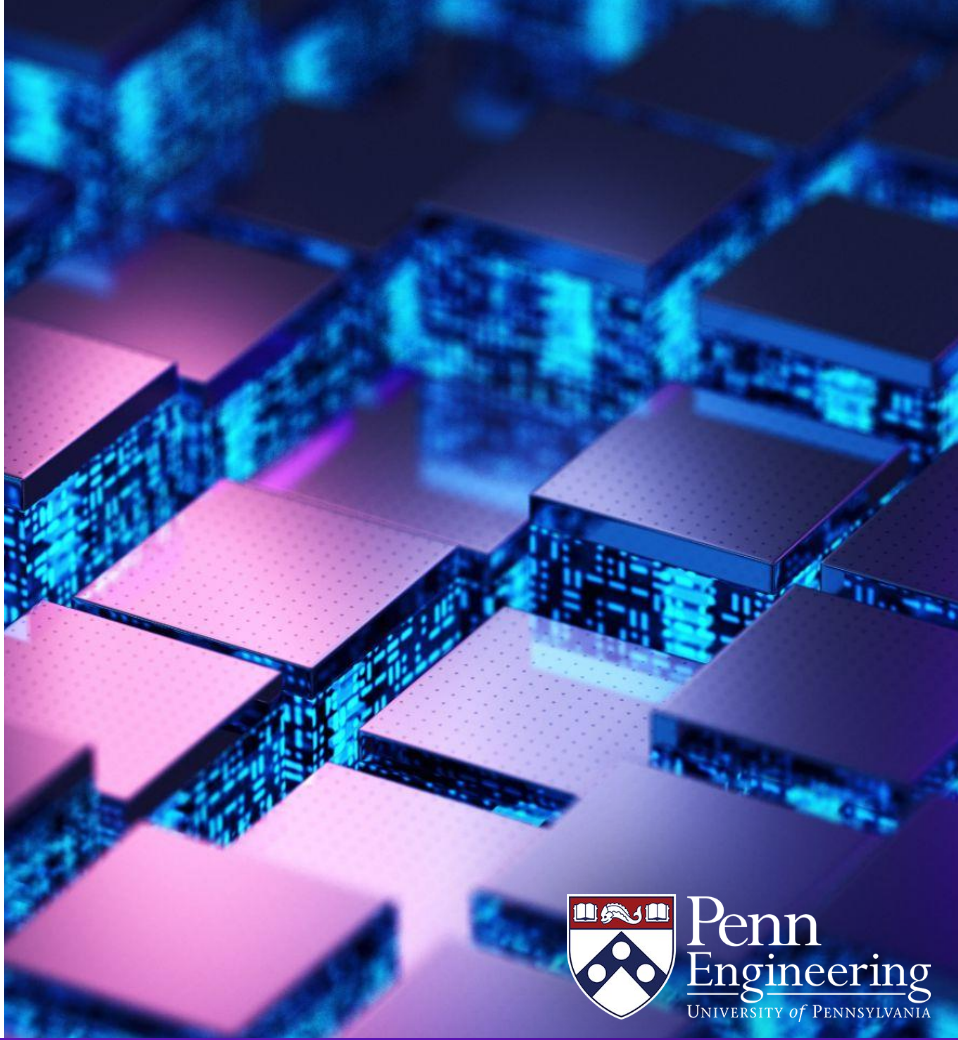
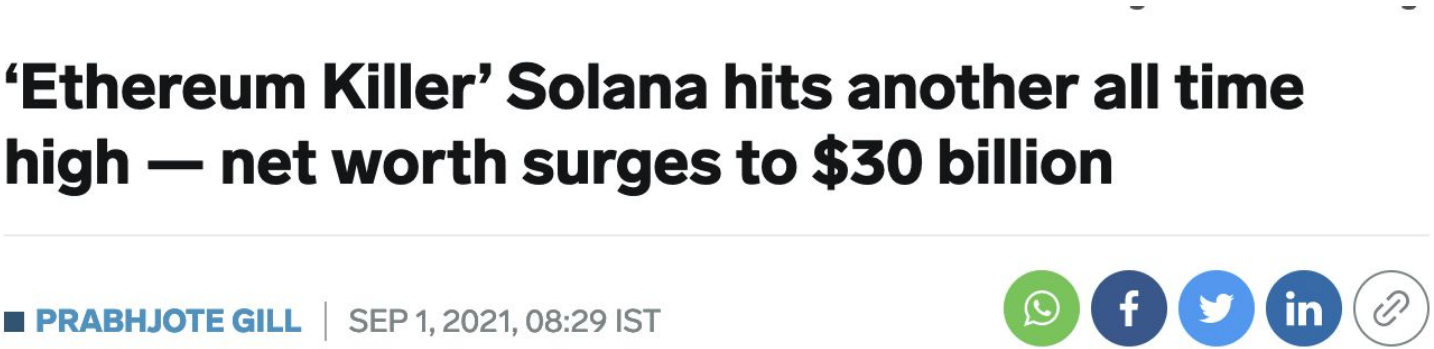
EAS 5830: BLOCKCHAINS

Solana

Professor Brett Hemenway Falk



Penn Engineering
University of Pennsylvania



‘Ethereum Killer’ Solana hits another all time high — net worth surges to $30 billion

■ PRABHJOTE GILL | SEP 1, 2021, 08:29 IST

WRITING

The World Computer Should Be Logically Centralized

BY **KYLE SAMANI**

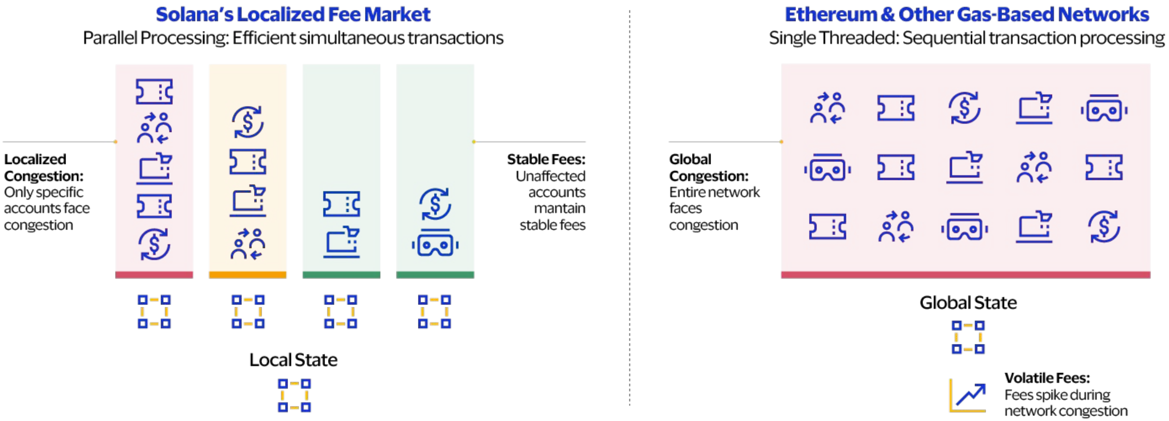
July 30, 2019 | 12 Minute Read

Solana

- 2017 - Whitepaper by Anatoly Yakovenko
- March 2020 - First block produced
- Block producers take turns, using Proof of History
- Blocks are finalized by stake-weighted voting
- Programs are executed in SVM
- More resources:
  - Near Whiteboard series
  - Anatoly at the Digital Garage

