long_Block from Blockchain and bcTree Add Next Block_Gen Event into EventList Store in Hidden_BLKs

Choose a neighbor randomly and create a transaction of random_amount > balance Add Next Transaction_Gen Event Add Transaction_Rec Event into its EventList by computing the Latency

Transaction_Gen

Block_Rec

zero_state

True

Add the block at appropriate position and update the longest chain. Also send the block to your neighbours other than your sender.

Discard

No

Valid?

Yes

Send To Peers and Update Revealed_BLK, zero_state

False

Is length of longest chain > length of chain having this block at the end?

Peer_type

Add the block in your blockchain at appropriate position and send the block to your neighbours other than your sender

True

Selfish

Lead goes from 0 to 0

check lead of private chain

Lead goes from 2 to 1

Lead goes from n to n-1 (n>2)

Broadcast your private chain to all the neighbors

Stop mining under the current block and start mining under the received block.

Lead goes from 1 to 0

.

Broadcast 1 block from your private chain to all your neighbors

Broadcast your block to all the neighbors and start mining another block under your block. Set zero_state as true.

200050019 - Bagathi Shiv Kiran
200050020 - Bale Teja Rama Chandra Murthy
200050075 - Moganti Harshadeep