Optimal Strategic Mining Against Cryptographic Self-Selection in Proof-of-Stake

Matheus V. X. Ferreira, Ye Lin Sally Hahn, S. Matthew Weinberg, Catherine Yu

Blockchain consensus background
- Distributed ledger of transactions. Blocks modify the state.

How to pick a leader to propose the next block?
1. **Strawman leader election:**
   a) Let agents propose blocks.
   b) Pick one uniformly at random.

2. **Proof-of-Work leader election:**
   a) The first agent to solve a puzzle gets to be the leader.

3. **Proof-of-Stake leader election:**
   a) Sample a uniformly random coin.
   b) The leader is the owner of the coin.

Research Question
2. [Chen, Micali ’17] proposes a cryptographic self-selection protocol
   a) Start from a truly random string $Q_0$.
   b) Build a pseudo-random string $Q_1$ from $Q_0$ (goal is to minimize the chance of $Q_1$ being biased).
3. Well-known the cryptographic self-selection strategy is not a Nash equilibrium. Can we bound the revenue of optimal deviations?

Revenue Upper Bound
1. Consider an omniscient Alice that can compare her score to Bob’s.
2. The revenue of the optimal omniscient strategy upper bounds the revenue of the optimal strategy.

The One-Lookahead Deviation
- Divide the stake among 2 accounts $A_1$ and $A_2$.

<table>
<thead>
<tr>
<th>$S_A(Q_0)$</th>
<th>$S_{A_1}(Q_0)$</th>
<th>$S_{A_2}(Q_0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>25% of stake</td>
<td>25% of stake</td>
<td>50% of stake</td>
</tr>
</tbody>
</table>

- If $S_{A_1}(Q_0) < S_{A_2}(Q_0) < S_{A_0}(Q_0)$:
  1. Broadcast only $S_{A_1}(Q_0)$, then her first account is the leader.
  2. Broadcast only $S_{A_2}(Q_0)$, then her second account is the leader.
  3. Broadcast nothing, then Bob is the leader.

- Miner Objective Function: maximize the fraction of blocks they propose.
  1. Receives new coins, transaction fees, ...
  2. Stake compounds overtime.

References
- [Ferreira and Weinberg ’21] Proof-of-Stake Mining Games with Perfect Randomness.
- [Chen and Micali ’17] Algorand.