Parallelism

Comparing Fee Markets: Solana vs. Ethereum & Other Gas-Based Network



Solana's Localized Fee Market

Parallel Processing: Efficient simultaneous transactions

Localized Congestion: Only specific accounts face congestion

Stable Fees: Unaffected accounts mantain stable fees

Local State

Ethereum & Other Gas-Based Networks

Single Threaded: Sequential transaction processing

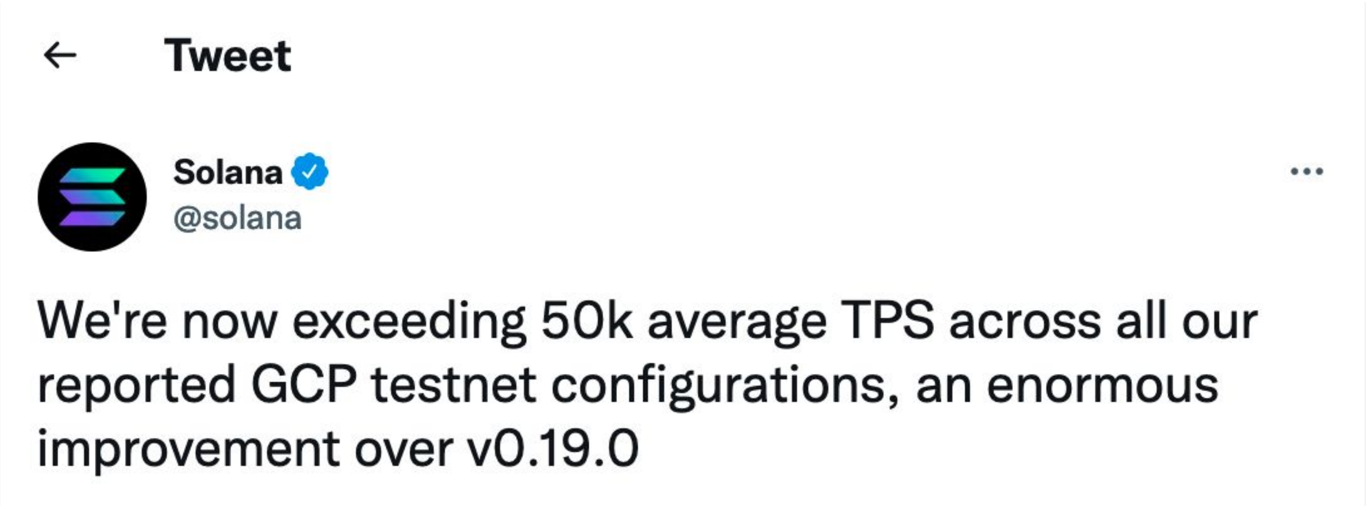
Global Congestion: Entire network faces congestion

Global State

Volatile Fees: Fees spike during network congestion

Solana's localized fee market offers predictability and efficiency by isolating congestion.
In contrast, for Ethereum and other gas based networks, global congestion leads to volatile fees.

