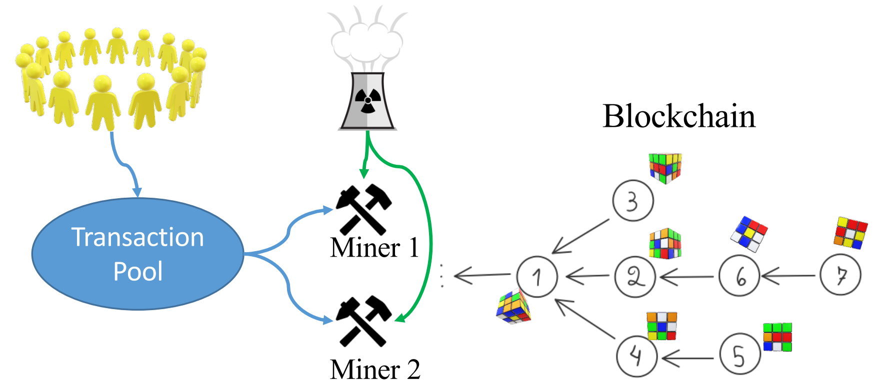
Proof-of-Stake Mining Games

Matheus V. X. Ferreira, S. Matthew Weinberg
{**mvxf**, smweinberg}@princeton.edu
Princeton University

OBJECTIVES

Problem: *How economic incentives in the Proof-of-Stake (PoS) consensus algorithm compare to Proof-of-Work (PoW)? Under which conditions honest mining is an equilibrium in PoS?*

Proof-of-Work and the Consensus Problem



Conflicting Histories:

Block 1
Bob: Owns $5

Block 2
Bob: Send $5 to Charlie

Block 3
Bob: Send $5 to Alice

Proof-of-Stake Consensus:
- ➢ Use public randomness to elect leader.
- ➢ No energy waste.
- ➢ Resilient to market volatility (energy cost).

Model

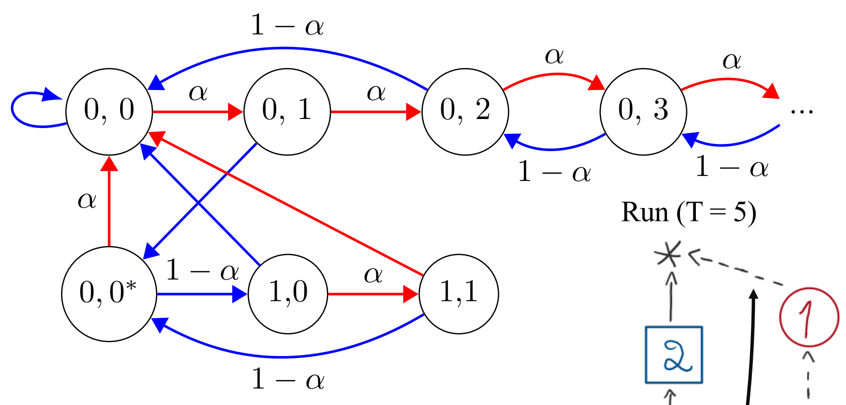
- **Miner 1** is strategic an owns $\alpha < ½$ of the stake.
- **Miner 1** is free to deviate to any strategy π that is ***undetectable.***
- **Miner 2** owns $1 - \alpha > ½$ of the stake and follows honest mining.
- The stake is constant through the game.
- At time $t \in \mathbb{N}$, **Miner 1** receives slot t with probability α.
- Only the elected owner of slot **t** can create a block with slot **t**.
- **Miner 1** wish to maximize their fraction of blocks in the longest chain in an unbounded execution:

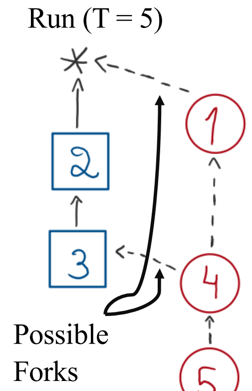
$$Rev(\pi) = E\left[\liminf_{T\to\infty} \frac{\sum_{t=1}^{T} r_t^1(\pi)}{\sum_{t=1}^{T}(r_t^1(\pi) + r_t^2(\pi))}\right]$$

