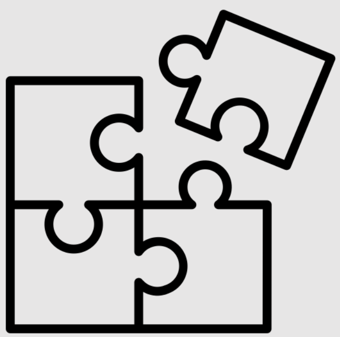
Proof-of-Stake Mining Games with Perfect Randomness

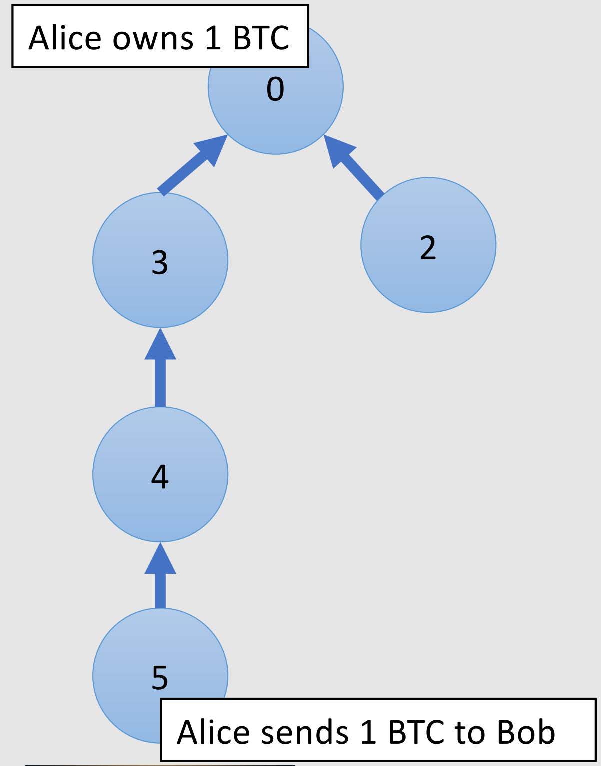
Matheus V. X. Ferreira, S. Matthew Weinberg

PRINCETON UNIVERSITY

Blockchains are Mechanisms

- **Users**
  - Alice owns 1 BTC.
  - Alice wishes to pay Bob with 1 BTC.
- **Miners (implement the longest chain rule)**
  - Extend the longest path with a block (containing transactions).
  - Receive new coins as incentive.

