



Maximum Viable Security: a framework for Ethereum issuance

adcv, Artem Kotelskiy, Danny McNut, Sonya Kim

Disclaimer

**cyber•Fund holds ETH, LDO
and is investor in P2P**

What are we trying to do?

Goal:

Develop a stable issuance policy

Steps:

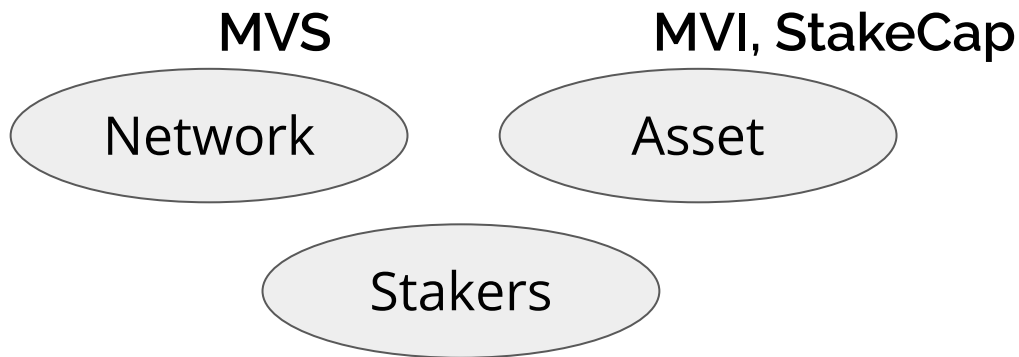
1. Set the north star & have a guiding framework
2. Collect the necessary data
3. Analyze scenarios individually
4. Analyze scenarios relative to each other

1. Northstar & framework

Why high-level framework?

- The topic is incredibly complex & contentious
- We need a community-wide rough consensus

How — what to optimize for?



What should be the framework?

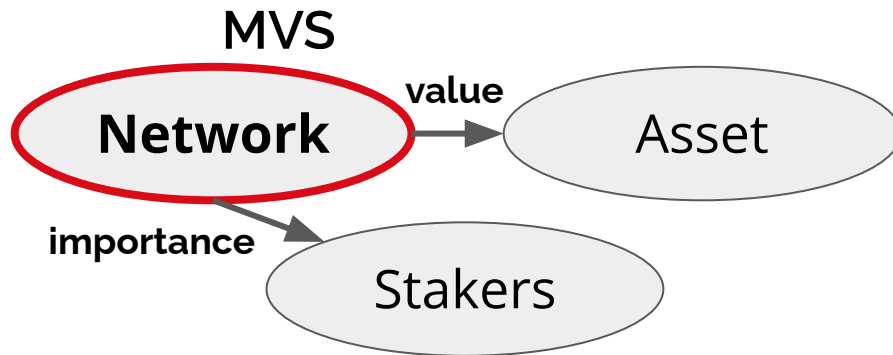
Evaluation from the perspective of the biggest value-proposition of the network: security & neutrality

1. Northstar & framework

Why high-level framework?

- The topic is incredibly complex & contentious
- We need a community-wide rough consensus

How — what to optimize for?



What should be the framework?

Evaluation from the perspective of the biggest value-proposition of the network: security & neutrality

1. Northstar & framework: security model

Key attack vectors:

- A. 34% double-signing attack (seen by protocol)
- B. 51% short reorg & censoring attacks (not seen)
- C. Gradual coercion by state actors (not seen)

Ethereum's autonomy = ability to resist B & C

Defenses:

- RE:A. Cryptographic slashing
- RE:A,B. Social slashing
- RE:A,B,C. Decentralization coming from distributed validator set, ensuring no single party controls 51%/34% of validators

1. Northstar & framework: security model

Key attack vectors:

- A. 34% double-signing attack (seen by protocol)
- B. 51% short reorg & censoring attacks (not seen)
- C. Gradual coercion by state actors (not seen)

Ethereum's autonomy = ability to resist B & C

Defenses:

RE:A. Cryptographic slashing

RE:A,B. Social slashing **Politically messy, complicated to automate**

RE:A,B,C. Decentralization coming from distributed validator set, ensuring no single party controls 51%/34% of validators

