Selfish Mining under General Stochastic Rewards

Maryam Bahrani*, **Mike Neuder**†, Matt Weinberg†

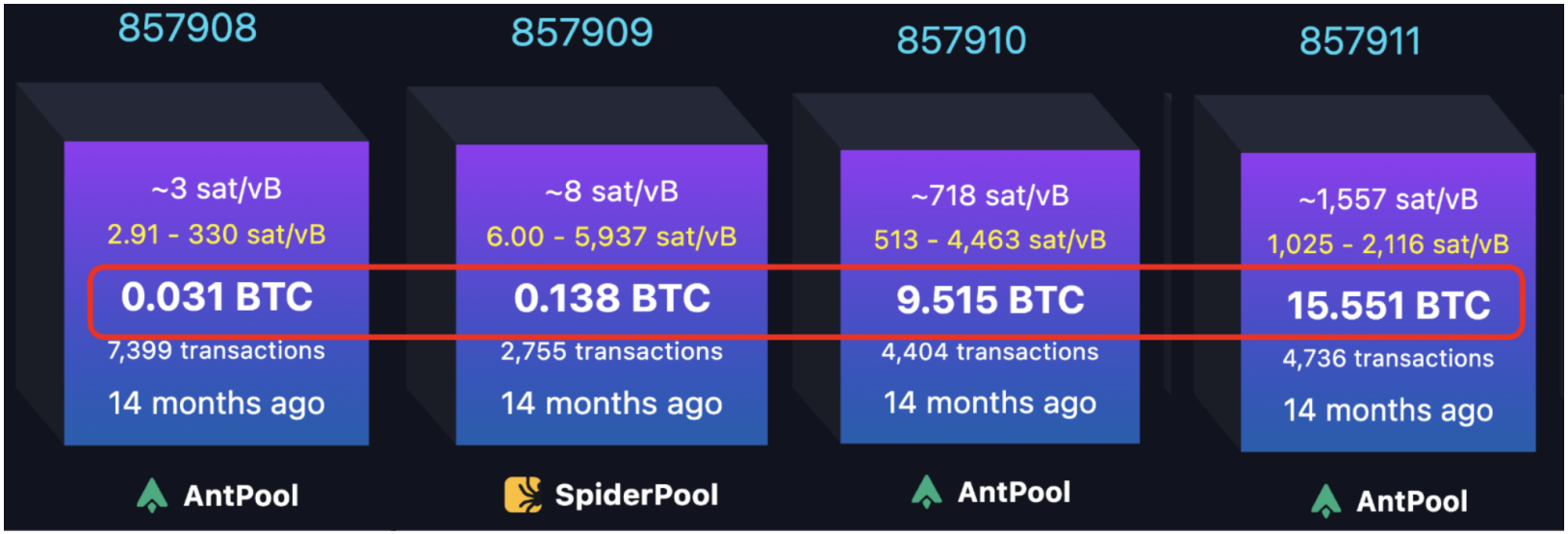
IC3 Winter Retreat

Tuesday – January 6th, 2026

*Ritual, †Princeton University

Motivating example

The launch of Babylon



- In August 2024, bitcoin fees spiked 500× from 0.031 → 15.551 BTC within four blocks.
- The block reward during that period was 3.125 BTC.

https://mempool.space/block/000000000000000000151faeaa14ca333a9a5edc3fa7da906413d27a1fe2532

Motivation

Related work

- The incentives of consensus mechanisms can depend **heavily** on exogenous events.
- Yet, the selfish mining literature has largely focused on the *block reward regime.* There are a few notable exceptions!
- [CKWN'16] show that selfish mining is still present (and actually even more profitable) when only considering transaction fees.
- [ZHET'23] show that "whale transactions" (those which pay extremely high transaction fees) can also lower profitability thresholds.
- Quoting [FNGA'25] "we find that only 3 works include transaction fees in their modeling."

[CKWN'16] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 154–167, 2016.

[ZHET'23] Roi Bar Zur, Ameer Abu-Hanna, Ittay Eyal, and Aviv Tamar. Werlman: To tackle whale (transactions), go deep (RL). In 44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023, pages 93–110. IEEE, 2023. doi:10.1109/SP46215. 2023.10179444.

[FNGA'25] Colin Finkbeiner, Mohamed E Najd, Julia Guskind, and Ghada Almashaqbeh. SoK: Time to be selfless?! demystifying the landscape of selfish mining strategies and models. Cryptology ePrint Archive, 2025.