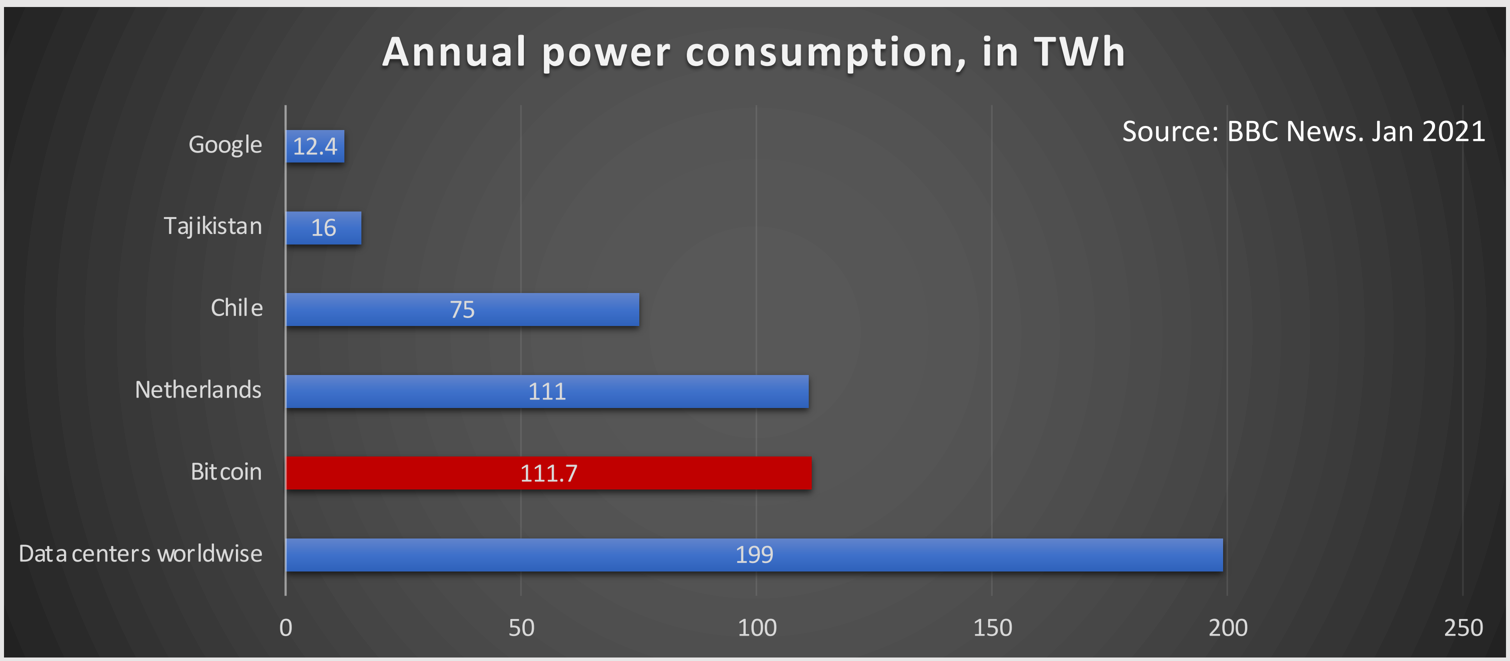




6.25 Bitcoins

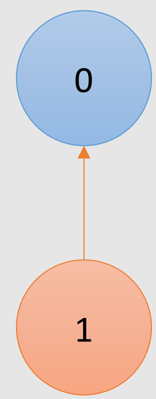
Environmental cost of Bitcoin

- Bitcoin's consensus algorithm is based on proof-of-work.
  - Energy intensive yet can only process 7 transactions per second.



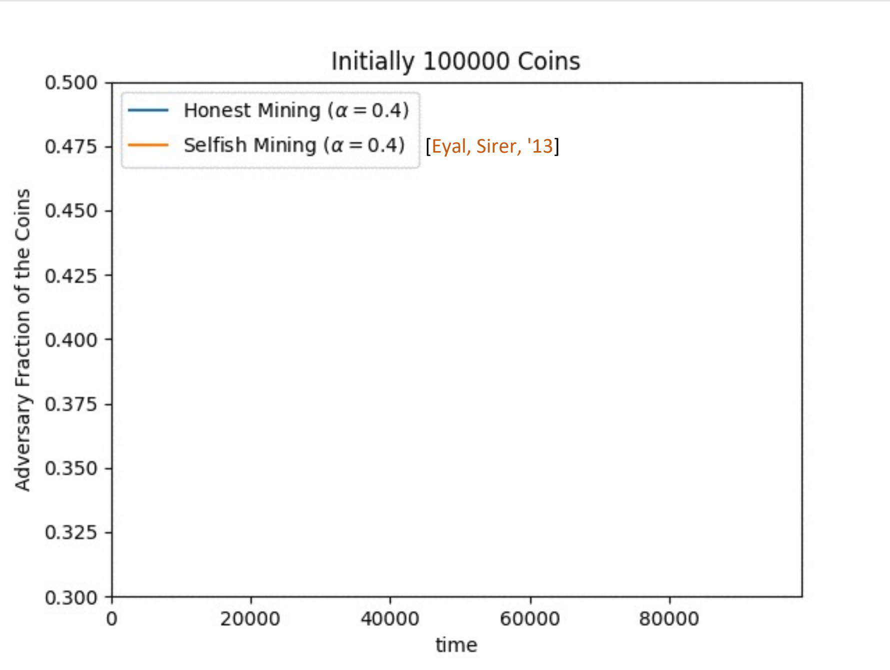
Beyond Proof-of-Work

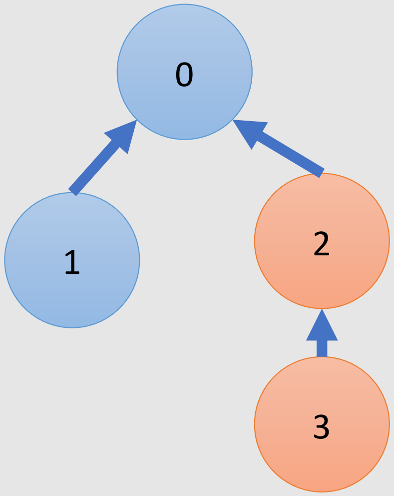
- **Proof-of-work** (PoW) requires miners to **compete** to solve crypto puzzles
- **Proof-of-stake** (PoS) is an energy friendly alternative.
  - **Tournament**: sample a uniformly random coin.



Incentives in Proof-of-Stake Blockchains

• Will miners be motivated to follow the protocol?





- **Adversary** owns 40000 coins.
- **Other** (honest) miners owns 60000 coins.

➢ **Adversary's Objective Function**:
  ➢ Maximize fraction of blocks in longest path.

Desiderata

Under which conditions is honest mining a Nash equilibrium?

[Brown-Cohen, Narayanan, Psomas, Weinberg ‘18] gave a **formal barrier**. For any longest-chain protocols, **IF**

- Mining is computationally **efficient** (like Proof-of-Stake).
- All source of pseudo-randomness comes from the blockchain itself.

THEN, Honest mining is **NEVER** a Nash equilibrium.

Proof-of-Stake mining games with perfect randomness [FW '21]

- There is a PoS protocol with access to **random beacon** [Rabin '83] where honest mining **IS** a **Nash equilibrium** when no miner owns more than 30.8% of the currency.

