Three Dice Decentralized Consensus Algorithm

Step 1: Independent verification of each transaction

Transaction creation and verification process:

1. Collecting UTXO(unspent transaction outputs)
2. Providing the appropriate unlocking scripts
3. Constructing new outputs assigned to a new owner
4. Every bitcoin node that receives a transaction will verify the transaction.
5. The resulting transaction is then sent to the neighboring nodes in the bitcoin network so that it can be propagated across the entire bitcoin network

Step 2: Independent aggregation of transaction into candidate blocks

1. Maintain a local copy of the blockchain.
2. Listening for
   - new transactions
   - new blocks discovered by other nodes
3. Collect, validate, and relay new transactions just like any other bitcoin node. After validating transactions, a bitcoin node will add them to the memory pool (transaction pool), where transactions await until they can be included into a candidate block.
4. Trying to mine a new candidate block by finding a solution to the Proof-of-Work algorithm. A block is called a candidate block because it does not contain a valid Proof-of-Work and therefore, it is not yet a valid block

Step 3: Independent verification of each block

Process done by every node

1. The node receives newly solved blocks sent from the miners.
2. The node validates the newly solved blocks.
3. The validated blocks are added to the blockchain.
4. The node propagate the valid blocks.

Step 4: Independent selection of blockchain

1. The final step in bitcoin's decentralized consensus mechanism is
   - The assembly of blocks into chains
   - The selection of the chain with the most Proof-of-Work
2. 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

Item	Three dices
Encoding	Dice 1 + Dice 2 + Dice 3
Objective	Throwing three dices whose summation is less than a specified number (= target = difficult target).
All possibilities	3 (both dices are 1) ~ 18 (both dices are 6)
Related to mining	One can estimate the amount of work it takes to succeed from the difficulty imposed by the target. For example, ▪ If the target of the dice game is 3, if someone has succeeded in casting a winning throw it can be assumed that they attempted, on average, 216 throws.
Total possible outcomes	216 = 6 * 6 * 6 = 6^3 • Each die has 6 outcomes
Easy Target	○ Target is 12 ○ The player must throw 11 = 12 - 1 or less to win. ▪ The player will only lose if he/she throws the sum of dices is greater than 11 ○ For example: 6 6 6, 6 6 1, 6 5 1, 1 6 6, 2 6 6 …..(81 different combinations) ○ The probability of win is 135/216 = 5 / 8 = 0.625. ○ The sum of win's combinations is (1+3+6+10+15+21+25+27+27) = 135 Sum of dices — number of combinations ▪ 3 — 1 ▪ 4 — 3 ▪ 5 — 6 ▪ 6 — 10 ▪ 7 — 15 ▪ 8 — 21 ▪ 9 — 25 ▪ 10 — 27 ▪ 11 — 27
Difficult Target	○ Target is 5: The probability of the sum is less than 5. ○ The player must throw 4 = 5 - 1 or less to win. ▪ To win need, ○ 1 1 1 , 1 1 2, 1 2 1 , 2 1 1 ▪ The probability of the player will lose is 4/216 = 1 / 54 = 0.0185