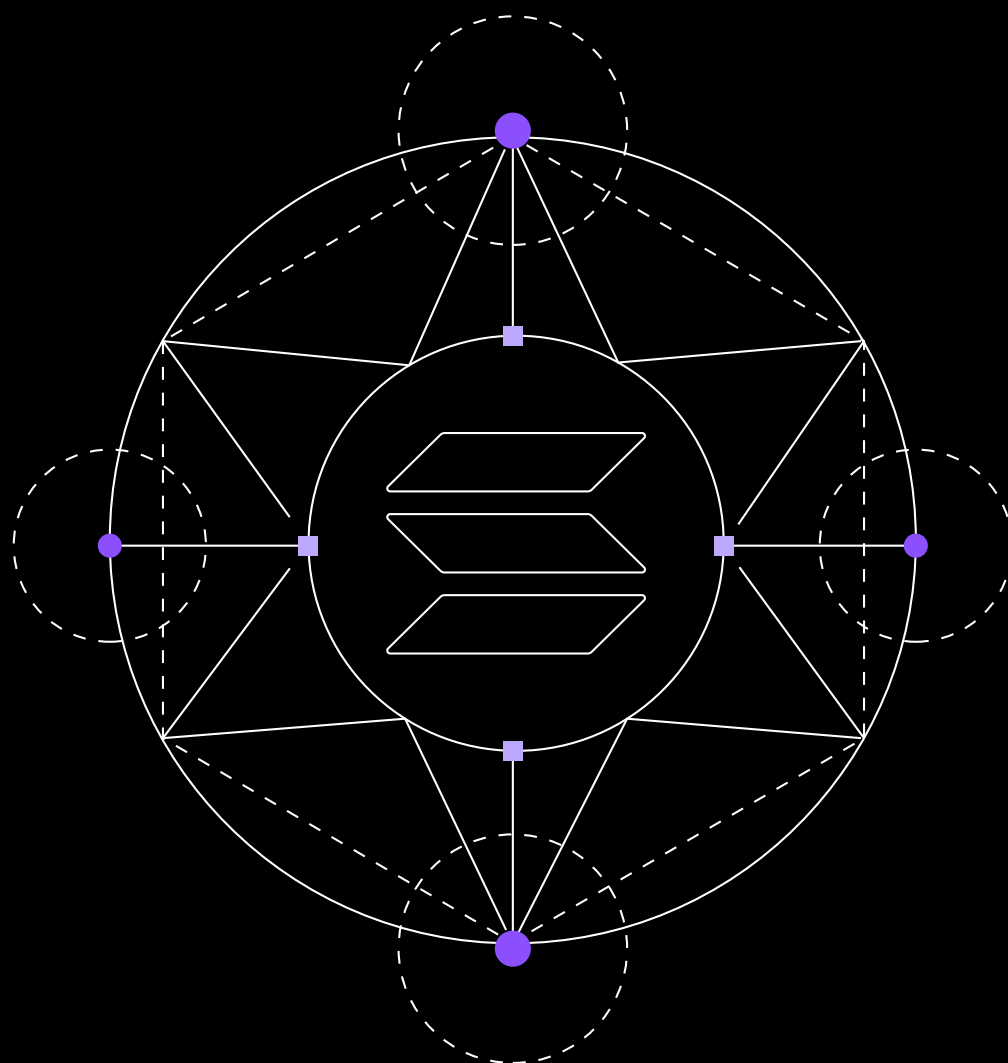galaxy

Galaxy Digital Research

Ready Layer 1: Surveying Solana

MAY 27, 2022

Author & Acknowledgements

Sal Qadir
Galaxy Digital Research
email: sal.qadir@galaxydigital.io
twitter: @sal_coin

We would like to thank the following people for their support in researching and publishing this report: Alex Thorn, Charles Yu, Christine Kim, Leulaye Maskal, Michael Marcantonio, William Nuelle, and Leland Lee.

Contents

This report is part of our Ready Layer One series.
Read the foundational first piece, *Ready Layer One,* at www.L1.report.

Introduction

Solana is a fast, low-latency, proof-of-stake Layer 1 blockchain with a differentiated technical architecture and growing usage across several vectors. While fundamental design problems currently limit its resilience, and centralization issues are apparent, complex technological fixes and upgrades suggested by the protocol team could mitigate or solve these issues. In spite of this, over the last 12 months, Solana has managed to separate itself from the pack of other Layer 1 blockchains to challenge Ethereum's status as the smart contract king of the crypto space.

Solana's unique approach to scaling stands in stark contrast to most other Layer 1 blockchains — achieving a theoretical throughput of 50k transactions per second with low, fixed transaction fees. From a developer's perspective, Solana prides itself on achieving composability without relying on a modular stack, layer 2s, and/or sharding. Additionally, Solana's ecosystem is both bolstered by robust developer building blocks, such as Serum and Pyth, and by strategic partnerships with industry behemoths such as FTX and Jump. This report will evaluate Solana in-depth and uncover how well-positioned it is to capture and retain market share in the Layer 1 blockchain landscape.

This report builds on Galaxy Digital Research's Ready Layer One report.

Market Capitalization	
BTC	$577bn
ETH	$250bn
BNB	$51bn
XRP	$21bn
ADA	$19bn
SOL	$19bn
DOT	$12bn
DOGE	$20bn
AVAX	$20bn
TRX	$7bn

Total Value Locked	
Ethereum	$71.17bn
BSC	$8.67bn
Avalanche	$5.10bn
Solana	$4.34bn
Tron	$4.32bn
Polygon	$2.79bn
Cronos	$1.82bn
Fantom	$1.70bn
Arbitrum	$1.41bn
Waves	$1.07bn

Solana Daily Active Users (Fee Payers) Since Jan 1, 2021
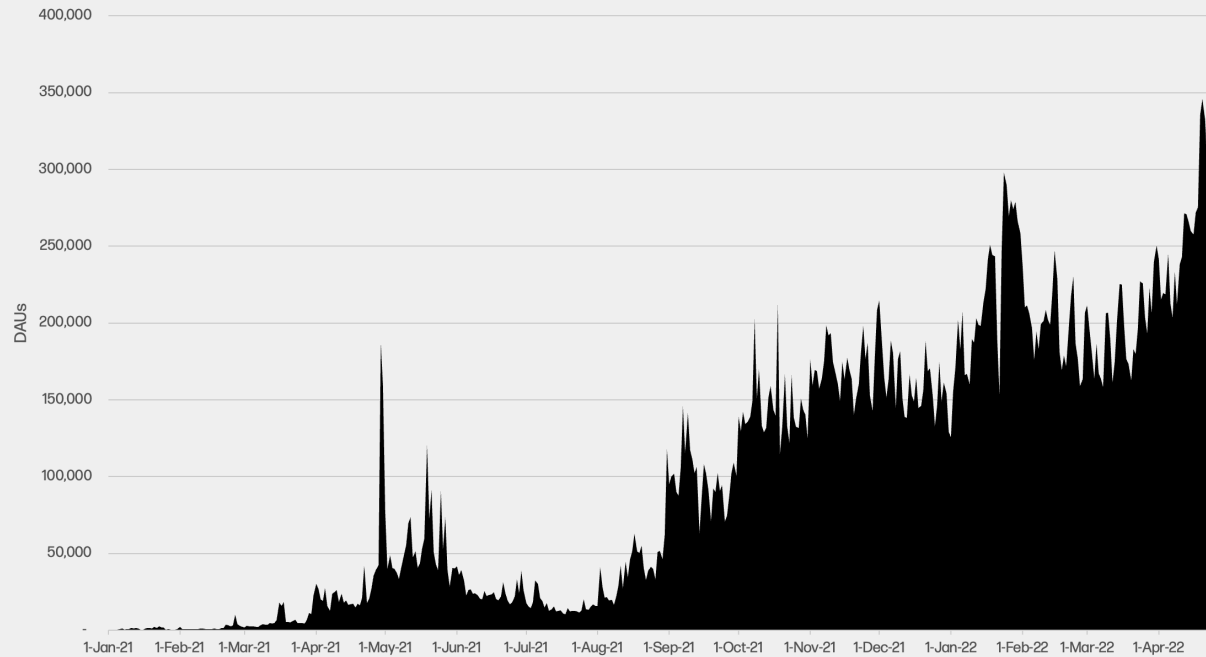
Data: Dune Analytics

Solana Price (SOL/USD) Since Mainnet Launch

Data: Footprint Analytics

Background & History

Who is Anatoly Yakovenko?

Anatoly Yakovenko founded Solana while working as an engineer in San Francisco, CA. He spent most of his career at Qualcomm, where he leveraged his applied-engineering expertise to solve challenging problems in the hardware optimization space. Anatoly had developed a reputation for his strong technical acumen—one of his most noteworthy accomplishments was designing high performance DSP software that powered Google Tango, the first mobile device to support augmented reality in smartphones. He first got interested in crypto in 2017 through a friend who was working on deploying deep learning hardware to the cloud (unsurprisingly, this type of specialized hardware shares many similarities with Solana validator nodes). Anatoly and his friend would leverage these powerful computers to mine Bitcoin profitably net of their initial capital expenditures. As Anatoly fell down the rabbit hole of studying Proof-of-Work mining, he became curious about why Proof-of-Work was necessary, what made it slow, and how it could be improved.

The proverbial "red pill" moment for Anatoly occurred when he explored single threaded mining one night in 2017. Anatoly reasoned that instead of measuring electricity, as was integral to Proof-of-Work mining, one could measure time. Anatoly was convinced that tying the security of a crypto network to a physical constant, such as electricity or time, was critical to long-term dependability. In this vein, Anatoly's epiphany came when he realized that sequential hashing can be leveraged to guarantee that two events took a certain amount of time to occur between them. Anatoly later described this concept as Proof-of-History, and he published these findings in a draft whitepaper in November 2017. By February 2018, Anatoly joined with Greg Fitzgerald to release both a Solana testnet and an official whitepaper.

One of Anatoly's Qualcomm colleagues, Stephen Akridge, suggested a modification to Solana's architecture that leveraged GPUs for parallelization of signature verification. Stephen's valuable contribution both validated the merits of Anatoly's initial protocol design and motivated him to go all-in on the project. In addition to Greg and Stephen, Anatoly recruited Raj Gokal and 3 additional Apple/Qualcomm veterans to form Solana Labs. While the project was initially called Loom, the team ran into naming confusion issues with the Loom Ethereum L2 network. The team ultimately decided to change their name to Solana, which is named after Solana Beach in Southern California (where the team lived in and worked at the time).

Building in a Bear Market

Solana Labs was formed in early 2018 and led by a visionary founder in Anatoly. The Solana Labs team was on a mission to take Solana from a proof-of-concept to production-grade, permissionless blockchain. The only problem was they were faced with a difficult fundraising environment in 2018 — the ICO bubble had just popped. Bitcoin prices were taking a nosedive and many investors had cold feet about blockchain/crypto startups. Solana Labs co-founder and COO, Raj Gokal, describes in an FTX podcast that, at the time, Solana's team was struggling to differentiate themselves in a competitive landscape where Dfinity (now known as ICP) had just raised $100 million and Avalanche Labs was established by renowned Cornell professor Emin Gun Sirer on basis of a novel consensus protocol. To some, Solana was simply another Layer 1 blockchain focused on "vanity metrics" like transactions per second (TPS). At the time, the Twitter-based "Cryptosphere" was more enthralled by startups focusing on privacy and interoperability, not scalability. By a stroke of luck, Anatoly was able to convince a friend he met playing underwater hockey to become an early investor, and this investor would then introduce the Solana team to two other backers.

The team was able to raise $20 million in funding through private token sales offered to accredited investors. Some of the early backers included Multicoin Capital, 500 Startups, and a founder of Race Capital. These investors were impressed by Solana's testnet's consistent ability to support for bursts of 250k transactions per second. The private token sales were announced as a Series A round in late 2019. While the team was fundraising, they also built out a public testnet called Tour de SOL (the majority of Solana's cofounders were cycling enthusiasts). By March, 2020, Solana did a $1.76 million public token auction on CoinList and launched their Mainnet Beta.

Technical Architecture

Solana's Blockchain and NASDAQ Speed

When Anatoly was first developing Solana, he drew on his personal fascination with programmatic electronic trading. Anatoly was frustrated that, as a regular end-user accessing the APIs of popular platforms like Interactive Brokers, his trades were getting front run by intermediaries with access to more capital and trading infrastructure than him. Anatoly's empathy with a retail-oriented use-case drove the initial vision for Solana. he wanted regular users of Solana to enjoy a level playing field with powerful institutions. In the long-term, Solana's goal was to eventually enable the scale and speed of NASDAQ on a blockchain. In fact, Solana's early seed-stage pitch decks were peppered with this phrase: "Solana's Blockchain and NASDAQ Speed." Anatoly's design decisions for Solana emphasized speed and information flow versus 'store-of-value' use-cases that other blockchains like Bitcoin focus on.

The key differentiating factors separating Solana from the vast majority of other Layer 1 blockchains are: 1.) hardware 2.) the physical passage of "wall clock" time and 3.) composability. Together, these 3 key attributes form the foundational pillars upon which Solana's tech stack is built.

First and foremost, Solana leans heavily on advancements in hardware to hedge against the challenges of protocol advancement at the software level, guaranteeing that its speed and scale will increase as hardware continues to improve. Starting about five years ago, progress in Moore's Law as it applies solely to CPU transistor density has slowed, though it is still advancing. More importantly, the field of AI/Machine Learning is fueling new breakthroughs in GPU/parallelization processing power, and it shows no signs of slowing down any time soon. The Solana team's view is that that progress at the software level, evidenced by notorious delays (such as Ethereum's 2.0 update), may hit roadblocks given only a small subset of people have the technical depth to implement protocol-level changes in a safe manner. Regardless of how quickly they can make progress on their underlying protocol, the Solana team is betting that the computer hardware industry will keep marching forward year after year. This ensures that Solana's underlying scalability can ride the coattails of the hardware sector at a regular cadence, all else equal. It also differentiates the Solana blockchain from other Layer 1 blockchains whose scaling roadmap is primarily reliant upon advancements in software design.

The second fundamental concept underlying Solana's technical architecture is time. Solana decouples time from consensus on state updates. Since each transaction on Solana is timestamped, transactions can be streamed in real-time as they occur. This approach diverges from most other blockchains where timestamps

Solana: A new architecture for a high performance blockchain v0.8.13

Anatoly Yakovenko
anatoly@solana.io

Abstract

This paper proposes a new blockchain architecture based on Proof of History (PoH) - a proof for verifying order and passage of time between events. PoH is used to encode trustless passage of time into a ledger - an append only data structure. When used alongside a consensus algorithm such as Proof of Work (PoW) or Proof of Stake (PoS), PoH can reduce messaging overhead in a Byzantine Fault Tolerant replicated state machine, resulting inn sub-second finality times. This paper also proposes two algorithms that leverage the time keeping properties of the PoH ledger - a PoS algorithm that can recover from partitions of any size and an efficient streaming Proof of Replication (PoRep). The combination of PoRep and PoH provides a defense against forgery of the ledger with respect to time (ordering) and storage. The protocol is analyzed on a 1 gbps network, and this paper shows that throughput up to 710k transactions per second is possible with todays hardware.

are processed in batches of transactions for each block. The advantage of separating time from state updates is that validators can pre-process blocks to boost throughput since the ordering of its transactions adhere to a global clock.

With that said, it is interesting to note that there is very little acknowledgement from the broader blockchain development/research community (outside of Solana) that time is a useful invariant for scaling blockchains. The only notable example of time being used for scaling distributed applications can be found in the telecommunications industry (which makes sense given the Solana founding team's experience in telecom sector). Specifically, Time Division Across Multiple Access (TDMA) has been the underpinning of cellular networks since 2G. The details of how TDMA works are outside the scope of this report, but it boils down to taking a limited resource (radiofrequency bandwidth) and slicing that bandwidth into timeslots created by a global clock to accommodate the connectivity of more devices without requiring more network resources. Ubiquitous mobile broadband would not exist today without this critical, time-based approach to scaling cellular networks. A great primer on how TDMA works can be found in this video. A simplified diagram of how TDMA works can be seen below.

