Name: Priyanka, Stu-id:20179

Title:
Three Dice Decentralized Consensus Algorithm for Blockchain Decentralization

---

Introduction

The Three Dice Decentralized Consensus Algorithm is a way for a blockchain network to reach agreement without a central authority. Here, we propose a consensus algorithm inspired by the "Three Dice" game, where nodes use random values generated from dice rolls to contribute to a shared decision-making process.Or, By using a "three dice roll" as a random, fair way to validate blocks, participants can independently verify and agree on the state of the blockchain. Each step of this process involves individual decisions by network nodes to confirm transactions, create new blocks, and choose the correct version of the blockchain. Through this approach, we create a decentralized consensus that everyone in the network can trust.

Step 1: Independent Verification of Each Transaction

Task: Verify each transaction
Description: Every full node independently verifies the validity of each transaction according to the blockchain's criteria (e.g., checking signatures, inputs, outputs).
Process:

1. Nodes collect, validate, and relay transactions to other nodes.
2. Valid transactions are added to the memory pool, where they wait until a mining node can aggregate them into a block.

Example: Alice's transaction to Bob's Coffee Shop is verified by multiple nodes and added to the memory pool.

Step 2: Independent Aggregation of Transactions into Candidate Blocks

Task: Aggregate validated transactions into candidate blocks
Description: Mining nodes aggregate transactions from the memory pool to create a new block. To achieve consensus, miners must validate blocks by completing a proof-of-work, represented by the dice roll in algorithm.
Process:

1. Each mining node independently selects and aggregates transactions into new candidate blocks.
2. Once ready, the node rolls three dice. If the dice roll sum meets or exceeds a target score, the node proposes the block.

Example: Miner Jing aggregates Alice's transaction into Block 277,318 and rolls three dice, seeking to match a predefined target score for validation.

Step 3: Independent Verification of Each Block

Task: Verify new candidate blocks
Description: Every full node independently verifies new blocks received from mining nodes. Nodes check the validity of transactions within the block and the correctness of the dice roll outcome.
Process:

1. Nodes rolls three dice to determine if they reach the target score. If the sum meets or exceeds the score, the node approves the block.
2. Each node communicates its decision to the network.

Example: For a target of 12, nodes roll the dice. If their sum equals or exceeds 12, they accept Block 277,318.

Step 4: Independent Selection of Blockchain

Task: Select the appropriate blockchain
Description: When forks occur, nodes must choose the version of the blockchain with the highest cumulative

"score," or in proof-of-work systems, the greatest computational power.
Process:

1. Nodes roll dice to determine which chain to prioritize.
2. Nodes adopt the longest valid chain.

Example: If multiple chains are available, nodes roll three dice to verify their selection aligns with the highest cumulative score, adopting the longest chain.

Probability Calculations for Various Targets Using Three Dice

In the Three Dice Decentralized Consensus Algorithm, reaching consensus depends on specific probability targets. Validators roll three dice to determine if they meet the required threshold to approve a block. Below, we calculate the probabilities for two target scenarios.

Simple Target: Probability of Winning if the Target is 12

1. Objective: To determine the probability of winning (achieving consensus) if the target sum is 12.
2. Explanation: To win, the validator must roll a total of 11 or less across the three dice. Only specific outcomes—like rolling a double six—will result in a total of 12 or more and thus prevent a win.
3. Calculation:

- When rolling two dice, the player would only lose if they rolled double sixes, so the probability of a win in that case is 33/36.
- When adding the third die to reach a total of 11 or less, the probability of a win remains relatively high.

If the target is 11, the player must roll 10 or less to win, only losing if the sum reaches 11 with combinations like (Dice 1 = 5, Dice 2 = 6) or (Dice 1 = 6, Dice 2 = 5) and (dice1=6, dice2=6).

Total is = (6+5),(5+6),(6+6)➔ Three possibilities. So, the probability of winning here is 33/36

Difficult Target: Probability of Winning if the Target is 5

1. Objective: To determine the probability of winning if the target sum is set to a more challenging number, 5.
2. Explanation: For this more difficult target, the validator must roll a sum of 4 or less across the three dice to win. Many possible outcomes will exceed a sum of 5, making this threshold much harder to meet.
3. Calculation:

- When rolling two dice, the player would lose most often if the sum exceeds 5.
- With three dice, the probability of rolling 4 or less is quite low, meaning more than half the rolls will not reach the target, resulting in a high rate of validation failures.

- **Summary**
- The Three Dice Decentralized Consensus Algorithm offers a unique approach to achieving decentralized consensus by utilizing random probability thresholds. This flexible and tamper-resistant method allows blockchain networks to adjust consensus difficulty by varying the target score, thus ensuring security and reliability.