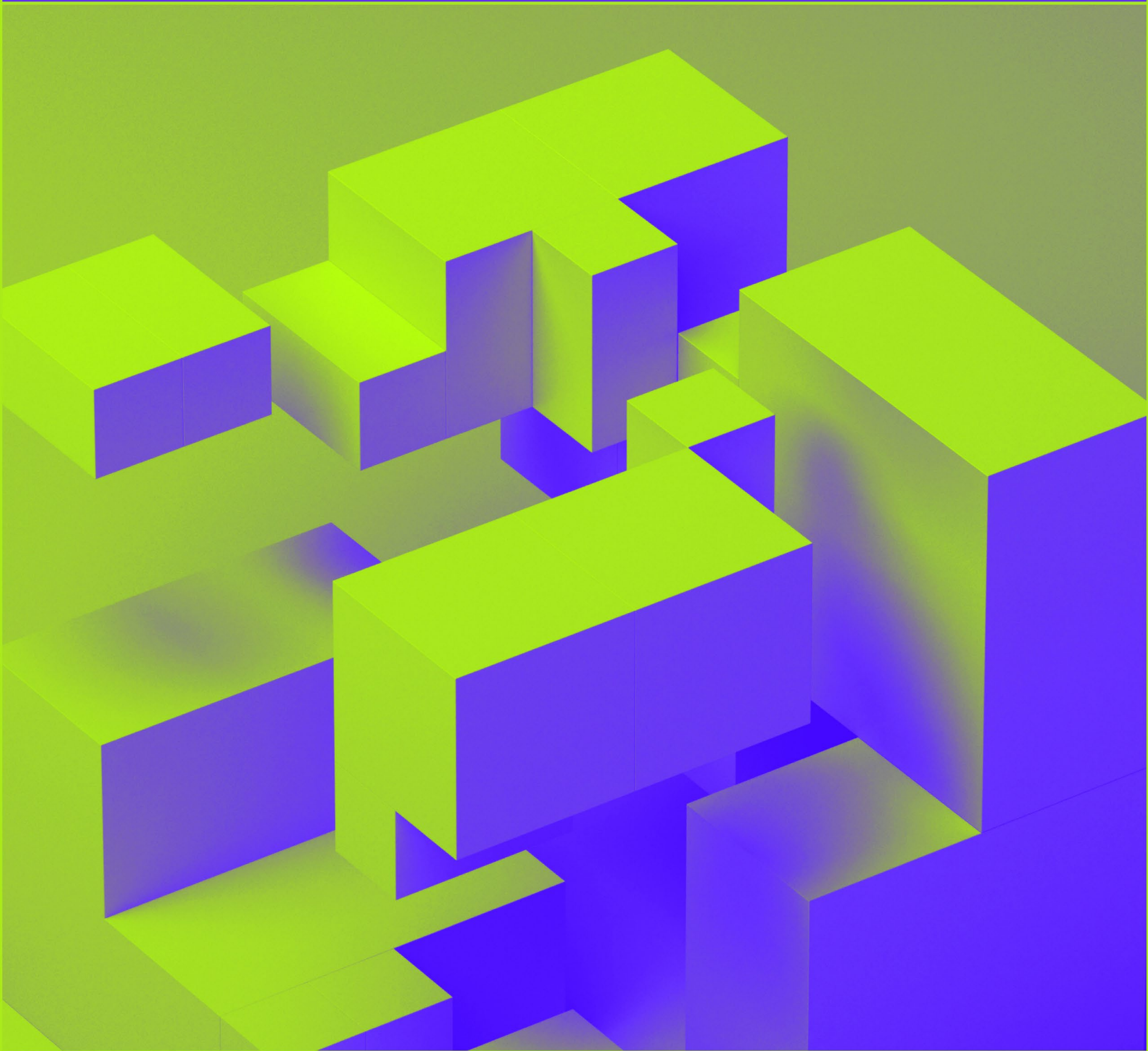
THE BLOCK · Research

Comparing Layer-1 Platforms: 2022 Edition



01/04/23

COMMISSIONED BY SOLANA FOUNDATION | Ava Labs

Comparing Layer-1 Platforms: 2022 Edition

PUBLISH DATE 01/04/23

Introduction

The general public has become familiar with the terms blockchain and Bitcoin. However, understanding what they do and how they do it, remains daunting for most. At the highest level, a public blockchain network is made of computers connected by the internet running the same set of instructions to continuously add new data (blocks) to an open, permanent, and distributed database (blockchain).

After that, many other questions remain that inevitably include, "so what?"

Commerce is Built on Trust

Trust is the fundamental building block of all commerce today. It is in the form of banks, custodians, regulators, and innumerable other identifiable third-parties that mediate every (non-cash) financial transaction that we make. Such third-party entities are not only crucial components of our payments infrastructure, but may also aid in detecting criminal activity via know-your-customer (KYC) and anti-money laundering (AML) regulations.

Notable challenges some may point to however, include KYC/AML (as implemented today) may only have limited real-world effectiveness in preventing crime, while compromising user privacy and increasing operational complexity/cost for payment mediators. These factors may contribute to creating barriers of entry not only for new competitor financial institutions but, likely for the ~25% of the world's "unbanked" and/or undocumented population, as well.

Regardless of where one may fall in the complex and nuanced discussion surrounding crime-prevention, financial-inclusion and privacy, we can state with some certainty that trust-assumptions and dependencies on centralized entities will likely become more prevalent in our daily lives. Especially as we move towards "cashless" societies through the introduction of central bank digital currencies (CBDCs) and other financial-technology solutions from the world of traditional finance.

Blockchains Advance Trust Minimization

Blockchain technologies are thus important and acutely disruptive because of their core function – minimizing the need for trust. In an

Introduction (Continued)

ideal scenario, blockchains allow trust to be decentralized away from single point(s) of power/control and towards mathematics (cryptography) and open-source code underpinning public databases that anyone with internet access can deterministically verify.

The introduction of Bitcoin in 2009 was significant as it was the first blockchain to overcome fundamental constraints in decentralized distributed networks (e.g., the Byzantine Generals' problem and Sybil resistance) and demonstrate that trust-minimized, peer-to-peer (P2P) transactions were indeed technically possible. Not long after, Bitcoin spawned the digital asset class known as "cryptocurrencies" and remains the most valuable blockchain network with a market capitalization of ~$325B USD, as of writing.