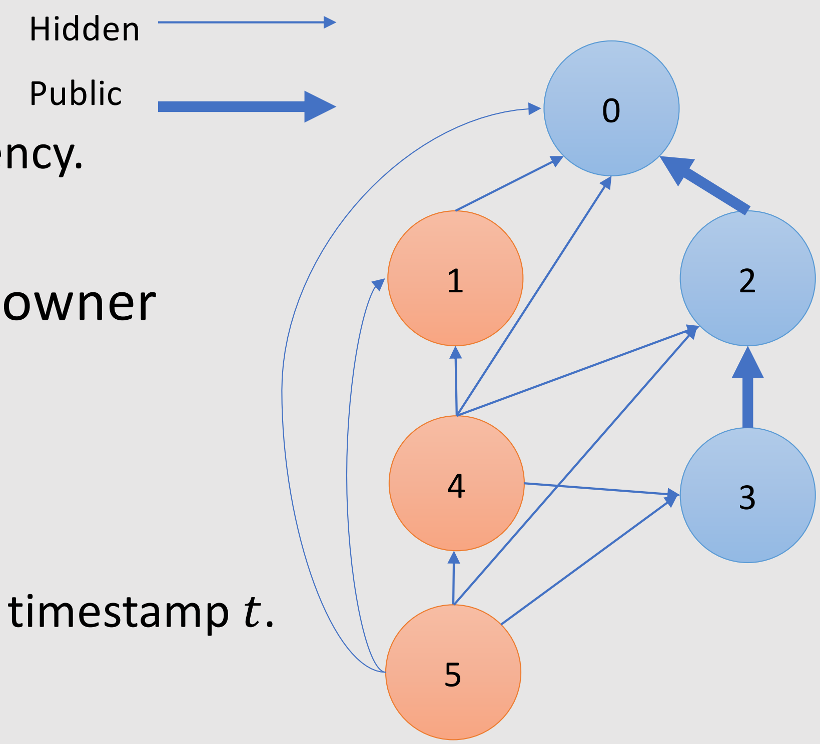
Existing public random sources

Country	Start date	Randomness source
USA	July 2018	Circuit noise
Chile	July 2018	Circuit noise, earthquakes, twitter, radio streams
Brazil	End of 2019	Circuit noise, radioactive decay

Source: **Science**. Why are countries creating public random number generators? Jun 2018.

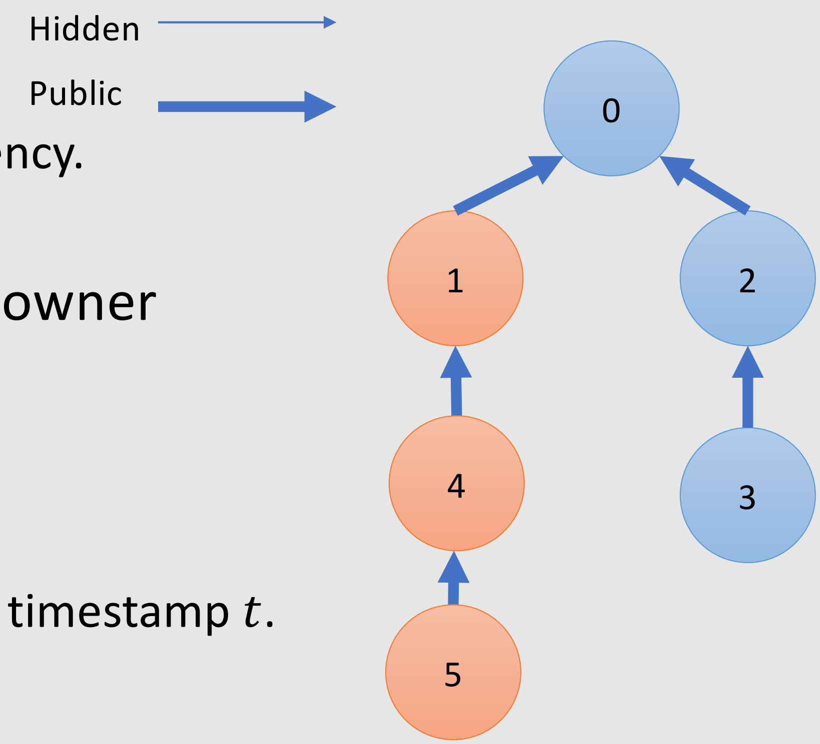
Model: PoS with random beacon

- Two player game:
  - **Adversary** owns $\alpha < 1/2$ fraction of currency.
  - **Everyone else** follows the honest strategy.
- Each time step t, sample one coin. The owner receives the privilege to create block t.
- Block t can point to any block $s < t$.
- Punish detectable dishonest behavior:
  - Example: publish two or more blocks with timestamp t.