Simplified Diagram of Time-Division Multiple Access (TDMA)
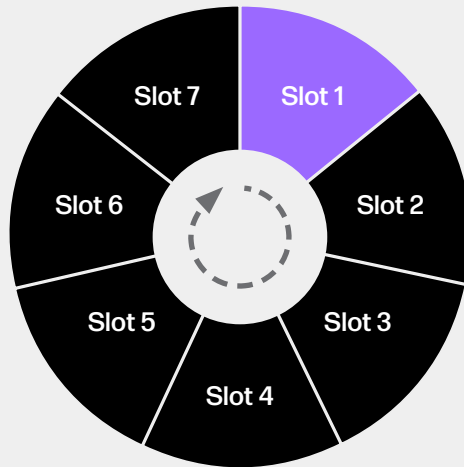
1 Second is Split into 7 Slices

- 1 slice = 1 phone call
- Each call is compressed
- Each call communicates with tower every 1/7th of 1 second
  - *Compression compensates for remaining 6/7^{ths} of 1 second*

Tower Continuously Rotates Through Timeslots

Source: Galaxy Digital Research

Doubling Down on a Monolithic Architecture

Finally, the third key concept underpinning Solana's technology is the idea of composability. Composability refers to Solana's intentional design as a monolithic blockchain. While the monolithic path Solana is taking is positioned as a killer feature in their eyes, this choice is certainly a contrarian blockchain design bet in the broader crypto landscape. Other blockchains, such as Ethereum and NEAR, view a monolithic architecture as an impediment to long-term scalability. These competing Layer 1 blockchains are exploring solutions such as modular scaling (advanced by projects like Celestia and Evmos in Ethereum), Layer 2 scaling (advanced by projects like Starkware and Aztec in Ethereum), and various forms of sharding (on Ethereum's roadmap and implemented currently in the NEAR protocol).

The design trade-offs between these technical approaches merit their own discussion in a separate research report. Regardless, Solana is hesitant to veer away from its monolithic vision of the future. The Solana team posits that the benefits of optimizing for composability is rooted in the elegance of building applications on top of a single, global state. Solana's team believes that, under a monolithic architecture, developers will not be burdened with multiple shards or layer 2 systems when writing smart contracts that require different pieces of Solana's state. Concretely, if an application developer wanted to create an atomic swap between an SPL token for an NFT platform and an SPL token for a DeFi app,

they could do it easily today thanks to Solana's global state. If that same developer had to write a smart contract for a sharded state, it's possible that they would need to add additional logic to check which shards each portion of the swap reside on, and this increases the complexity of the transaction in question.

As blockchain applications get more complicated and intertwined with one another, the developmental complexities of building on modular and/or sharded systems could become exponentially more difficult. From an end-user's point-of-view, an application built on one Layer 2 protocol may not be natively interoperable with an application built on a different Layer 2 protocol despite the Layer 1 being the same blockchain (such as two separate apps built on Optimism or Arbitrum, both of which are L2s of Ethereum). Solana is very committed to the end-user experience, and they see modularity/layer 2s/sharding as "last resorts" as opposed to "necessary evils." It's worth emphasizing that Solana's line-of-thinking here, while well-intentioned, stands in stark contrast to the roadmaps underpinning almost every other Layer 1 blockchain today. The jury is still out regarding how much more onerous the user experience will be for blockchains that leverage multiple Layer 2s at scale. Most Layer 1 blockchains are still monolithic today, and only time will tell how each blockchain's scaling approach will hold up to high usage. Solana has made some educated guesses as to what that future of crypto might look like under a non-monolithic regime and they are, for now, committed to maintaining the simplicity of a global state afforded by a composable, monolithic architecture.

Eschewing the EVM

The Ethereum Virtual Machine (EVM) is a computational engine that serves as the runtime environment for Ethereum smart contracts. The EVM is what developers use to build decentralized applications (dapps) on the Ethereum blockchain. Its purpose is to manage "state" on the permissionless ETH blockchain. Additional details on the concept of "state" on blockchains can be found here.

Many other Layer 1 blockchains and sidechains, such as Avalanche, Binance Smart Chain, Harmony, and Polygon, (among many others) tout EVM-compatibility as a core feature. This is because there is already a lot of code written in Solidity for dapps that run on the EVM, and porting that code over to an EVM-compatible chain is a relatively trivial exercise. These EVM-compatible, alternate Layer 1s can also leverage existing tooling on both the developer side (Hardhat, Truffle, Remix) and the UI/UX side (MetaMask, Coinbase Wallet).

Solana, on the other hand, was intentionally designed to operate within the LLVM instead of the EVM. The LLVM is a standard compiler toolchain that separates human readable code, such as code written in Rust, from assembly, which is low-level code that can take advantage of hardware optimizations. Pragmatically,

one can imagine the flow for LLVM-based deployments looking like source code → LLVM → assembly. There are two key reasons Solana made this architectural choice. 1.) Solana is designed to be hardware-optimized, which is not natively supported by Solidity/EVM. 2.) Programming languages like Rust allow for extremely fast, low-level code that is more widely adopted in the developer community, and, theoretically, easier for an experienced developer to audit. According to the Stack Overflow Developer Survey 2020, 65,000+ developers voted Rust as the most beloved programming language for the 5th year in a row (by a wide margin).

However, the trade-off Solana made with this decision is that not many blockchain-specific developers know Rust, so recruiting new talent from competing crypto companies/protocols is often a difficult endeavor. Some would argue that this as a positive, however, as the Solana developer community is less "mercenary" in nature and more committed to the Solana ecosystem by virtue of having a skillset that can only be useful to Rust-based blockchain projects.

The high-level technical decisions, described above, are the "why" Solana's 8 Core Innovations described in the following section.

Simplified Diagram of the EVM *(adopted from Ethereum EVM Illustrted)*
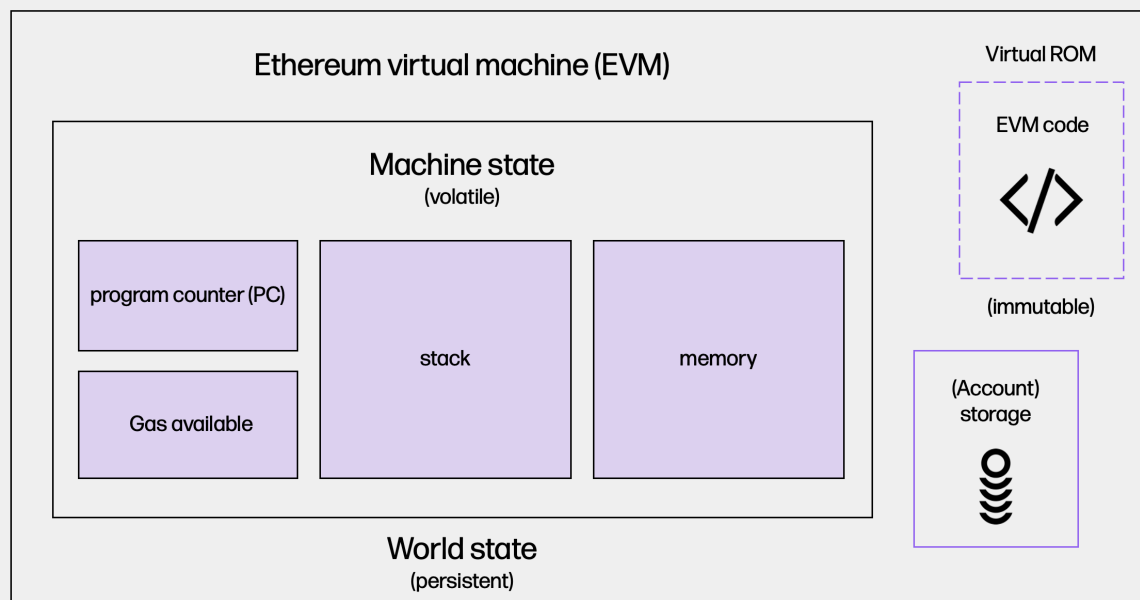
Source: Galaxy Digital Research

Solana's 8 Core Innovations

Proof of History (POH) *a clock before consensus:* Proof of History is neither a consensus protocol nor a sybil-resistance mechanism. Rather, PoH is a high-frequency, Verifiable Delay Function (VDF). VDFs are functions that sequentially produce unique outputs that can be verified much faster than they can be generated. In other words, VDFs take time to produce outputs in their sequential manner, but they can be verified in parallel. In the case of Solana's Proof of History, the VDF is actually a SHA256 hash function running in a constant loop. The way this works is an arbitrary value is initially fed into the SHA256 function (such as the word "Solana"), and each hash's output is fed as an input back into SHA256 to be hashed again. By repeating this process, one can be sure that it took real time to produce the final output since it is not possible to parallelize production of hashes that each depend on the previous hash. This sequentially hashing data structure is what allows Solana to effectively create a global "wall clock" that all transactions on the Solana blockchain can reference to prove the order in which those transactions occurred.
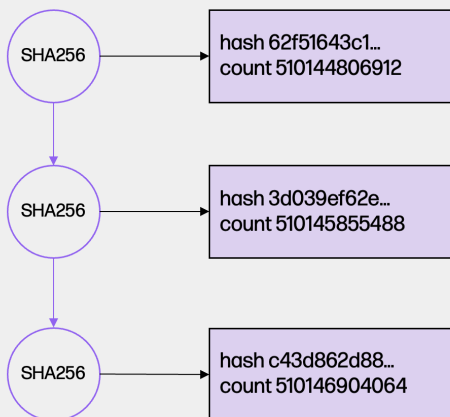
Proof of History in a nutshell:

1. SHA256 loops as quickly as possible on a single core where each output is the next input

2. The Solana network samples this repeating loop and records the number of iterations and the state

3. Messages can be inserted into the PoH loop as hashes with the state. This guarantees the order in which messages were delivered
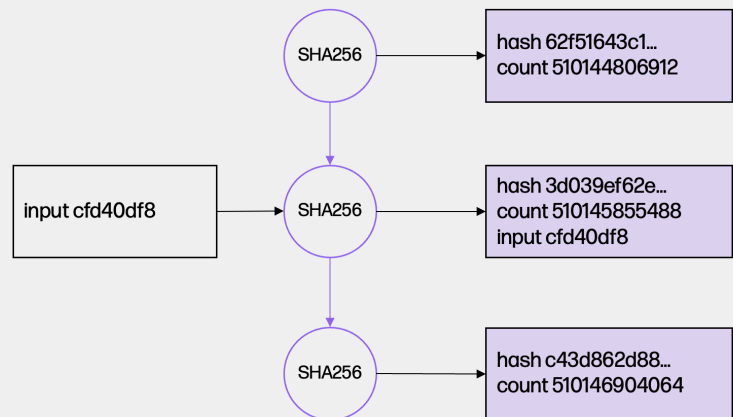
Tower BFT *Byzantine fault tolerance:* Tower BFT is essentially Solana's consensus mechanism. It refers to Solana's implementation of Practical Byzantine Fault Tolerance (PBFT). As a refresher, Byzantine Fault Tolerance describes one's approach to solving the Byzantine Generals Problem – the problem of coordinating an attack between two geographically distributed generals who can only communicate through messengers. Fault tolerant systems seek to guard against bad actors who may try to spread misinformation or intercept the "messenger" before they can get to their destination.

In Solana, Tower BFT is a twist on traditional BFT systems where validators who vote for a block in a certain manner (let's call this initial vote "X") will only vote for blocks descending from "X" for the ensuing two blocks. Every time a validator votes for a block that derives from "X", this "rollback timout" doubles. Since each validator can verify the information inside of a block, thanks to PoH, they can discard blocks that are incongruent with Solana's history. Nodes on the network will receive inflation rewards only when they stay within this maximum vote lockout. This helps guarantee that validators' economic interest are aligned with the fork they believe the supermajority of the network is voting for.

In Tower BFT, liveness, which refers to the ability to always add new blocks, is prioritized over consistency, which refers to the number of potential forks in finalized blocks (see diagram). The difference between Tower BFT and standard PBFT implementations is that Tower BFT relies on PoH as a global clock prior to consensus being reached. This is what allows Solana to reduce latency and messaging overhead, a commonly-cited pitfall of traditional pBFT. Under Tower BFT, validators can vote during a fixed period of hashes or "slots". Generally, one slot is equivalent to 400ms (though this can change over time as hardware continues to advance). As stated earlier, each subsequent slot doubles the amount of wall clock time that the network would have to stall to "unroll" a potential vote (also referred to as the timeout period).

Proof of History Timestamps

Inserting Data into Proof of History

Source: Galaxy Digital Research

consistency refers to blockchains not producing forks in final blocks

Liveness refers to blockchains always having the ability to add new blocks

finalized blocks

pending proposed blocks

Source: Galaxy Digital Research
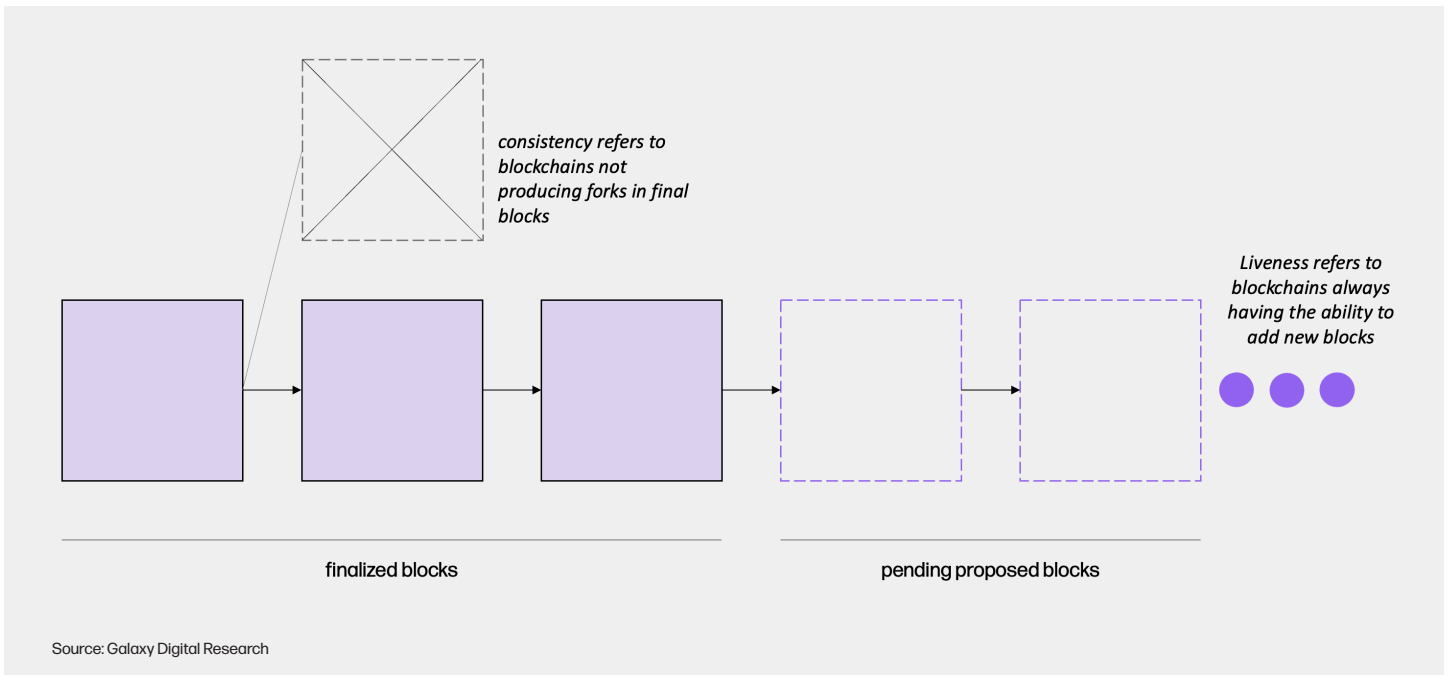
For example, if every validator on the Solana blockchain voted 38 times in the past 15 seconds (15,000 ms / 400 ms = ~38 slots), the network would effectively have a timeout of ~3,400 years. (2^38*400)/1000/60/60/24/365. This approach to BFT is predicated on time-outs *exponentially* increasing as blocks are produced. Unlike in Proof-of-Work, once a super-majority of validators vote on a PoH hash, the hash cannot be rolled back. Finality is *not* probabalistic.

Under Tower BFT, the network can asynchronously compute timeouts without the need for peer-to-peer communications. Each vote carried out by a validator contains a small sequence of verifiable information (tied to PoH). If other validators observe a proposed vote that contains information that is not verified by PoH, that vote is simply discarded. This is why having a "wall clock", enabled by PoH, *decoupled from* the BFT mechanism itself is critical to Solana's scalability approach.

Tower BFT vs Practical BFT (pBFT)

	Tower BFT	pBFT
Year of Introduction	2018	1999
Used by	Solana (SOL)	Zilliqa (ZIL), Hyperledger
Liveness vs. Consistency	Liveness	Liveness
Deterministic vs. Probabilistic	Deterministic	Deterministic
Leader Schedule	Predetermined Round Robin	Consensus-driven Round Robin
Advantages	Highly Scalable	Modularity and Flexibility
Drawbacks	Reliance on PoH	Leader Selection, Unscalable As-is

Source: Galaxy Digital Research

**Gulf Stream** *memory-less transaction forwarding protocol:* In mempools, unconfirmed transactions sit idle waiting to be processed by the network. Under a mempool structure like Bitcoin or Ethereum, a transactor who pays a higher fee (or a tip) can incentivize network miners or validators to confirm their transaction faster and remove it from the pool. Both the size of the mempool and the cost to get a transaction recognized by the blockchain represents the supply and demand for blockspace on that particular blockchain.

