CS572_Week7_HW2_19604_Yujia_Lin

GitHub Repot: https://github.com/blueandhack/Three-Dice-Decentralized-Consensus-Algorithm

Step 1: Independent Verification of each transaction

Create transaction and verify block:

- Collecting UTXO: Bitcoin full nodes track all available and spendable outputs, known as unspent transaction outputs, or UTXO.
- Providing the appropriate unlocking scripts
- Constructing new outputs assigned to a new owner
- Every bitcoin node that receives a transaction will verify the transaction.

Step 2: Independent aggregation of transaction into candidate blocks

- Maintain a local copy of the blockchain.
- Listening for new transactions and new blocks discovered by other nodes
- Collect, validate, and relay new transactions like any other bitcoin node. After validating transactions, a bitcoin node will add them to the memory pool (transaction pool), where transactions wait until they can include in a candidate block.
- Trying to mine a new candidate block by finding a solution to the Proof-of-Work algorithm. A block calls a candidate block because It does not contain a valid Proof-of-Work and, therefore, it is not yet a right block

Step 3: Independent verification of each block

- The node receives newly solved blocks sent from the miners.

- The node validates the newly solved blocks, the block data structure is syntactically valid, and the block header hash is less than the target, block size should be within acceptable limits. The first transaction is a coin base transaction. All transactions within the block are independently verified.
- The validated blocks are added to the blockchain. The honest miners of the solved blocks can spend their earned rewards, and the dishonest miners will have their blocks rejected and lose the reward.
- The node propagates the valid blocks.

Using Three dice to explain the Proof-of-work algorithm

- Target is 12

So the player must throw 11 = 12 - 1 or less to win.

Dice are three thus total possible outcomes are = 216

The player will only lose if player throws dice 1, dice 2 and dice 3:

666,665,664,663,662,661,656,655,654,653,652,651,646,645,644,643,642,636,635,634,
633,626,625,624,616,615,566,565,564,563,562,561,556,555,554,553,552,546,545,544,
543,536,535,534,526,525,516,466,465,464,463,462,456,455,454,453,446,445,444,436,
435,426,366,365,364,363,356,355,354,346,345,336,266,265,264,256,255,246,166,165,156

The probability of win is 135/216

- Target is 5

The player must throw 4 = 5 - 1 or less to win.

Dice are three thus total possible outcomes are = 216

The player will only win if player throws dice 1, dice 2 and dice 3:

1 1 1, 1 1 2, 1 2 1, 2 1 1

The probability of win is 4/216

Step 4: Independent selection of blockchain

- This is the final step in bitcoin's decentralized consensus mechanism: the assembly of blocks into chains and the selection of the chain with the most Proof-of-Work.
- Only the new blocks satisfying validation criteria are maintained by every node:

- Main Blockchain: Those connected to the main blockchain.
- Secondary Blockchain: Those that form branches off the main blockchain.
- Orphan Blocks: Those that do not have a known parent in the known chains.