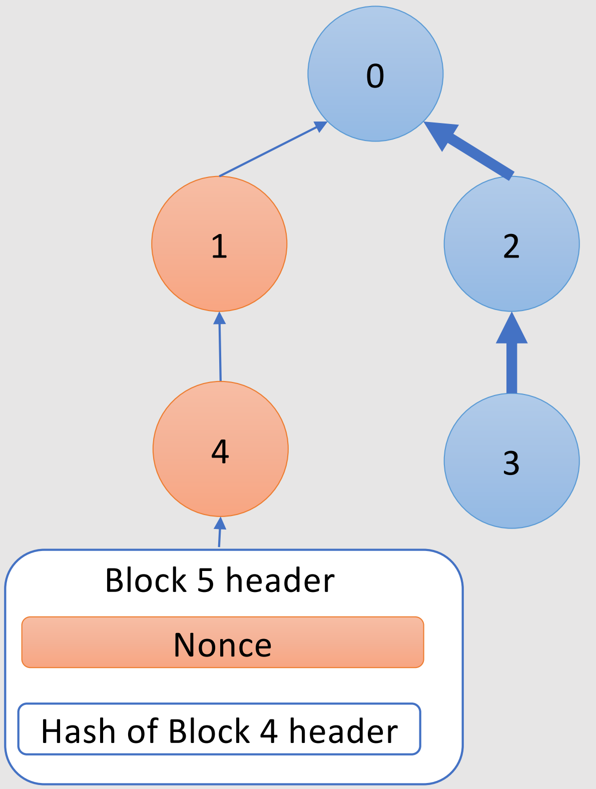
Model: PoS with random beacon

- Two player game:
  - **Adversary** owns $\alpha < 1/2$ fraction of currency.
  - **Everyone else** follows the honest strategy.
- Each time step t, sample one coin. The owner receives the privilege to create block t.
- Block t can point to any block $s < t$.
- Punish detectable dishonest behavior:
  - Example: publish two or more blocks with timestamp t.

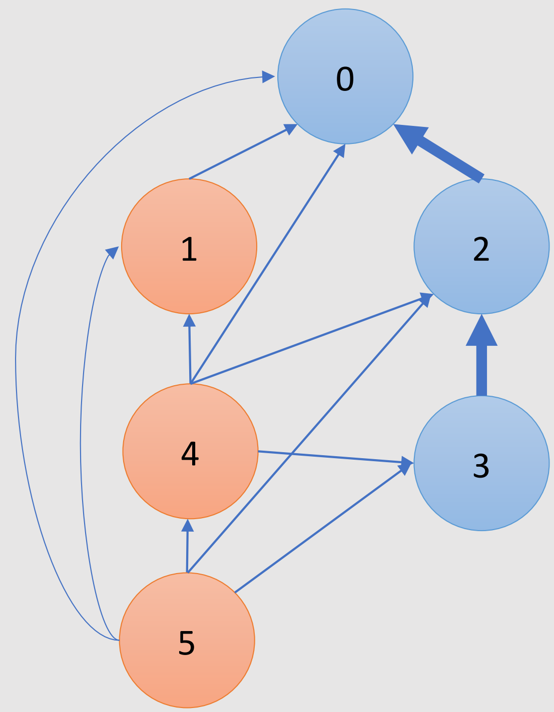


PoW games are a special case of PoS games

Proof-of-Work (PoW)

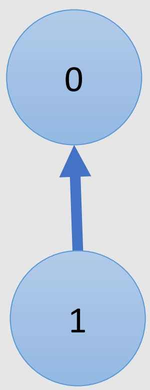


Proof-of-Stake (PoS)