Bitcoin's Success has Opened Pandora's Box

There is enormous interest in pushing the technical limits of what blockchain technology is capable of. A prominent example was the introduction of Ethereum in 2015 that popularized "smart contracts," giving rise to the concept of "programmable money." Successful deployment and adoption of Ethereum is another significant milestone for the field as it demonstrated that highly composable and self-executing programs encoded on a blockchain can inherit some of the same properties afforded by decentralization.

The flurry of dedicated research and development (R&D) activity has only grown since then, both in academia and industry. The Block's internal reporting shows that ~6,200 funding rounds have been completed for blockchain-related startups just in the past 5 years. These efforts have resulted in notable advancements in cryptography, development of diverse blockchain consensus mechanisms, novel blockchain architectures, purpose-built hardware and blockchain-related applications – primarily centered around smart-contract enabled blockchains.

The biggest challenge for blockchain technologies currently is to ensure robust functionality (transaction speed, cost, security, etc.) for potentially billions of concurrent users. On the one hand, there is intense activity to discover compelling new applications (centering around commerce and

Introduction
(Continued)

other applications) that require the functionality of a blockchain. Product-builders are asking: what novel blockchain-enabled applications will target the next billion users?

On the other hand, developers and other specialists are advancing blockchain technologies with the assumption that it's only a matter of time before a flood of new users do arrive.

Why are we writing this report?

Dozens of new smart contract blockchains (focus of this report) have been deployed in the past years. Objective side-by-side comparisons between these ecosystems are few and far between. This report is an update on The Block's 2021 report on the same subject, and aims to chronicle the rapidly evolving landscape of smart contract blockchains.

How are we structuring this report?

This report will start off with an overview of smart contract platforms, the applications they enable and introduce the ten blockchain ecosystems that will be the focal point of this report. As the most dominant smart contract platform with the longest history in the industry, we will first dive into the current state of Ethereum and its planned roadmap over the coming years. We will then segway into comparing the network architectures, on-chain and ecosystem data for the selected blockchain ecosystems. Finally, we will end with our conclusions and outlook over the coming months and years.

Commissioned by

The Solana Foundation is a non-profit organization dedicated to the decentralization, growth, and security of the Solana network.
More about The Solana Foundation: solana.org
More about Solana: solana.com | docs.solana.com | GitHub | Discord | Twitter

Ava Labs makes it simple to launch decentralized finance applications on Avalanche, the fastest smart contracts platform in the blockchain industry. We are empowering people to easily and freely digitize all the world's assets on one open, programmable blockchain platform.
Ava Labs was founded by Cornell computer scientists who brought on talent from Wall Street to execute their vision. The company has received funding from Andreessen Horowitz, Initialized Capital, and Polychain Capital, with angel investments from Balaji Srinivasan and Naval Ravikant.
More about Ava Labs: avalabs.org
More about Avalanche: avax.network | docs.avax.network | GitHub | Discord | Twitter

Researched by

THE BLOCK Research

The Block Crypto, Inc. - The Block is an information services company founded in 2018. Its research arm, The Block Research, produces research content covering the digital assets, fintech and financial services industries.

Contact

The Block
Email: support@theblockcrypto.com
Twitter: @TheBlock__

The Block Research
Email: research@theblockcrypto.com
Twitter: @theblockres

Acknowledgements

We would like to thank The Solana Foundation and Ava Labs for commissioning this research report. We would also like to thank everyone at The Block who assisted with this report - research team: Andrew Cahill, Marcel Bluhm, Saurabh Deshpande & Jason Michelson; data team: Edvin Memet, Simon Cousaert & Rebecca Stevens; design team: Zoe Ellyse Del Rosario. We are also grateful to those that shared their valuable perspectives through interviews conducted specifically for this report (chain / organization: individuals):

Avalanche / Ava Labs: Luigi Donorio Demeo & Matthew Schmenk

Cardano / Cardano Foundation: Mel McCann & Renagh Mooney

Cosmos / Osmosis Labs: Sunny Aggarwal

Polkadot / Web3 Foundation: Joe Petrowski

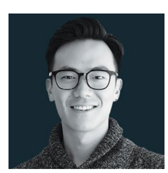
Solana / Solana Foundation: Austin Federa

The authors of this report may hold tokens mentioned in this report. Please refer to The Block's financial disclosures page for author token holdings.

Finally, while this report aims to provide a general overview of the Layer-1 landscape, it does not analyze the technology and data related to all Layer-1 projects. For a comprehensive list of these projects, please refer to the list of Layer-1 protocols in this document. If you believe that your project was miscategorized or would like your project to be considered for next year's report, please contact: research@theblockcrypto.com

Authors

Dipankar Dutta
Research Analyst, Reports
Twitter
LinkedIn



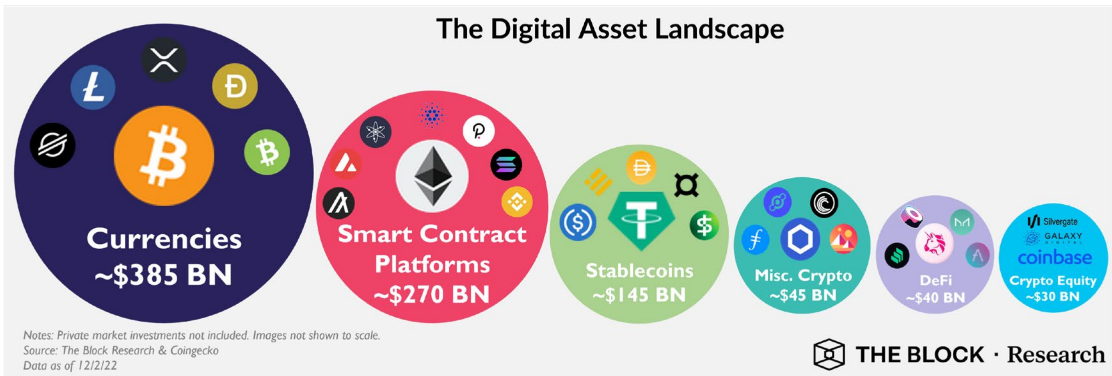
Hiroki Kotabe
Research Analyst, Reports
Twitter
LinkedIn

Comparing Layer-1 Platforms: 2022 Edition

Table of Contents

I The Layer-1 Landscape

The digital asset class has only been around for ~13 years, yet its landscape is already vast. This asset class is now made up of distinct asset types that range from what may be loosely defined as "currencies" (e.g., Bitcoin (BTC), Litecoin (LTC), etc.), to smart contract platforms (e.g., Ethereum (ETH), Solana (SOL), etc.), stablecoins, a host of utility tokens (can be divided into many sub-categories) and others. As of recently, publicly-listed companies that specialize in digital assets (e.g., Coinbase, etc.) have also started trading on the NYSE (COIN).