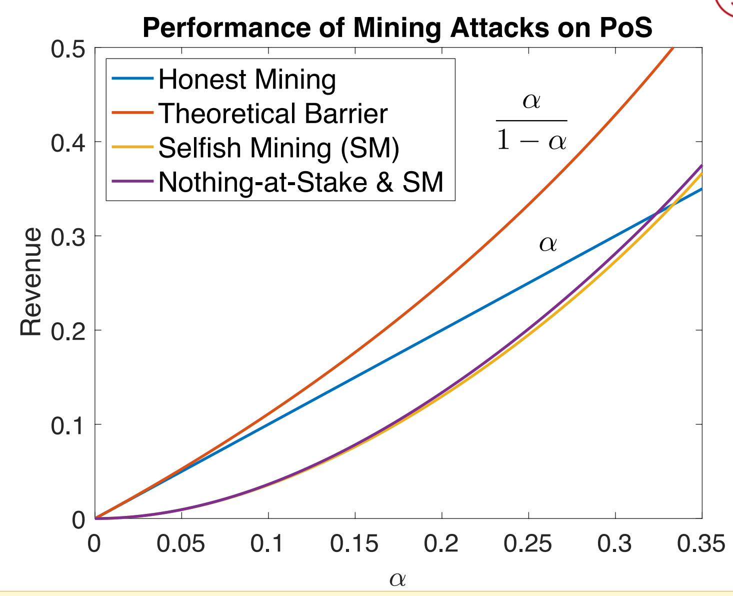
Nothing-at-Stake and Selfish Mining Attacks

There are strategies in **PoS** that are more profitable than any strategy in **PoW**!

*Markov Chain Representing a **Selfish Mining** Attack augmented with **Nothing-at-Stake** Attack*







Optimal **PoS** strategies **must** forget the history often.

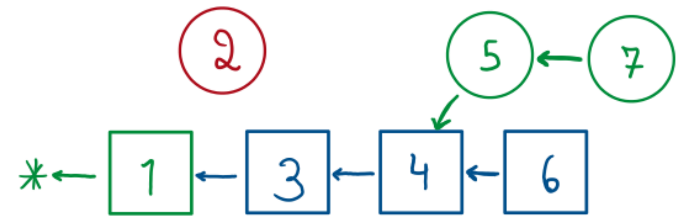
Definition – ***Ergodic Strategy***

A strategy π is ergodic if π can be represented by a Positive Recurrent Markov Chain (i.e., the expected time to forget $E[\tau]$ is finite):

$$\lim_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T} r_t^k(\pi) \overset{a.s.}{=} \frac{E[\sum_{t=1}^{\tau} r_t^k(\pi)]}{E[\tau]}$$

Reduction to Ergodic Strategies

Definition - ***Checkpoints***
- The genesis block (block 0) is a **checkpoint**.
- If block **s** is a **checkpoint**, then **t > s** is a checkpoint if **t** is the first block after **s** such that the number of blocks owned by **Miner 1** in the path from **s** to **t** (not including **s**) is bigger or equal than the number of unpublished slots from **s+1** to **t**.



Checkpoint Reduction Lemma
- ➢ For every strategy π, there is a strategy $C(\pi)$ that never overrides a checkpoint and $Rev(C(\pi)) \geq Rev(\pi)$.
- ➢ $C(\pi)$ can only be optimal if it reaches checkpoints often.
- ➢ If $C(\pi)$ is optimal, then $C(\pi)$ is ergodic.

➢ Ergodic → Linear Comparison Test:

$$v^\pi(\rho) = E\left[\sum_{t=1}^{\tau}(1-\rho)r_t^1(\pi) - \rho r_t^2(\pi)\right]$$

$$v^\pi(Rev(\pi)) = 0$$

$$v^{\tilde\pi}(Rev(\pi)) \geq 0 \iff Rev(\tilde\pi) \geq Rev(\pi)$$

Theorem (Strong Law of Large Numbers for Ergodic Strategies)

Honest mining is optimal if and only if for all ergodic strategies π:

$$E\left[\sum_{t=1}^{\tau}(1-\alpha)r_t^1(\pi) - \alpha r_t^2(\pi)\right] \leq 0$$

Example - Self Override

For $\alpha = \sqrt{2} - 1$, honest mining is not optimal, and there is an event **E** such that **Miner 1** prefers to override their own blocks.