Detailed Steps of Decentralized Consensus

Step 1: Independent verification of each transaction

1. Collecting UTXO
    - Bitcoin full nodes track all available and spendable outputs, known as unspent transaction outputs, or UTXO.
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.

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

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.
    a. One can estimate the amount of work it takes to succeed from the difficulty imposed by the target.
    b. Easy Target:
        i. Target is 12
        ii. The player must throw 11 = 12 - 1 or less to win.
        iii. The player will only lose if he/she throws double-six.
        iv. The probability of win is 35/36.

c. **Difficult Target:**
    i. Target is 5: The probability of the sum is less than 5.
    ii. The player must throw 4 = 5 - 1 or less to win.
    iii. More than half the dice throws will exceed the target and therefore be invalid.

4. The node propagates the valid blocks.

Step 4: Independent selection of blockchain

1. The final step in bitcoin's decentralized consensus mechanism is
    a. the assembly of blocks into chains
    b. the selection of the chain with the most Proof-of-Work.
2. Only the new blocks satisfying validation criteria are maintained by every node:
    a. Main Blockchain: Those connected to the main blockchain
    b. Secondary Blockchain: Those that form branches off the main blockchain
    c. Orphan Blocks: Those that do not have a known parent in the known chains