What are Layer-1 Blockchains?

Layer-1 (L1) refers to any blockchain that is capable of independently generating new blocks of data based on its architecture and rules (e.g., node hardware requirements, data availability, consensus mechanism, etc.) without reliance on another blockchain. Examples of L1s include both crypto "currencies" (e.g., Bitcoin, Litecoin, etc.) and smart-contract platforms (e.g., Ethereum, Solana, Avalanche, etc.).

Bitcoin is generally characterized as the "digital gold" of this asset class. One prominent feature/flaw of Bitcoin's ecosystem (depending on who is asked) is its rigid and slow approach when it comes to any proposed change to the core protocol. As of now, there is no clear pathway towards addressing critical barriers of implementing highly composable transactions on Bitcoin's base layer (L1). These challenges include: 1) limited expressiveness of its scripting language, 2) 10-minute block time that affects settlement time/assurances and, 3) limited block size that may mean high transaction fees.

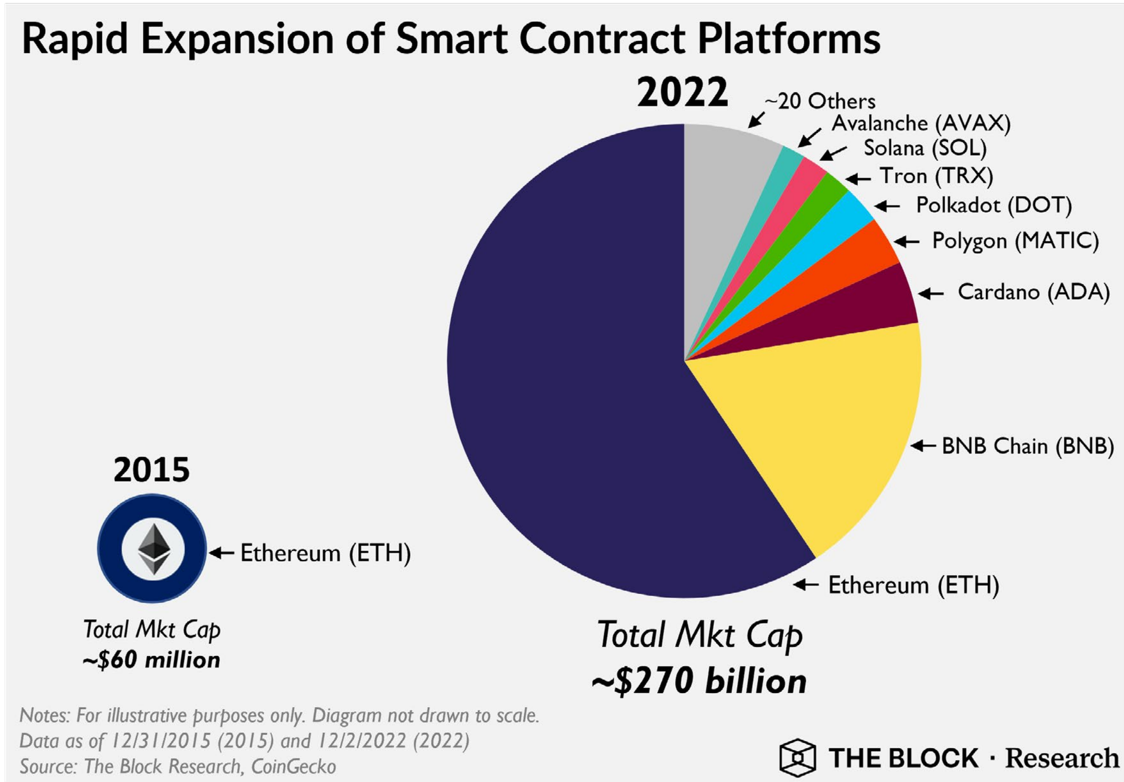
Indeed, efforts to bring programmability and scalability to Bitcoin have moved off its base layer and onto various iterations of Layer-2s (L2s) (complementary blockchains that leverage the security framework of another L1) and other solutions. Readers are encouraged to refer to The Block's recently released report titled "Bitcoin: Beyond the Base Layer" dedicated to developments around Bitcoin's ecosystem.

Another approach for builders has been to propose entirely new platforms that aim to address these challenges head-on.

What are Smart Contract-Enabled Blockchains?

Smart contracts are programs whose rules and logic are encoded on a blockchain and can self-execute when predetermined conditions are satisfied. Smart contract-enabled blockchains (or, smart contract platforms) have all the tooling necessary for smart contracts to be deployed on-chain. Theoretically, anyone with the appropriate technical knowledge can create smart contracts, which, once deployed on the blockchain, cannot be altered. Similarly, anyone with internet access can engage with an on-chain smart contract, provided they cover the necessary transaction fees.

Since its launch in 2015, Ethereum has remained the largest smart contract L1 platform in the market. However, a number of other platforms have emerged over the past few years that are experimenting with innovative new consensus algorithms, blockchain architectures, and execution environments to meet the market demand for scalable blockchain-enabled general-purpose applications (e.g., asset issuance, NFT minting and trading, payments, decentralized exchanges, decentralized lending, etc.).



Applications Enabled by Smart Contract Blockchains

As the first smart contract platform, Ethereum has been the de facto playground for developers experimenting and competing to create novel decentralized applications (DApps) – an application running on a blockchain that combines smart contract(s) along with a front-end user interface. Many of the popular blockchain applications such as, decentralized finance (DeFi) and non-fungible tokens (NFTs), were invented in Ethereum's ecosystem by a global community of independent developers. The following are a few notable applications for smart contract platforms that have emerged.

Decentralized Finance (DeFi): The influx of investment capital into decentralized finance (DeFi) applications has been one of the most prominent investment trends since 2020. Smart contract-enabled L1s served as the hub for new applications that aim to provide greater transparency and composability for virtually every type of financial service, including trading (spot and derivatives), lending, event prediction, and a variety of other use cases.

