Improving Proof of Stake Economic Security via MEV Redistribution

Tarun Chitra [1] Kshitij Kulkarni [2]

[1]Gauntlet

[2]UC Berkeley

SBC MEV Workshop, September 1, 2022

Outline

MEV in a Proof of Stake world

- Proposer-builder separation increases the action space for MEV and enables new forms of MEV redistribution (*e.g.* MEV smoothing)
  - Why does PBS help? Reduces the likelihood that off-chain agreements (OCAs) have higher EV than redistribution
  - Makes redistribution more realistic
- Question: What is the simplest, non-trivial model of how redistribution changes the economics of the PoS protocol?
  - Obadia and Vemulapalli performed the first heuristic analysis of smoothing, but it provided no formal guarantees

MEV Redistribution

- MEV redistribution: MEV collected is redistributed to stakers pro-rata
- While there is no known credible way to prevent OCAs, we assume that there exists such a mechanism
- Seek to understand how MEV redistribution can improve PoS economic security

Staking, Lending, and MEV

- Chitra 2019 showed that lending yields compete with staking and can reduce the security of a PoS system if the block rewards aren't high enough
- However, lending creates MEV via liquidations — can this MEV if redistributed avoid the staking vs. lending problem?
- It was observed empirically, especially after Terra crashed, that high lending yields corresponded to high liquidation volume
- We assume that this correlation holds to model MEV

Outline

PoS Protocols

- A PoS protocol has a token supply $S(k)$ and a reward schedule $R(k+1)$ at block height $k \in \mathbb{N}$
- An amount $\epsilon(k)$ is 'frozen' liquidity (protocol-owned if $\epsilon(k) > 0$ or burned if $\epsilon(k) < 0$)
- The supply evolves as $S(k+1) = S(k) + R(k+1) + \epsilon(k)$

Staking and Lending

- There are $i = 1, \ldots, n$ agents, who can choose between staking and lending
- They hold portfolios $\pi_i^{\text{stake}}(k), \pi_i^{\text{lend}}(k)$ such that $\pi_i^{\text{stake}}(k) + \pi_i^{\text{lend}}(k) = W_i(k)$, the total wealth of agent i
- Lent supply is $\ell(k) = \sum_{i=1}^{n} \pi_i(k)$ and staked supply is $T(k) = \sum_{i=1}^{n} \pi_i(k)$
- By definition: $S(k) = \ell(k) + T(k) + \epsilon(k)$

Lending Yields

- The lending yield $\gamma(k)$ is given by the following update:

$$\gamma(k+1) = (1+\gamma_0)U(k)$$

- $U(k) = \frac{NS(k)}{\ell(k)+S(k)}$ is the *utilization* for $0 < N \leq 1$

MEV

- At every k, an amount $Q(k)$ of MEV is extracted from the PoS system
- We assume that lending yields in the past are *positively correlated* to this amount
- That is, there exists $c_{\max}$ such that:

$$Q(k+1) = \sum_{p=0}^{c_{max}} \beta_p \gamma(k-p)$$

- Assume $c_{\max} = 0$. Then, $Q(k+1) = \beta_0 \gamma(k)$

Staking Yields

- The staking yield $\gamma_i^s(k)$ for every i is given by:

$$\gamma_i^s(k+1) = \frac{\pi_i^{\text{stake}}(k)}{T(k)}(R(k+1) + \alpha Q(k+1))$$
$$= \frac{\pi_i^{\text{stake}}(k)}{S(k) - \ell(k) - \epsilon(k)}(R(k+1) + \alpha Q(k+1))$$

- Question: how to choose portfolios $\pi_i^{\text{stake}}(k), \pi_i^{\text{lend}}(k)$?

Choice Model

- How to choose portfolios $(\pi_i^{\text{stake}}(k), \pi_i^{\text{lend}}(k))^\top$?
- Fix a positive definite covariance matrix: $\Sigma = \begin{bmatrix} \frac{1}{\kappa_i} & 0 \\ 0 & \frac{1}{\eta_i} \end{bmatrix}$ where $\frac{1}{\kappa_i} \sim \text{Exp}(\tau_{\text{stake}})$, $\frac{1}{\eta_i} \sim \text{Exp}(\tau_{\text{lend}})$
- And $\mu_i(k) = (\gamma_i^s(k), \gamma(k))^\top$ is the mean return vector
- λ is a risk parameter

