Decentralized Consensus

Step-1. Independent verification of each transaction

- Transactions creation and verification process:
    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.
    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.
    - The block data structure is syntactically valid
    - The block header hash is less than the target (enforces the **Proof-of-Work**)
    - The block timestamp is less than two hours in the future (allowing for time errors)
    - The block size is within acceptable limits
    - The first transaction (and only the first) is a coin base transaction
        - A dishonest miner could write themselves a coin base transaction for a thousand bitcoin instead of the correct reward.
        - An invalid coin base transaction would make the entire block invalid.
    - All transactions within the block are independently verified.
3. The validated blocks are added to the blockchain.
    - The honest miners of the solved blocks can spend their earned rewards.
    - The dishonest miners will have their blocks rejected and
        - lose the reward
        - waste the effort expended to find a Proof-of-Work solution, thus incurring the cost of electricity without compensation.
4. The node propagates the valid blocks.

Proof of Work Algorithm Example:

Item	Three dices
Encoding	Dice 1 + Dice 2 + Dice 3
Objective	Throwing three dices whose summation is less than a specified number.
All possibilities	3 (all three dices are 1) ~ 18 (all three 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 • Each die has 6 outcomes
Easy Target	○ Target is 12 ○ The player must throw 11 = 12 - 1 or less to win. Probability of a sum of 12: 25/216 ; sum of 13: 21/216 ; sum of 14: 15/216 sum of 15: 10/216 ; sum of 16: 6/216 ; sum of 17: 3/216 sum of 18: 1/216 ⇨ Total of 12 or more = 25+21+15+10+6+3+1 = 81 ⇨ Total of less than 12 = 216 – 81 = 135 $P(E_3)$ = 135 / 216 = 5/8 = 62.5%
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. Number of events of getting a total of less than 5 = 4 i.e. (1, 1, 1), (1, 1, 2), (1, 2, 1) and (2, 1, 1). Therefore, probability of getting a total of less than 5 $P(E_3) = \frac{\text{Number of favorable outcomes}}{\text{Total number of possible outcome}}$ = 4/216 = 1/54 = 1.85%

Step-4. Independent selection of blockchain

- 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:
  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