Non-fungible Tokens (NFTs): Unique digital collectibles, art, and profile pictures (PFPs), along with marketplaces like OpenSea that made trading NFTs accessible to anyone, were critical drivers of the surge in attention in the NFT space in 2021. News of NFT purchases by celebrities and sky-rocketing valuations of some NFT projects also played an important role in capturing the attention of a range of new users. Applications for NFTs have already diversified to potentially disrupt many other diverse sectors, including ticketing, monetization, music, domain names, and fashion/luxury goods.

Blockchain-Based Gaming: GameFi is a portmanteau of gaming and finance that has rapidly become one of the most talked about sectors of blockchain applications. One of the core components of GameFi is a play-to-earn (P2E) business model in which players can earn money from owning and controlling in-game assets. GameFi has broken into the mainstream largely due to the resounding initial success of the blockchain-based game Axie Infinity. The introduction of scalable smart contract-enabled L1s (and L2s) has marked a turning point making high-throughput blockchain-based games a viable use case for blockchain technologies.

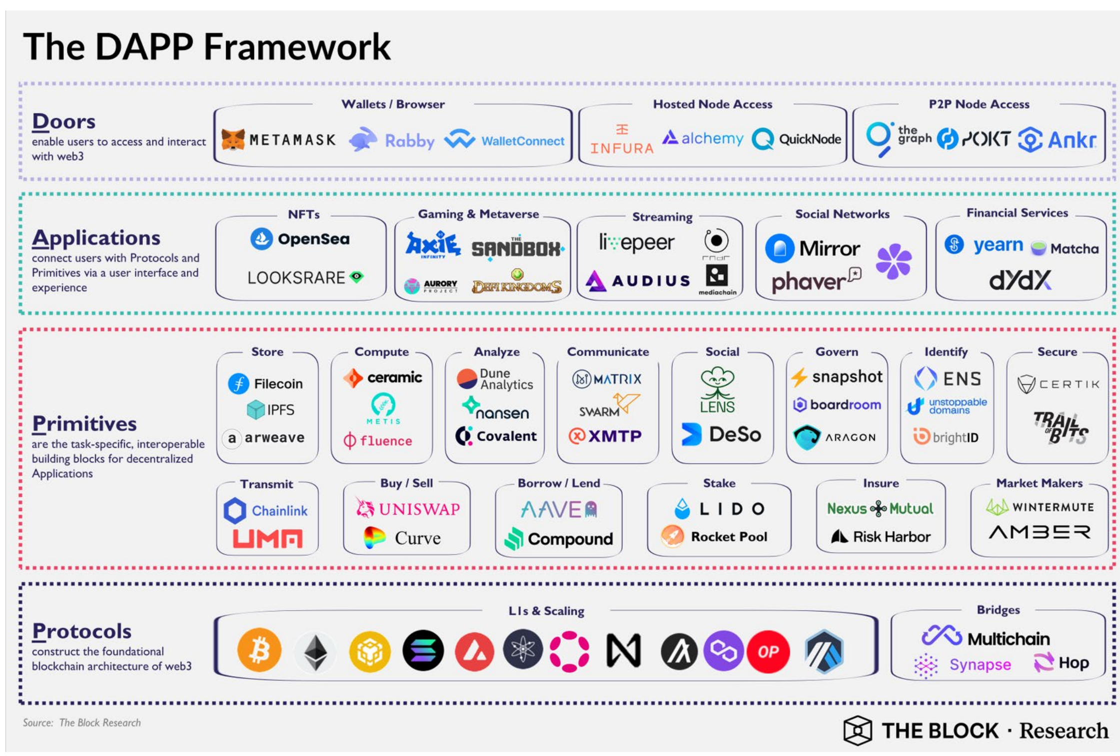
Decentralized Autonomous Organizations (DAOs): DAOs have the potential to create complex incentive structures using blockchain-enabled mechanisms (i.e., token issuance). There is significant ongoing experimentation on how DAOs may impact how humans coordinate and work together on the internet to reach shared goals. A notable example includes an effort from an internet-based community to purchase a rare copy of the US constitution in a Sotheby's auction that eventually failed in the final bidding stage.

Decentralized File Storage / Streaming / Social Media and Others: The growth in the NFTs/Gaming sector has led to increased interest in decentralized data storage solutions like Storj and Arweave. In Arweave's case, one of its primary use cases to date has been storing the hypermedia content of NFTs (image, gif, video, or sound). Decentralized data storage projects may eventually play much more prominent roles in enabling permanent blockchain data storage, as well as aid in efforts to decentralize popular internet-based services such as messaging, social media, and content streaming.

Web3

All of the categories listed above collectively shape what is becoming known as "web3." Web3 is an idea born of the DApps it is composed of. What makes web3 unique is that it uses smart contract platforms to allow anyone to participate without monetizing their data. Moreover, smart contract platforms allow something web2 lost as it became dominated by companies providing services in exchange for personal data: decentralization.

While centralization helped onboard billions of people to the web, it has also resulted in a handful of large companies having a stronghold on large swathes of the web with unilateral decision making power. Web3 tries to solve this dilemma by embracing a decentralized ecosystem of apps that are built, operated, and owned by its users. As such, sometimes web3 is succinctly described as the "read-write-own" web in contrast to web2 (the "read-write" web) and web1 (the "read-only" web).



The figure above illustrates how smart-contract-enabled L1s fit within the web3 stack.

In short, the applications of web3 are built from basic protocols, including L1s and task-specific "building blocks" that we call "primitives." The basic protocols form the foundational blockchain architecture that primitives are built on to provide various functions, including transaction (e.g., buying/selling, borrowing/lending, staking, insurance), storage, computation, communication, social interaction, and governance. See The Block's recent report, Accessing Web3: Developments and Opportunities, for a deeper look into the DAPP framework.

Discovery of New Applications

We must keep in mind that none of the above applications were around just a few years ago. The execution environment for DApps in most smart contract platforms are Turing complete – meaning DApps can theoretically perform any calculation if the required computational resources are made available.

Discovery of novel applications and how to implement them is expected to be a major part of this field as interest from developers, academia, industry, and the general public continues to grow. Moreover, tooling for blockchains to interact with real-world objects, events and physical hardware will further expand the sea of possible applications (e.g., augmented/virtual reality, tokenization of physical assets like real estate, insurance, supply-chain management, internet of things, etc.).