Our contributions

- **Practical:** We analyze selfish mining under a reward function encompassing block rewards, transaction fees, and MEV spikes.
  - Answers the pragmatic question: "how vulnerable is Proof-of-Work to selfish mining under combined rewards?"
  - Painting a more unified picture between thresholds of $\alpha = 0.329$ from [SSZ'16] and $\alpha = 0.07$ from [CKWN'16].
- to do $\uparrow$, we also develop a more general framework $\downarrow$
- **Modeling**: We characterize *properties* of reward functions.
- **Methodology**: We present a new technique for calculating expected attacker profits under general stochastic reward functions.

Model

Nakamoto Consensus Game

- We study the Nakamoto Consensus Game.
- There is a set of miners M, where at each time t, each $m \in M$ has
  - the public view V_t, and
  - a private view $V_t^m \supseteq V_t$.
- Each round, every miner picks a block to mine on.
- The wining miner can publish the block (update the public view) or keep it private; **(new)** this decision now factors in exogeneous rewards.
- **(new)** Because rewards are time-dependent, we have to explicitly model difficulty adjustment.

Model

Reward function examples

- Block rewards are constant at 3.125 BTC.
- Transaction fees are modeled as linear-in-time since parent block $t - \text{timestamp}(B)$ in [CKWN'16].
- MEV/Whale transactions are modeled as the result of a Bernouli trial

$$R = \begin{cases} 10 & \text{if } X = 1 \\ 0 & \text{otherwise} \end{cases}, \text{ where } X \sim \text{Bernoulli}(p),$$

  in [ZHET'23].
  - Our model is general enough to capture all of these.

Model

Static rewards

- We focus on a specific, time-dependent set of reward functions, which we call static.
- Static rewards only depend on the *time since the parent block*.
- We can rewrite static reward functions as a (potentially random) function of Δ.
- Note that static rewards can still be random and/or non-linear in Δ.

Transaction fee example

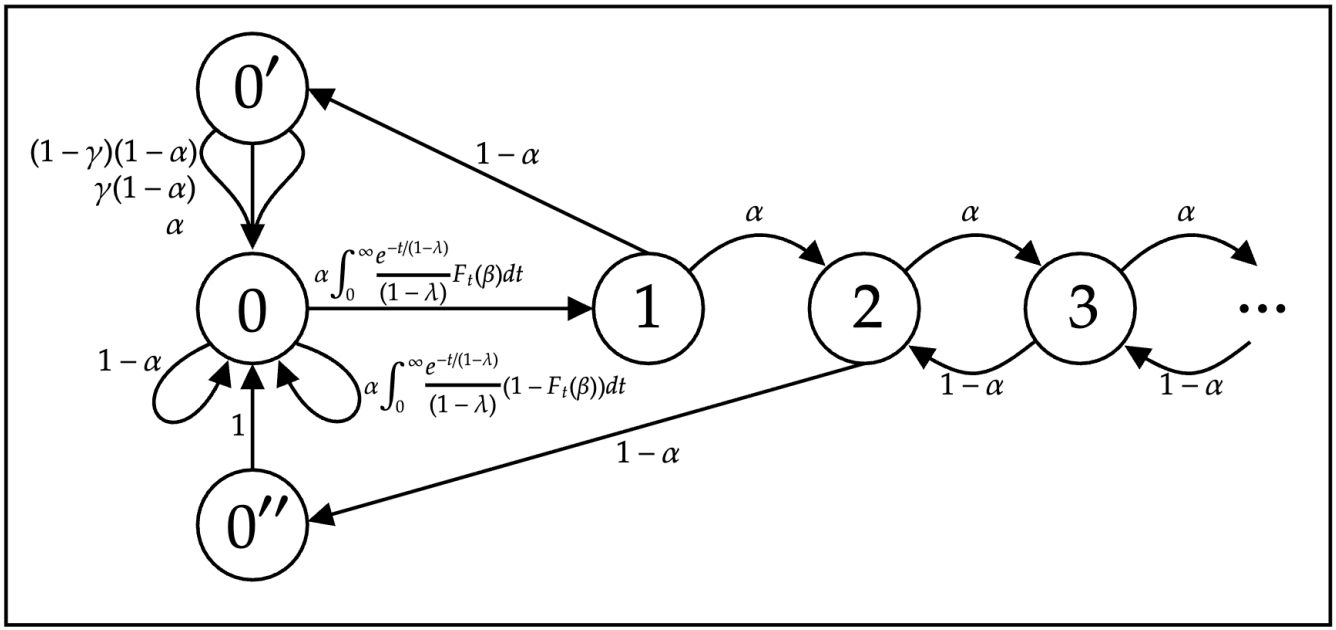
Static rewards cont'd.

