Three Dice Decentralized Consensus Algorithm

- Decentralized Consensus: a public blockchain network that everyone agrees on even though no one trusts each other or any other authority.

- Step 1: Independent verification of each transaction.
    - Transactions creation and verification process:
        - 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.
    - Listens for new transactions and new blocks discovered by other nodes
    - 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.
    - 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 doesn't contain a valid Proof of Work so it isn't a valid block.
- Step 3: Independent verification of each block
    - Process done by every node
        - The node receives newly validated blocks sent from the miners.
        - The node validates the newly validated blocks.
            - It confirms that the block data structure is valid and the header hash is less than the target. All transactions within the block are also independently verified.
        - The validated blocks are added to the blockchain.
            - The honest miners of the validated blocks can spend their earned rewards.
            - The dishonest miners will have their blocks rejected and lose the reward. Will also not receive any compensation.
        - The node propagates the valid blocks.

- Step 4: Independent selection of blockchain
    - Several blockchains could exist at the same time because of forking
    - 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

    - 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.
- Three Dice Decentralized Consensus Algorithm
    - Simple Target = 12
        - The player needs to roll dice 11 = 12 -1 or less to win.
        - There are three dice so possibility is 216 (6x6x6)
        - The player would lose if the dice is thrown like so:
            - Sum of 12: 25 ways
            - Sum of 13: 21 ways
            - Sum of 14: 15 ways
            - Sum of 15: 10 ways
            - Sum of 16: 6 ways
            - Sum of 17: 3 ways
            - Sum of 18: 1 way
        - 216 - 81 =135
        - Probability of winning is 135/216
    - Difficult Target = 5
        - The player needs to roll dice 4 = 5 - 1
        - The player would win if the dice is thrown like so:
            - (1,1,1) (1,1,2) (1,2,1)(2,1,1)
        - Probability of winning is 4/216