Criterion for Including L1 Chains in this Report

This report focuses on smart contract-enabled L1s[1] that rank highest based on the following criteria: market capitalization, total value locked (TVL), and daily active addresses. TVL refers to the total value of tokens locked in smart contracts that facilitate DeFi functions such as exchange and lending. We considered market capitalization as our primary selection factor for an L1 ecosystem because it is the sum representation of the market's medium-term confidence in the development team, their project roadmap, the underlying technologies, and the potential to generate sustainable network effects for specific L1s. Whereas TVL and daily active addresses were secondary factors that are correlated more closely with present-day usage for each L1.

Readers should be aware of nuances surrounding the usage of the "L1" terminology. There is an emerging idea for "Layer-zero" (L0) protocols that act as a low-level communication primitive aiming to provide trustless cross-chain messaging across compatible blockchains in an ecosystem. Polkadot is one of the pioneers of this approach, where multiple parallel chains ("parachains") connect to the Polkadot relay chain enabling data to natively flow between them. Here, the Polkadot relay chain may be labeled as an L0 since it has minimal functionality by design (e.g., no smart-contract functionality). Whereas, the connected parachains designed for a specific application(s) may be more comparable to L1 and L2s. For the sake of this report, the Polkadot relay chain is considered an L1 as it provides a universal settlement layer for all parachains in its ecosystem.

The concept of generalized chains versus application-specific chains (or "app chains"), as well as monolithic chains versus modular chains (or "task chains") have also gained significant attention in recent months, as discussed in more detail in Part 3, Network Architecture. For example, any of the above blockchains may include a monolithic architecture either on a single chain (e.g., Ethereum, Solana, BNB Chain, Tron, Flow, Algorand) or across multiple parallel chains (e.g., Avalanche, Cosmos, Polkadot,

1 Bitcoin's exclusion in this report is not a representation of our view on its role in the digital asset class, relative to smart contract platforms. The reader should also be aware of the myriad of unknowns that are beyond the scope of this report. To begin with, regulatory uncertainty across the asset class is a major hurdle. Bitcoin also remains the only major cryptocurrency still using proof-of-work (PoW) in its consensus mechanism. Thus, Bitcoin faces unique challenges (e.g., potential environmental impact & caveats) but may benefit from other factors (e.g., fewer explicit links between amount of tokens owned/custodied, the block production process and network governance). The relevance of the above and more on the growth/maturation of the digital asset class over the coming years and decades, remains to be seen.

Blockchain Ecosystems Selected for Comparison

Count	Platform	Native Token	Market Cap ($MM)	*# of DeFi Protocols*	*Total Value Locked ($MM)*	*Daily Active Addresses (x10^3)*
1	Ethererum	ETH	$154,075	*570*	32,040	*470*
2	BNB Chain	BNB	$47,286	*475*	5,500	*1,049*
3	Cardano	ADA	$11,109	*12*	76	*63*
4	Polkadot	DOT	$6,634	*15*	286	*1.3*
5	TRON	TRX	$5,002	*10*	5,700	*1,900*
6	Solana	SOL	$4,924	*81*	1,330	*640*
7	Avalanche	AVAX	$4,061	*261*	1,610	*41*
8	Cosmos	ATOM	$2,993	*13*	702	*15*
9	Algorand	ALGO	$1,748	*9*	198	*34*
10	NEAR	NEAR	$1,450	*11*	270	*93*

Notes: For Polkadot and Cosmos, TVL accounts for all subnets and parachains >5M USD in locked value. TVL for Avalanche only represents value in the C-chain.
Data as of 12/2/2022
Source: The Block Research, Dune, Messari, Gokustats, IntotheBlock, Nansen, Defillama, CoinGecko & relevant block explorers.

THE BLOCK · Research

Near). Other protocols will be included in our discussion where they are pertinent. We also briefly discuss the recent rise of L2 scaling solutions (e.g., Arbitrum and Optimism for Ethereum) that significantly complicates the overall composition of L1 ecosystems.

We must also note that our L1 selection criterion mentioned above is in no way comprehensive. It comprises a range of platforms with differing levels of ecosystem growth and maturity, different approaches to scaling, and different approaches toward decentralization. The combination of these factors makes them a useful sample set for drawing conclusions about the broader L1 landscape. Inclusion or exclusion of platforms from our sample set does not constitute support or disapproval.

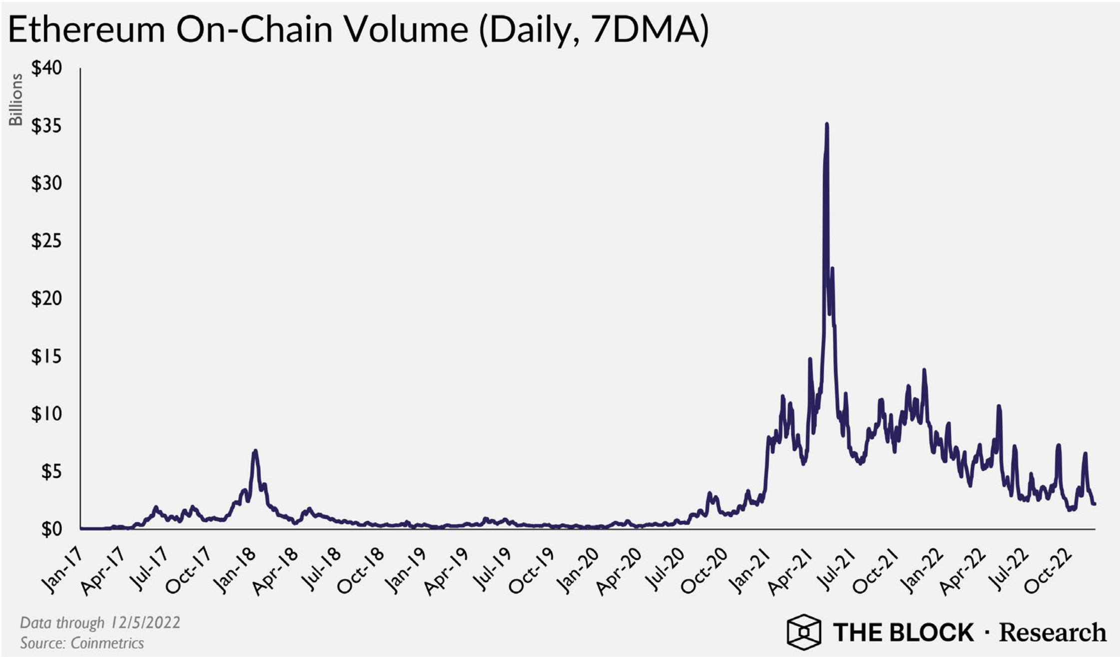
See the Appendix for a brief introduction to each of the ten blockchains we focus on in this report. That section also includes a brief synopsis on the notable founding members as well as, foundations and ecosystem development organizations involved with each.

