

# Consensus Incentives on Algorand

Michele Treccani, Algorand Foundation

Salerno University, April 24 2024

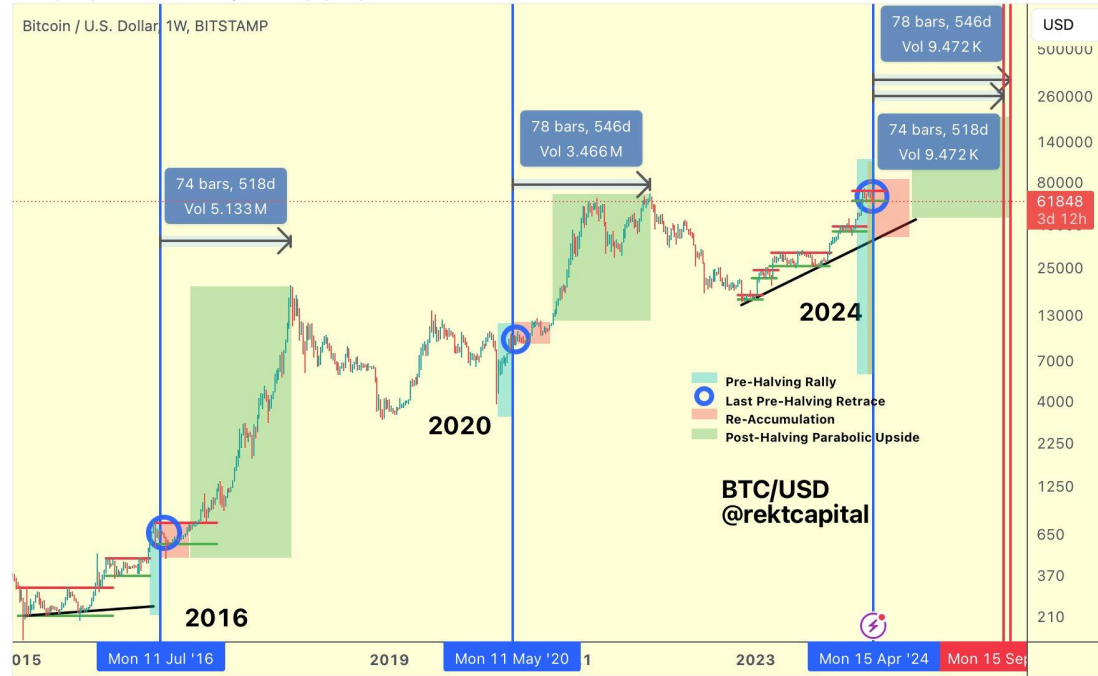


## Summary

- Economic Aspects of Consensus
- Ethereum: the benchmark Proof of Stake?
- Algorand Consensus Evolution
- Path towards Self Sustainability
- Conclusions

# BTC: The Halving Craze!

rektcapital published on TradingView.com, Apr 18, 2024 12:39 UTC



TradingView

# Economic Aspects of the Crypto Market

- It's not a deterministic system!
- Economic aspect is sometimes dominant over the technological aspect.
- When the Economic aspect kicks in, the Efficient Market Hypothesis is always advocated:  
***"Prices reflect all available information."***
- Is it true in crypto? Yes & No!
- Fundamentalist vs Turtle Trader!

It could not be sufficient to design an optimal product, you also have to create the proper “market conditions” to prosper

# PoW vs PoS: is there a definitive winner?

## Proof of Work:

- enormous negative externalities!
- it's not a closed system
- It's "programmed to be slow"

## Proof of Stake:

- Can have small ( $\neq 0$ ) carbon footprint
- Self-referred
- the incentives are aligned: Gini Distribution = Validator Distribution

Ethereum: "the Merge" in Sep '22 transitioned from PoW to PoS

# Ethereum Stake Model

What can we learn from Eth?

- 120M current CircSupply ([steady](#))
- Eth: 25% of Staking
- Centralization: Lido is 30% (but with Govs)
- Eth: 1M validators ([caveat](#): not entities!)
- The rigidity of the consensus protocol forces a choice of the validation quantum: 32 Eth. Side effect: higher threshold for entering in the validation game. ([Vitalik explanation](#))
- Slashing (around 3%) is present, but rarely happens ([here](#))

# Lido: Liquidity for staked assets

Stake any amount of ETH to receive daily rewards and increase your balance through DeFi.

