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

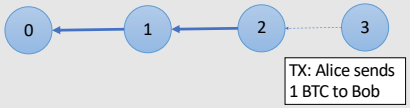
Harvard John A. Paulson School of Engineering and Applied Sciences

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

PRINCETON UNIVERSITY

Blockchain consensus background

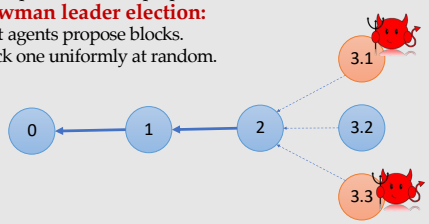
- Distributed ledger of transactions. Blocks modify the state.



- How to pick a leader to propose the next block?

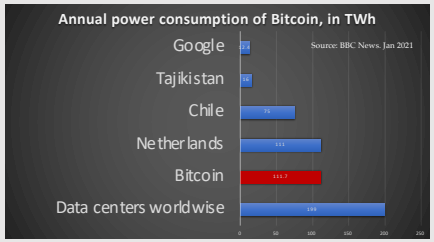
1. Strawman leader election:

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.

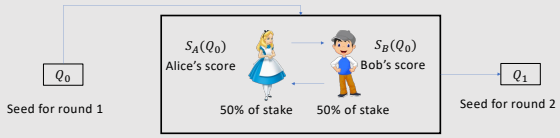
a) Sample a uniformly random coin.
b) The leader is the owner of the coin.

Research Question

- **How to reach consensus on a uniformly random coin?**
  1. [Ferreira, Weinberg, '21] considers an external random source.
     a) Obtain Nash equilibrium guarantees similar to Proof-of-Work.
  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)
- Well-known the cryptographic self-selection strategy is not a Nash equilibrium. Can we bound the revenue of optimal deviations?

The cryptographic self-selection game

1. Start with a pseudo-random string Q_0 (seed for round 1).
2. Each account samples (privately) a random string $S_i(Q_0)$ (referred as a score).
3. The lowest scoring account is the leader for this round.
4. The score of the leader is the seed for the next round $Q_1 = S_i(Q_0)$ (seed for round 2).



$\Pr[S_A(Q_0) < S_B(Q_0)] = Alice's\ stake$

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

The One-Lookahead Deviation

- Divide the stake among 2 accounts A_1 and A_2.

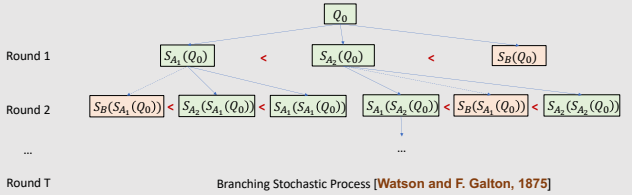
- If $S_{A_1}(Q_0) < S_{A_2}(Q_0) < S_B(Q_0)$:

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.

4. Broadcast only the score most likely to win this round and the next.

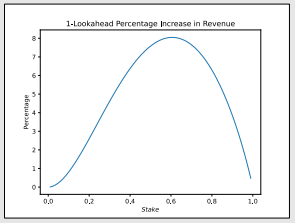
Revenue Upper Bound

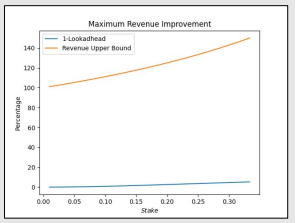
1. Consider an omniscient Alice that can *compare* her score to Bob's.
2. The revenue of the optimal omniscient strategy upper bounds the revenue of the optimal strategy.



Branching Stochastic Process [Watson and F. Galton, 1875]

- **Technique**: upper bound the revenue by analyzing a stopping time.
- **Stopping time**: a sufficient condition for the adversary to reset the state of the game.
  - The event where Bob has the smallest score is a stopping time since the next seed is unbiased.
  - The height of the tree upper bounds the stopping time.
- [Phase Transition Theorem]: the height of the branching tree is finite *if and only if* Alice owns less than 38% of the stake.





References

- [Ferreira and Weinberg '21] Proof-of-Stake Mining Games with Perfect Randomness.
- [Chen and Micali '17] Algorand.
- [Watson and F. Galton, 1875] On the Probability of the Extinction of Families.