Choice Model

- At every k, the agents choose their portfolios by solving a Markowitz mean-variance optimization problem:

$$(\pi_i^{\text{stake}}(k), \pi_i^{\text{lend}}(k))^\top = \arg \min_{w \in \mathbb{R}^2} w^\top \Sigma w - \lambda \mu_i(k)^\top w$$
$$\text{such that } w^\top \mathbb{1} = W_i(k)$$

- Optimal solution: $w^\star = \lambda \Sigma^{-1} \mu_i(k)$

MEV Redistribution Feedback System

- This turns the joint staking-lending dynamics into a feedback system!

$$\gamma_i^s(k+1) = \frac{\lambda \kappa_i \gamma_i^s(k)}{S(k) - \ell(k) - \epsilon(k)} (R(k+1) + \alpha \beta_0 \gamma(k))$$

$$\gamma(k+1) = (1+\gamma_0) \frac{NS(k)}{S(k) + \ell(k)}$$

- States: $(\gamma_1^s, \ldots, \gamma_n^s, \gamma)$

- Goal: understand how this system behaves as α changes

Outline

Dynamics, Equilibria, and Stability

- Prototypical dynamical system with initial condition x_0

$$x_{k+1} = f(x_k)$$

- An equilibrium point $x^\star$ satisfies

$$x^\star = f(x^\star)$$

- System doesn't move from equilibrium!
- Equilibrium is (locally) stable if

$$\lim_{k \to \infty} x_k = x^\star$$

for $x_0 \in \text{ball}_\delta(x^\star)$

Stability from Linearization

- Main idea: tell the stability of $x^\star = 0$ for

$$x_{k+1} = f(x_k)$$

from

$$x_{k+1} = \frac{df}{dx}\Big|_{x^\star}(x_k) = Ax_k$$

- $|\text{spec}_i(A)| < 1 \implies x^\star$ is locally stable
- $|\text{spec}_i(A)| > 1 \implies x^\star$ is unstable

Outline

Bad Equilibrium Points

$$\gamma_i^s(k+1) = \frac{\lambda\kappa_i\gamma_i^s(k)}{S(k)-\ell(k)-\epsilon(k)}(R(k+1)+\alpha\beta_0\gamma(k))$$

$$\gamma(k+1) = (1+\gamma_0)\frac{NS(k)}{S(k)+\ell(k)}$$

- What's the really bad equilibrium here?
- Staking goes to zero $\implies$ PoS security doomed
- Mathematically: $\gamma_1^s = 0, \ldots, \gamma_n^s = 0$

Characterizing Undesirable Equilibria

- Formally, $(\gamma_1^{s,\star}, \ldots, \gamma_n^{s,\star}, \gamma^\star) = (0, \ldots, 0, \gamma^\star)$ is an equilibrium point of the dynamics for $\gamma^\star = \frac{(1+\gamma_0)N}{2}$
- Undesirable from a PoS security viewpoint! No one is staking, so can't guarantee security (at this equilibrium, $\pi_i^{\text{stake}} = 0$ for all i)
- Question: can we avoid this equilibrium using α?

Boosting Out of the Equilibrium

- Make α large enough so that $(0, \ldots, 0, \gamma^\star)$ becomes unstable
- How? Look at $\frac{df}{dx}\big|_{x^\star}$
- For our system:

$$\begin{bmatrix} \lambda\kappa_1 \frac{R(k+1)+\alpha\gamma^\star}{-\epsilon(k)} & 0 & \ldots & 0 & 0 \\ * & \lambda\kappa_2 \frac{R(k+1)+\alpha\gamma^\star}{-\epsilon(k)} & \ldots & 0 & 0 \\ * & * & \ldots & \ldots & \\ * & * & \ldots & \lambda\kappa_n \frac{R(k+1)+\alpha\gamma^\star}{-\epsilon(k)} & 0 \\ * & * & \ldots & * & 0 \end{bmatrix}$$