Staked amount  
**9,336,994 ETH**  
\$28,397,766.661

Lido APR  
**3.6%**  
[More info](#)


Rewards paid  
**511,648 ETH**  
\$1,556,139.194


[Stake Ethereum](#)


[Lido on Ethereum Scorecard](#) >

## Why Lido?

With Lido Ethereum staking is made simple and accessible to anyone

  
**Biggest Ethereum pool**  
Lido is the leading Ethereum staking pool letting you benefit from efficient liquidity and pool security


  
**A global community**  
Chat with the team, others in the community, and have your say in shaping the future of the Lido protocol


  
**Growing Protocol Ecosystem**  
The growing Lido ecosystem lets you to put your staked ETH to use across Curve, Yearn, Sushi, 1inch and more to compound rewards


## Why does Lido APR differ from various liquid staking protocols?


The main differences between APR in various liquid staking protocols are formed due to the unique solutions of each protocol and approaches to the formation of a validator set.

Here are Lido-on-Ethereum distinctive approaches on rewards:

  
**Compounding**  
APR increases as EL rewards are got due to staking of received EL rewards.  
[Compounding statistics](#)

  
**Performance of Lido validators**  
The better the underlying validator sets are, the more robust, resilient, and performant the staking protocol. [Operator Statistics and Metrics](#)

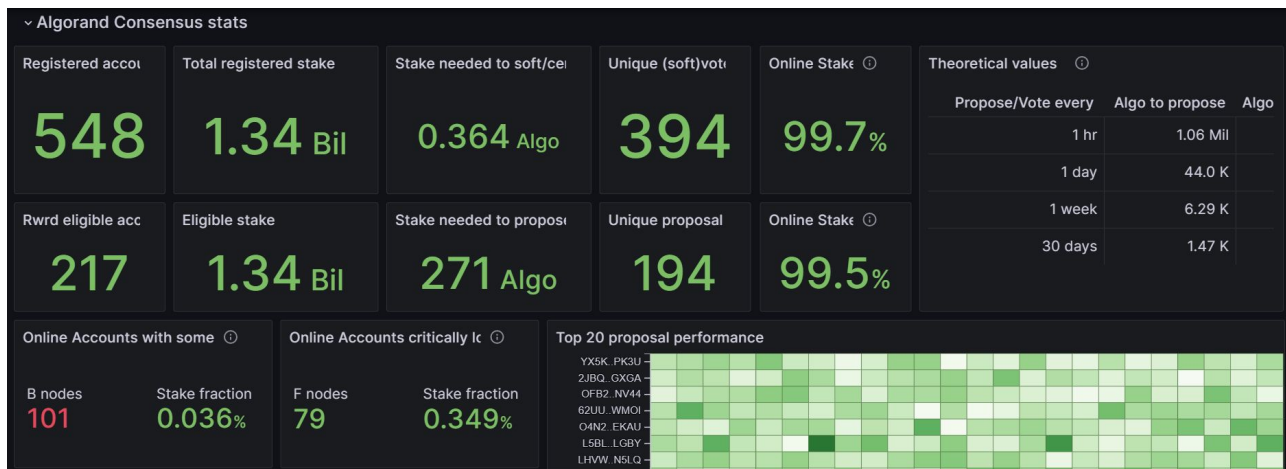
  
**Rewards socialization model**  
With Lido, you receive staking rewards within 24 hours of your deposit without waiting for validator activation.

  
**Protocol fee**  
Lido applies a 10% fee on staking rewards that are split between node operators and the DAO Treasury.

# Algorand Consensus: $\epsilon \neq 0$

**Algorand's original thesis:** a sufficient number of end-users would naturally be incentivised to run a node and contribute to online stake, motivated by the desire to secure their own funds, and as a corollary the network.

Current Situation: Tragedy of the commons! (see [here](#))