With regards to Solana, imagine if a Solana validator could manage a theoretical "mempool" of 100,000 transactions (Solana doesn't actually employ a mempool in the literal sense). Under these parameters, assuming a throughput of 50,000 transactions per second, a Solana validator could clear this mempool in a manner of seconds. However, this oversimplification ignores the importance of block propagation. In most blockchains, mempool transactions are propagated across the network of nodes using a gossip protocol. Gossip protocols refer to peer-to-peer communication methodologies for transmitting data through a network of distributed nodes. Gossip protocols work well due to advancements like bloom filters which are used to help nodes more efficiently propagate transactions to other nodes. This efficiency stems from the fact that bloom filters leverage hashing functions to identify if an element is *not* contained inside of a given data structure (in constant time, O(1)). However, bloom filters can be too computationally expensive to run as blockchains scale up in throughput due to the sheer number of hashes that would need to compute for each instantiation of the bloom filter. Therefore, the Solana team took a decidedly different approach to block propagation than what is seen in most other blockchains.

Gulf Stream describes Solana's unique approach to transaction propagation by pushing both transaction caching and forwarding to the edge of the network. Since validators are aware of both the transaction's order and who the future leaders will be, they can execute transactions in advance. This allows validators who serve as leaders to switch quicker (similar to how track athletes running a relay race will start running their leg of the race just *before* their teammate passes over the baton). The innovation that makes Gulf Stream possible is the known leader schedule (again using the running analogy, a team competing in a relay race will determine the order each member is running *in advance*). This leader schedule, generated every epoch (~2 days), means that transactions are sent directly to the current and next leader rather than being gossiped randomly like the Ethereum mempool. Most blockchains are not structured with this principle of *certain leaders*. In addition to allowing transactions to executing ahead of time and facilitating seamless leader switching, this approach also reduces the memory loads on validators by virtue of them not needing to track unconfirmed transactions and reduces confirmation times. The main risks of Gulfstream come down to 1.) increased risk of validator collusion (since the leaders are predetermined though the Solana team views this risk as minimal due to Solana's fast block times) and 2.) propensity for spam since Gulf Stream is mempool-less and spam transactions are instead sent directly to the leader.

Solana Transaction Flow
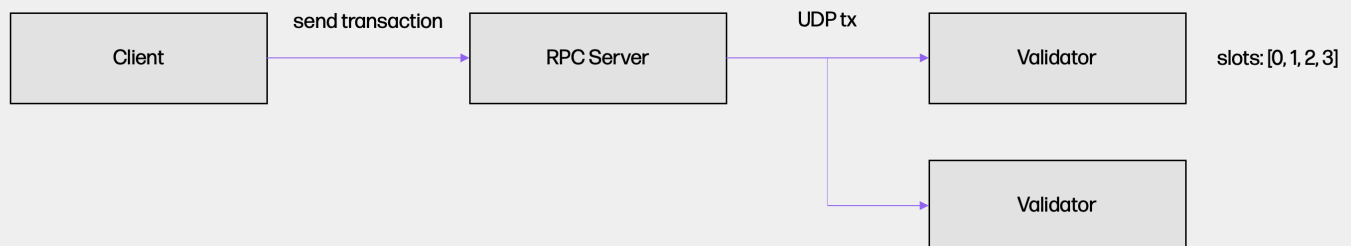
Source: Galaxy Digital Research

Sealevel *parallel smart contracts:* Sealevel is a virtual machine that allows smart contract executions to happen simultaneously on blockchains with the same state. In contrast, EVM-compatible blockchains are single-threaded and can only have one smart contract modify the blockchain's state at a time. Sealevel's parallel execution engine for smart contracts is powered by a verifier at its core, enabling transactions to be executed simultaneously on blockchains with the same state. Sealevel works similarly to an operating systems technique called scatter-gather. Developers on the Solana ecosystem must declare which state they will be reading and writing upfront. Though this increases development complexity, it also allows Solana to parallelize any smart contract executions that are deemed non-overlapping. Sealevel ultimately hands off transaction execution to the hardware level using Berkeley Packet Filters. By leveraging the Sealevel VM, transactions on Solana that only read the same state can be executed concurrently and non-overlapping transactions can be executed at the same time.

Executed Batches need to be Parallelizable

Transaction must be able to be processed in parallel

The Initial transaction reading c is processed, the subsequent transactions are buffered

☐ writeable
☐ readable
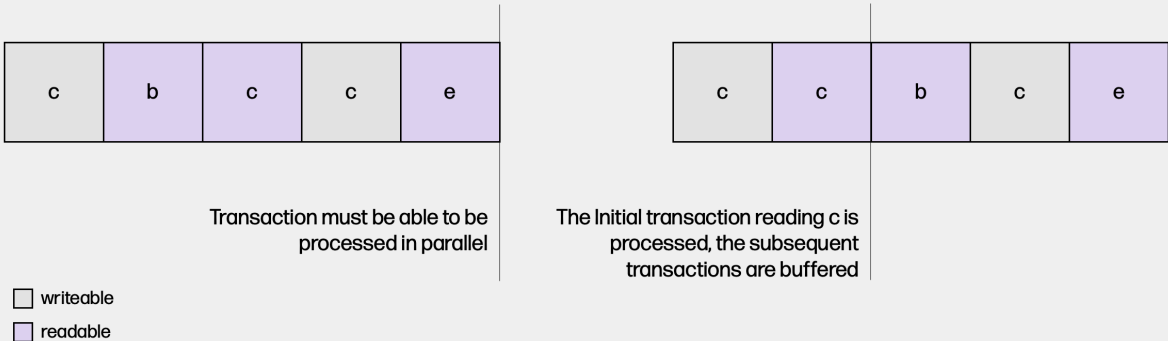
Source: Galaxy Digital Research

Processing Multiple Batches

The top pipeline reads-in account c and sends it to the bottom pipeline

The top pipeline executes the whole batch, while the bottom pipeline buffers c

Solana can process multiple batches at the same time. In this instance, when the bottom pipeline fails to grab a lock on c, it will buffer c for the next iteration.

☐ writeable
☐ readable
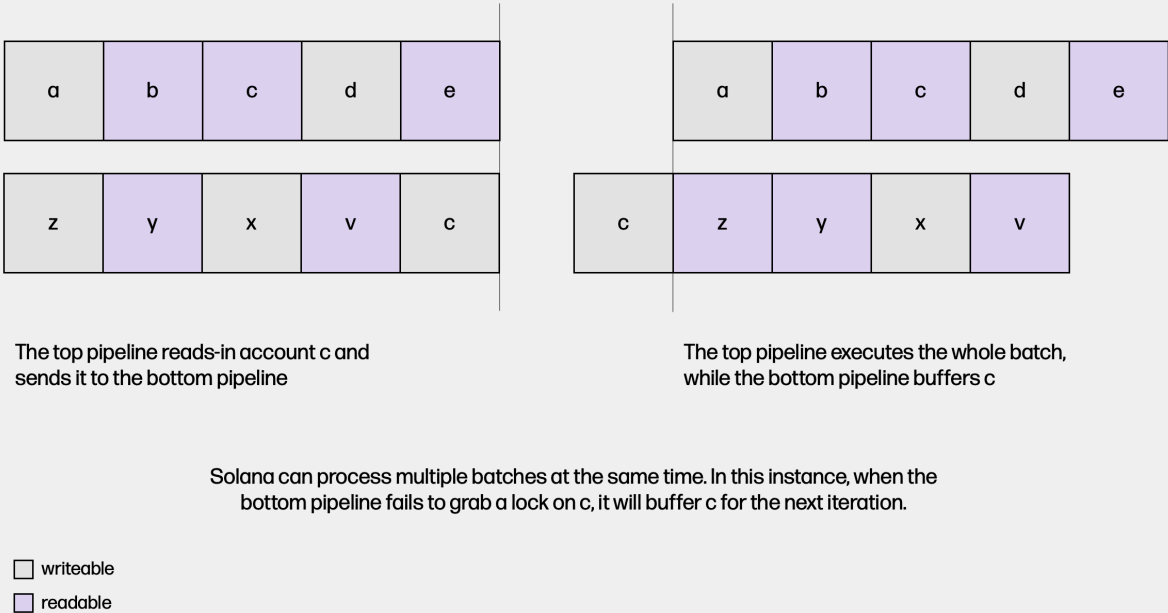
Source: Galaxy Digital Research

Turbine *a block propagation protocol:* Turbine's approach for block propagation borrows heavily from principles used by platforms such as BitTorrent. Turbine works be breaking data stored in blocks into smaller packets. The leader of the current block divides the block's data into packets up to 64kb in size, with each packet sent to a different validator. Once a validator receives a packet, the validator will then transmit this packet to its neighbors. Those neighbors will then propagate the packet to neighbors below it. Additionally, Turbine accounts for potentially dishonest nodes who may either broadcast incorrect data or no data to neighboring nodes. To counteract this problem, the Leader generates Reed-Solomon erasure codes. Erasure codes allow each Validator to reconstruct the entire block without receiving all of the packets. If the Leader sends 30% of packets in erasure codes, the network can drop any 30% of the packets without losing the block.

Leaders may also adjust this percentage depending on the state of the network. These changes are based on leaders' observed packet drop rate from previous blocks.

Pipelining (a transaction processing unit for validation optimization): Pipelining refers to an optimization at the hardware level that enables the Solana blockchain to split a stream of input data into different processes that run on different portions of hardware. Pipelining leverages message queues powered by Rust channels to structure a pipeline that is broken down into 3 stages.

In the first stage, data is fetched and sent out to blocks at the kernel (operating system) level. Concretely, the Kernel Space will pass off data that is sent to the next GPU stage where signatures are able to be verified in parallel. Once signatures are verified, the GPU hands off data to the CPU for the next Banking stage. Meanwhile, the Kernel Space has already fetched the next set of data and will obtain the data to be written to the blockchain from the CPU and send it out to other blocks.

An analogy that can help explain this concept is dishwashing. Normally, this occurs in multiple stages: Rinsing, Sanitizing, Drying, Storing. Instead of a single person running through each of these steps sequentially, the first person would be responsible for rinsing dirty dishes and storing clean, dry dishes. However, they would pass the dish off to another person who would focus solely on sanitizing. And perhaps this person also can soap/sanitize many dishes at once with a basin full of clean, soapy water. (a crude analogy for GPU parallelization). Finally, a third person will focus on drying these dishes and handing off finished dishes back to the first person, who will store them where they are supposed to go.

Throughput, Latency, and Bandwidth

Throughput
Measures the quantity of water (data) flowing through the pipe over a fixed timeframe.

Latency
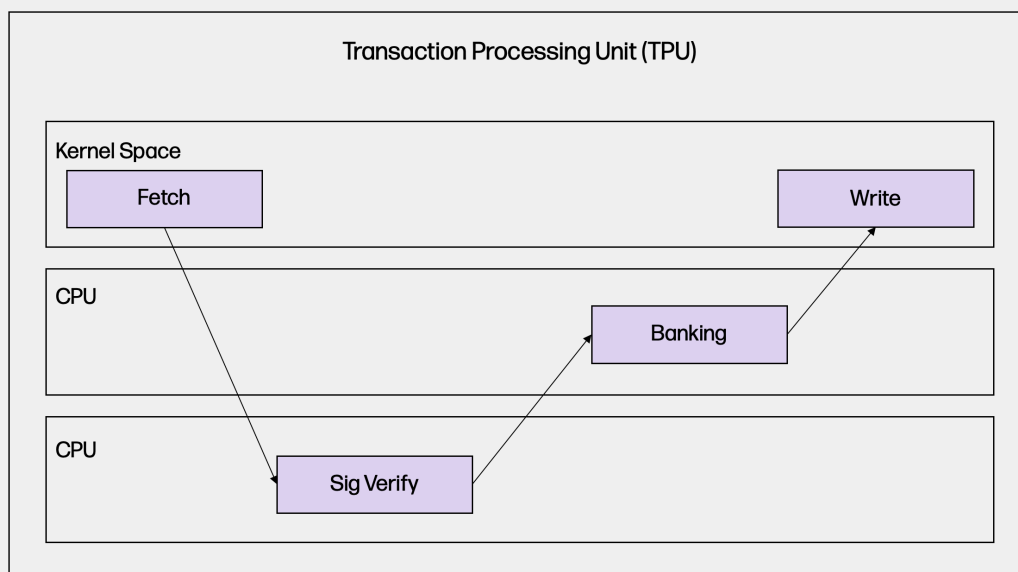Refers to how quickly water (data) moves from point a to point b

Bandwidth
Refers to the pipe's capacity, a larger pipe yields a higher bandwidth
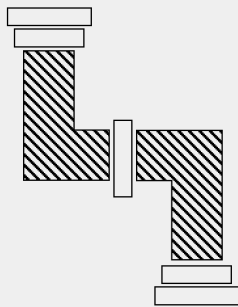
Source: Galaxy Digital Research

Pipelining in Solana

Transaction Processing Unit (TPU)

Kernel Space — Fetch — Write

CPU — Banking

CPU — Sig Verify

Source: Galaxy Digital Research

Cloudbreak *horizontally-scaled accounts database:* Cloudbreak is what enables Solana to leverage concurrent reads and writes at the hardware level. Instead of relying on a traditional database to do this, which is incredibly difficult, Solana instead built a different type of database that borrows from principles used by operating systems. Architecturally, Cloudbreak handles accounts data as follows:

- Accounts and forks indexes are stored in RAM

- Accounts are memory-mapped

- Each memory map stores an account from a single proposed fork

- Maps are distributed across SSDs randomly

- Copy-on-write semantics are utilized

- Writes are added to a random memory map for the same fork

- The index is updated after each write is finished

Rather than rely on general-purpose database abstractions, the Solana team had to build all querying and data manipulation tooling from scratch. This is what enables the Solana network to compute the merkle root of the state updates for a given fork with sequential reads that are scaled horizontally across SSDs. Even when Solana surpasses 10 million accounts, which would be too much data to store entirely in RAM, Cloudbreak still supports 1 million reads and writes per second on a single SSD.

Archivers *distributed ledger storage:* Archivers can best be thought of as light clients that are not downloading the entirety of Solana's ledger. This is important as Solana generates about 4 petabytes of data per year, and only massive validators with large storage specifications will be able to store all this data.

Archivers help reduce centralization risks by giving a wider spectrum of nodes the ability to store pieces of Solana's historical data. Essentially, archivers are the same validators verifying transactions who also download parts of Solana's ledger and provide Proofs of Replication (ProReps) to the broader validator set to ascertain that they are not acting maliciously.

Solana's Real-World Performance

One cannot make an objective assessment of Solana's performance as a scalable blockchain without controlling for factors that might invalidate an apples-to-apples comparison with other blockchains. For instance, Solana's whitepaper claims a theoretical throughout of 710,000 transactions per second. Yet, at the time of this writing, Solana's website shows an average of ~1,500 transactions per second (tps) over the past 6 hours. Right off the bat, there is a ~500x delta between Solana's ideal future and current reality. Taking Solana's self-reported tps at face-value is problematic because it counts internal consensus messages as transactions, which is not standard practice for any other blockchain. In Solana, consensus messages are referred to as "vote transactions" — these are validators with voting accounts handling vote registration, vote collection, and new vote signing. Transactions on Solana that involve dapp smart contract interactions are called "non-vote" transactions (most other blockchains only factor "non-vote" transactions into their tps numbers). According to Dune Analytics, from the period March 2, 2022 – April 3, 2022, vote transactions account for 80-90% of all of Solana's transactions. Thus, after subtracting out this "consensus overhead" from Solana's reported ~1,500 tps metric, one arrives at a true tps of ~300 non-voting transactions per second (though this is a constantly moving target).