Preventive, apparent, Ethereum's biggest differentiator, key to neutrality

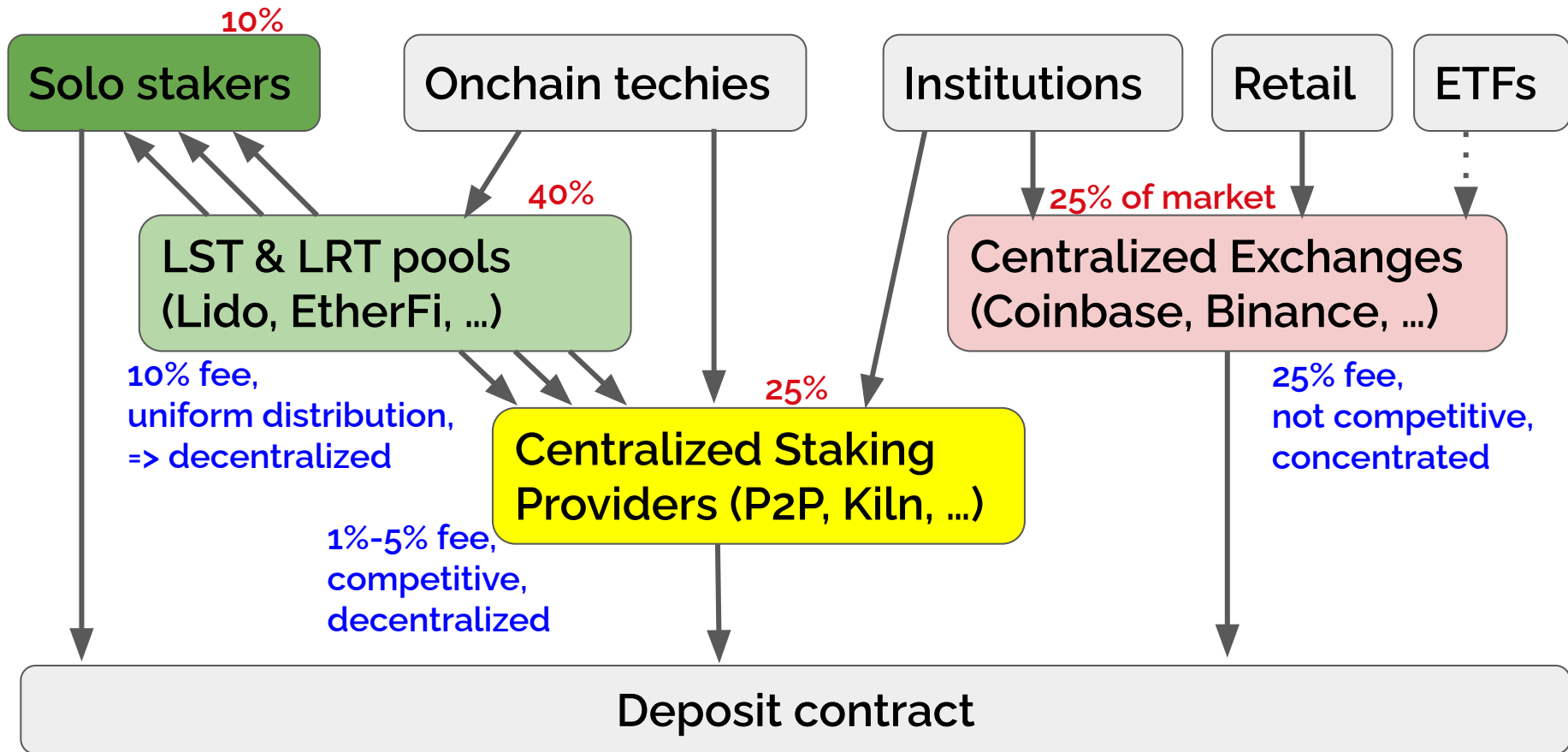
1. Northstar & framework: upshot

MVS: Maximum Viable Security (and neutrality), largely coming from geographically distributed & disconnected validators

MVS vs MVI:

- MVS maximizes security without compromising scarcity, while MVI minimizes issuance without compromising security
- MVS prioritizes expansion & sustainability over efficiency, while MVI does the opposite

2. Data: staking market structure



2. Data: market segmentation

		Staker elasticity	Fees	Decentralization	Costs	Market share
Offchain market segment	Centralized Exchanges	Low	25%	Low	Low	25%
	Centralized Staking Providers	Mid	1-5%	Mid	Low	25%
Onchain market segment	LST+LRT pools	High	10%	High	High (×38)	40%
	Solo Stakers	Mid	0	Very high	Mid	10%

Important: margin compressions are not given in segmented markets
=> there is a chance to sustain expensive decentralized solutions

3. Analysis: issuance cut impact

On stakers:

- LST+LRT+CSP stakers are sophisticated => some of them churn => “decentralized” market share decreases
- CEX stakers are inelastic => they largely don't churn, thus increasing CEX market share
- Solo stakers will churn, potentially at a slower rate at first due to diverse costs & preferences, but at a higher rate later due to high fixed costs & inflexibility

On staking providers & middleware:

- LSTs+LRTs have high costs (support many NOs) => some of NOs drop => loss of decentralization
- CEXs preserve customers & maintain margins due to low costs
- CSPs lose customers & but maintain margins due to flexible low costs

3. Analysis: issuance cut impact upshot

1. CEXs market segment largely untouched
2. Decentralized LRT+LST+CSP feel the pressure
=> some stakers & some CSPs leave
3. CEXs market share grows
=> less decentralization, undermining security

Coinbase has 15% share, huge unstaked reserves, and ETF assets incoming. With issuance cut, we show how all this combines into a real scenario of Coinbase achieving 34% of network, in a 40m staked ETH cap world

3. Analysis: issuance cut pro-arguments through the lens of MVS

- **Real vs nominal yield:** concerned with stakers, not the network
- **Current issuance is costly:** using Anders' methodology, the saved costs from cutting issuance are in single billions / year — a relatively small price considering that Ethereum buys security assurance in return, also bolstering ETH value
- **Boosting monetary hardness of ETH:**
 - Bitcoin won that market
 - ETH's moneyness may actually decrease due to credibility & security losses
 - ETH's value is best bolstered by Network's success

4. Relative analysis: cut VS no cut

- **MVS-aligned argument pro cut: LST dominance**
 - The risk is largely mitigated by dual governance (formally verified)
 - The market is competitive (Lido share 33% -> 28%)
- **MVS-aligned argument against cut: CEX stake concentration**
 - Coinbase getting to 33% scenario is very real
 - While security will likely be preserved due to social slashing, neutrality will be lost

On balance, it is better to aggregate staked ETH on the transparent smart contract layer that boosts decentralization, rather than on the opaque TradFi layer that undermines neutrality.

[!] More analysis needs to be done.

Closing thoughts

We have lots to do:

1. ● Set the framework: Network vs Asset
2. ● Collect the necessary data
3. ● Analyze scenarios individually
-> cyber•Fund MVI grants
4. ● Analyze scenarios relative to each other

Let's collaborate: having agreed on framework, let's drill deep into disagreements, and then based on data and research try making an objective resolution

*"Let's accelerate what we want, fearlessly.
Its an infinite game, there is no endgame."*



Thank you!