II The State of Ethereum

Ethereum has been front and center this year with one of the most anticipated events in crypto – The Merge – being executed on September 15. Here, we will take a closer look at The Merge and its impacts and Ethereum's new technical roadmap.

Ethereum is the first and leading smart contracting L1 both in terms of usage and capital invested. While the landscape of other smart contracting L1s is rapidly developing, the developments within the Ethereum ecosystem have repercussions for the entire crypto market. A report on L1s would be incomplete without a thorough discussion of the current state of Ethereum and what lies ahead.

There is a lot going on in the Ethereum ecosystem. Every day, the Ethereum network facilitates the transfer of several billions of dollars. Moreover, over $30B of value is stored in Ethereum smart contracts facilitating decentralized exchange, lending, insurance, and payments, among other use cases. That value represents over 50% of the entire value locked across L1s.



On the technical front, the Ethereum community is developing an array of solutions to improve the network's security and scalability. The most notable recent event was the successful execution of "The Merge" whereby Ethereum changed its consensus mechanism from proof-of-work (PoW) to proof-of-stake (PoS) by merging its original mainnet with a separate PoS blockchain called the Beacon Chain. Now, they exist as one chain, and Ethereum's energy consumption has been cut to a small fraction of its previous usage. Some more context around PoS and PoW can be found in Part 3, however given the significance of The Merge, let's take a deeper look into it and its implications for the Ethereum ecosystem.

The Merge

The Ethereum Foundation likens The Merge to "changing an engine on a rocket ship mid-flight." The way it was designed, The Merge could be performed without needing to pause anything during the switch. Changing that engine was a two-step process – first, the Bellatrix upgrade and second, the Paris upgrade.

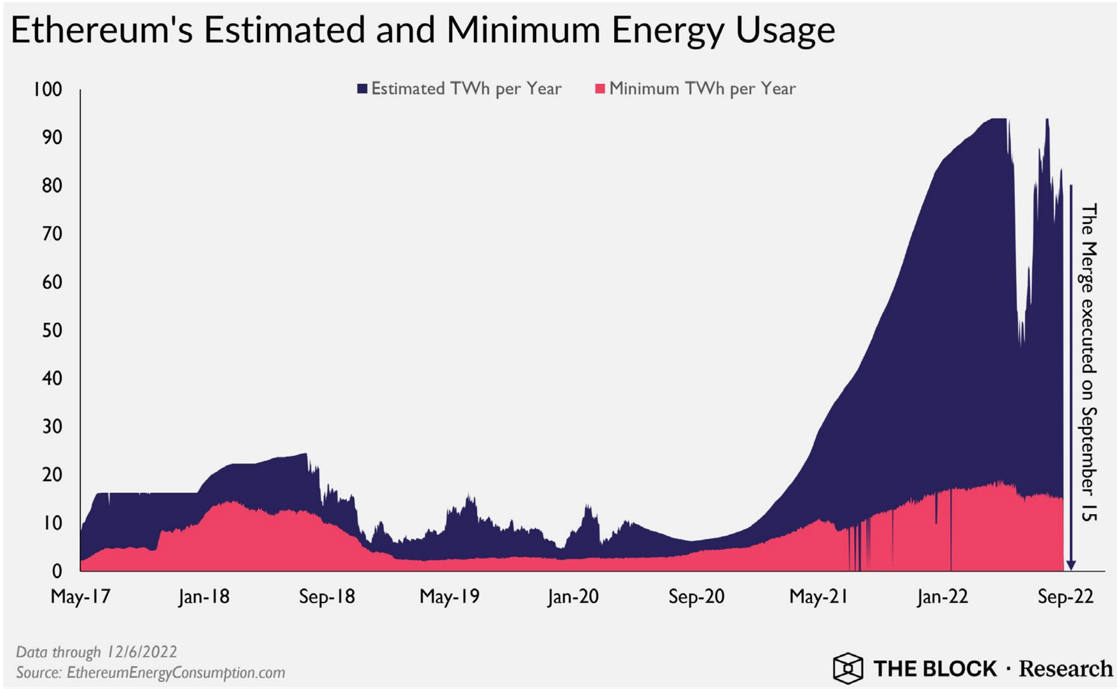
Bellatrix was activated on September 6th. Bellatrix was a Beacon Chain hard fork that introduced an execution payload parameter needed for validators to start creating mainnet blocks, which had previously been missing from the Beacon Chain. In essence, the new parameter "prepared" the Beacon Chain consensus layer to merge with the execution layer.

Paris – activated on September 15 – was the second and final step that officially switched Ethereum from PoW to PoS. It occurred when terminal total difficulty (TTD) reached 5.875 x 1022, where total difficulty refers to the cumulative sum of hash power put into Ethereum over its history. Syncing by block rather than by time ensured that Ethereum clients used by miners on the existing PoW mainnet would be perfectly synced by block at the time of The Merge. At this moment, Ethereum clients stopped accepting PoW blocks and the first PoS block was confirmed on the new Ethereum chain after two epochs – equal to about 12.8 minutes.

The Merge's Impact on Energy Consumption

Energy reduction: One of the immediate effects of The Merge was a significant reduction in the amount of energy needed to run the Ethereum network – estimated by the Ethereum Foundation to be about 99.95%

(from 100 to 0.01 TWh per year). Note, however, that pre-Merge Ethereum only used ~100 TWh per year when miner incentives were driven up by a high ETH value.



Before The Merge, the Ethereum network used 90+ TWh per year, in the order of the amount of energy consumed by countries like the Philippines and Kazakhstan or global video streaming services like Netflix. Now Ethereum is estimated to use ~0.01 TWh per year, much less than even PayPal, which is already energy efficient at ~0.26 TWh per year.

In addition to fulfilling one of the original motivations for the PoS design – carbon footprint reduction – the reduction in Ethereum's electricity consumption and hardware requirements may make it more feasible for average users to participate in block validation either by running their own validators (requires 32 ETH minimum) or using a custodial/pooling option.

