Economics of Proof-of-Stake Payment Systems

by Giulia Fanti, Leonid Kogan, and Pramod Viswanath

Discussion by Emiliano S. Pagnotta

Imperial College London

WFA, June 20, 2020

Why Modeling PoS?

PoW: one unit of computing power one vote
PoS: one coin one vote

Why Modeling PoS?

PoW: one unit of computing power one vote
PoS: one coin one vote

Top 20 public chains	Token	Consensus algo
Ethereum (now)	ETH	PoW
Ethereum (near future)		PoS (FFG)
Ethereum (future)		PoS (CBC)
Cardano	ADA	PoS (Ouroboros)
Tron	TRX	Delegated PoS
Neo	NEO	dBFT (~DPoS)
EOS	EOS	Delegated PoS
Tezos	XTZ	Delegated PoS

Key to Economics: Validators' Problem

Validators in Proof of work (miners)

$$\max_{\text{hashrate}H} \underbrace{(\text{Rewards+Fees})p}_{\text{conditional revenue}} \times \Pr(\text{winning}|H) - \underbrace{H}_{\text{investment}} \times \underbrace{C(H)}_{\text{mining cost}}$$

- $C(H)$ consistent with equilibrium in input markets (electricity, hardware)
- Token equilibrium determines $\{p, H\}$

Key to Economics: Validators' Problem

Validators in Proof of work (miners)

$$\max_{\text{hashrate}\, H} \underbrace{(\text{Rewards+Fees})p}_{\text{conditional revenue}} \times \Pr(\text{winning}\,|\,H) - \underbrace{H}_{\text{investment}} \times \underbrace{C(H)}_{\text{mining cost}}$$

- $C(H)$ consistent with equilibrium in input markets (electricity, hardware)
- Token equilibrium determines $\{p, H\}$

Validators in Proof-of-Stake (this paper)

$$\max_{\text{stake}} \underbrace{(\text{Rewards+Fees})p}_{\text{conditional revenue}} \times \Pr(\text{winning}\,|\,\text{stake}) - \underbrace{\text{stake} \times p}_{\text{investment}} \times \underbrace{r_C}_{\text{opp. cost}}$$

- r_C consistent with equilibrium in financial markets
- Token equilibrium determines $\{p, \phi\}$, $\phi := \frac{\text{stake}}{\text{total supply}}$

Comments/Suggestions

General

1. Relevant and interesting to address PoS directly. Economics are not the same as in PoW!

Specific

1. Bounds on token value
2. Security budget and valuation: Different from PoW?
3. Payment channel modeling

#1 Bounds on token value

Building block 1: Quantity theory of money with staking

- Fisher's equation of exchange with S_t total number of tokens, staking ϕS_t for PoS securing

$$(1-\phi)\, S_t V_t = \frac{Y_t}{P_t}$$

P_t price of tokens (inverse price level), Y_t real goods transferred within t, k inverse velocity

- Re-expressing $p_t = P_t S_t$ and assuming inverse velocity k is constant:

$$(1-\phi)\, p_t = k Y_t$$

Building block 2: What is the value of validators' stake ϕp_t? Driven by user fees and block rewards

- Fees: cY_t
- Block reward: new issuances goes to validators (rate g_S)

#1 Bounds on token value

- Fair compensation for capital locked in the PoS stake is λ_Y, Y growth rate g_Y
- Authors show that

$$p_t = \left(k + \frac{c + kg_S}{\lambda_Y - g_Y} \right) Y_t$$

#1 Bounds on token value

- Fair compensation for capital locked in the PoS stake is λ_Y, Y growth rate g_Y
- Authors show that

$$p_t = \left(k + \frac{c + kg_S}{\lambda_Y - g_Y} \right) Y_t$$

- If $k = 0$, we obtain a lower bound for token value

$$p_t = \frac{cY_t}{\lambda_Y - g_Y}$$

#1 Bounds on token value

- Fair compensation for capital locked in the PoS stake is λ_Y, Y growth rate g_Y
- Authors show that

$$p_t = \left(k + \frac{c + k g_S}{\lambda_Y - g_Y} \right) Y_t$$

- If $k = 0$, we obtain a lower bound for token value

$$p_t = \frac{c Y_t}{\lambda_Y - g_Y}$$

- Nice to derive a new bound on value based on observables

#1 Bounds on token value

- Fair compensation for capital locked in the PoS stake is λ_Y, Y growth rate g_Y
- Authors show that

$$p_t = \left(k + \frac{c + kg_S}{\lambda_Y - g_Y} \right) Y_t$$

- If $k = 0$, we obtain a lower bound for token value

$$p_t = \frac{cY_t}{\lambda_Y - g_Y}$$

- Nice to derive a new bound on value based on observables
- But if $k = 0$ users' demand for the token is zero. Shouldn't we have $p_t = 0$?