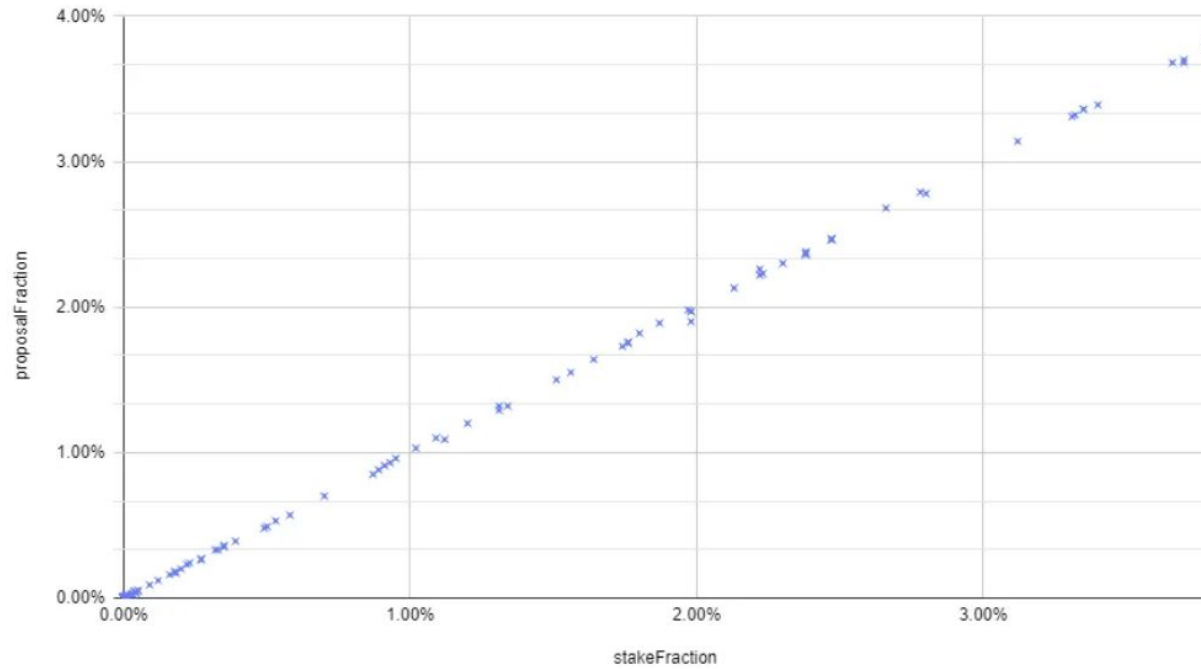


# Consensus Participation

- You can participate in Consensus with an arbitrary amount of Algo!
- You have to voluntarily signal your will to participate in Consensus through a special txn: KeyReg
- The spending keys are separated from the Participation keys!
- The relevant quantity for quantitative assessment is your fraction of Total Online Stake

# To VRF or not to Vote? [See here](#)

proposalFraction vs. stakeFraction



# Ethereum vs Algorand

What can we learn from Eth? We are at the same time better and worse than Eth!

- Eth: 120M current CircSupply (steady), Algo: 8B (evolving)
- Eth: 25% of Staking, Algo: 17% (w/out AF: 5%)
- Centralization: Lido is 30% (but with Govs), Algo: AF 75%
- Eth: 1M validators (caveat: not entities!), Algo: 548(w/out AF: 390)
- ETH: The rigidity of the consensus protocol forces a choice of the validation quantum: 32 Eth. Algo: 0.01 Algo!
- Eth: slashing (around 3%) is present, Algo: not present!

# What do we ask to a Consensus Incentive?

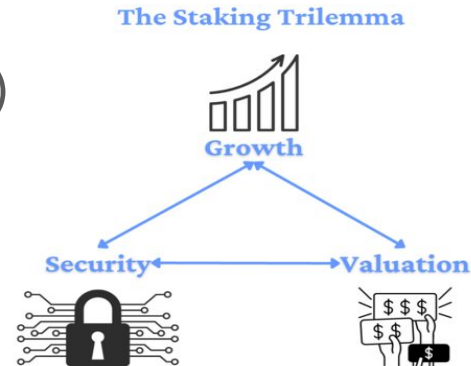
**To perturb the system in order to approach states with positive feedback loop!**

- Must move the needle!
- Must align goals
- Must leverage the current consensus framework
- Must eliminate (minimize) attacks

**Problem:** users think in APR, we have to think in quantities!  
Fees? Avg 0.03A per block! (a blessing is sometimes a curse!)