User Experience: For most users, the user experience (UX) is unlikely to be significantly different from the pre-Merge UX as there were no direct improvements to network throughput or bandwidth.

Some users may notice a change in block time, as Ethereum's PoS uses a deterministic 12-second block time while Ethereum's PoW produced blocks stochastically as a function of mining difficulty (average 13.3 seconds but 10-30 second block times can happen regularly). Given the similar deterministic PoS block time and average PoW block time, the end user is also unlikely to see much difference in throughput or associated gas fees.

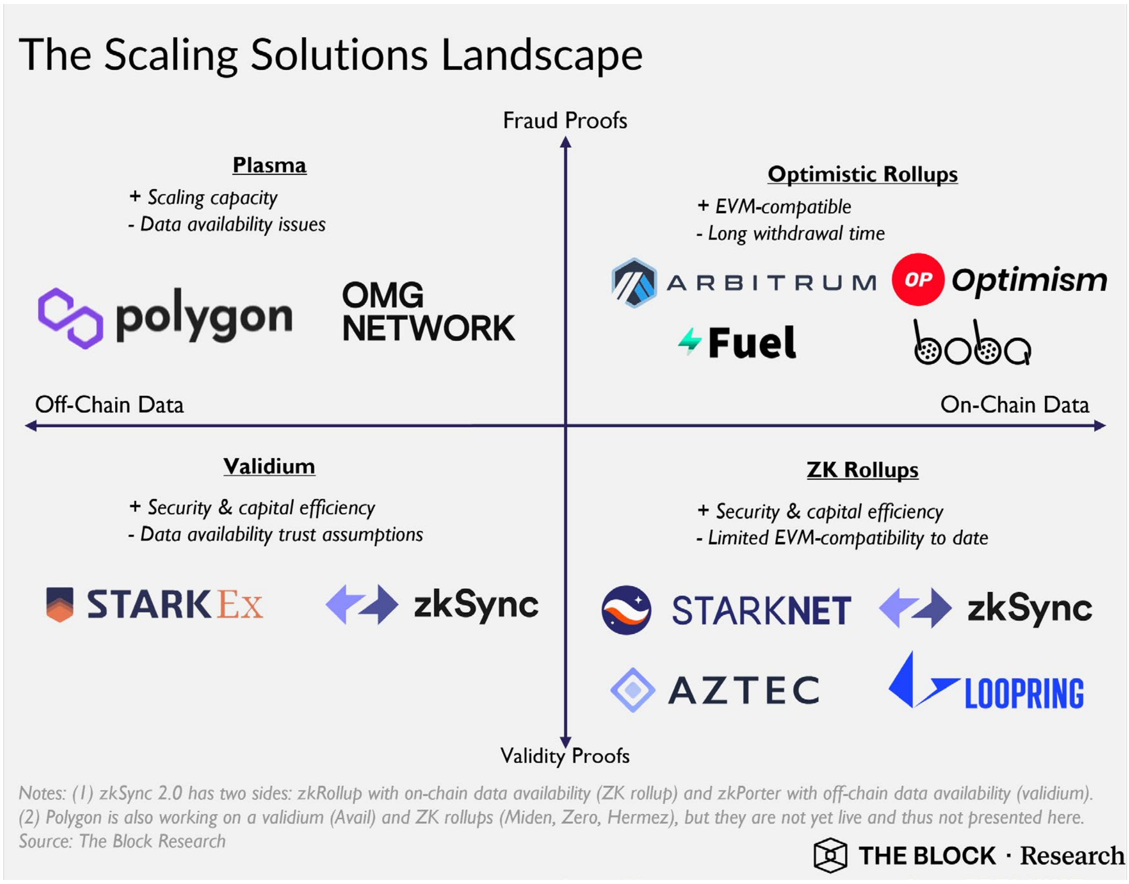
Beyond The Merge: Ethereum's Technical Roadmap

While The Merge may be the biggest upgrade to the Ethereum network in its history, it does not directly solve one of the biggest challenges facing the Ethereum community: scalability.

According to data from Coin Metrics, the average fee a user paid to execute a transaction on Ethereum was about $0.08 at the start of 2020. But since DeFi Summer 2020, the explosion of DeFi activity has driven a more pronounced and sustained increase in transaction fees that has brought Ethereum's scalability issues center stage. During certain periods in 2021 and 2022, average fees have reached over $40 per transaction. And under extreme demand, gas fees on Ethereum have soared to thousands of dollars per transaction.

Currently, Ethereum relies on a patchwork of scalability solutions to try to increase its throughput. As discussed in last year's L1 report, there are four popular categories of scaling solutions currently employed to scale Ethereum (which can also be adopted for scaling other L1s). They all approach scalability by offloading transaction execution from the main chain, but they do so in a diverse range of ways.

As shown below, current scalability solutions range in terms of (i) how much they inherit security from the underlying L1 chain by posting transaction data on chain; and (ii) to what degree they impose additional requirements on users beyond what is expected on the base layer (e.g., dispute periods in fraud proofs).



In the near-to-medium term, rollups are likely to be the most popular scaling solution, especially since Ethereum has taken up a rollup-centric roadmap. So far, optimistic rollups (e.g., Arbitrum, Optimism) have seen the most adoption, owing to their ease of development. Validity rollups and Validium solutions, on the other hand, have limited support for general-purpose smart contracting but are still being actively deployed.

Meanwhile, Ethereum has its own plans for solving for scalability, though the ambitious roadmap will likely give existing scaling solutions a generous head start. Let's look at what's in store for Ethereum next.

The Surge, (The Scourge), The Verge, The Purge, and The Splurge

At EthCC in Paris this past July, Vitalik Buterin explained the next major phases of making Ethereum more scalable, decentralized, and secure. The roadmap includes upgrades he's calling The Surge, The Verge, The Purge, and The Splurge.

> *"The Merge is proof of stake. The Surge is sharding. And The Verge is Verkle Trees. The Purge is things like state expiry and deleting old history. And The Splurge is basically just all of the other fun stuff."*
> – Vitalik Buterin, co-founder of Ethereum (EthCC Paris, July 2022)

More context can be found in the Ethereum protocol development roadmap that Buterin shared near the end of 2021. However, Buterin later shared an updated roadmap in November 2021 presenting two major changes:

1. The Verge is no longer just Verkle Trees, it's about verification and the endgame is a "fully SNARKed Ethereum" – referring to an Ethereum that uses validity proofs to protect digital privacy.
2. Between The Surge and The Verge, a new category called "The Scourge" has been added with the aim to address maximum-extractable-value (MEV) issues.