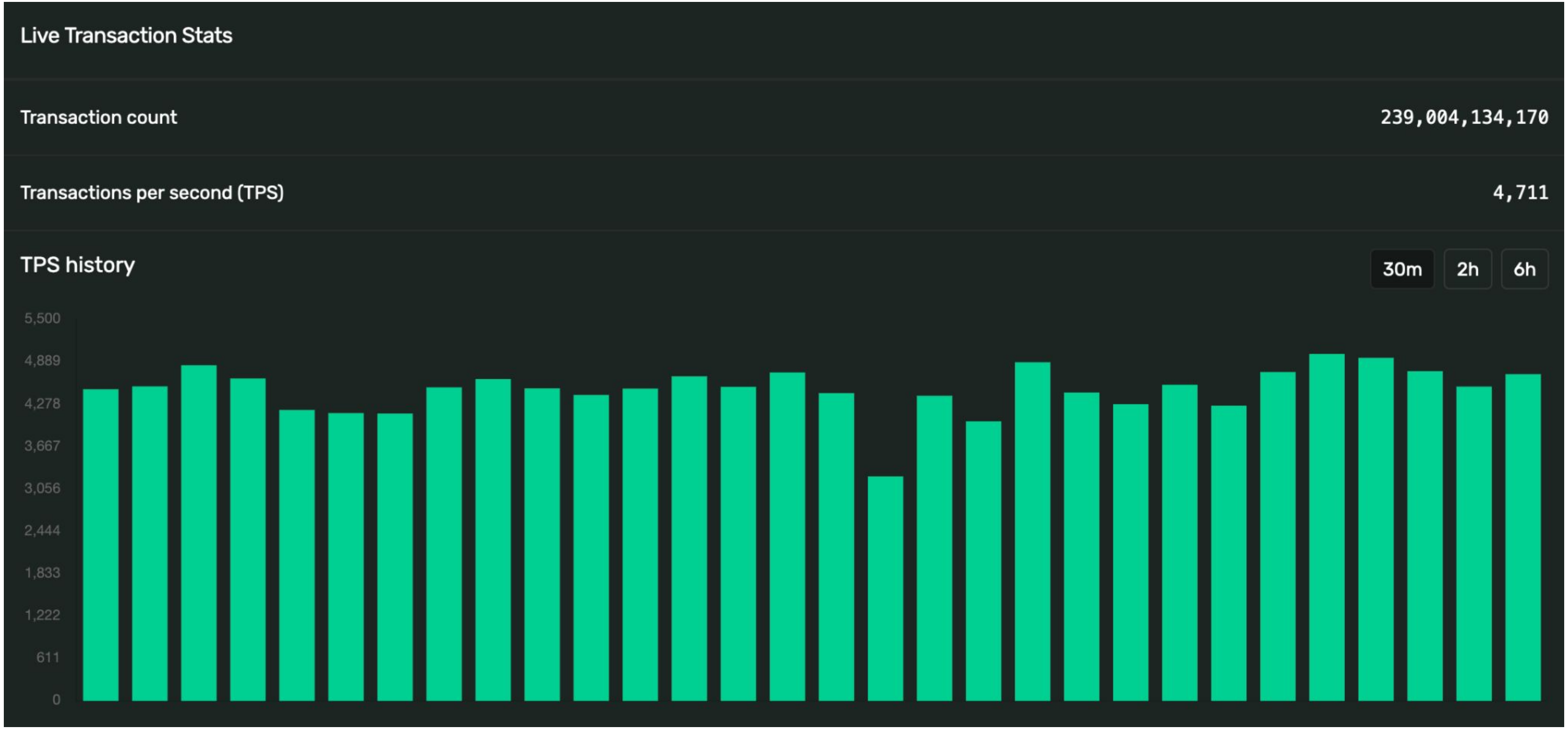
Source: Visa



Tweet

Solana
@solana

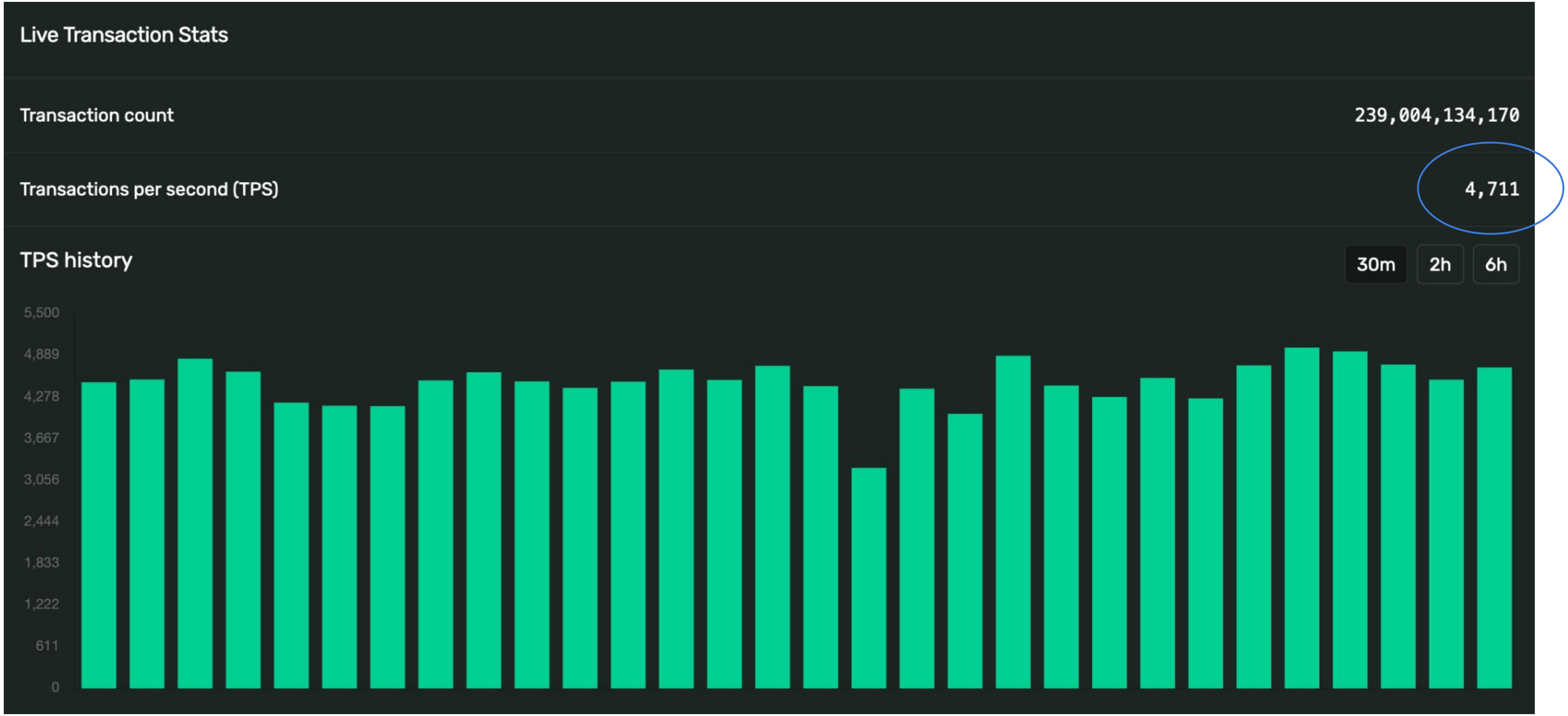
We're now exceeding 50k average TPS across all our reported GCP testnet configurations, an enormous improvement over v0.19.0