Solana Vote vs. Non-Vote Transactions, Jan 1, 2022 - Present
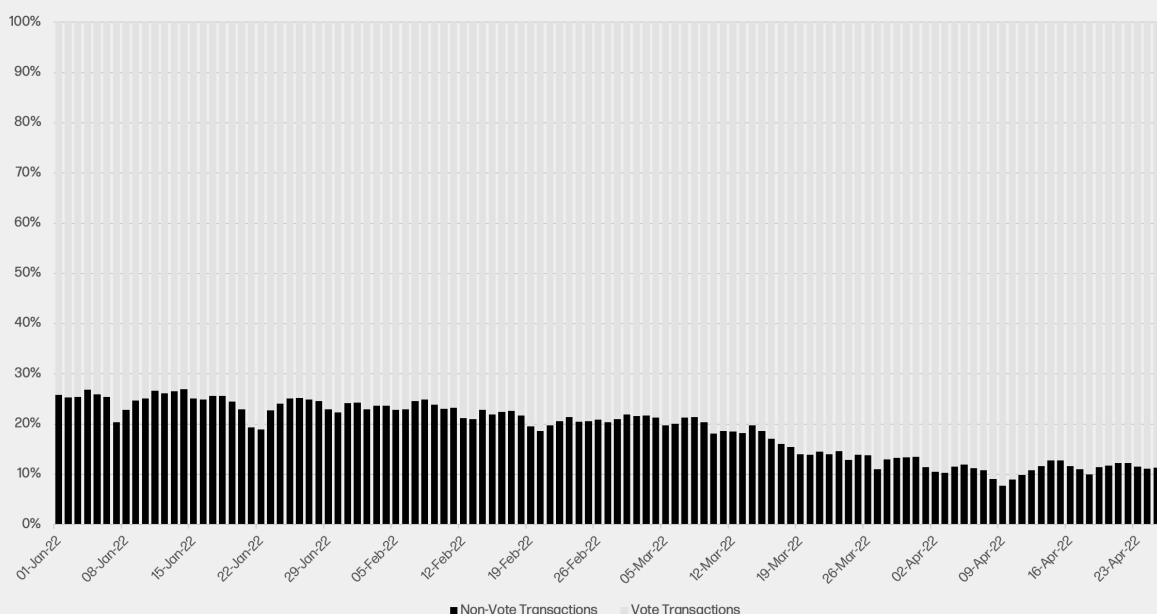

Data: Dune Analytics

According to research from Dragonfly Capital, Solana's true scalability performance edge over competing layer 1s is on the order of 10-25x better, but not 100x or 1,000x as is frequently reported if Solana's reported metrics are taken at face-value. Dragonfly's methodology normalizes blockchain performance by spamming each network with fully packed blocks doing AMM trades on testnets. While not a perfect measure, it is certainly more of an apples-to-apples comparison than what the various Layer 1 blockchains claim. Though Solana's real-world performance based on these benchmarks (~272 Orca swaps per second) pales in comparison to its theoretical 710,000 tps cited in its whitepaper, it is still an incredibly impressive number compared to what is capable on other protocols such as Ethereum's 12-15 TPS limit. It also underscores Solana' tech is seemingly best-in-class from a scalability perspective (for now). With that being said, it is likely that high "real world throughput" numbers can be achieved by other non-EVM blockchains such as NEAR.

Tying together all the concepts described thus far, here is an overview of the lifecycle of a theoretical Solana transaction:

1. (Pre-transaction): During development, the Solana smart-contract developer explicitly declares a list of all accounts that a transaction interacts with — this is essential for Solana's parallelization of state changes enabled by Sealevel

2. Dapp sends a transaction to the user's wallet (such as Phantom) to be signed

3. User signs a transaction with their private key, pays fee of 0.000005 SOL (this number is currently fixed and deterministic)

4. Dapp sends user's signed transaction to a Solana RPC server using the sendTransaction HTTP API call

5. RPC server reads the validator schedule (which changes every ~2 days) and forwards the transaction to the current and next validator leader as a UPC packet

6. The leader validator receives the transaction via its Transaction Processing Unit (Pipelining)

A detailed overview of this process can be found in the following article.

Automated Market Maker (AMM) Transaction per Second, by Chain
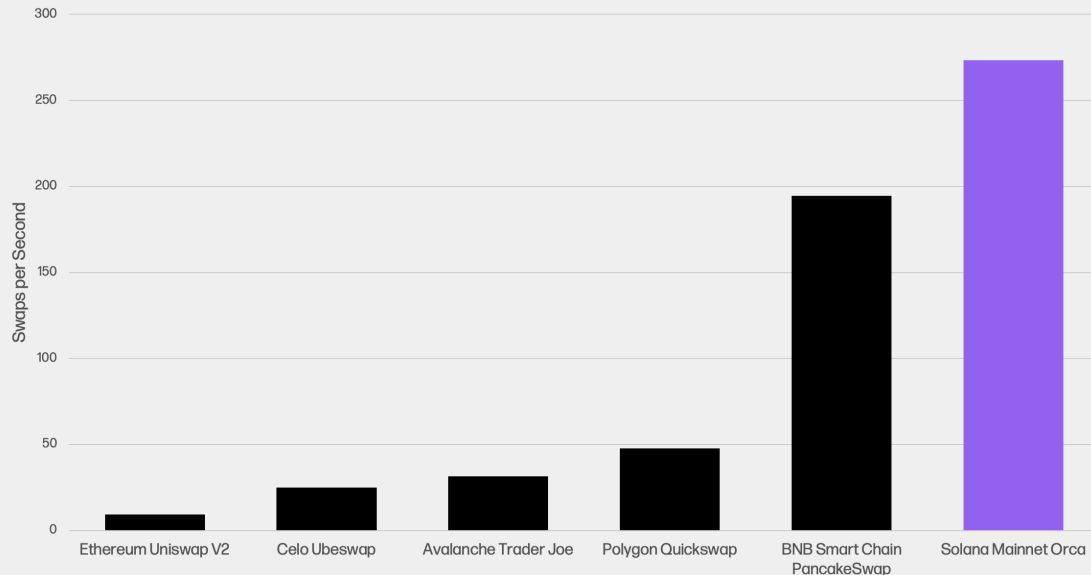
Data: Dragonfly Research *The AMM Test: A No BS Look at L1 Performance*

Solana's Transaction Processing Unit
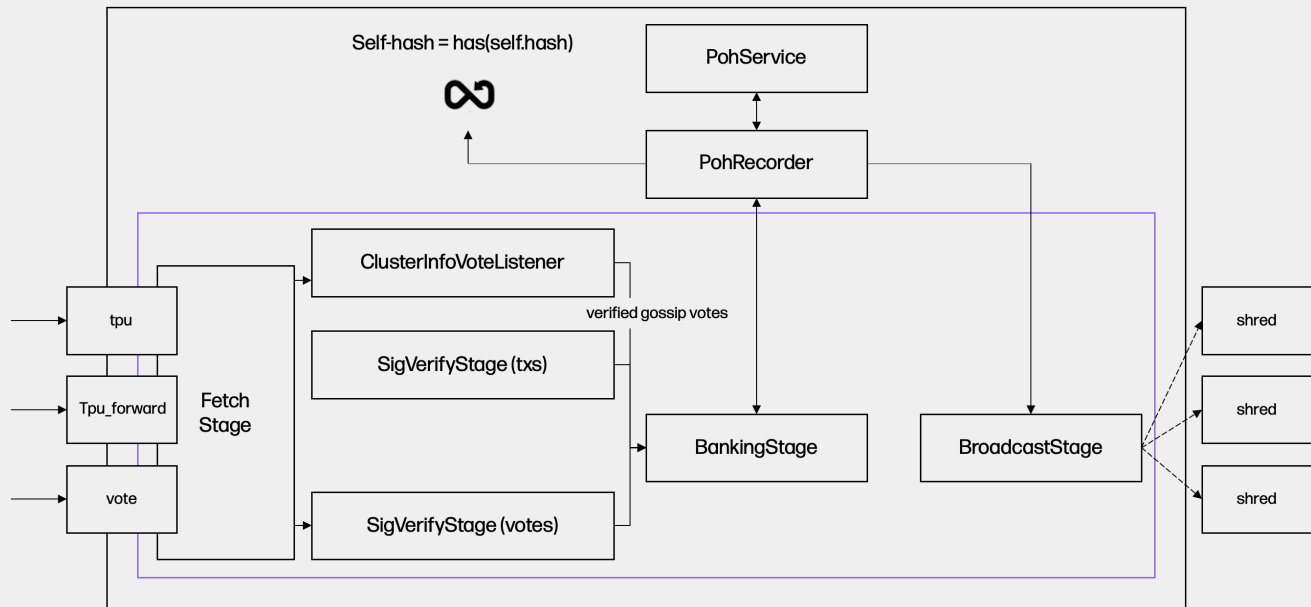
Source: Galaxy Digital Research

Tokenomics

The SOL token is Solana's native cryptocurrency and operates similarly to those of other smart contracting platforms such as Avalanche and Ethereum. SOL has three primary use-case. 1.) Pay transaction fees in exchange for using compute resources on the Solana network 2.) Securing the Solana network by either staking SOL tokens directly with one's own validator or delegating one's stake to another validator. 3.) Voting in governance decisions related to the Solana network.

In addition to Solana's native SOL token, the Solana blockchain also supports the Solana Program Library for developers to create their own Solana-compatible fungible tokens. Put simply, the Solana SPL token standard is to Solana as the ERC-20 token standard is to Ethereum.

According to CoinGecko, the collective market cap of SOL + SPL tokens is estimated to be ~$25.1bn. This figure pales in comparison to Ethereum's ETH + ERC-20 market cap figure of ~$510bn (SOL's ecosystem is ~5% of ETH's ecosystem size). What these figures indicate is that the Solana ecosystem still has a tremendous amount of room to grow before it can start to seriously challenge the likes of Ethereum. Some of the more well-known "pure" SPL tokens (versus cross-chain tokens) include STEPN (GMT), Serum (SRM), Marinade staked SOL (mSOL), and Audius (AUDIO).

Solana Initial Supply Breakdown
(500mn SOL Tokens)
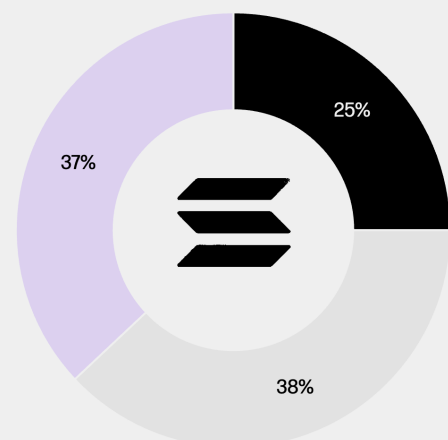
- Founders and Project   Rewards and Airdrops   Investors

Data: Messari

Token Sales

The Solana team launched five funding rounds with four of them being private sales. These private sales began in Q1 2019 and concluded in July 2019, when MultiCoin Capital led a $20 million Series A investment for Solana Labs. Other firms that participated in the fundraise include Distributed Global, BlockTower Capital, Foundation Capital, Blockchange VC, Slow Ventures, NEO Global Capital, Passport Capital, and Rockaway Ventures. In exchange for their investments, the companies received SOL tokens (the exact amounts have not been disclosed). Solana announced this capital raise in a Medium post in mid-2019.

By 2020, Solana completed its fourth private sale (known as a Strategic Sale) and held a public auction organized by CoinList, which added another approximately $4 million to its coffers. On April 8th, 2020, Solana Labs also transferred all IP related to the protocol and 167m SOL tokens to the newly-formed Solana foundation. The remaining tokens from the initial SOL supply were distributed as follows: The Solana Labs team members, the Solana Foundation (to help fund development and balance validator voting power), and a "community reserve" (also managed by the Solana Foundation) to support community activities and application developers.

Following the network's debut, the Solana Foundation's allocation began vesting every month. At launch, the foundation also unlocked 11 million SOL to lend to a market maker for six months. This caused some backlash within the community who were upset that these tokens were not included in circulating supply calculations, dramatically altering the token distribution at a whim. While working with market makers is a common practice in the crypto community, Solana holders were upset that this activity was seemingly done in secret. These lingering concerns ultimately led the Solana team to burn an equal amount of tokens from the foundation's allocation.

Round	Amount USD	Amount SOL	Price per SOL	Dates	Description
Seed Sale	$3.17mn	79.29mn SOL	$ 0.040	April 4, 2018	Seed stage sale in early 2018
Founding Sale	$12.63mn	63.15mn SOL	$ 0.200	June 2, 2018	Part of Series A, led by Multicoin
Validator Sale	$5.70mn	25.33mn SOL	$ 0.225	July 8, 2019	Part of Series A, led by Multicoin
Strategic Sale	$2.29mn	9.18mn SOL	$ 0.250	February 17, 2020	Pre-Mainnet Beta launch sale
Public Auction	$1.76mn	8.00mn SOL	$ 0.220	March 23, 2020	Public Dutch auction, non-US buyers, $110mn valuation

Token Supply

Solana's token supply has an inflationary schedule, and its inflation rate is currently 7.2%. This inflation rate will decrease by 15% each year (dubbed a "dis-inflation rate"). Solana's inflation rate will decrease by 15% until it plateaus at 1.5%. In other words, Solana's inflation rate has a 15% straight-line depreciation schedule starting at 7.2% and ending at 1.5%. Newly-minted tokens will be distributed to validators and stake delegators in proportion to their amounts staked to the network. In the long-term, Solana plans to keep inflation at 1.5% in perpetuity.

As seen in the supply curve, the pre-launch private token sales only came with a nine-month lockup. These tokens unlocked on January 7, 2021. Additionally, the founders' allocation is set to fully vest by January, 2023. Both of these massive tranches have already unlocked a large amount of token supply. The entire grant pool allocation also fully unlocked in January, 2021. These tokens will be used for ecosystem funds, such as the $100mn fund announced in January, 2022, and to grow the validator ecosystem with incentive programs.

Solana Token Initial Distribution	
Allocation %	Beneficiary
15.86%	Seed Rounder Investors
2.63%	Founding Sale Investors
5.07%	Validator Sale Investors
1.84%	Strategic Sale Investors
1.60%	Public Auction Sale Investors
12.50%	Team Members
12.50%	Solana Foundation
38.00%	Community Reserve Fund

Source: Messari

Solana Token Initial Distribution

Legend: ■ Staking Rewards ■ Founders ■ Grant Pool ■ Community Reserve ■ Solana Foundation ■ Seed Sale ■ Founding Sale ■ Validator Sale ■ Launch Sale ■ Public Auction
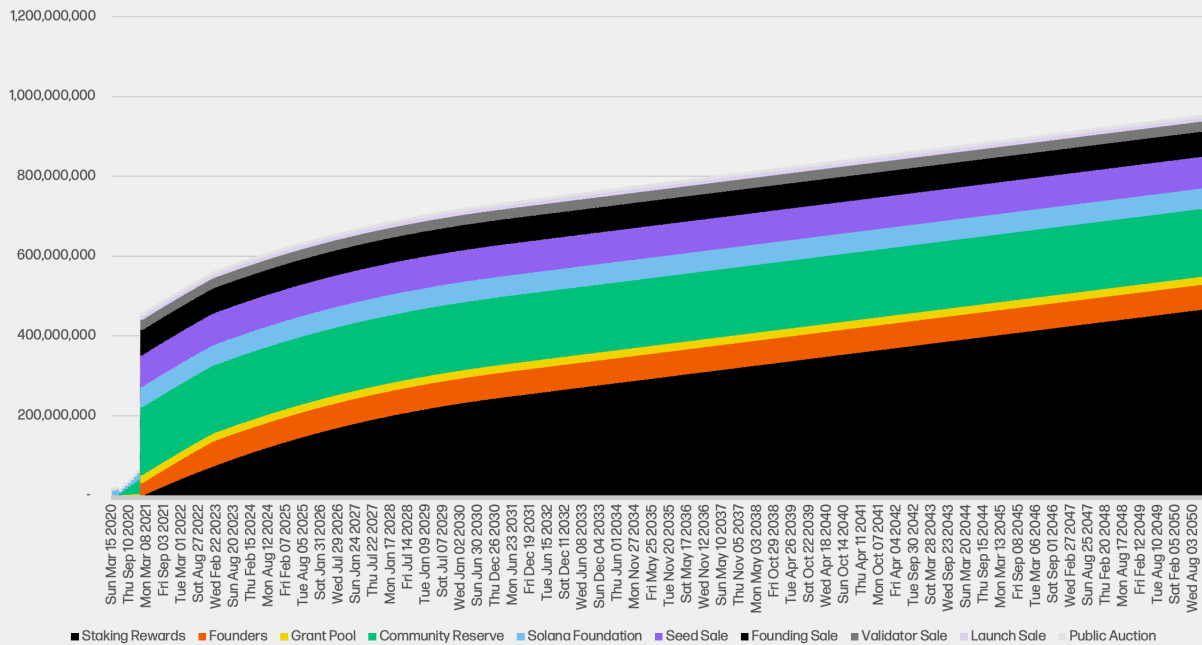
Data: Messari

Validators

Solana's proof-of-stake network is secured by a set of 1,763 validators (as of May, 6 2022 according to solanabeach.io). The stake distribution of these validators is relatively concentrated, with only 22 validators holding ~33% of all Solana staked in the network. In other words, these 22 validators could theoretically halt the network on their own due to the sheer amount of influence they exert over the network with their stakes. This issue of centralized stake is not unique to Solana (the Avalanche network exhibits similarly concentrated levels of stake across its validator set).

There are a couple factors driving this level of centralization. First and foremost, custodians and centralized exchanges have large balances of Solana tokens, through their day-to-day operations, that they can earn additional yield on by running their own validators. Compared to running miners on proof-of-work blockchains like Bitcoin, running proof-of-stake validators is orders-of-magnitude simpler. Instead of buying dozens of Bitcoin mining ASICs that require datacenter-grade cooling coupled with copious amounts of electricity, a Solana proof-of-stake validator can be run on a single (albeit powerful) computer. Centralized exchanges need only point their massive Solana balances to their own validator, and they can instantly start voting on and proposing blocks to the Solana network. Validators on proof-of-stake networks achieve economies of scale by simply controlling (either directly or through delegation) large amounts of that network's native token. If a centralized exchange has a large amount of Solana on its balance

sheet, that exchange can run a very profitable validator operation almost immediately with minimal effort/overhead. The same could not be said if that exchange wanted to start mining Bitcoin, since the operational challenges of running proof-of-work Bitcoin miners at scale is beyond the core competencies of a centralized exchange's business operations.

