CS572 Week9
Name: Quan Zhou
ID: 19539

4 stpes of Decentralized Consensus:

1. Independent verification of each transaction

   Summary:

   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.

2. Independent aggregation of transaction into candidate blocks

   Summary:

   - Maintain a local copy of the blockchain.
   - Listening for
     a. new transactions
     b. new blocks discovered by other nodes
   - Collect, validate, and relay new transactions just like any other bitcoin node.
     a. 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. A block is called a candidate block because
        1. It does not contain a valid Proof-of-Work
           a. and therefore, it is not yet a valid block

3. Independent verification of each block

   Summary:

   Process done by every node

   - The node recieves newly solved blocks sent from the miners.
   - The node validates the newly solved blocks.
   - The validated blocks are added to the blockchain.
   - The node propagate the valid blocks.

4. Independent selection of blockchain

   Summary:

   a. 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.
   b. Only the new blocks satisfiying 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

Three Dice Decentralized Consensus Algorithm:

<table>
<tr><th>Three dices</th><th>Phrase + Nonce (0 ~ 19)</th></tr>
<tr><td><b>Encoding</b></td><td>Dice 1 + Dice 2 + Dice 3</td></tr>
<tr><td><b>Objective</b></td><td>Throwing three dices whose summation is less than a specified number.</td></tr>
<tr><td><b>All possibilities</b></td><td>3 (both dices are 1) ~ 18 (both dices are 6)</td></tr>
<tr><td><b>Related to mining</b></td><td>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.</td></tr>
<tr><td><b>Total possible outcomes</b></td><td>216 = 6 * 6 * 6
- Each die has 6 outcomes</td></tr>
<tr><td><b>Easy Target</b></td><td>- Target is 12
    - The player must throw 11 = 12 - 1 or less to win.
<table>
<tr><th>The sum of the dice</th><th>Combination(kinds)</th></tr>
<tr><td>3</td><td>1</td></tr>
<tr><td>4</td><td>3</td></tr>
<tr><td>5</td><td>6</td></tr>
<tr><td>6</td><td>10</td></tr>
<tr><td>7</td><td>15</td></tr>
<tr><td>8</td><td>21</td></tr>
<tr><td>9</td><td>25</td></tr>
<tr><td>10</td><td>27</td></tr>
<tr><td>11</td><td>27</td></tr>
</table>
- Based on the table above the total combinations of sum less than or equal to 11 is (1 + 3 + 6 + 10 + 15 + 21 + 25 + 27 + 27) = 135
- Thus, the probability of winning is 135/216 = 5/8</td></tr>
</table>

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. ▪ The player will win if he gets (1, 1, 1), (1, 1, 2), (1, 2, 1), (2, 1, 1) ▪ Then the probability of win is 4/216