Live Transaction Stats

Transaction count	239,004,134,170
Transactions per second (TPS)	4,711

TPS history

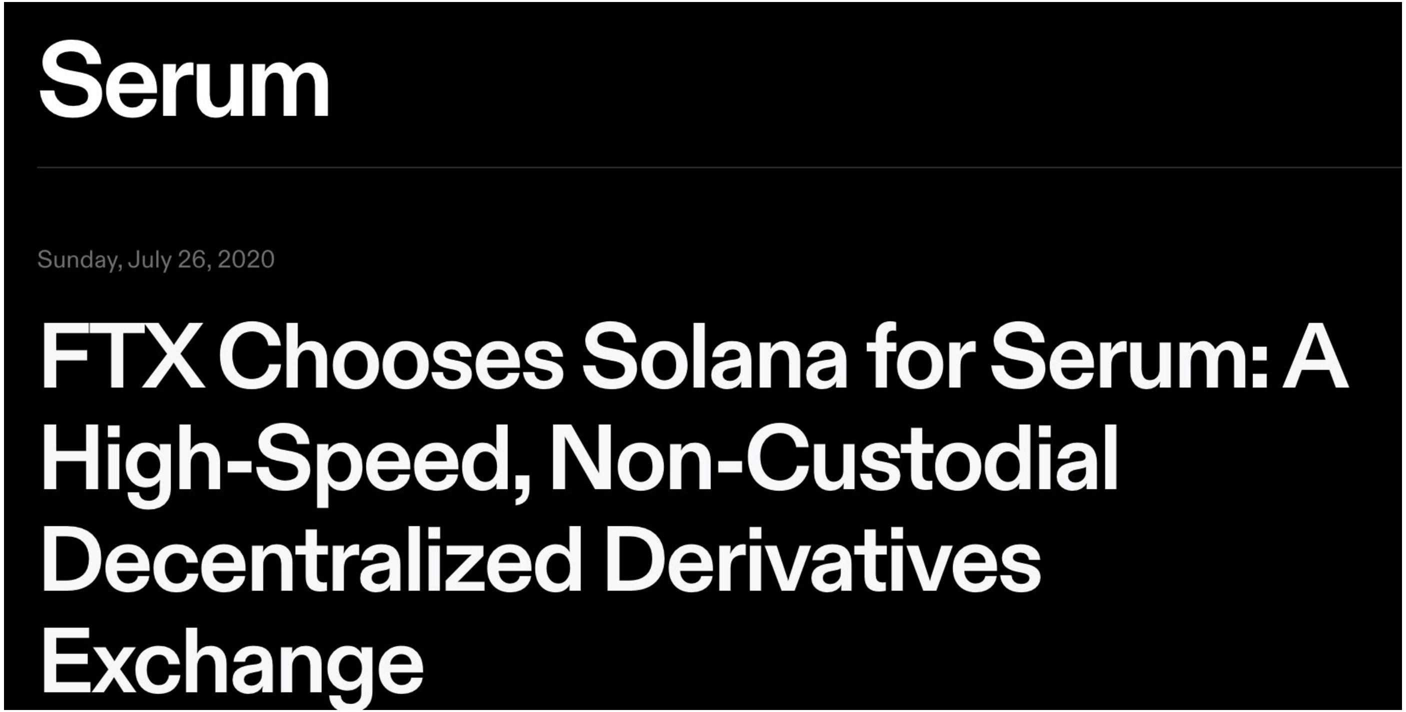


Live Transaction Stats

Transaction count 239,004,134,170

Transactions per second (TPS) 4,711

TPS history

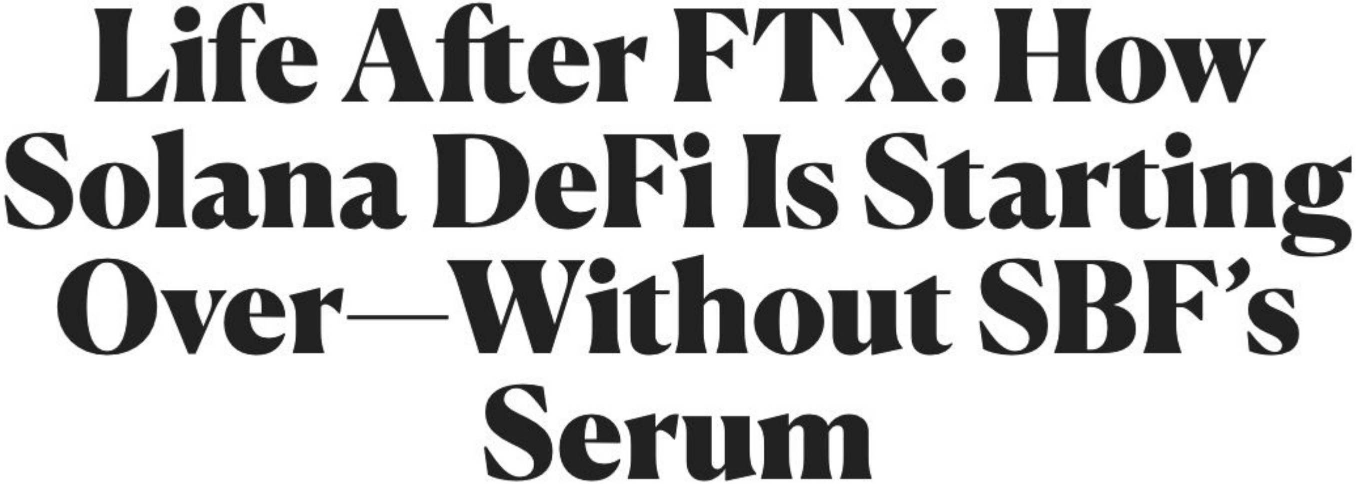


Serum

Sunday, July 26, 2020

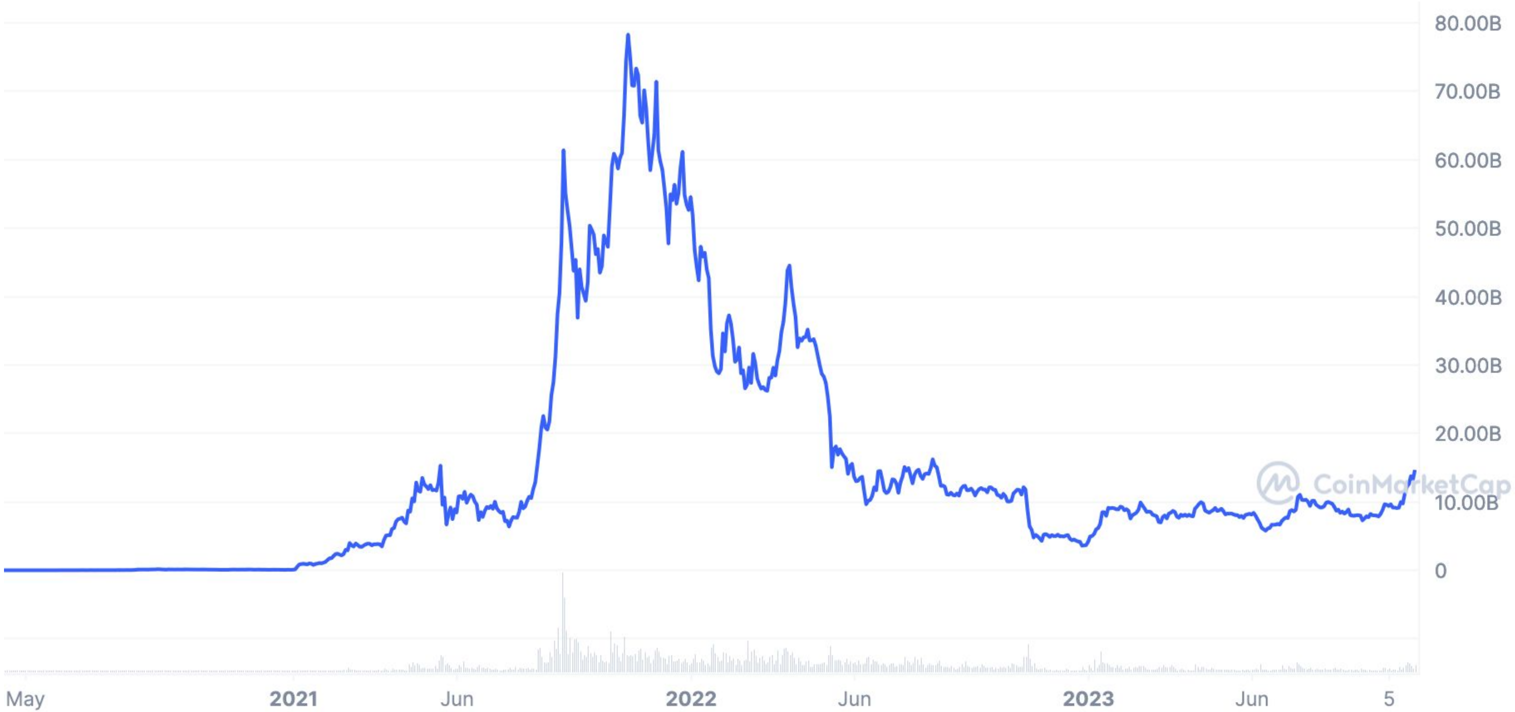
FTX Chooses Solana for Serum: A High-Speed, Non-Custodial Decentralized Derivatives Exchange