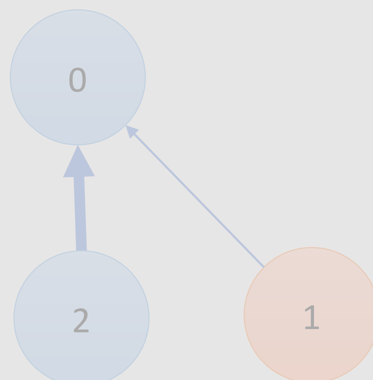


Nash equilibrium

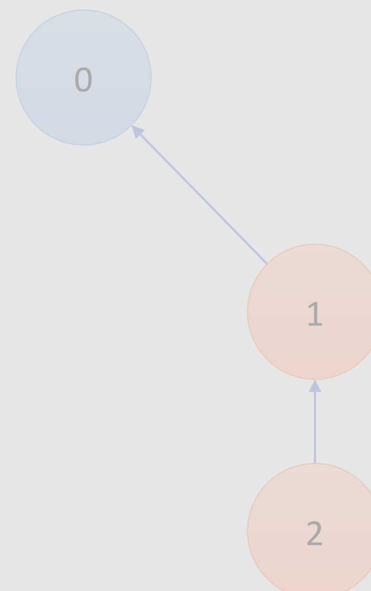
Case 1



Case 2

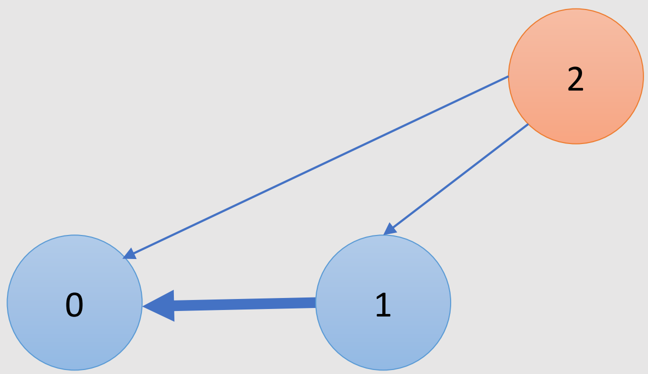


Case 3



Nash equilibrium – Case 1

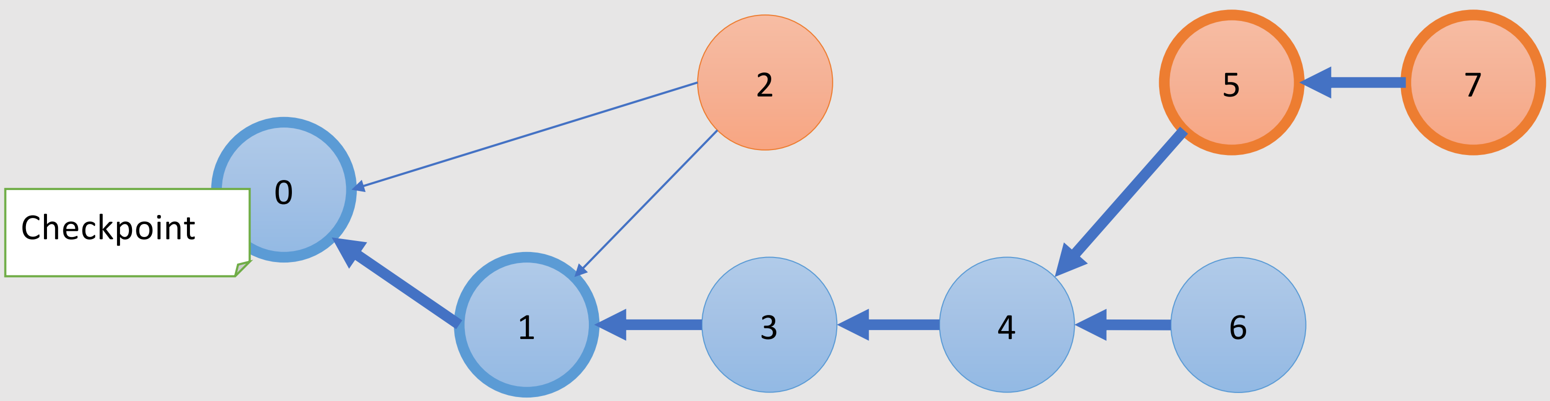
- Honest miner publishes the first block.



Claim: There is an optimal strategy for the adversary that never forks block 1.

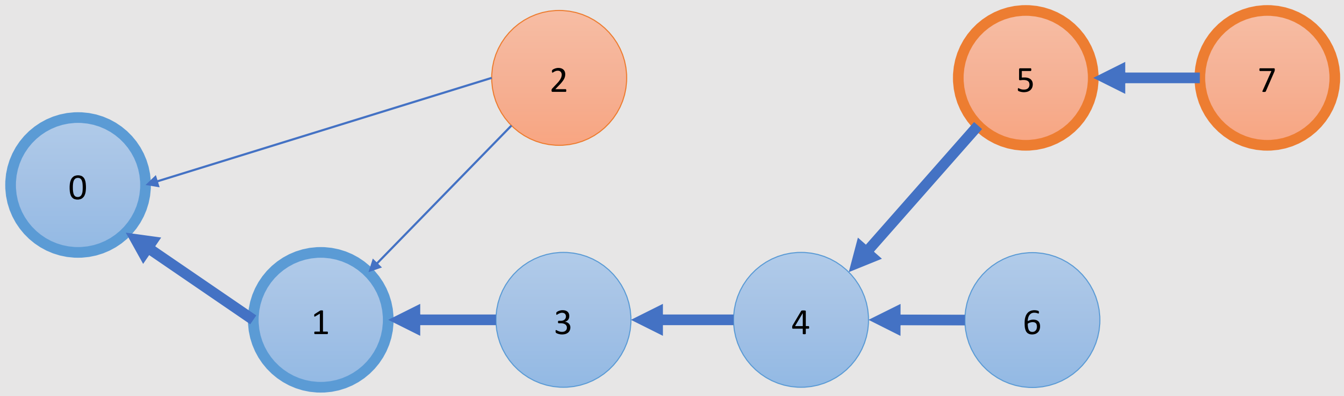
Checkpoints

- Increasing sequence of blocks $P_0, P_1, P_2, \ldots$ in the **longest path**.
  - Block 0 is P_0.
  - P_1 is the first block after P_0 where the # published blocks the adversary owns in interval $(P_0, P_1]$ is at least the # unpublished blocks from the interval $(P_0, P_1]$.