#1 Bounds on token value

FIGURE: Block Reward and Transaction Fees in Ethereum

- For validators, fees and rewards are perfect substitutes

#1 Bounds on token value

- Validators' real revenue per period (growth g_R)

$$\underbrace{(\text{block reward}(R_t) + \text{fees}(F_t))}_{\text{token units}} \times P_t$$

- Valuing the stream: λ_R opportunity cost of capital from asset with similar risk profile. Value of the stake must be

$$\phi S_t P_t = \frac{(R_t + F_t) P_t}{\lambda_R - g_R}$$

- Adding users' and validators' valuation again:

$$p_t = \left(\frac{\lambda_R - g_R}{\lambda_R - g_R - \frac{1}{S_t}(R_t + F_t)} \right) k Y_t$$

- Here, null demand implies zero price ($k = 0 \implies p_t = 0$)

#2 Security Budget and Token Valuation

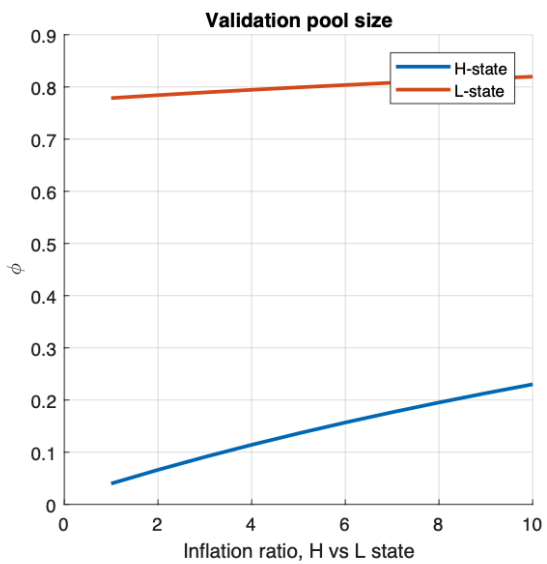
- What is the relation between validators' income and security?
- Insight 1:

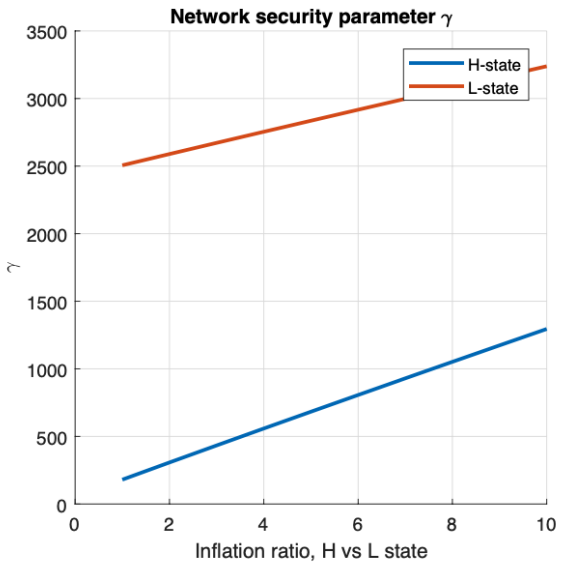
$$\gamma \underbrace{\frac{Y_t}{N}}_{\text{exp. volume}} = \underbrace{\mathcal{Z}\frac{cY_t}{\lambda_Y - g_Y}}_{\text{take slashing}} = \mathcal{Z}\phi p_t$$

- $\mathcal{Z}$ slashing fraction in $[\frac{1}{3}, \frac{2}{3}]$, γ **security threshold**
- High token valuation serves as a deterrent
- Different from PoW? Yes. In PoS, if a fraudulent attack is detected, penalties applied (slashing is like "burning the mining farm"). PoW works only through rewards

#2 Security Budget and Token Valuation

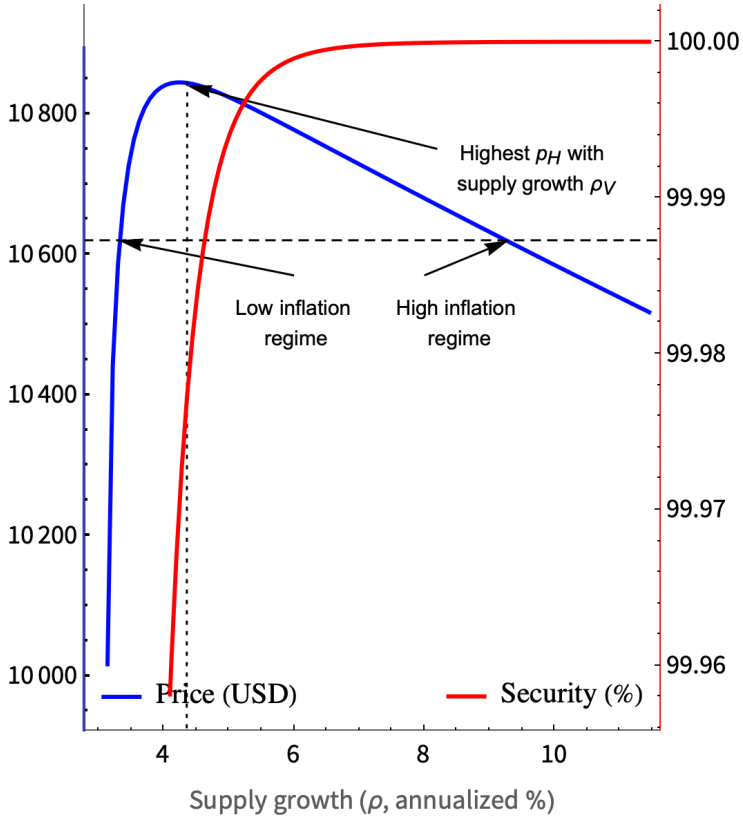
- Insight 2: presence of investors with irrationally optimistic beliefs can reduce validator's stake (more risk compensation), reducing security
- Proposed solution: state-contingent monetary policy can help stabilizing security budget. When size of the stake is low, issue rewards faster
- Practical adoption:
  1. Nice that one does not need to condition on valuation level
  2. But how much to issue? Monetary policy is very powerful here