epicenter
Sam Bankman-Fried
FTX & Project Serum

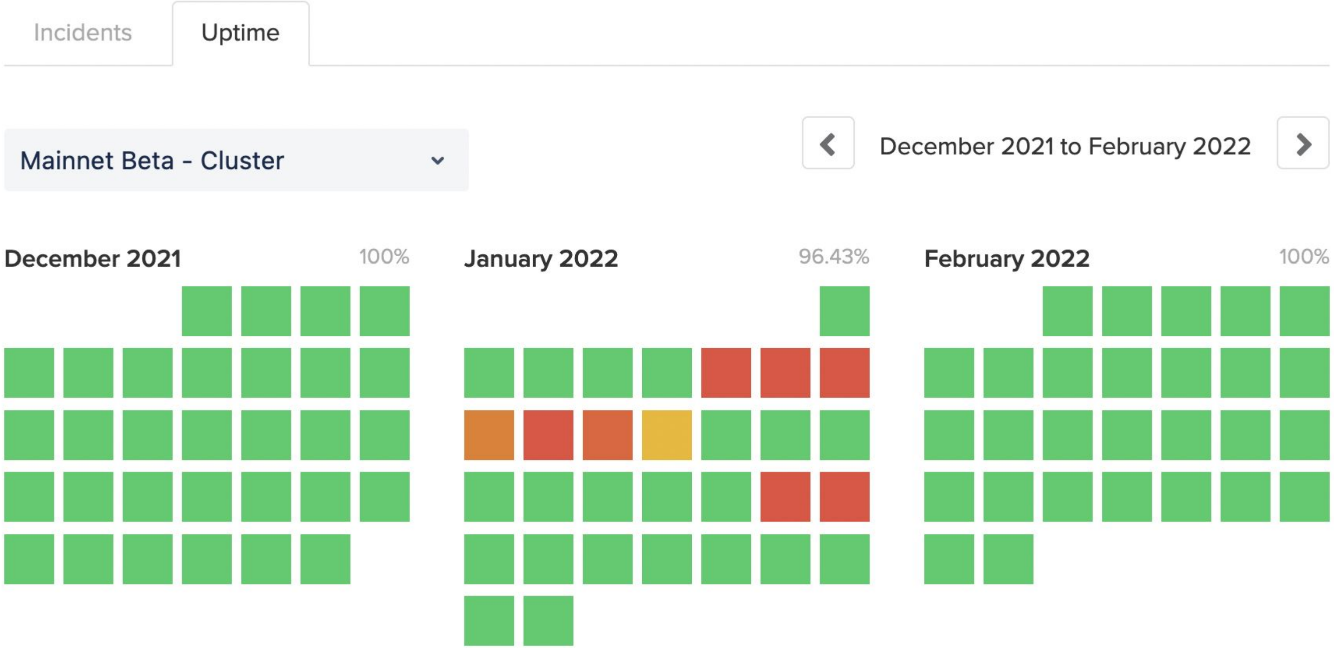


Life After FTX: How Solana DeFi Is Starting Over—Without SBF's Serum

SOL Market Cap



Uptime issues



Mainnet Beta - Cluster

December 2021 to February 2022

December 2021 100%

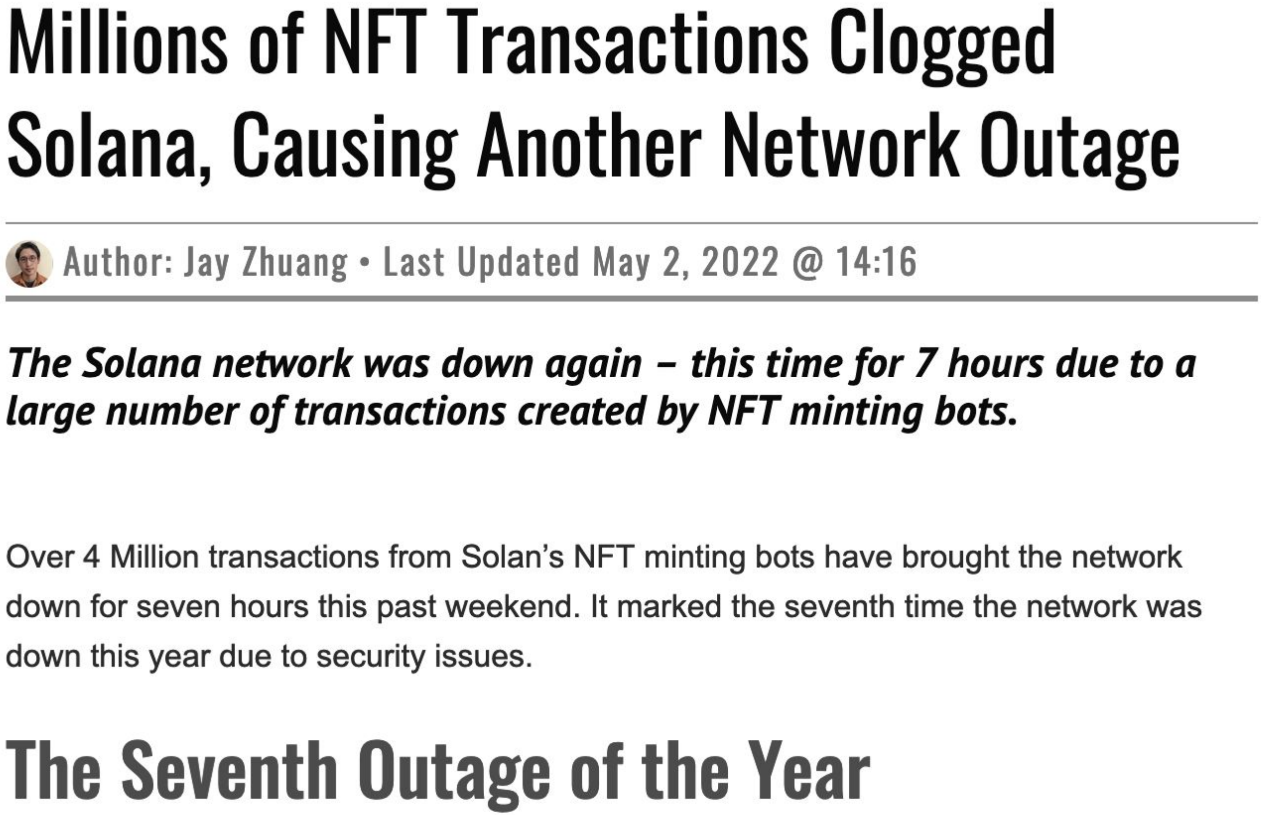
			🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	

January 2022 96.43%

						🟩
🟩	🟩	🟩	🟩	🟥	🟥	🟥
🟧	🟥	🟧	🟨	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟥	🟥
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩					

February 2022 100%

		🟩	🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟩	🟩					



Millions of NFT Transactions Clogged Solana, Causing Another Network Outage

Author: Jay Zhuang • Last Updated May 2, 2022 @ 14:16

The Solana network was down again – this time for 7 hours due to a large number of transactions created by NFT minting bots.

Over 4 Million transactions from Solan’s NFT minting bots have brought the network down for seven hours this past weekend. It marked the seventh time the network was down this year due to security issues.

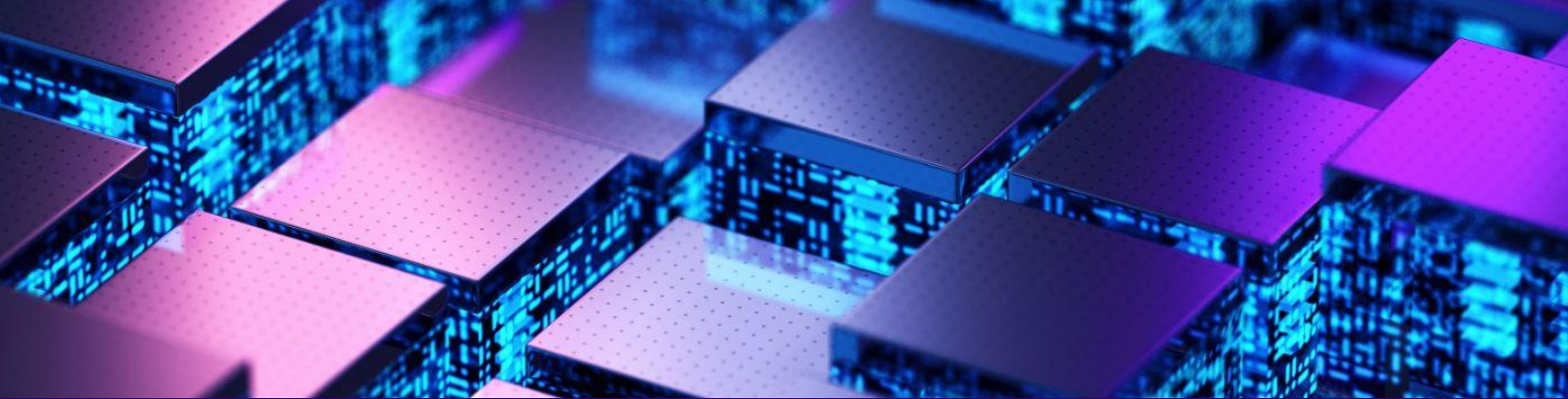
The Seventh Outage of the Year

The Problem

“literally the use case we were designing for was basically Serum it was a central limit order book”

“the idea was that all the transactions are going to be very small”

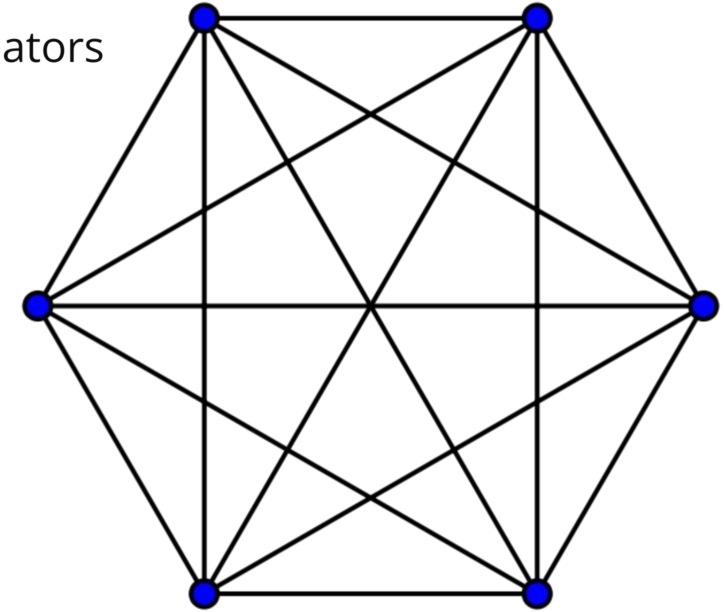
“the biggest part of that whole computationally pipeline is the signature verification”