# Yet Another Trilemma

- Sec: an attack should be sufficiently expensive (in \$)
- Growth: the fees should not be too high
- Valuation: Inflation should be controlled (or absent)



## Main ingredients

- Fair acknowledgement of the effort needed
- Temporal locking of resources
- Adequate risk remuneration

# Algorand Consensus Incentivisation

AN ALGORAND FOUNDATION DISCUSSION PAPER

John Woods

john@algorand.foundation  
john@postquantum.dev

Michele Treccani

michele@algorand.foundation

John Jannotti

jj@algorand.com

Naveed Ihsanullah

naveed@algorand.foundation  
naveed@jamsni.com

Version 1.0, 14th December 2023

- Attract new validators with a competitive APR
- Frontloaded to overcome upfront costs
- Must compete with other Consensus participations
- Degrees of freedom: initial value, duration & decay rate

## Potential risks!

- Absenteeism: It's peculiar to the Algorand Network: registering and not participating!  
**Bad Validators:** Empirical Production Rate  $\neq$  Theoretical PR  
They are kicked out by the Consensus, they can still re-enroll  
Minimum Staking amount (30k) is enforced to ease the “Garbage Collection” procedure: **Risk Mitigated!**
- Pooling: **too many Part Keys in a single node** could degrade performance in Consensus, hence less rewards: **Risk Mitigated!**
- Modifying clients: **A bad actor could modify the client** to focus only on Block Production, thus skipping fundamental steps of the Consensus. The benefit is currently infinitesimal, thanks to the efficiency of the VRF: **Risk Assessed!**

# Next Step: Self sustainability!

Fee Base	PROJ_VolMultiplier		from	30/6/2023	to	29/11/2023	#Rounds		SIMULATE
0.001	10		Block Height	30000000		34,031,387	4,031,387		FALSE
BlockSpeed	2.8								
	Txn Type		Count	Avg#PerBlock	VolMultiplier	PROJ_Avg#PerBlock	FeeMultiplier	FeeModel	PROJ_AvgFee
1	pay	Payment	22,650,138	5.61844794	10	56.18447944	10	0.01	0.0056184
2	keyreg	KeyRegistration	1,435	0.00035596	10	0.00355957	1	0.001	0.0000004
3	acfg	AssetConfig	2,037,147	0.50532162	10	5.05321618	10	0.01	0.0005053
4	axfer	AssetTransfer	59,197,283	14.68409830	10	146.84098302	10	0.01	0.0146841
5	afrz	AssetFreeze	13,302	0.00329961	10	0.03299609	10	0.01	0.0000033
6	appl	ApplicationCall	40,805,629	10.12198258	10	101.21982583	10	0.01	0.0101220
7	StateProof	StateProof	15,727	0.00390114	10	0.03901139	1	0.001	0.0000039
		TOTAL	124,720,661	30.93740715		309.37407150		AVG_Rewards_Block	0.0309374
		TPS		11.04907398		110.4907398			



# Conclusions

- Consensus is the heart of decentralization!
- Inclusiveness should be a priority
- Remuneration should be proportional to the effort needed
- The final goal is full self sustainability
- The technical advantages of VRF allows to achieve all this goals!

**We are just at the beginning of the journey!**

# Cardano

- Current circulating supply is around 35B, on a total fixed quantity of 45B: the (decreasing) difference is defined as reserve.
- The source for incentives is twofold: collected fees and a fixed fraction (0.3% of the reserve) from the reserve, hence obtaining an asymptotically zero inflation rate, with a current value of 2%, in analogy with Bitcoin case (currently at 1.8%).

$$f(s, \sigma) := \frac{R}{1 + a_0} \cdot \left( \sigma' + s' \cdot a_0 \cdot \frac{\sigma' - s' \frac{z_0 - \sigma'}{z_0}}{z_0} \right)$$

The [complete formula](#) for pool rewards assignment

The key ingredients are  $R$ , the available rewards, and  $\sigma'$ , the quantity staked by a pool, which represents the maximum possible reward and it is capped to  $0.2\% = 1/k$  ( $k=500$ ), in order to discourage oligopoly creation. The second term represents a “pledge” correction ( $s'$  is the analogous of capped  $\sigma'$ , but for pledged quantity) in order to persuade pool operator to put their own stake into the pool, thus ensuring alignment of incentives.

After pool rewards have been calculated and adjusted for pool performance, **a fixed fraction (20%) is devoted to fund the Cardano Treasury System.**

# Cardano

- Everestake offers non-custodial staking, without locking: **APR 4%**
- Delegation is encouraged: funds never leave the wallet, just signal delegation to the pools
- Current staking 70%, most of (65%) it from delegation
- **Slashing is not present**
- Time is organized in epochs (about 5 days each): at the end of each epoch (275, for example) a snapshot is taken and used for delegation in the next-to-next epoch (277). The reward calculation is performed in the following epoch (278) and rewards are distributed in the next one (279): **the total delay could range from 15 to 20 days.**
- **Annual inflation around 2.5%: APR adjusted for inflation 1.4%**