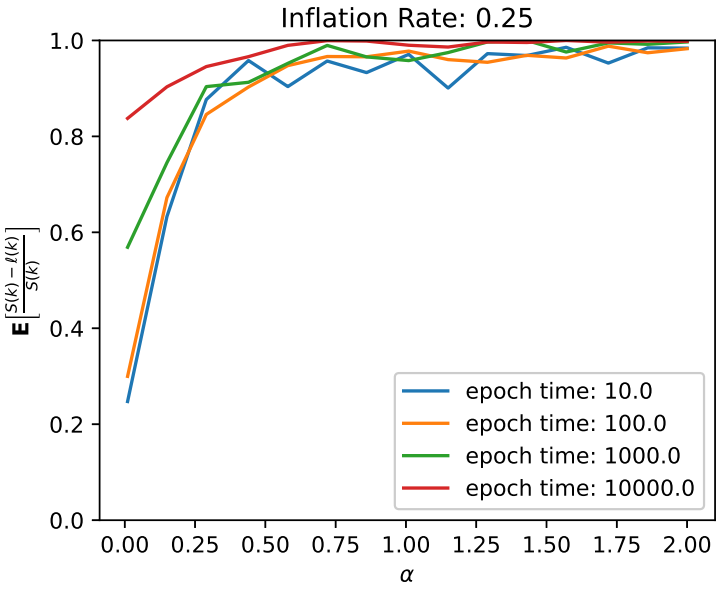
- As α grows, $\max_i |\text{spec}_i(A)|$ grows!

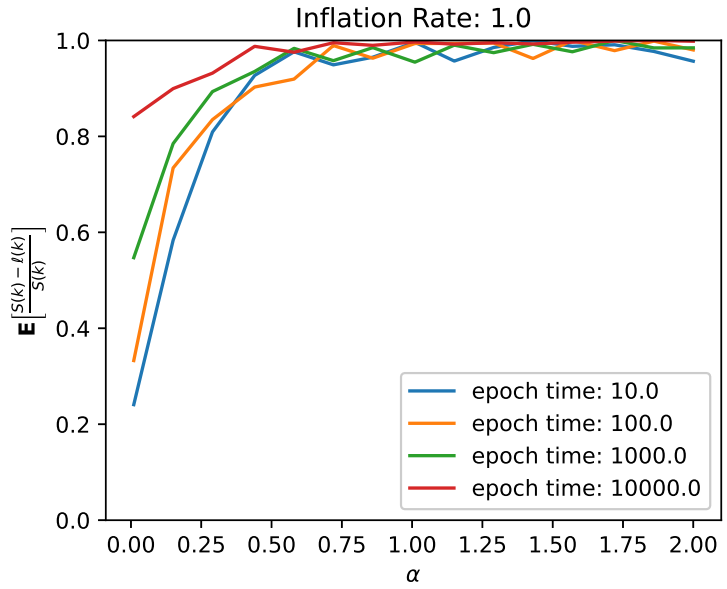
Insights

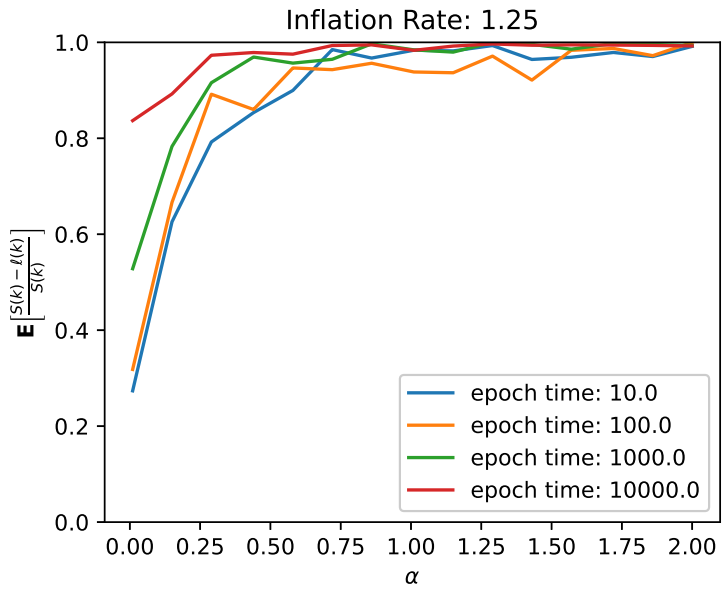
- In the absence of MEV redistribution, need fast growing reward schedules (Chitra 2019) to avoid no-staking equilibrium
- When $\alpha > 0$, can make the bad equilibrium unstable
- Requires a slower rate of inflation

Outline

Simulations: MEV Redistribution Avoids Bad Equilibria!







Outline

Takeaways

- Can use MEV redistribution to *avoid* bad economic equilbria between staking and lending
- Require less inflation than otherwise necessary

Questions?

References

Chitra, Tarun (2019). "Competitive equilibria between staking and on-chain lending". In: *arXiv preprint arXiv:2001.00919*.