Solana Consensus

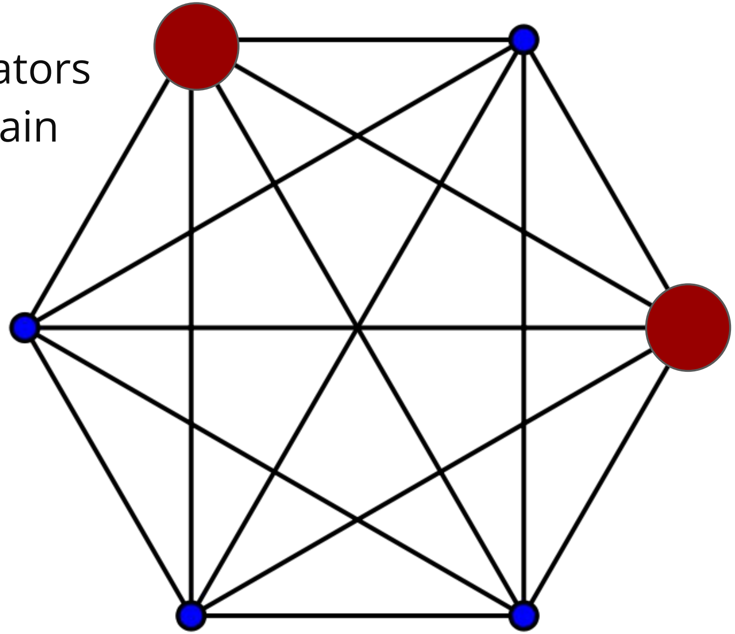
Solana Consensus

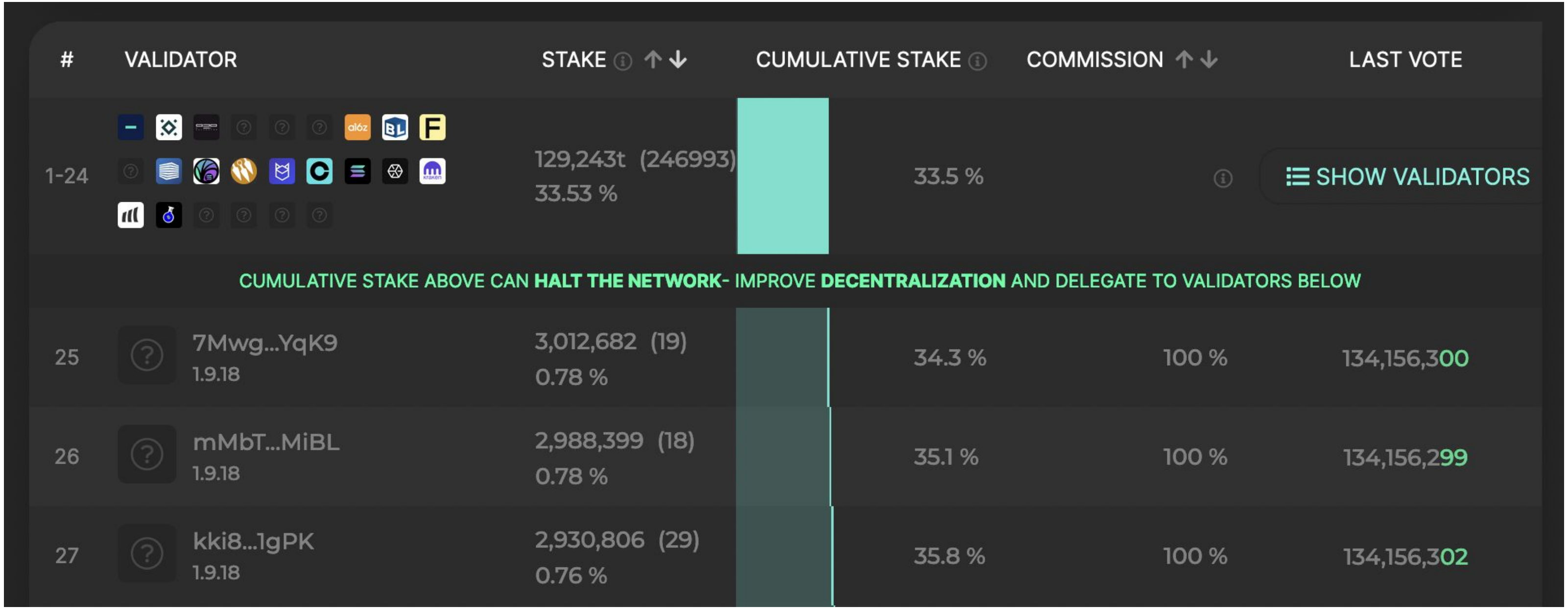
- Proof-of-Stake Consensus
- Safety Requires ⅔ honest majority of validators



Solana Consensus

- Proof-of-Stake Consensus
- Safety Requires ⅔ honest majority of validators
  - ⅓ malicious validators can fork the chain





#	VALIDATOR	STAKE ⓘ ↑↓	CUMULATIVE STAKE ⓘ	COMMISSION ↑↓	LAST VOTE
1-24		129,243t (246993) 33.53 %	33.5 %	ⓘ	☰ SHOW VALIDATORS

CUMULATIVE STAKE ABOVE CAN **HALT THE NETWORK**- IMPROVE **DECENTRALIZATION** AND DELEGATE TO VALIDATORS BELOW

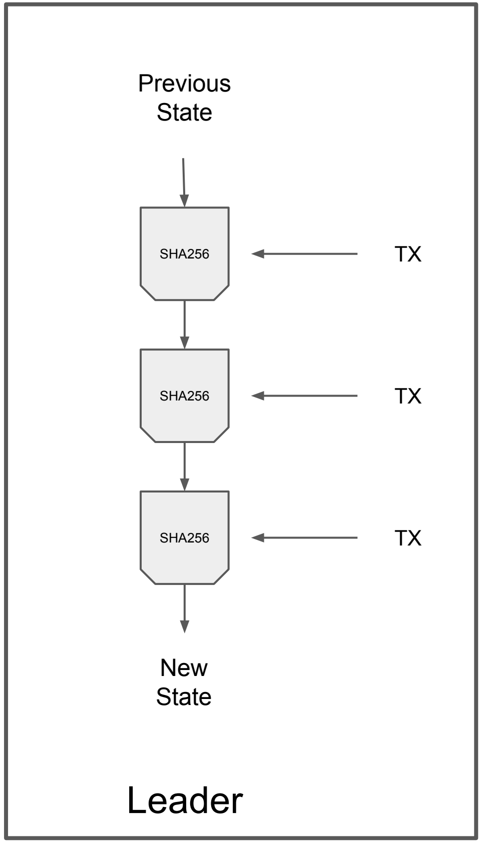
#	VALIDATOR	STAKE ⓘ ↑↓	CUMULATIVE STAKE ⓘ	COMMISSION ↑↓	LAST VOTE
25	7Mwg...YqK9 1.9.18	3,012,682 (19) 0.78 %	34.3 %	100 %	134,156,300
26	mMbT...MiBL 1.9.18	2,988,399 (18) 0.78 %	35.1 %	100 %	134,156,299
27	kki8...1gPK 1.9.18	2,930,806 (29) 0.76 %	35.8 %	100 %	134,156,302

Solana consensus requires ⅔ honest stake

Solana Consensus: Leader Rotation

- Time is divided into periods called “epochs”
  - In practice, Epochs are 432,000 “slots” (a few days)
- Each slot is given a “leader”
- Leader schedule is determined by stake in the previous epoch
  - The ordering of leaders is public
  - Can be viewed by calling getLeaderSchedule
- Approximately 1700 distinct leaders per epoch