Additionally, from the retail user's perspective, it is trivially easy for a user to delegate their stake of Solana tokens to a popular validator. Some centralized exchanges even make delegating stake a feature of their product offering, and they offer users additional yield on their static token balances in exchange for taking a cut of staking rewards. Furthermore, users may be more apt to delegate their tokens to a staking provider they might recognize from a branding perspective. In this sense, the "rich get richer" as dominant validators will to attract newly-delegated capital and further increase their influence over the network. This is a particular centralization vector for proof of stake systems like Solana which we wrote about the "Bootstrapping a New Network" section of *Ready Layer One*. With that said, there are two potential solutions that may help mitigate the currently high level of centralization of Solana's proof-of-stake network.

On the demand side, the first potential mitigant to centralization issues for proof-of-stake networks may be found in the growing trend of "liquid staking." Liquid staking providers, such as Marinade, are protocols that delegate stake on their users' behalf like any staking provider. In exchange for a user choosing to delegate their

stake through a provider like Marinade, the liquid staking provider will issue liquid staking tokens (such as mSol). These tokens are issued 1:1 to the amount of Solana staked and give the user the freedom to use other DeFi products in the Solana ecosystem while simultaneously obtaining a staking yield on their principle amount of Solana staked. Since the liquid staking provider has a vetted onboarding process with new partner validators, they would be able to delegate their users' tokens in such a manner that decentralization is optimized (i.e. they would spread their stake out to smaller validators). In fact, the quickest way new Solana validators receive delegations to hit profitability is precisely by partnering with liquid staking providers to receive delegations from liquid staking users. However, there is no guarantee that liquid staking providers ultimately provide or encourage more validator decentralization. Seeking decentralization in underlying validator selection is not a given for liquid staking protocols, but it could be a powerful strategy.

On the supply side, the solution to increasing the decentralization of the Solana network is by simply incentivizing more validators to secure Solana's network. Validators have been slow to onboard onto Solana because its network is currently one of the most difficult and expensive networks to run a validator on top of. The economic viability of running a validator is not particularly enticing, primarily because the price of Solana has increased much faster than the protocol has been able to modify the core requirements to be a validator. Namely, the high voting costs for validators, the high hardware costs, and the large amount of delegated stake required (in USD terms) are all major impediments to economic prosperity for Solana validator operations. With that said, staking on Solana is still in some ways more attractive than other networks like Avalanche, which cap the amount of delegated stake an individual validator can receive relative to their self-stake. Solana has no cap on the amount of delegated stake to self-stake ratio, which increases the opportunity for a motivated validator to achieve economies of scale once they get a validator up-and-running and can attract unlimited amounts of delegated SOL to their validator's stake weight. The Solana Labs team is mindful of the challenging economics of running a validator, and they have shown some early interest in modifying parameters, such as the high voting costs. However, the Solana validator network will always require extremely fast computers to operate, and it is unlikely that the cost to run a validator on the Solana network will ever be particularly affordable compared to running a validator on most other Layer 1 blockchains. As a result of the high minimum compute requirements, validators on the Solana network will likely have some degree of centralization. The question for the broader crypto community to ponder here is, how much decentralization is enough?

Solana Superminority Validator Composition

Rank	Validator	Stake	Stake %	Cumulative Stake
1	Everstake	12,805,887	3.23%	3.20%
2	Chorus One	11,635,259	2.94%	6.20%
3	Kraken	9,243,457	2.33%	8.50%
4	Jump Crypto	8,518,031	2.15%	10.70%
5	Coinbase Cloud	8,385,215	2.12%	12.80%
6	Staking Facilities	7,325,942	1.85%	14.60%
7	EVw8...3Dv	6,600,005	1.67%	16.30%
8	3N7s...iD5g	6,011,610	1.52%	17.80%
9	DokiaCapital	6,010,276	1.52%	19.30%
10	Figment	5,196,138	1.31%	20.60%
11	SOL Community	5,112,475	1.29%	21.90%
12	Shinobi Systems stakeview.app	4,990,145	1.26%	23.20%
13	55bm...1ywA	4,722,772	1.19%	24.40%
14	P2P.ORG - P2P Validator	4,659,109	1.18%	25.60%
15	a16z	4,577,767	1.16%	26.70%
16	4khY...eP5A	4,369,520	1.10%	27.80%
17	Block Logic	BL	4,237,619	1.07%	28.90%
18	6BbT...EEPE	4,080,338	1.03%	29.90%
19	VymD	3,939,695	1.00%	30.90%
20	0% Fee to TOP #1	melea.xyz	3,813,958	0.96%	31.90%
21	5KAX...Pruw	3,578,030	0.90%	32.80%
22	Blockdaemon Validator	3,456,678	0.87%	33.70%

Source: Solanabeach.io   Data as of May 1, 2022

Profitability Analysis of Running a Solana Validator Node

Price of SOL	$48.08
Self Stake	100 SOL (bare minimum required)
Delegated Stake	50,000 SOL (recommended amount)
USD Value of Self Stake	$4,808
USD Value of Delegated Stake	$2,404,000
Commission %	10%
APY (via Cogent Crypto API)	5.87%
Epochs per Year	107.10 Epochs
Voting Costs per Epoch	2.1 SOL

Expense	Monthly Costs	Annualized Costs
Server Costs (rental + data center)	~$1000/month	~$12,000/year
Bandwidth Costs	~$50/month	~$600/year
Voting (~2.1 SOL per Epoch)	~$901/month	~$10,814/year
Total Costs	~$1,951/month	~$23,414/year

Validator Revenue Projections		
Self Stake Revenue	$282/year	
Delegated Stake Revenue	$14,111/year	
Network Fee Revenue	$1,927/year	
Total Revenue	$16,320/year	
Total Costs	$23,414/year	
Net Income	$6,493 annual loss	

Source: Cogent Crypto Validator Profit Calculator

Major Players

## Wallets — The Gateway to Web3

Non-custodial cryptocurrency wallets are a pre-requisite for users to interface with the world of crypto. Wallets are the fundamental pillar sitting between end-users and decentralized applications that enable these activities to take place fully on-chain — from minting NFTs to taking collateralized loans in DeFi to paying for goods and services. Wallet's serve as the user's identity in the "accountless internet" model embodied by web3, and many point to wallet user interfaces as a constant bottleneck towards mainstream crypto adoption worldwide. Solana's bull run in 2021 produced multiple Solana-compatible wallets in the marketplace including Solflare, Sollet, and Phantom. However, Phantom emerged from the pack as the current juggernaut in the Solana ecosystem (similar to MetaMask's role in Ethereum).

Phantom wallet was established in March 2021 and went through several stages of private beta before becoming publicly available in July 2021. In just the 9 months since, the userbase of Phantom has climbed to ~2 million monthly active users. The wallet itself operates as both a browser plugin and a mobile application (just like MetaMask). However, Phantom separates itself from the pack with its emphasis on a user-friendly interface and advanced features. These include staking SOL directly to validators and displaying a user's NFTs on separate tabs within the wallet. Hardware wallet support (such as Ledger) for key management and swap functionality (powered by Raydium) is also baked in. Onboarding users directly from fiat currencies is streamlined thanks to a direct integration with FTX where users can buy Solana with cash and deposit their SOL tokens directly into Phantom (Coinbase has a similar offering with their exchange and wallet coupling). According to Phantom's Twitter account, the wallet facilitated $16.1b in SOL staking, $1.37b in swap volume, 2m dapp transactions, and 1m token transfers. This is in addition to a userbase of 2m MAUs of which 1.6m own at least one NFT. This high level of engagement led to a fundraise of $109m for the Phantom team at a valuation of $1.2b. For comparison, MetaMask parent Consensys most recently raised $450m at a $7b valuation driven 30m MAUs for MetaMask.

Phantom's success thus far coupled with its war chest of funding has yielded synergistic benefits for Solana developers who can rely on a battle-tested Solana wallet API to bridge an existing userbase of 2m users into their respective dapps. This is a crucial, yet often overlooked, aspect of Solana's unique ecosystem that explains why dapp usage has been consistently high on Solana vs other Layer 1 blockchain platforms

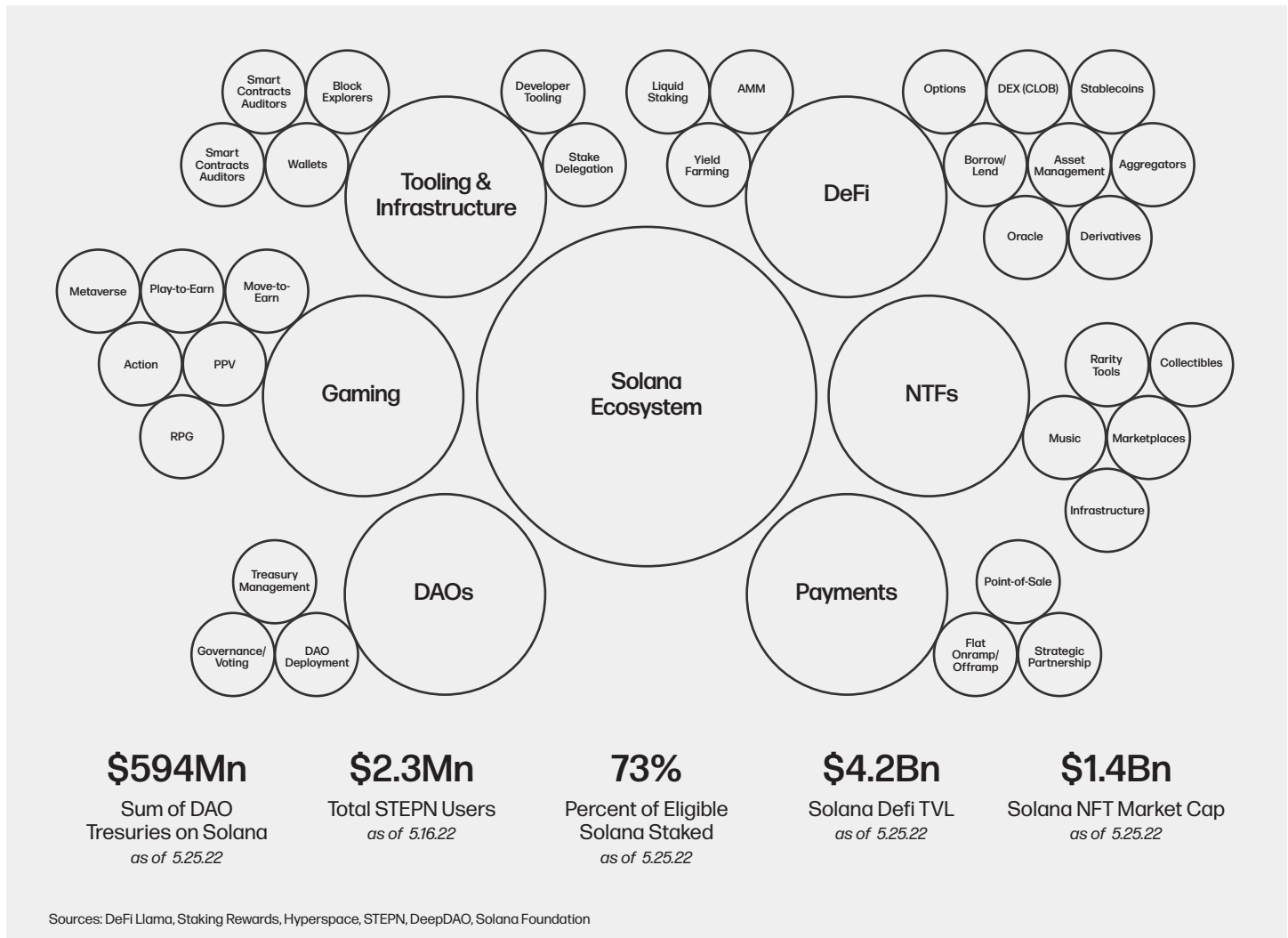## Number of Active Wallets Trailing 30-Days, by Chain
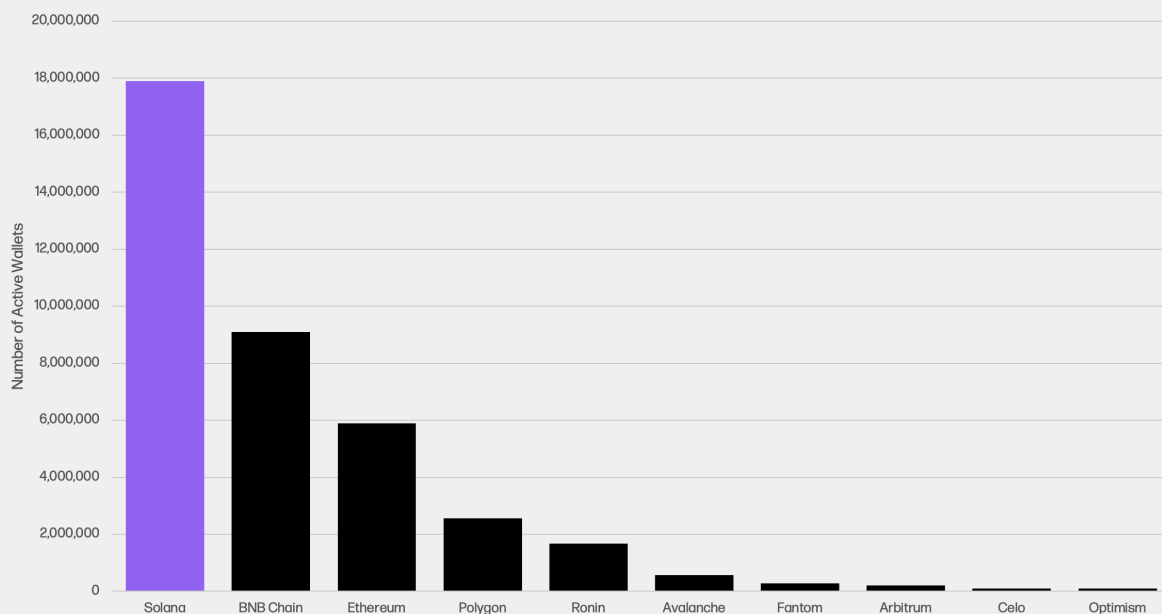
Data: Nansen, as of May 25, 2022

Solana's Ecosystem

Solana's ecosystem can best be broken down into the following buckets: *DeFi, NFTs, Payments, DAOs, Gaming, and Infrastructure.*

Sources: DeFi Llama, Staking Rewards, Hyperspace, STEPN, DeepDAO, Solana Foundation

DeFi

DeFi is currently the biggest vertical within the Solana ecosystem and, perhaps, its most important. Solana's technical infrastructure was built from the ground-up to accommodate a trading use-case that could enable any user of the Solana blockchain to operate at the same level as a high-frequency trader could in traditional finance.

According to DeFi Llama, Solana has about a 3.74% market share of DeFi TVL across all chains. This currently trails Ethereum (63.78%), BSC (8.26%), and Avalanche (3.89%). However, these high-level metrics don't tell the full story of each network's extent of innovation from a DeFi perspective. Except for Ethereum, one could argue that BSC and Avalanche, while more impressive in absolute TVL terms, are less impressive once one digs into the DeFi protocol dominance within each of these chains.

In the case of BSC, 47% of BSC's TVL is driven by PancakeSwap which is known to be the preferred DEX for questionable, low-cap token projects. Additionally, 21% of Avalanche's TVL can be attributed to Aave which was simply ported over to Avalanche by virtue of its EVM compatibility. In other words, Avalanche's top project in TVL terms wasn't even purpose-built for the network (though some might argue this may be a feature rather than a bug given the ease of integrated existing EVM-based projects into AVAX). On the other hand, Solend is Solana's top DeFi protocol with only 13% dominance. Rounding out Solana's top 5 protocols in TVL terms is Tulip (#2), Atrix (#3), Raydium (#4), and Marindate (#5). All these protocols have comparable levels of total value locked, and they represent a wide variety of use-cases within Solana's growing DeFi growing ecosystem. The following section will describe a couple of key primitives enabling developers to build powerful DeFi applications on the Solana network.