- If transaction fees are i.i.d. from a distribution parameterized by Δ,
- and blocks are fully claiming (i.e., infinite capacity),
- then transaction fees are static.
- Conversely, if transactions arrive at different rates during different times of the day (e.g., higher trading volume during daytime hours in Asia), then they are not static.

Methodology

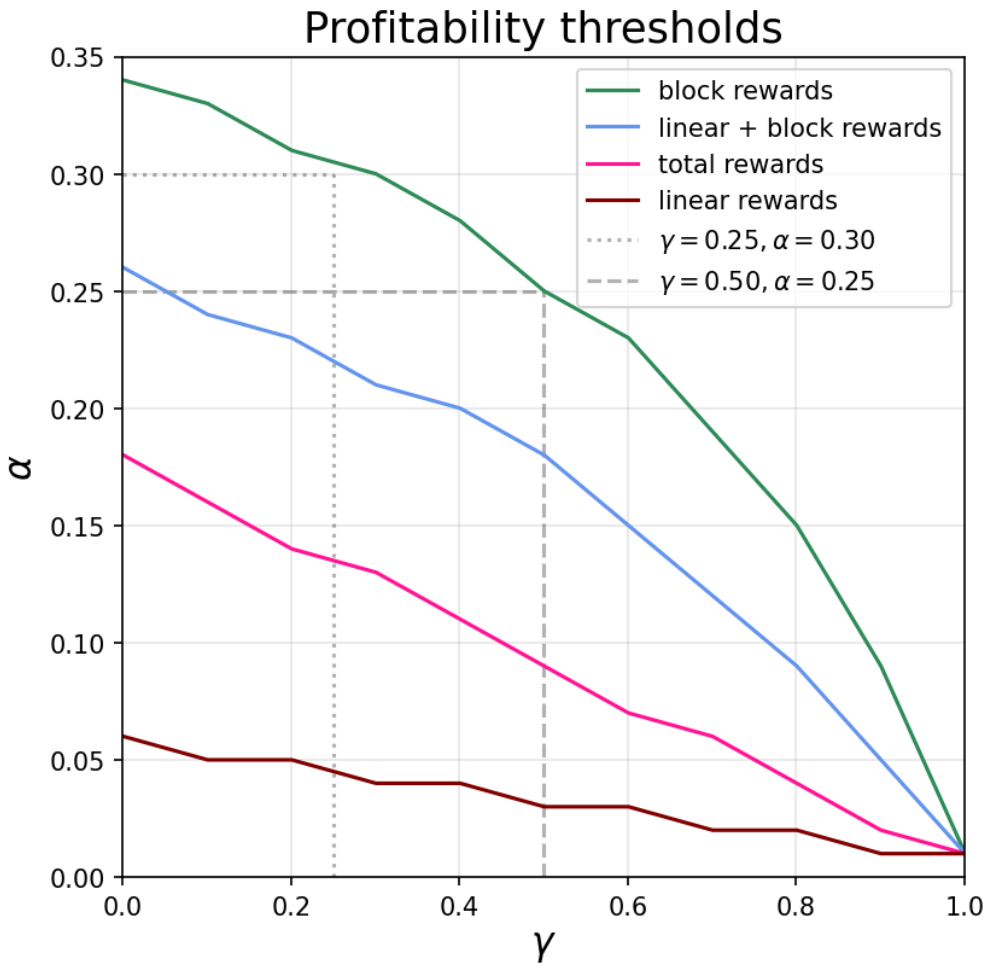
Markov Chain

- We use a similar Markov Chain to [ES'13] and incorporate the "β-cutoff parameter" from [CKWN'16].
- Each state indicates how much longer the attacker chain is than the canonical chain.



Results

Profitability thresholds



- **Key point**: Different reward functions yield *extremely* different assessments of protocol vulnerability.
- Green, just block rewards (i.e., [ES'13]), looks pretty safe.
- Red, just linear rewards (i.e., [CKWN'16]), looks pretty unsafe.
- Pink, the combined reward function (i.e., this paper) looks moderately unsafe.

thanks :)