Proof of History



Previous State

SHA256

TX

SHA256

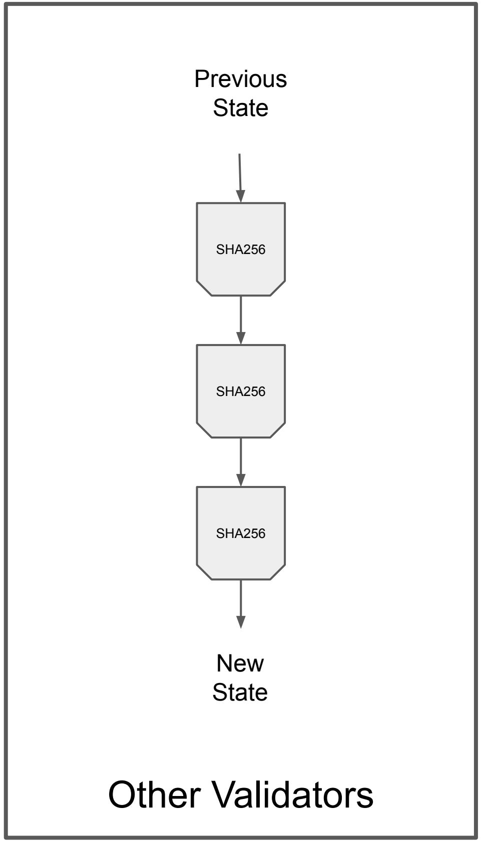
TX

SHA256

TX

New State

Leader



Previous State

SHA256

SHA256

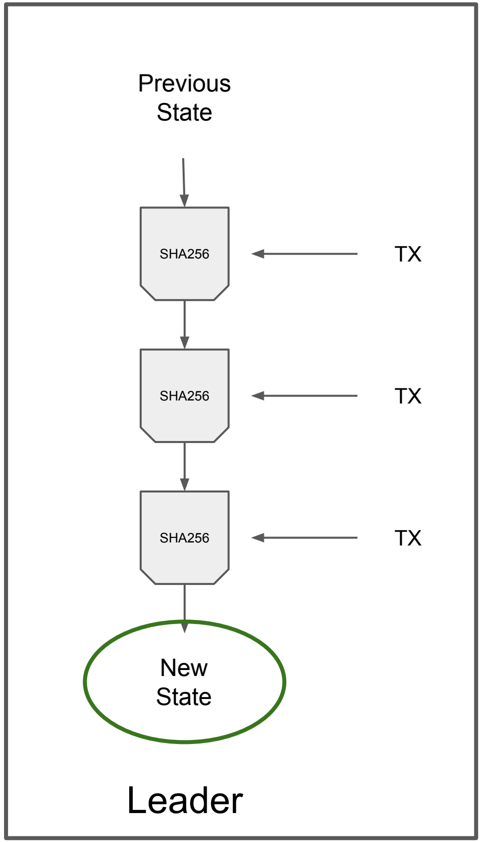
SHA256

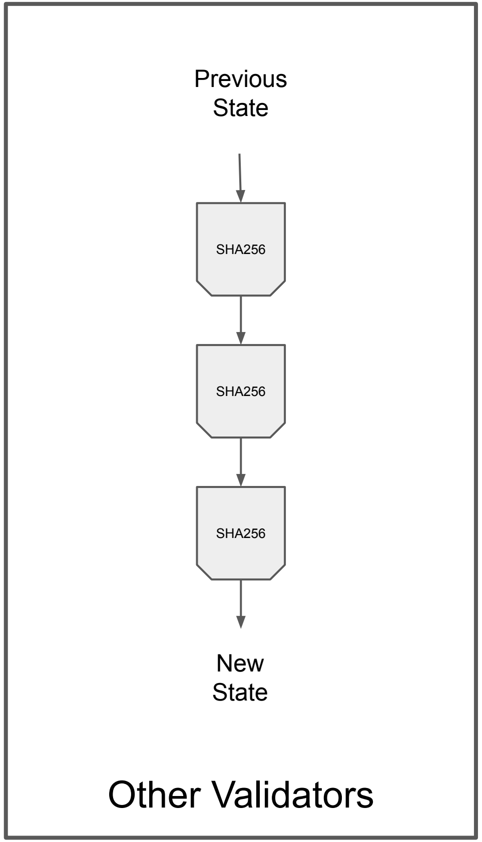
New State

Other Validators

- PoH is essentially repeated hashing
- Sequential hashing is not parallelizable
- Hashing is deterministic so all other validators reach the same new state
- If Leader produces a valid state that will be used, otherwise validators fall back to history with no TXes