Total Value Locked (TVL) – Most Popular Blockchains
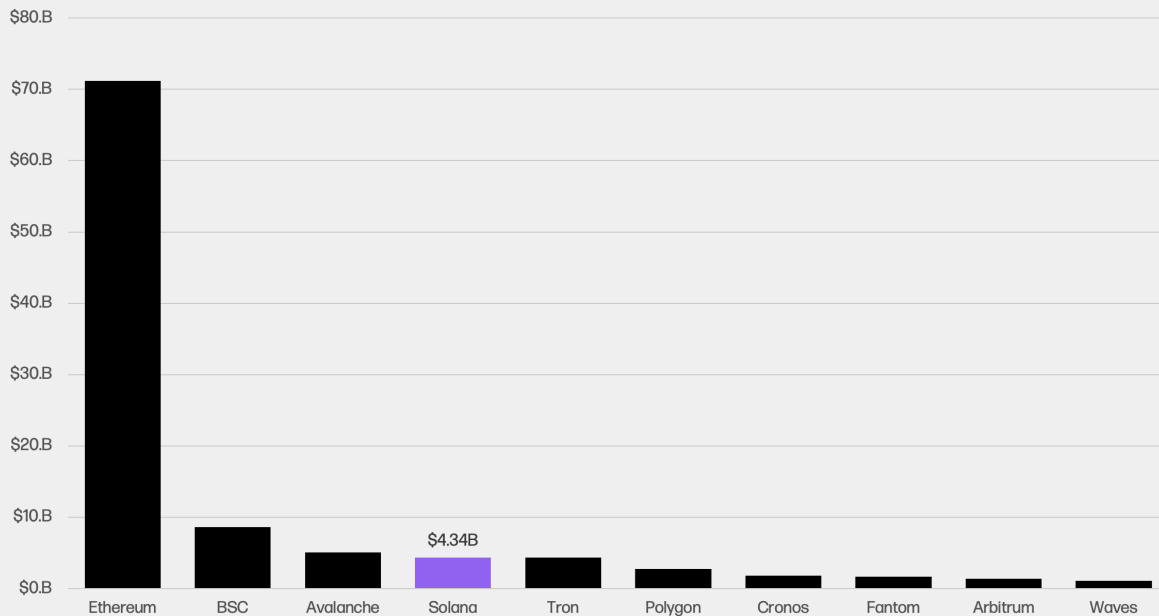
Data: DeFi Llama

Serum

On the 31st of August 2020, Serum was released as an open-source software project built on top of Solana. It is sponsored by the Serum Foundation and backed by a group of cryptocurrency trading and DeFi experts, including FTX, Alameda Research, and the Solana Foundation. Serum aims to be the "infrastructure layer for $10 trillion worth of economic activity" by building a centralized orderbook, matching engine, rapid settlement/trading, and low transaction costs fully on-chain. There are 2 key assumptions driving Serum's design philosophy.

- **Central limit orderbooks** will replace Automated Market Makers (AMMs) as the de-facto standard for trading on DeFi

- **Composability in DeFi** will unlock a step-function improvement due to synergistic specialization of disparate protocols

Until Solana came around, central-limit orderbooks (CLOBs) were seen as a pipe-dream in DeFi. Ethereum's scalability limitations coupled with its high gas costs led to an explosion of automated market makers with rudimentary design patterns, such as the constant product formula powering Uniswap. On Ethereum, it's simply not feasible to have all the transactions necessary to operate a CLOB on-chain due to the sheer demand for blockspace. Passively-traded, double-sided liquidity pools anchored by a constant-product pricing model were the only credible approach to bringing decentralized trading fully on-chain. The Serum team realized the limitations of AMMs during peak DeFi summer in 2020, and they pivoted away from Ethereum over towards Solana as a result.
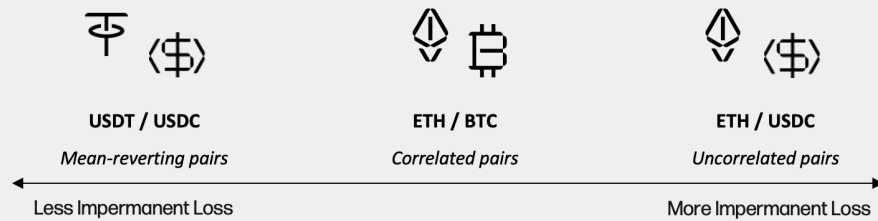
The primary challenge facing AMMs centers on the idea of impermanent loss. Essentially, AMMs only benefit liquidity providers (LPs) when the two assets forming a given liquidity pool have a price relationship that is mean-reverting. Stablecoin pairs, such as USDT/USDC, are examples of ideal pairs for AMMs that will maximize fees for LPs while minimizing impermanent loss in the form of adverse price movements that will be exploited by arbitrageurs. However, users want to trade far more than stablecoin pairs. And there lies the key problem. Many believed that AMMs would never take off because of their limitations, though the AMM has proven to be an incredibly useful platform that commands a lot of trading volume even outside mean-reverting assets. But a lot of the rise of AMMs perhaps occurred due to the lack of any on-chain CLOB. Presumably, the achievement of a decentralized CLOB will eat a lot of volume from AMMs, due to their several major advantages to AMMs These advantages include:

1. Active liquidity management (each order shows a desire to execute a certain amount at a certain price)

2. Market makers (drawn to the active nature of CLOBs)

3. Limit orders (which help curtail impermanent loss)

4. More liquidity (which yields larger trades, lower slippage, and hedging capabilities)

The second key factor driving Serum's design philosophy is that DeFi ought to be open, permissionless, and composable. In other words, one should be able to leverage Serum alongside other DeFi protocols to build something greater than the sum of its parts. Composability implies that any DeFi-based app may simply

Limitations of Automated Market Makers (AMMs)

USDT / USDC	ETH / BTC	ETH / USDC
Mean-reverting pairs	*Correlated pairs*	*Uncorrelated pairs*

Less Impermanent Loss ← → More Impermanent Loss

Source: Galaxy Digital Research

integrate Serum into its existing stack to create its own full-service financial system. What does this composability look like in practice?

Assume one wanted to launch a fast and cheap decentralized exchange on Solana. That individual could learn Rust, create an on-chain matching engine, test it, find market makers to source liquidity, build GUIs, and finally release the app into production. With Serum, that same person could create a DEX GUI, plug Serum into its backend, and have a fully working app running in less than 10 minutes. What's more is that the liquidity on Serum is shared across all the apps built on top of it. There are massive economies of scale achieved with this approach that evoke similarities to the rise of cloud kitchens in the hyper-competitive restaurant and food delivery space.

Many products and protocols have already been built on top of Serum, which was only possible from a technical standpoint due to the monolithic and speed-optimized architecture of the Solana blockchain. The perhaps best exemplified by Raydium, which created a frontend for a DEX built on Serum that was so compelling, it led Serum to deprecate their own DEX frontend in order to focus solely on building their backend DeFi primitive for other protocols to use. Raydium specialized in creating a killer DEX frontend, obtained a substantial comparative advantage over Serum, and forced both parties to keep doing what they each respectively do best. This is the path forward that Serum envisions for the rest of DeFi.

Pyth

Aside from liquidity, pricing data is the most important primitive for developers to build decentralized finance applications. In Ethereum, oracles such as Chainlink, which are 3rd-party services that connect on-chain smart contracts with off-chain data, handle pricing feeds for DeFi. Thus, even though an Ethereum DeFi smart contract call can only access information available within Ethereum's state, the Chainlink oracle would allow the smart contract developer to tap into data that exists outside of Ethereum's state (such as Bitcoin's current USD price). Most decentralized applications rely on oracles as a critical piece of infrastructure and Solana is no exception.

In Solana, Pyth is the predominant oracle data provider. Pyth is overseen by the Pyth Data Association which includes members such as Jump, Jane Street Capial, and Susquehanna International Group. The Pyth network was built to satisfy the needs of these trading juggernauts who rely on incredibly fast and accurate pricing data for their day-to-day trading operations. Pyth was also architected to be used by developers for free, though they can pay for what is effectively an insurance policy against their pricing data being inaccurate. The Pyth protocol can be broken down into 3 key stakeholders:

- **Publishers:** The source of all Pyth data. Includes existing market participants such as exchanges, proprietary trading firms, and market makers. Publishers are incentivized to share their data feeds by earning PYTH in exchange for doing so.

- **Consumers:** Decentralized app developers fall into this bucket. Consumers can leverage pricing data for free or elect to pay a data fee in exchange for reduced risk if a pricing feed fails. Consumers leverage Pyth's API to incorporate off-chain data into their smart contracts.

- **Delegators:** Delegators further secure the network by staking their Pyth tokens with specific data publishers. In exchange, a delegator will earn a portion of the data fees paid out by consumers. However, if a data publisher is inaccurate, the delegator would lose their stake. Delegators effectively serve as insurance if a pricing feed is inaccurate. Consumers directly pay the delegators a premium with their optional fee, and delegators would need to pay consumers with their staked Pyth in the event the data feed is erroneous.

These three key stakeholders in Pyth form a virtuous cycle that transports quality off-chain data into Solana, serving as a critical building block for Solana's burgeoning DeFi ecosystem. Ultimately, Pyth's success will be tied-at-the-hip with Solana's network performance. Since Pyth updates its prices with every Solana block (every ~400ms), it can provide much more frequent and accurate price updates than oracles like Chainlink. This opens a whole suite of programmatic trading use-cases that might not otherwise be economically feasible on ETH-based oracles. On the other hand, when Solana's network goes down, so does Pyth's. In one infamous incident, Solana's 17-hour September 2021 outage caused the Bitcoin price reported by Pyth to drop by 90%. These types of systemic errors, while infrequent, could jeopardize hundreds of millions of dollars tied up in Solana's DeFi ecosystem and derail trust in Pyth as a data provider. So far, Pyth has been able to endure and prosper as an oracle.

## Top Solana Program (Smart Contract) Calls Training 30 Days
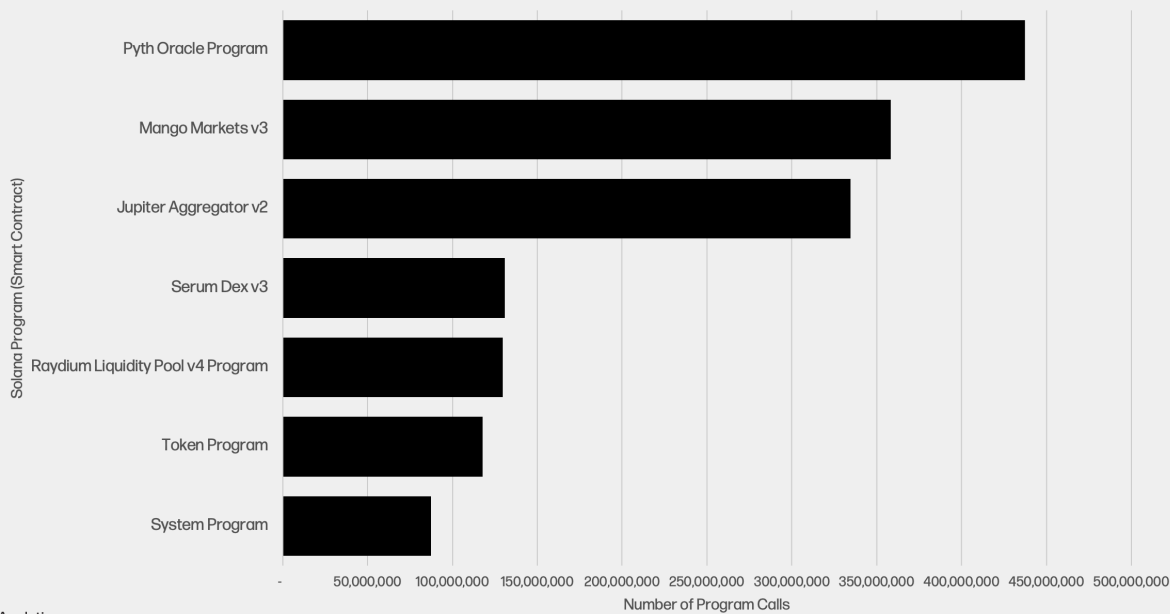
Data: Dune Analytics

NFTs

The Solana NFT space has quietly amassed ~$1.4bn in total market cap according to Hyperspace.xyz. In comparison, the Ethereum NFT landscape is currently worth $10.5Bn according to data from Coinmarketcap. However, there is an incredibly high degree of "Yuga dominance" in the Ethereum NFT landscape. The NFT collections owned by Yuga Labs (Bored Ape Yach Club, Mutant Ape Yacht Club, Bored Ape Kennel Club, Otherside, CryptoPunks, and Meebits) are collectively worth ~70% of the entire Ethereum NFT market cap. In contrast, Solana's top NFT project, STEPN, is currently only worth ~18% of Solana's NFT market cap. This implies that the Solana NFT space is less "power law" distributed than Ethereum's NFT space. If one were to subtract out Yuga Labs' collections, Ethereum's NFT landscape would be worth roughly twice that of Solana. Data from Dune Analytics pegs Solana NFT volumes at ~$45M per month compared to $3-5B for Ethereum-based NFTs (equating to ~1% of ETH volume). While the Solana NFT is growing to a very respectable size in totality, its usage appears to be driven by small-dollar, mainstream users.

Solana's growing importance in the NFT landscape, powered by its ease-of-accessibility compared to Ethereum-based NFTs, is what prompted OpenSea to initially add Solana to its list of supported Layer 1 blockchains in April, 2022. Kraken followed suit when they announced both Ethereum and Solana support for their upcoming NFT marketplace. Already, FTX supports Ethereum and Solana NFTs for its marketplace. Given that a potential Solana integration is the most complicated from a technical standpoint (considering that the chain is not EVM-compatible), this move by all these prominent companies is especially noteworthy. OpenSea, Kraken, and FTX all felt that the opportunity cost of their scarce engineering resources, regardless of new potential exploits unique to Solana's rust-based smart contracts, was worth the price of admission to make Solana NFTs available to their massive userbases. This collective sign-off from industry incumbents represents as win for the entire Solana ecosystem, and it lends further credibility to Solana's unique approach towards building a scalable Layer 1 blockchain that is user-friendly.

Top Solana NFT Collections by USD Market Cap

Data: Hyperspace, updated May 25, 2022
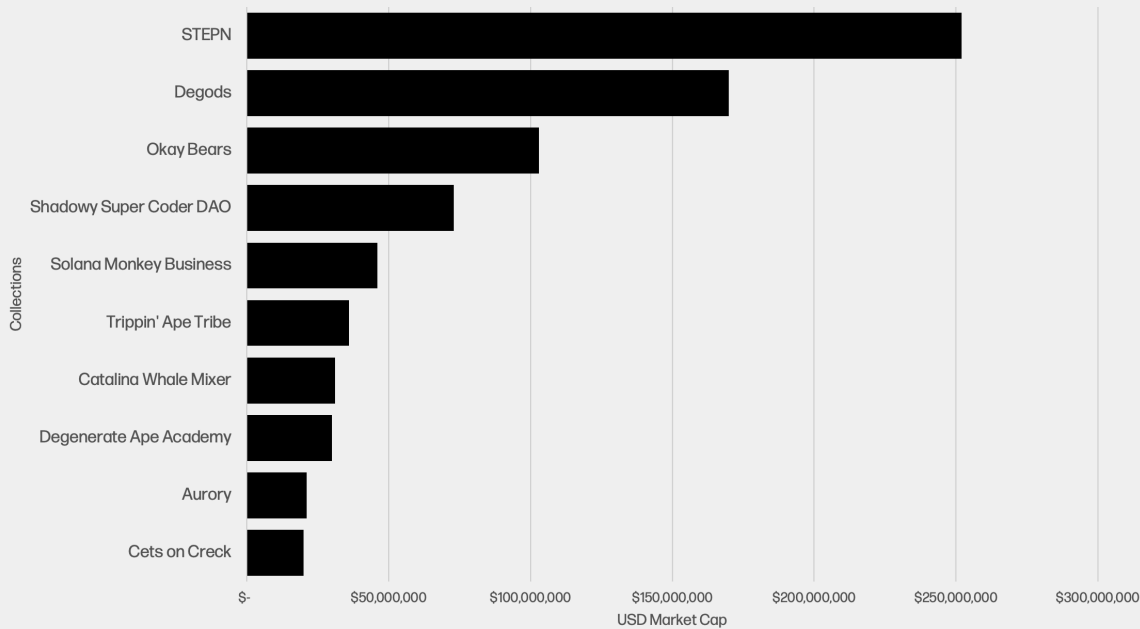
Daily Solana NFT Marketplace Volume USD – Trailing 90 Days