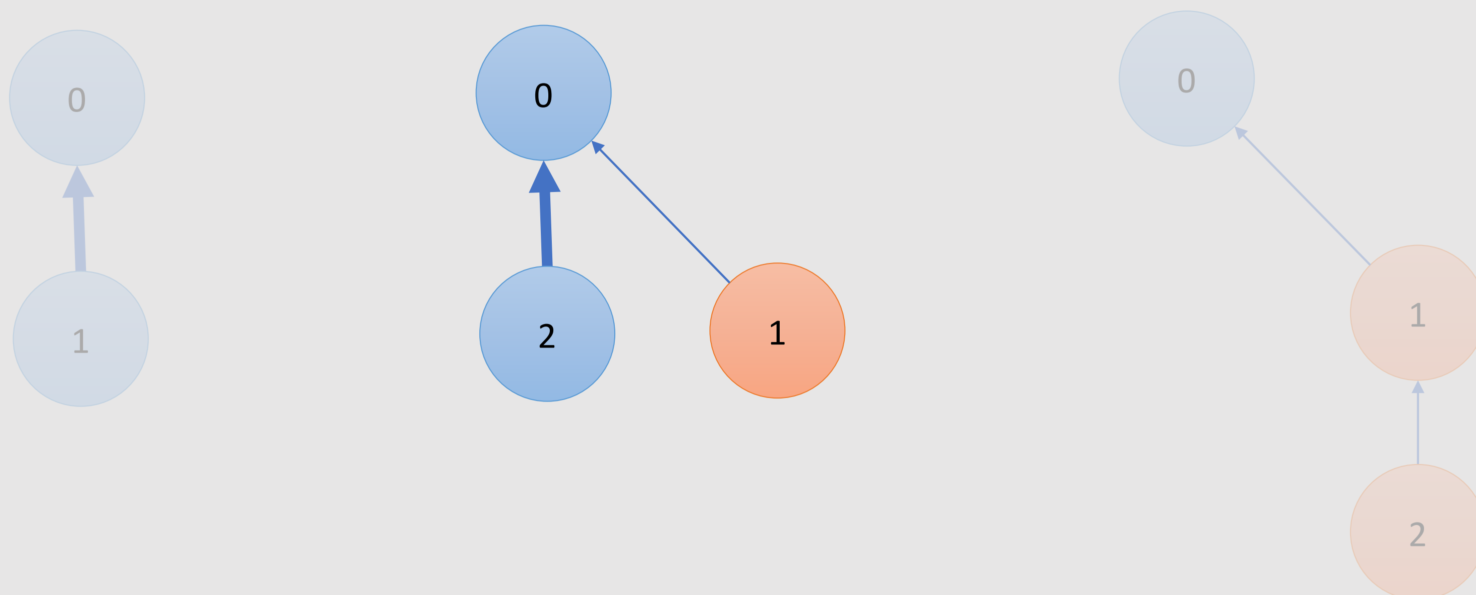
Strong Recurrence

- **[Theorem]** There is an optimal strategy that returns to the **initial state** whenever a new **checkpoint** is defined and $\mathrm{E}[\tau] < \infty$.
  - Random variable $\tau \geq 1$ denotes the time step checkpoint P_1 is defined.