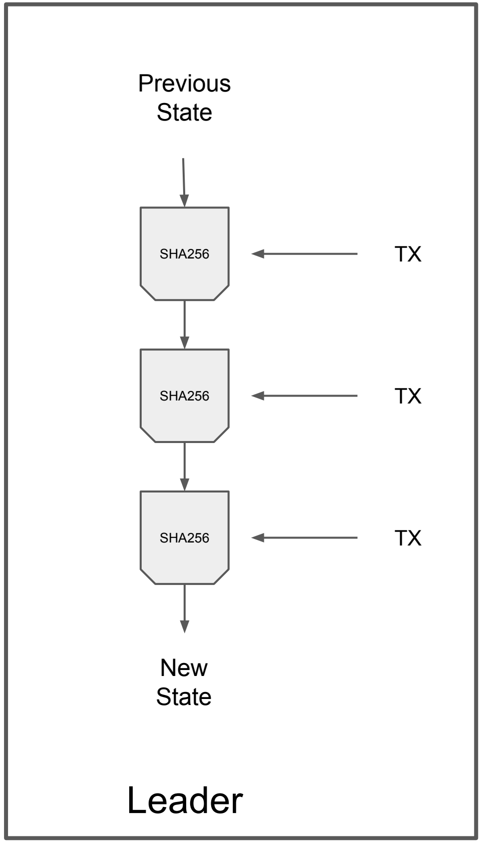
Proof of History

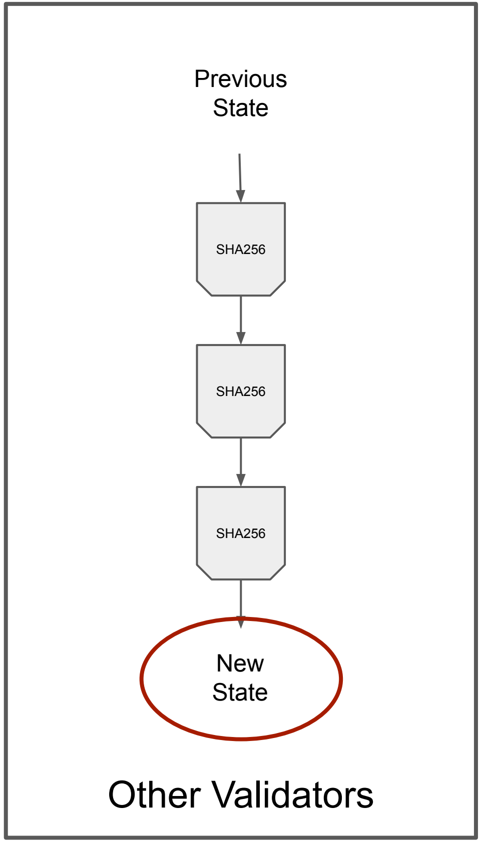




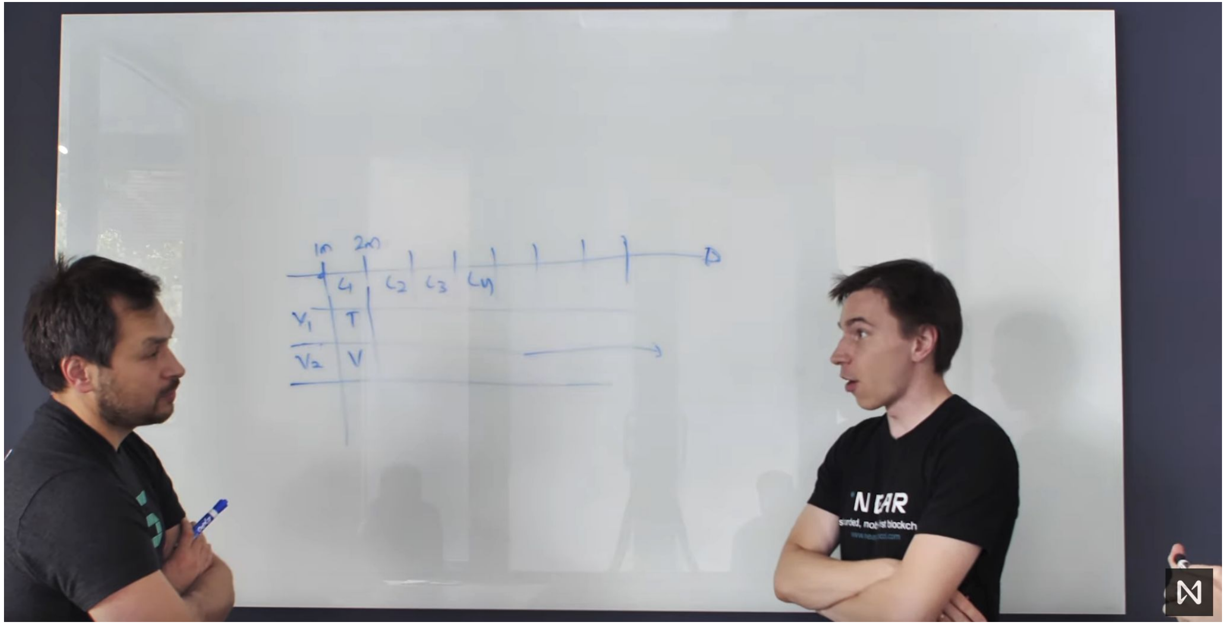
- PoH is essentially repeated hashing
- Sequential hashing is not parallelizable
- Hashing is deterministic so all other validators reach the same new state
- If Leader produces a valid state that will be used, otherwise validators fall back to history with no TXes

Proof of History



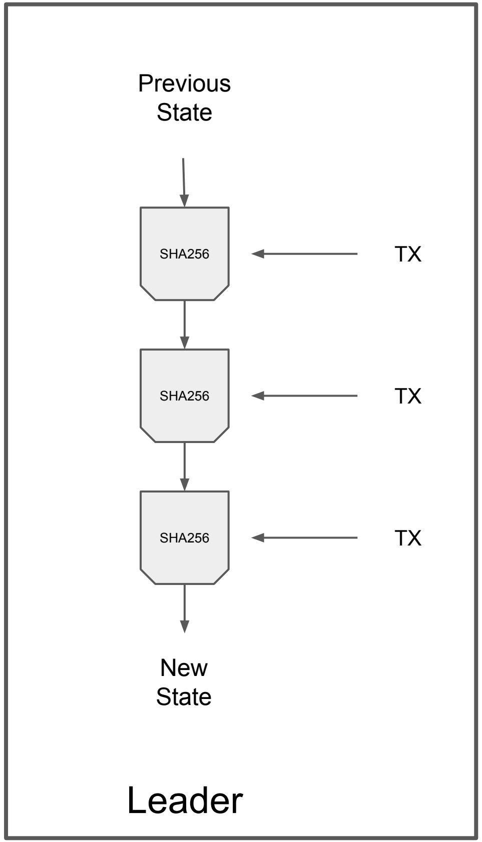


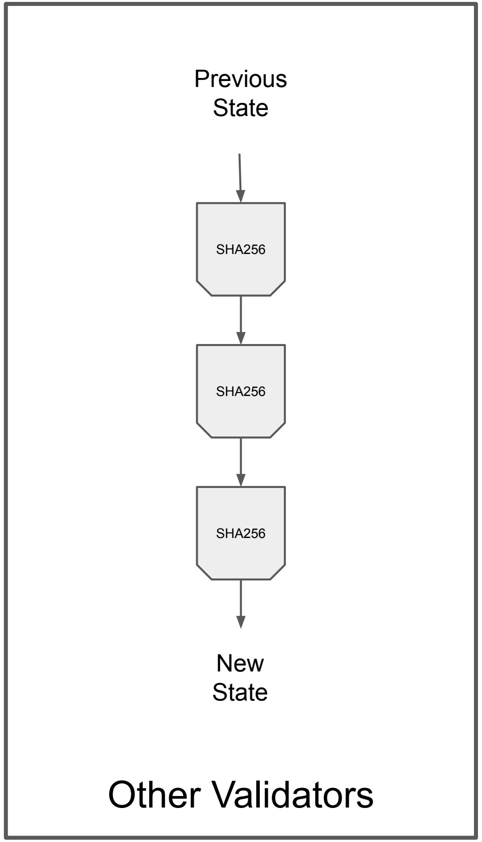
- PoH is essentially repeated hashing
- Sequential hashing is not parallelizable
- Hashing is deterministic so all other validators reach the same new state
- If Leader produces a valid state that will be used, otherwise validators fall back to history with no TXes



Alex: “So every validator is constantly computing hashes, so then we’re burning trees again”
Anatoly: “No, it’s just one core per node”

Proof of History





Proof of History is not a consensus mechanism, or even a sybil-resistance mechanism like PoS or PoW

- PoH is essentially repeated hashing
- Sequential hashing is not parallelizable
- Hashing is deterministic so all other validators reach the same new state
- If Leader produces a valid state that will be used, otherwise validators fall back to history with no TXes

Proof of History

- Proof of History can be seen as a (Verifiable) Delay Function (VDF)
  - x_1 = hash(x_0)
  - x_2 = hash(x_1)
  - …
  - Calculating x_n requires n *sequential* steps of computation
  - Verification can be parallelized if prover outputs "checkpoints" e.g. $x_{n/10}$, $x_{2n/10}$, …
- When leader hashes TXes into this cements their ordering
- If a leader fails to include TXes, next slot leader can pick up once they have completed their own PoH sequence

Consensus

- The blockchain can fork at the end of each slot
  - If leader produces multiple new states, this is a provable offense, and their stake will be slashed
  - Two remaining choices
    - Leader produced a valid state
    - Leader failed to produce a valid state
- Blockchain can split at the end of every slot
- Validators vote on a fork
  - Once a validator votes on a fork, they are committed to the children of that fork for a number of time steps
- Fork is “finalized” once it has a sufficient vote weight associated with it

If the use of proof of history as a trusted source of time can indeed be used to significantly improve the performance of proof-of-stake consensus protocols, then the consensus research community would undoubtedly welcome a scientific paper that includes a clear and concise formulation of such a consensus protocol, a precise statement of its properties, an explicit statement of underlying assumptions, and a precise statement as to which assumptions imply which properties (and hopefully a proof of such a statement).

Indeed, given the current lack of published details and analysis, the lack of any meaningful peer review, and the inherent subtlety of designing secure consensus protocols, in our opinion, there currently seems to be little reason to have much confidence in the security of Solana’s consensus protocol