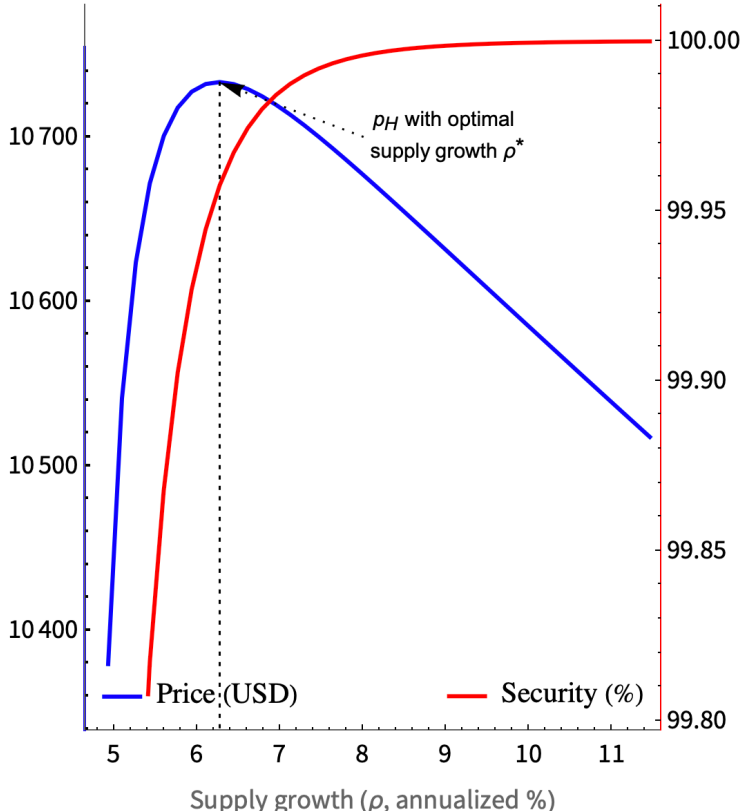




#2 Perspectives from PoW Analysis

- Active monetary policy could help with security stability. But it is challenging, even when everybody is rational: tension between **security** and **scarcity.** Generally, valuation effect $\neq$ traditional quantity theory
- Right panel: attacker has more resources. Valuation-optimal issuance $\uparrow$, but it is not that maximizes seigniorage. What exact level to target?
- Token price enhances security in PoS, some insights could be extrapolated (except welfare)





#3 Payment Channel Networks

- Analysis of off-chain transactions and payment channels is a promising direction to apply the framework. Currently, lacks a bit of structure
- Suggestion: together with consumers (i.e., $\phi_{\text{validators}}$, ϕ_{PCN}), bring block capacity to the analysis to incorporate (i) consumer trade-off, (ii) asymmetric fees
- Fees are pricing different objects on-chain and off-chain
  - On-chain: block space (fee expresses "tokens per Kbyte"). They should be near zero unless limit is binding by fees from opening–closing channels (new consumers join)
  - PCN: locked capital by PCN operators routing transfers (fee expresses "tokens per economic value transferred") $\rightarrow$ similar to current version

Additional Comments

- **Cost of Staking**. If could short-sell my stake in an exchange, would I do it? Bringing cost of shorting into the analysis seems interesting
- **Bubbles**. Couldn't we analogously say that bubbles are potentially good for security? If instead stakers are generally too optimistic about returns? Empirical way to know which story is more plausible?
  - Example: Jan 2020, $\phi = 77\%$ for Tezos and 73% for Cosmos
  - Could potential users be deterred by "over investment" in staking? (future crashes)

Conclusions

- Very interesting contribution on the mechanism behind growing number of blockchains adopting PoS consensus
- Excited to see how this area evolves and addresses more specific features of the consensus mechanism
- Opportunity to build on framework to study optimal design questions