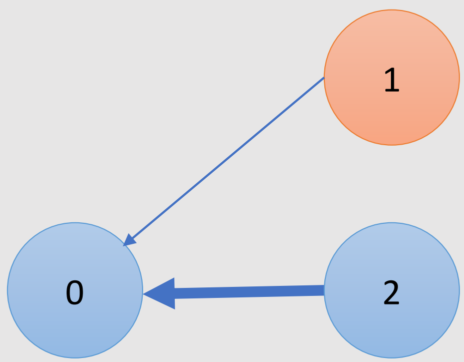
Nash equilibrium

Case 1 Case 2 Case 3



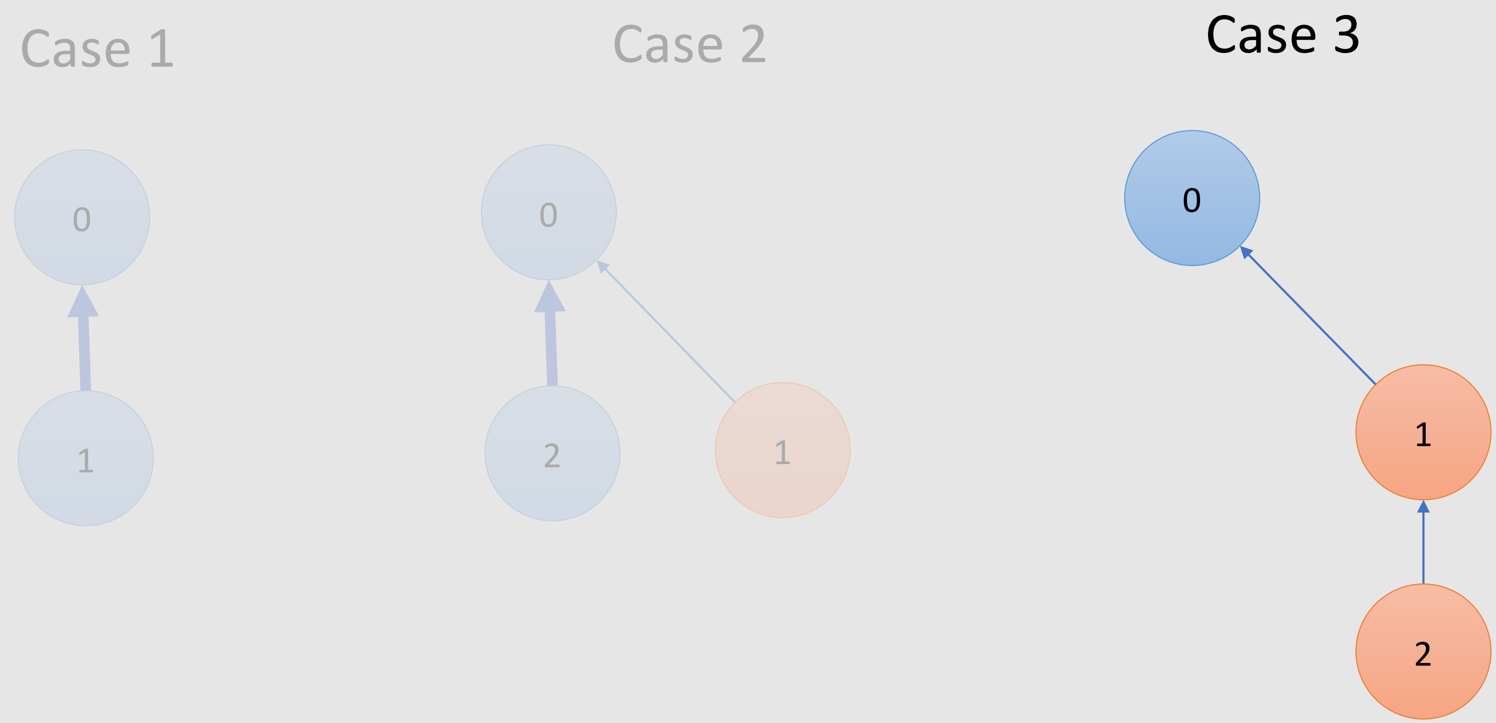
Nash equilibrium – Case 2

- Adversary wins the first block, but honest miner wins the second



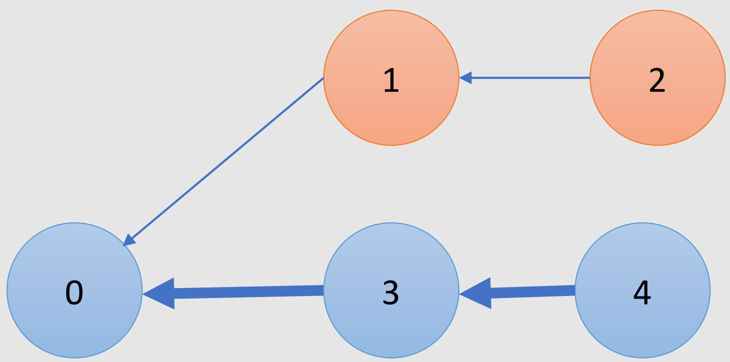
The probability of winning a tie-breaking is at most $\frac{\alpha}{1-\alpha}$