Data: Dune Analytics
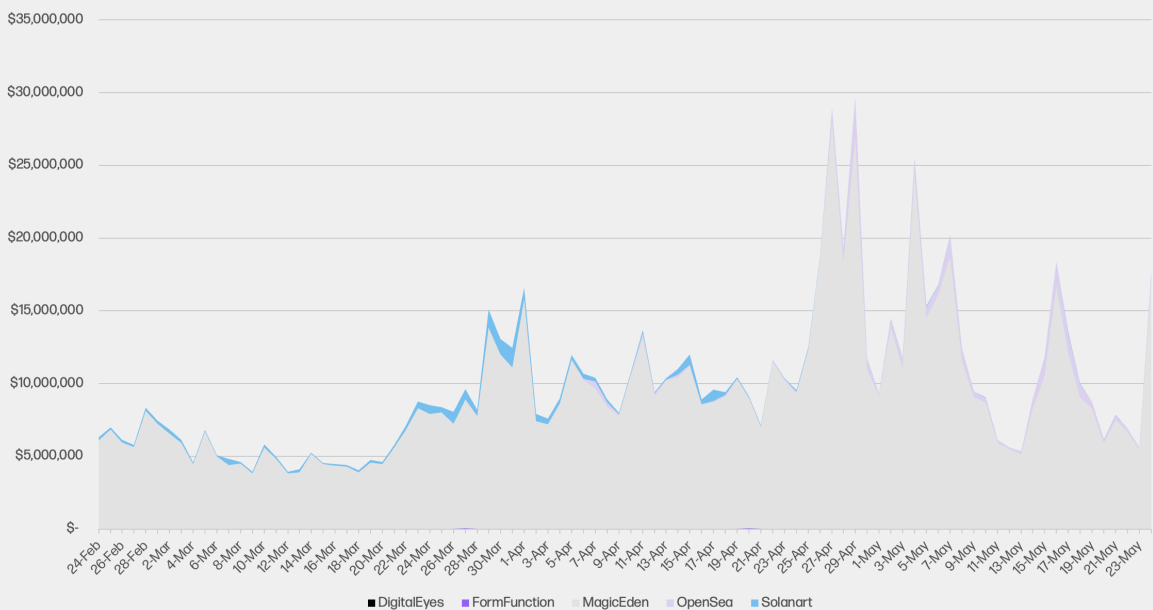
The top 10 Solana NFT collections are summarized in the following chart. What is especially impressive about these collections is that most of them were only launched in the last 6 months. Okay Bears in particular took the NFT world by storm in late April 2022 when it sold out its 1.5SOL mint within hours. Within a few days, its floor price rocketed up to 170SOL. On April 27th, Okay Bears topped all of OpenSea's collections for most volume in a day with $18mn in sales. This milestone represents the first time a Solana-based NFT ever outperformed all Ethereum-based NFT collections for daily volume. As of early May, 2022, Okay Bears still regularly ranks in the top 10 volume on OpenSea. Clearly, Solana NFTs aren't a passing fad. They are being incorporated into multiple first-rate marketplaces and are, in some instances, doing volume numbers that are comparable to top-tier Ethereum NFT collections. From a business standpoint, it makes sense that a company would want to capitalize on the growing prominence of Solana NFTs. No other Layer 1 blockchain has come anywhere near the level of prominence that Solana NFTs have achieved thus far. Flow, a blockchain developed by Dapper Labs that underpins popular NFT platforms such as NBA Topshot, is perhaps the only major "competitor" to Solana.(Yuga Labs is rumored to be considering Flow for a potential post-ETH future in light of its Otherside mint scalability challenges). However, Solana is built from the ground-up to be permissionless and has a more robust set of primitives outside of NFTs, including powerful DeFi protocols and integrations with prominent US-based exchanges. This may prove to be instrumental as Solana continues is path towards onboarding the mainstream, particularly those in the US, into crypto.

Celebrities have also taken note of Solana's rise as a cheap and fast alternative Layer 1 blockchain to power NFT applications. Solana's mature wallet infrastructure coupled with its ease-of-use and predictably low transaction fees have made it a popular choice for influencers, especially those outside of crypto, to launch NFT ventures. Listed below are some prominent celebrity-backed NFT projects that have been built on top of Solana:

- **HEIR**: A Solana-based NFT platform founded by Michael Jordan (who is also an investor in Metaplex and Mythical Games) and his son Jeffrey Jordan that connects fans with professional athletes. Its inaugural collection was launched in early March and is inspired by MJ's six championship rings. This collection featured 5,005 NFTs sold at a price of 2.3 SOL ($221 at time of launch) for net primary sale proceeds of ~$1m.

- **2974 Collection**: An NFT collection launched by NBA superstar Steph Curry to commemorate Steph surpassing the all-time NBA 3-point record. There is one unique NFT for each of Steph's 2,974 3-pointers with each sketch created entirely from the number 2, 9, 7, or 4. 100% of the profits from this collection will be donated to the Eat. Learn. Play. Foundation which was created by Steph and his wife to benefit the lives of kids and families in the Oakland/Bay Area.

- **Fractal:** A Solana-based NFT marketplace focused exclusively on gaming NFTs co-founded by Twitch co-founder, Justin Kan (Twitch was sold to Amazon in 2014 for $970m). Fractal partners directly with game studios to support verified NFT drops, and it also allows for players to directly trade NFTs with each other. By using the gaming sector as a wedge, Fractal ultimately aims to be a crucial onboarding layer for the Metaverse.

The Tech Stack of Solana's NFT Ecosystem

Applications:
Fifth Layer
Banksea · UNLOC · Releap · CAMPUS LEGENDS · parcl

Marketplaces:
Fourth Layer
OpenSea · MAGIC EDEN · Solanart · FTX

NFT Collections:
Third Layer
SMB · DeGods · OKAY
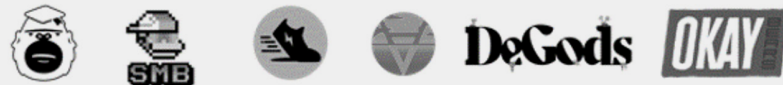
Smart Contact Infrastructure:
Second Layer
METAPLEX

Solana Blockchain:
Base Layer
SOLANA

Source: Galaxy Digital Research

Solana Pay

According to Visa's 2022 Back to Business study, 59% of small businesses plan to use digital payments exclusively in the next two years. Traditionally, small businesses have shied away from crypto payments due to both crypto's price volatility and a crypto's scalability challenges resulting in high transaction fees. In February 2022, Solana announced a partnership with Circle to address both common pain points. Solana Pay, a decentralized payment standard and protocol for merchants to accept USDC (in addition to other SPL tokens), enables digitally native payments with the fast time-to-finality and low transaction costs associated with Solana's blockchain. USDC issued on Solana currently accounts for 10% of USDC's current issuance (as of Feb 2022), and Solana Pay aims to unlock a step-function increase in utility from Solana-based USDC.

From the merchant's perspective, Solana-based USDC can be deposited into the merchant's Circle account. From there, the USDC can be converted to fiat and transferred to the merchant's preferred bank account. From the consumer's perspective, payments will look like other crypto applications where users will either scan QR codes at the physical point of sale (POS) or users will sign a transaction with their non-custodial wallet in a browser. The main challenge from the end-user's perspective is funding an initial balance of USDC into their non-custodial wallet, though this is partially mitigated by partnerships such as FTX's fiat-onramp to direct wallet deposit feature on Phantom. What's more, merchants can attach NFTs to purchases and deposit those directly into the user's wallet. This additional utility, only made possible by making payments in a crypto native manner, enables new channels for merchants to drive customer loyalty and ongoing engagement. In the Web2 world, companies like Chipotle are already doing this with in-app gamification and tiered rewards systems for being regular customers. It's not hard to imagine a world where these siloed-off loyalty programs can interoperate with each other through permissionless blockchains.

Bank of America stated in a research note that Solana could become the "Visa of the digital asset ecosystem." While Solana still has a long way to go, it does stands out from other Layer 1 blockchains as a credible threat to the massive payments industry, estimated to have brought $2Tn in revenue in 2021 according to a report from McKinsey, for a few key reasons:

1. Solana's technical underpinnings as a user-friendly blockchain → fixed and low transaction fees, fast confirmation times

2. Solana's mature wallet infrastructure with built-in fiat onramp capabilities via FTX → wallet has strong mobile and web UI, minimum steps for users to bridge fiat into the Solana ecosystem

3. Solana's strong business development/partnerships presence → Solana Pay → Circle partnership

STEPN — Crypto's First Mainstream Breakout App?

Stepn bills itself as the world's first Web3 "move-to-earn" game. Stepn works by fusing both Game-Fi and Social-Fi elements where users earn an in-game SPL token (either GMT or GST) by running or walking outdoors while "wearing" one of the game's NFT sneakers. Stepn's game mechanics require the user to activate the sneaker before their walk/run and for the user to share their GPS data throughout their workout. Stepn also caps the amount of tokens a user can earn per-day. All of these mechanics work in tandem to limit the number of cheating users who may try to farm GMT/GST tokens from the game. Stepn earns money by taking a small fee on in-game asset sales, asset swaps, sneaker mints, and sneaker rentals. These fees clearly can add up as STEPN is apparently generating $3mn - $5mn in net profit a day and earning up to $100mn a month from. In a testament to the power of Web3, all of the in-game assets, including the two fungible SPL tokens and the NFT sneakers, are owned by the users. One caveat here is that STEPN leverages a hybrid-custodial model where actively used sneakers and newly minted sneakers are held in a custodial wallet until the user is ready to transfer their assets to a non-custodial wallet. However, STEPN allows the user to manage both their custodial and non-custodial wallets within the same interface. Through their non-custodial wallet, users are free to trade their tokens on any Solana DEX and can list their NFT sneakers for sale on any Solana NFT marketplace like Magic Eden. The sheer amount of liquidity unlocked by virtue of being a Web3 game is what ultimately makes the time invested into earning assets via Stepn a worthwhile experience for users. In comparison to the walled-garden ethos of Web2, Stepn represents a monumental "step forward" in showcasing to the world what a crypto-enabled gaming future might look like. The best part about these that Stepn produce positive externalities for its users in the form of increased exercise.

The user metrics behind Stepn support the narrative behind how game-changing Web3 technologies can be for gaming applications. Since launch, Stepn has increased its active user count almost every single day, doubling its users roughly every 2 weeks. Due to the composability of the Solana ecosystem, Stepn was able to leverage Orca for handling all in-game swaps of its native tokens (GMT and GST). As the number of users and in-app interactions increased, so did the amount of daily active user on Orca. This is another example of the power of composable primitives in Solana, and how the broader ecosystem can yield positive-sum outcomes for all participants while minimizing the developmental redundancy needed to create feature-rich applications. Stepn may very well be the first Web3 application to bring crypto to the mainstream, and it likely won't be the last. The fact that Stepn was built on Solana was no coincidence. No other Layer 1 blockchain has the combination of robust developer/user tooling coupled with the low transaction fees needed to make frequent, game-based interactions a possibility on-chain.
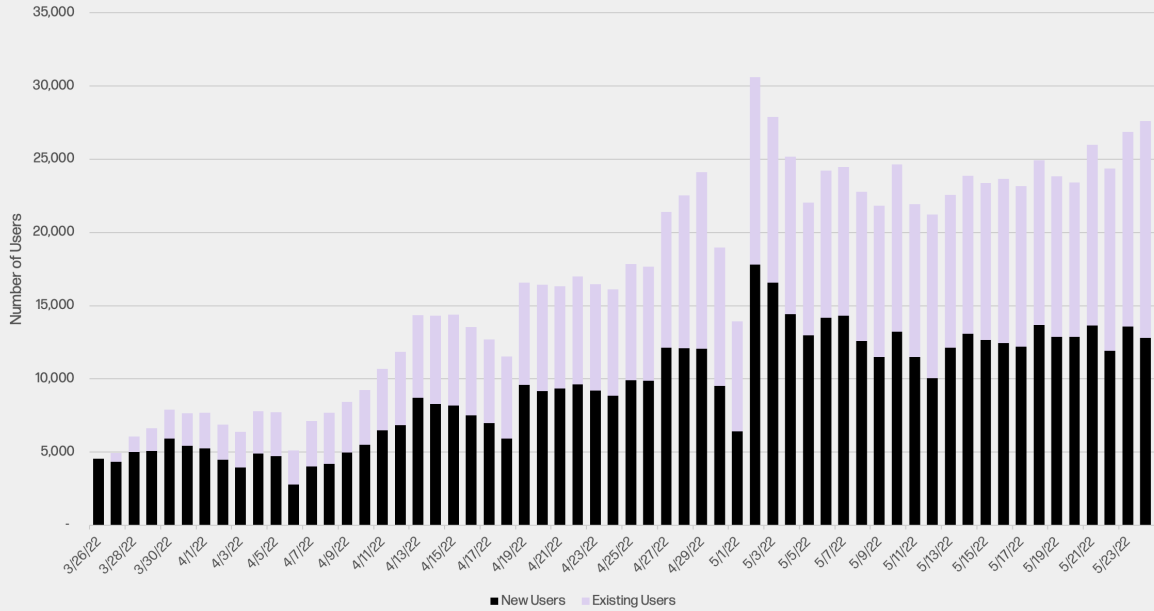
STEPN Drives Parabolic Growth in Orca Daily Active Users
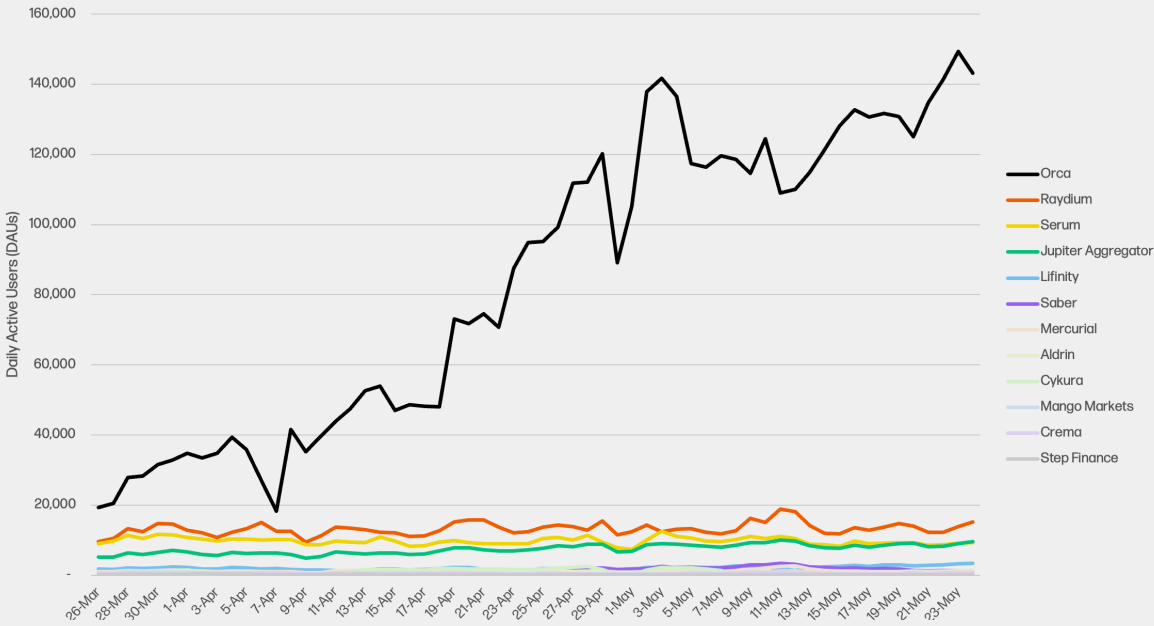
Data: Dune Analytics

STEPN User Growth – Trailing 60 Days


Data: Dune Analytics
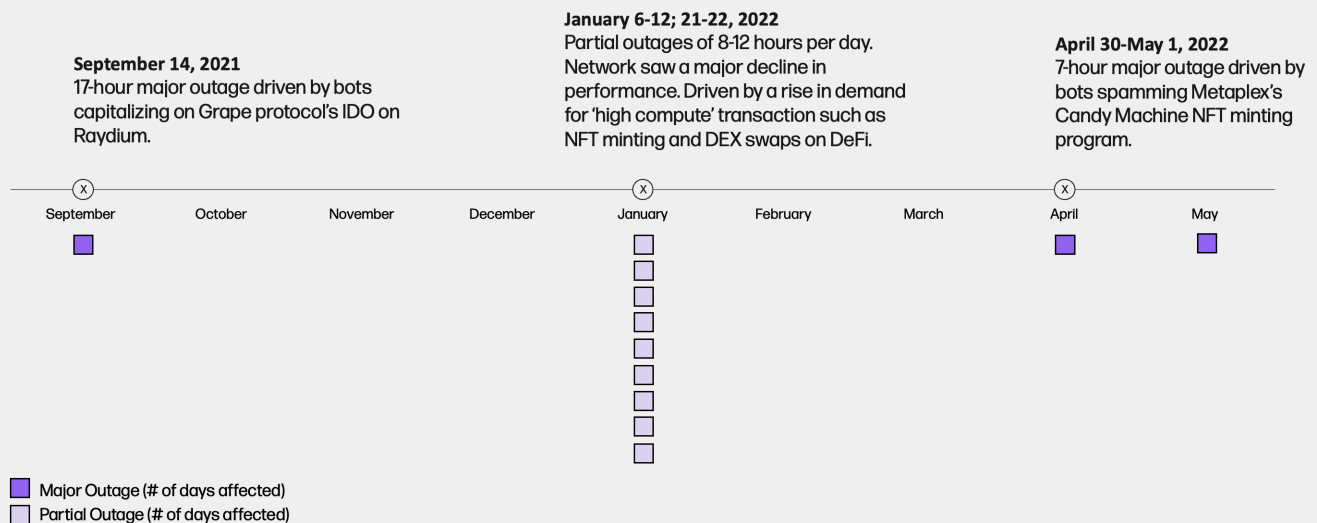
Outages: Solana's Existential Risk

One of Solana's biggest criticisms is its history of outages. Dating back to September 2021, Solana has endured partial or complete outages on 12 separate days. This equates to either a degraded or halted network performance on approximately 4.44% of all days that occurred in the months between September 2021 and May 2022 (inclusive). While the circumstances around each outage differ, the primary factors contributing to these outages boils down to the same core problem: spam. Solana's fixed fee architecture incentivizes spam when there is a strong enough economic incentive for actors to spam the network. Whether this economic incentive is in the form of capturing Grape Protocol's tokens during its Raydium IDO or, most recently, minting an NFT through Metaplex's Candy Machine program, spammers have, at times, completely overwhelmed the Solana network.

