The Decentralized Consensus Algorithm

Introduction

The goal of decentralized consensus is to create a secure, reliable, and trustless environment for transaction validation and record-keeping in blockchain networks. This innovative approach addresses long-standing issues related to trust and verification in digital transactions while promoting decentralization as a core principle of modern financial systems.

Steps of the Three Dice Decentralized Consensus Algorithm

1. Independent Verification of Transactions

Before a transaction is added to the blockchain, it undergoes a rigorous validation process by each node in the network. This ensures the integrity and security of the Bitcoin network.

Key Validation Steps:

1. The transaction must adhere to the Bitcoin protocol's specific format and data structure.
2. Each input must reference a valid, unspent output (UTXO) in the blockchain.
3. The total value of outputs cannot exceed the total value of inputs.
4. A transaction fee must be included to incentivize miners.
5. The unlocking script provided in the transaction must correctly match the locking script of the referenced UTXO.
6. Digital signatures on inputs must be verified to ensure the authenticity of the transaction.
7. Transactions must adhere to network rules like maximum block size and minimum transaction fees.

By independently verifying transactions, nodes prevent the propagation of invalid or fraudulent transactions, ensuring the overall security and integrity of the Bitcoin network

2. Aggregating Transactions into Blocks

After validating transactions, Bitcoin nodes collect and add them to a transaction pool. These transactions wait to be included in a new block.
A miner, like Jing's node, aggregates these transactions into a candidate block. This block, however, is not yet valid until it contains a valid Proof-of-Work solution.
Once a miner solves the puzzle, the block is added to the blockchain, and the process repeats. The network prioritizes the chain with the most proof-of-work, ensuring consensus and security.

3. Validating a New Block

Bitcoin's blockchain relies on a decentralized consensus mechanism to ensure security and integrity. This mechanism involves a series of steps:

1. Miners compete to solve complex mathematical puzzles, and the first to solve it adds a new block to the blockchain.
2. Each node in the network independently validates the new block, checking its validity and ensuring it adheres to the protocol rules.
3. The network selects the longest chain with the most proof-of-work as the main chain.
4. Blocks that are not part of the main chain are considered orphans and may be added later if their parent block is included.

This consensus mechanism ensures that the network remains secure and that no single entity can manipulate the blockchain. Miners are incentivized to follow the rules and honestly validate blocks, as any dishonest behavior would lead to the rejection of their blocks and the loss of potential rewards.

4. Assembling and Selecting Chains of Blocks

Bitcoin's blockchain operates on a consensus mechanism that ensures the integrity and security of the network. Nodes validate new blocks, adding them to the chain with the most cumulative proof-of-work. This chain becomes the main chain, while others are considered secondary. Miners compete to solve complex puzzles, and the first to solve adds a new block, casting a vote for the chain. This process ensures that the network agrees on the order of transactions and prevents fraudulent activity.

The probabilities calculation of various targets

Simple Target:
What is the probability of win if the taget is 12?

- The player must throw 11 = 12 - 1 or less to win.
  - The player will only lose if he/she throws double-six.
  - Total possible outcomes when rolling 3 dice: 6 * 6 * 6 = 216
  - Only one outcome results in a sum of 12: (6, 6, 6)
  - Therefore, the probability of not rolling a 12 is 215/216.
- The probability of win is 35/36

Difficult Target:
What is the probability of win if the taget is 5?

The probability of the sum is less than 5.

- The player must throw 4 = 5 - 1 or less to win.
  - More than half the dice throws will exceed the target and therefore be invalid.
  - So let's list all the combinations that result in a sum of 4 or less:
  - (1, 1, 1)
  - (1, 1, 2)
  - (1, 2, 1)
  - (2, 1, 1)
  - There are 4 favorable outcomes out of 216 total possibilities.
  - Therefore, the probability of winning (rolling 4 or less) is 4/216