Nash equilibrium



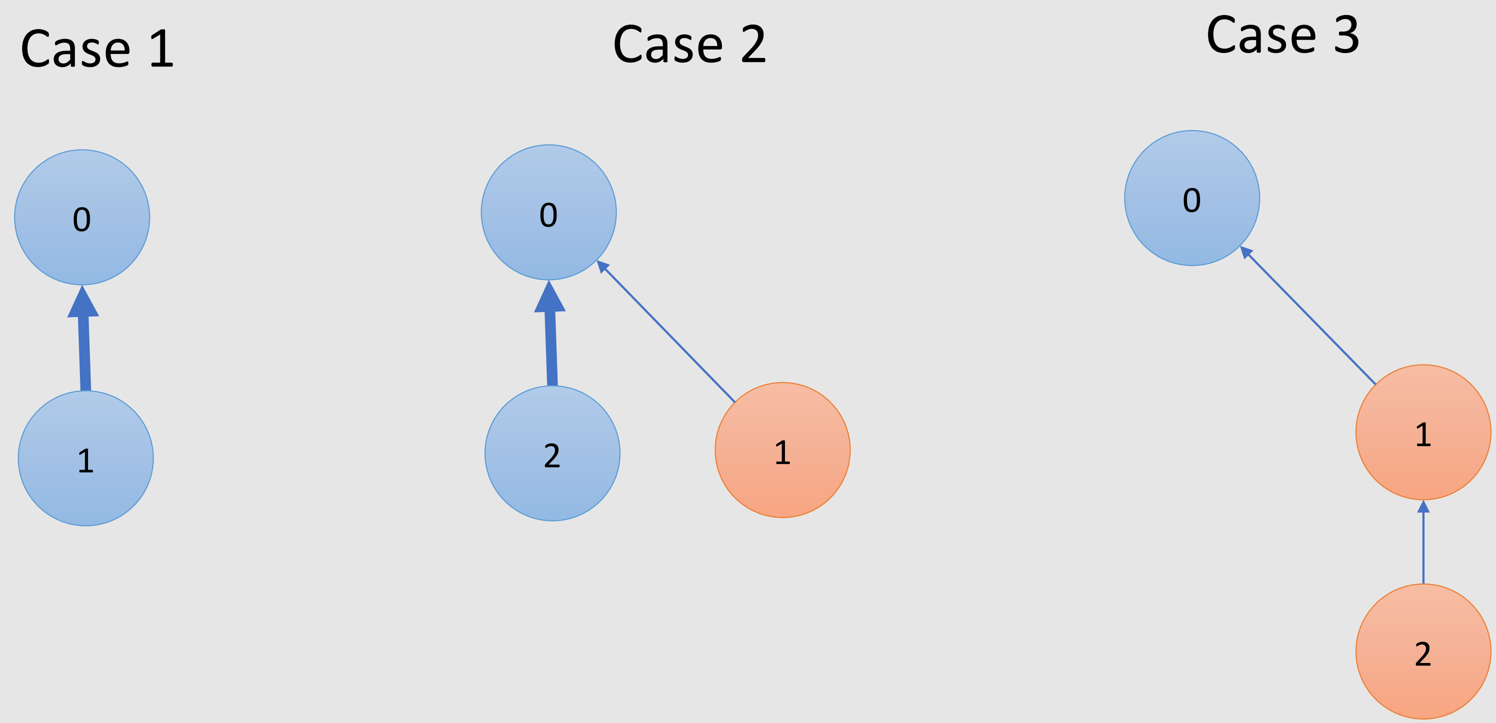
Nash equilibrium – Case 3

- Adversary wins the first two blocks.



The probability of winning a tie-breaking is at most $\frac{\alpha}{1-\alpha}$

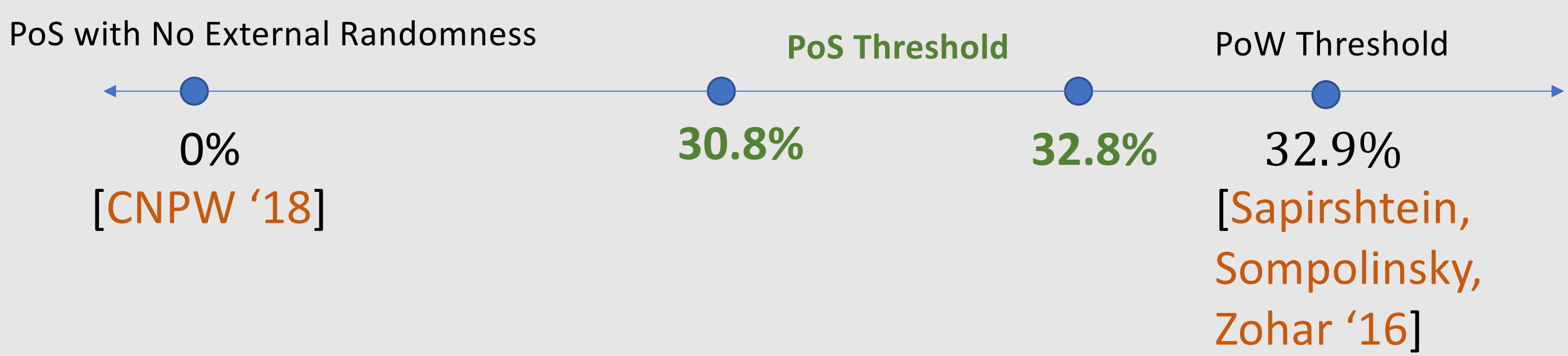
Wrapping up



Main results

- Honest mining **IS** a **Nash equilibrium** if all miners own at most 30.8% of currency.

- Honest mining **IS NOT** a **Nash equilibrium** if some miner owns more than 32.8% of the currency.



Conclusions

Proof-of-stake with access to trusted randomness overcomes the limitations of Proof-of-work and can approximate the security guarantees.

How to leverage existing public random sources to design proof-of-stake blockchains?