These spam-driven outages on Solana underscore a bigger problem that has plagued the internet itself since its incentive. This issue of combating spam transactions can perhaps best be examined through the "transaction quality" framework first espoused by Polynya. Similar to the blockchain scalability trilemma, the transaction quality trilemma framework posits that a blockchain's transactions must choose between two of the following properties: spam mitigation, censorship resistance, and low fees. In the Web2 world, a world devoid of of blockchains, censorship resistance is usually sacrificed to combat spam and fees. In the world of blockchains, Bitcoin and Ethereum both implement fee markets and mempools to keep spam at bay while

Transaction Quality Trilemma

Spam

Censorship Resistance — Low Fees

Source: Galaxy Digital Research

Source: Galaxy Digital Research
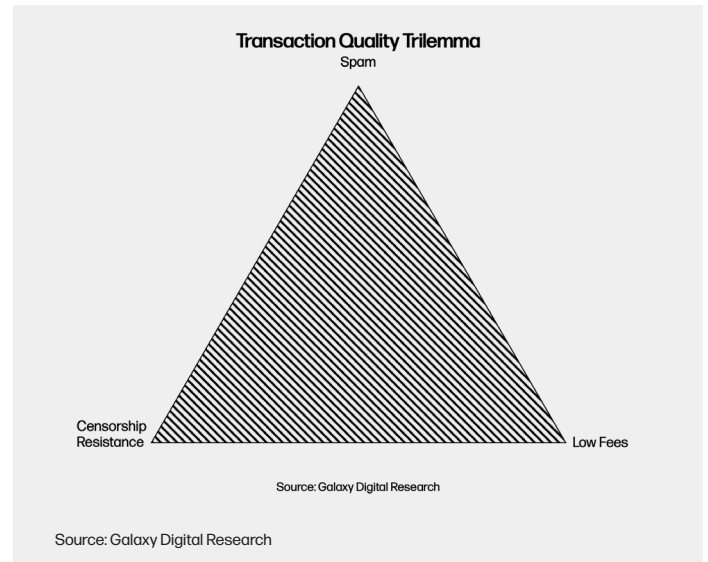
preserving their decentralized networks (censorship resistance). Solana, on the other hand, has prioritized a good UX, anchored by low fees and a relatively decentralized network. As a result, the transaction quality trilemma correctly indicates that Solana is paying for its low fees and decentralization with a propensity for spam. Due to Solana's unique technical architectural choices, the level of spam seen on Solana's network is similarly unique and not seen in any other popular Layer 1 blockchain.

Timeline of Solana Outages
September 2021 – May 2022, Mainnet Beta Cluster

September 14, 2021
17-hour major outage driven by bots capitalizing on Grape protocol's IDO on Raydium.

January 6-12; 21-22, 2022
Partial outages of 8-12 hours per day. Network saw a major decline in performance. Driven by a rise in demand for 'high compute' transaction such as NFT minting and DEX swaps on DeFi.

April 30-May 1, 2022
7-hour major outage driven by bots spamming Metaplex's Candy Machine NFT minting program.

September October November December January February March April May

☐ Major Outage (# of days affected)
☐ Partial Outage (# of days affected)

Source: Galaxy Digital Research

On the one hand, some interpret Solana's spam problem as a "good problem" since it indicates that:

1.) Solana is capable of handling a large volume of transactions (before shutting down)

2.) There is enough economic value on the Solana network for actors to be incentivized to capture this value in the first place (prevalence of bots)

3.) Developers on the Solana ecosystem are not deterred by this recurring problem (Solana dapp and developer activity continues to grow despite the outages)

On the other hand, critics of Solana indicate that this issue of spam will keep happening until Solana implements fundamental changes to its protocol that are already being utilized by virtually every other major Layer 1 blockchain: concretely,, mempools and fee markets. These two tools exist precisely to prevent spam transactions from clogging up precious block space. By holding off on implementing mempools and fee markets in spite of enduring multiple outages, the Solana team has positioned themselves in a very unique design space for potentially addressing these problems. In light of the most recent outage driven by Metaplex's Candy Machine, the Solana team announced three significant changes to combat spam on the network:

- **QUIC:** Short for [Quick UDP Internet Connections](#). QUIC was originally developed by Google to make the web faster and more efficient. QUIC will replace UDP for packet delivery on the Solana network (packets are sent from the RPC Node directly to the block leader). Solana originally chose UDP because UDP connections do not require handshakes or receipt acknowledgments. However, as seen in the spam-driven outages, UDP's inability to distribute origin and control network traffic means that all spam will make it through to the block leader. By switching to QUIC, Solana can retain most of the speed-oriented properties offered by UDP while increasing its ability to throttle incoming spam traffic. QUIC will help ensure that block producers are not hammered by millions of transactions through Gulfstream and that they can verify all their transactions within Solana's 400ms block time.

- **Stake-weighted transaction Qos:** Stake-weighted QoS works in parallel with QUIC. It essentially ensures that network traffic cannot be washed out by any node with at least X amount of stake. This change seeks to solve for prioritizing network traffic when bandwidth is constrained. Stake-weighted transaction QoS operates similarly to proof-of-stake in this regard where transaction "quality" will partially be weighted by a given stake's weight relative to the rest of the network.

- **Fee and Prioritization Changes:** Users will soon be able to attach arbitrary "additional fees" to transactions to boost their transaction's execution priority weight. Previously, there was no methodology for users to express urgency for their transactions. All fees were fixed and all transactions were processed first-in-first-out. Some in the Solana community are referring to this forthcoming change as "neighborhood fee markets". In other words, certain Solana programs, such as a DeFi protocol, might see spikes in fees for its users during times of network congestion. However, this fee spike would be local to the DeFI program, and it would not impact other smart contract programs on the network.

The unfortunate reality of this situation is, until these protocol-level changes are working in production, Solana applications will be left high-and-dry to, in some cases, create their own fee markets. Metaplex has already added a new 0.01 SOL charge on any wallets that attempt to complete invalid (spam) transactions. Application-based fee markets are a suboptimal and inelegant solution to this problem, and app developers are not particularly well-equipped to design bespoke, on-chain economic incentive structures to mitigate spam while preserving a good user experience. This type of decision is best left to the expertise of Solana's protocol engineers, and it does seem like the team is urgently working on implementing their 3 protocol-level changes into production.

However, the more important question here is how will Solana ensure that a future outage does not trigger a dangerous dominos effect on multiple stakeholders across its ecosystem. Unlike NFT and gaming applications, where an outage may only inconvenience and impact people at the individual level, DeFi applications are very much intertwined with one another and are not meant to ever go down. Time-based DeFi systems are most at risk since liquidations may trigger the moment a lost Orcale comes back to life. In this nightmare scenario, positions may suddenly show up as undercollateralized, triggering hundreds of automated trading calls that could impact a large number of people in a short period of time. As more money pours into the Solana ecosystem, the ramifications of an outage will increase exponentially. Solana has had the good fortune of dealing with these outages while its network is still in a state of relative infancy, and they would be wise to take advantage of these valuable lessons as they build a sustainable protocol. Finally, it's important to note that, while these suggested improvements are technologically elegant and potentially very powerful, they are still untested innovations that could fail to mitigate the issues or give rise to new ones. If the Solana team is ultimately forced to adopt existing, more battle-tested solutions like mempools and network-wide fee markets in the long run, then significant time may have been wasted and technology debt incurred in the interim.

Conclusion

Solana stands out from the incredibly competitive alt-Layer 1 blockchain space by doubling down on a fast, monolithic vision for scalability. This is perhaps best evidenced by the fact that Solana's gaming projects accounted for only 3% of total NFTs and Gaming deals in Q3'21, but that increased to 11% and 22% in Q4'21 and January 2022, respectively (according to The Block). Clearly, investors are paying close attention to the capabilities afforded by Solana in the DeFi and Gaming spaces by virtue of its low transaction fees and high throughput. Nevertheless, the Solana network has had its fair share of road bumps in the form of outages and network degradations. So far, these trials and tribulations have not been deterrents to its adoption by users and developers. Over the past year, Solana has materialized into the most complete alternative to the Ethereum network as evidenced by its full integration with multiple marquee NFT platforms, the rapid rise of consumer dapps like STEPN, and its impressive engagement metrics (such as active wallet addresses). When the Solana network is running, it is anchored by a great UX, strong fiat on-ramps in Coinbase/FTX/Moonpay, powerful DeFi primitives in Pyth/Serum/Raydium/Orca, a fully composable execution environment, and strong growth on both the end-user and developer front. Solana's growth is relatively diversified as it is seeing strong adoption on the NFT, DeFi, and Web3 app front. All of these factors combine to make Solana an incredibly compelling platform for an entrepreneur to build a crypto, web3, DeFi, gaming, and/or NFT company on top of. Today, Solana cannot be considered a theoretical experiment. The only question for this flourishing ecosystem is whether it handle additional increases in concurrent users with its existing technical architecture. The latest outage suggests that some massive protocol-level changes are due for the network to reach the next level. Without improvements in network resilience and greater decentralization of its validator set, though, Solana will continue to face issues that could inhibit its growth and adoption.

Key Takeaways:

- **Solana is the best hedge against the EVM today.** While Solidity is still king when it comes to blockchain development, the EVM itself is seemingly hitting its limits in terms of scalability. Ethereum is still years away from realizing its scalability vision. In the interim, blockchain demand shows no signs of slowing down. In this capacity, Solana is poised to capture some of this block space demand with its unique approach that is completely decoupled from the EVM. Even academics have shown skepticism that the EVM, in its current form, can satisfy the demand of billions of users. Solana is the most well-developed layer 1 blockchain that has met or exceeded the scalability performance of the EVM (including EVM derivatives like Binance Smart Chain).

- **Solana is anchored by a robust set of DeFi primitives.** Serum, Raydium, and Pyth combine to create a formidable combination of building blocks upon which new applications can be built. These primitives were built for an institutional use-case that is in some ways over-engineered for a retail audience. The sheer amount of headroom for retail usage helps guarantee a consistent user experience. Look no further than the massive uptick in Orca usage as Stepn grew in popularity.

- **Solana's key players and partnerships give it a unique edge over other layer one blockchains.** From the fiat onboarding experience, to the protocol itself, to the user-friendly browser wallet, to the suite of applications, Solana has a relatively mature product offering that gives web3 developers confidence to leverage existing tools to create new blockchain-based experiences for their users. FTX's onboarding directly into Phantom coupled with its custodial offerings for new application developers makes for a compelling draw to the Solana ecosystem for developers. Jump's patching of the Wormhole hack for $600m, compared to when Binance had to step in for the Ronin hack, signals strong capital backing to backstop outages and worst case scenarios. Finally, DAO tooling and Phantom are ensuring that user experiences at both the group and individual level are meeting a certain threshold, opening the floodgates for novel applications to build on this entire stack of existing infrastructure.

- **Solana is a contrarian bet on monolithic blockchains**. To-date, most blockchains are monolithic in nature, but few blockchains plan to stay monolithic forever as they seek to increase scaling performance. Avalanche, for instance, is planning on rolling out subnets to split up blockspace demand across siloed applications who rely on a limited sample from the main validator set. Ethereum has seemingly doubled down on a roll up approach with a more modular stack. Solana, however, is choosing to stay the monolithic course and betting that hardware coupled with its unique protocol design will be able to handle the rapidly increasing demand for blockspace. While a monolithic approach is most elegant for sharing state across different apps built on the same chain, it is unclear if this approach is feasible as Solana's userbase hopes to 100x and hit the mainstream. Jevan's paradox may become an insurmountable challenge to the blockchain industry, and monolithic approaches are the least-equipped to handle this trend.

- **Solana's recurring outages are its biggest risk to long-term viability.** Ultimately, the takeaway here is whether or not it is better for a blockchain to have 100% uptime with variable user experiences or 99% uptime with a consistently good user experience. The caveat with this comparison, however, is that Solana has experiences outages during inopportune times, such as when traders need to top-up margin to avoid liquidation. Because blockchains are powered so heavily by the DeFi space with billions of dollars on the line, it is hard to say whether any downtime is truly acceptable. Some would argue this is the case, pointing to web2 where taking servers down for maintenance is a common practice. Regardless, the Solana team is working on a solution to this problem, and only time will tell if their newest tweaks to the protocol will finally put these recurring outages to rest.

- **Solana is leading the way for NFTs and GameFi outside of Ethereum.** Powered by its consistently low transactions fees, Solana has already seen a large degree of success in both the NFT space and GameFi space (StepN is a great example that marries both of these spaces). As liquidity flows into the Solan ecosystem to transact in these economies, Solana's strong DeFi offerings, in the form of deep liquidity pools, may increase its moat around capital allocated to this space compared to other blockchains. Users who earn $DUST with their DeGod NFTs and GMT in STEPN may prefer to sweep these accruals into USDC on Phantom rather than flock to another GameFi or NFT application on another chain. This effect draws comparison to the gaming industry where incumbents like PlayStation and Xbox have high switching costs for users and ultimately rely on exclusive titles to retain their userbases. To the extent that Solana can deliver killer apps in NFTs and GameFi, it can control a larger retail userbase who may not be eager to move to another chain even with shiny new incentives like a higher yield. This is perhaps best embodied by the TVL metric compared to wallet address metric. Retail users don't hold as much capital, but their influence still reflects in wallet activity and will be enough to convince developers to choose Solana over other blockchains when delivering novel product ideas.

Legal Disclosure

■ This document, and the information contained herein, has been provided to you by Galaxy Digital Holdings LP and its affiliates ("Galaxy Digital") solely for informational purposes. This document may not be reproduced or redistributed in whole or in part, in any format, without the express written approval of Galaxy Digital. Neither the information, nor any opinion contained in this document, constitutes an offer to buy or sell, or a solicitation of an offer to buy or sell, any advisory services, securities, futures, options or other financial instruments or to participate in any advisory services or trading strategy. Nothing contained in this document constitutes investment, legal or tax advice. You should make your own investigations and evaluations of the information herein. Any decisions based on information contained in this document are the sole responsibility of the reader. Certain statements in this document reflect Galaxy Digital's views, estimates, opinions or predictions (which may be based on proprietary models and assumptions, including, in particular, Galaxy Digital's views on the current and future market for certain digital assets), and there is no guarantee that these views, estimates, opinions or predictions are currently accurate or that they will be ultimately realized. To the extent these assumptions or models are not correct or circumstances change, the actual performance may vary substantially from, and be less than, the estimates included herein. None of Galaxy Digital nor any of its affiliates, shareholders, partners, members, directors, officers, management, employees or representatives makes any representation or warranty, express or implied, as to the accuracy or completeness of any of the information or any other information (whether communicated in written or oral form) transmitted or made available to you. Each of the aforementioned parties expressly disclaims any and all liability relating to or resulting from the use of this information. Certain information contained herein (including financial information) has been obtained from published and non-published sources. Such information has not been independently verified by Galaxy Digital and, Galaxy Digital, does not assume responsibility for the accuracy of such information. Affiliates of Galaxy Digital own investments in some of the digital assets and protocols discussed in this document. This document provides links to other websites that we think might be of interest to you. Please note that when you click on one of these links, you may be moving to a provider's website that is not associated with Galaxy Digital. These linked sites and their providers are not controlled by us, and we are not responsible for the contents or the proper operation of any linked site. The inclusion of any link does not imply our endorsement or our adoption of the statements therein. We encourage you to read the terms of use and privacy statements of these linked sites as their policies may differ from ours. Except where otherwise indicated, the information in this document is based on matters as they exist as of the date of preparation and not as of any future date, and will not be updated or otherwise revised to reflect information that subsequently becomes available, or circumstances existing or changes occurring after the date hereof. The foregoing does not constitute a "research report" as defined by FINRA Rule 2241 or a "debt research report" as defined by FINRA Rule 2242 and was not prepared by Galaxy Digital Partners LLC.

For all inquiries, please email contact@galaxydigital.io.

galaxy