The updated roadmap outlines a series of upgrades that would effectively transition Ethereum from a single-chain monolithic blockchain to an auto-modular blockchain with enshrined modules to upgrade data availability (i.e., sharding enabling massive scalability for rollups) and execution environment (i.e., Verkle trees enabling stateless client execution).

To understand how this transformation would play out, we should look a bit closer at each of the planned phases.

The Surge

Now that Ethereum runs on a PoS consensus mechanism, it is easier to implement a form of data partitioning commonly employed to increase throughput and scalability called sharding. Sharding involves splitting a blockchain into pieces (shards) and storing those pieces in different places, in essence creating a bunch of mini-blockchains. Ethereum aims to create a sharded system comprising 64 of these linked databases (mini-blockchains).

Currently, the plan is to first roll out a limited form of sharding called "data sharding" – per the rollup-centric roadmap – whereby shards will store data and attest to the availability of ~250 kB "blobs" of data. In effect, Ethereum data sharding will open up a space of 16 MB every 12 seconds that can be filled with any data, with the system guaranteeing consensus on the availability of that data.

Importantly, this data space can be used for L2 protocols such as rollups, and it is a ~23x improvement on the existing storage capacity of the Ethereum chain. With data availability guarantees baked in, this means a secure and high-throughput data layer that could support massive scalability:

- Monolithic Ethereum: 15-40 tps
- With rollups: 1,500-4,000 tps
- With rollups + data sharding: 100,000+ tps

The potential downside of The Surge is that sharding may disrupt the 'composability' property of Ethereum – in other words, the ability of different DApps to easily talk with each other. Composability may be stymied in some special cases where transaction 'synchronicity' is crucial.

For example, in flash loans, traders spot arbitrage opportunities then borrow assets, profit off the difference in prices for the same asset in different places, and repay the loan all in a single synchronous transaction. There's little to no risk when all of this happens in a single transaction because if the loan isn't repaid, the whole transaction including borrowing is canceled. But, in sharding, a flash loan transaction may be split into several asynchronous transactions, which can introduce risks such as borrowing a loan without repaying it.

That said, Buterin argues that transactions within a shard could happen as before The Surge.

> *"… most use cases would not be significantly disrupted or could be trivially rewritten to survive in a cross-sharded model."* – Vitalik Buterin, Co-Founder of Ethereum (Ethrear.ch Forum, October 2019)

The Verge

Up next is The Verge, which will introduce Verkle Trees, a "powerful upgrade to Merkle proofs that allow for much smaller proof sizes," according to Buterin. Smaller proof sizes mean more optimal storage and smaller validator node size, which means more security and scalability potential for Ethereum.

The Verge is a significant upgrade of the database structure that provides pathways to all of the data on the Ethereum blockchain. It will be upgraded from the Merkle Patricia tree to a Verkle tree node structure.

Verkle trees serve the same function as Merkle trees – one can put a large amount of data into the tree, make a short proof ("witness") of that data or a piece of it, which can be verified by someone who only has the root of the tree.

Compared to Merkle proofs, Verkle proofs are much more efficient and small, meaning smaller validator nodes. This makes stateless clients viable, which would be a major upgrade to the Ethereum blockchain in that blocks can be validated by nodes that don't hold the full account state. In theory, this will make the validation process more scalable, faster, and easier to set up. It will also boost decentralization because validators can join more easily as they don't need to store extensive amounts of state data.

The Scourge

Various measures will be enacted to prevent censorship associated with MEV operations, with the end goal being "reliable and credibly neutral transaction inclusion."

MEV refers to the income that block producers and validators can earn in excess of the standard block reward and gas fees by including, excluding, or reordering the order of transactions in a block. However, the economies of scale behind MEV make it a risk to Ethereum's decentralization and security – opportunities for MEV increase proportionally with the size of the staking pool.

One way to reduce MEV-driven centralization is proposer-builder separation (PBS), which effectively separates the role of validators and block builders. PBS creates an auction market where builders negotiate with validators selling block space. By using a commit-reveal scheme, validators (and everyone else) do not learn the contents of the block until after the auction ends, so builders don't need to trust validators to not steal their MEV opportunity or expose it to others. PBS thus helps minimize attacks by copycat bots that steal and profit from others' MEV strategies (generalized frontrunners).

Flashbots is the research and development organization that created MEV-Boost, the leading implementation of PBS. Block proposers (validators) running MEV-Boost maximize their staking reward by selling block space to an open market of block builders. Since The Merge, the number of validators registered for MEV-Boost relays has rapidly increased from a few hundred in early September 2022 to over 420K as of writing. And, as of writing, Flashbots' MEV-boost has ~80% market dominance in the MEV-boosted block market.

This raises new concerns about MEV-driven risks to Ethereum's censorship, as Flashbots' MEV-Boost relays are known to be OFAC-compliant after censoring transactions related to the Tornado Cash sanction. As of writing, over 70% of Ethereum transaction blocks were labeled OFAC-compliant. In response, Flashbots is working on open-sourcing its code to help decentralize the block-building process.

The Scourge will also support the move toward more neutral, fair, and decentralized block building with protocol upgrades, including native PBS, MEV burn, and inclusion lists. Native PBS would move builder-proposer auctions in protocol. MEV burn aims to burn most MEV through block-proposer auctions that auction off the "right to build a block" on the consensus layer. Inclusion lists would allow validators to combat censorship by forcing the inclusion of some transactions.

The Purge

Excess historical data will be “purged” from the Ethereum network, reducing network congestion and the hard drive space requirements for validators.

The Purge will further cut down the hardware requirements and storage space required to participate in validating the Ethereum network, thus encouraging network growth and decentralization. Clients will stop serving historical data more than one year old, which means less wasted bandwidth and getting rid of “technical debt” associated with old state data.

The Splurge

The last and final phase is “all the other fun stuff,” according to Buterin. This includes smaller updates and maintenance to ensure that all the other previous upgrades are running smoothly. There are also miscellaneous upgrades aimed at accessibility and improving Ethereum’s user experience.

III Comparison of Selected Layer-1 Platforms

This report uses a multifaceted approach to compare each of the ten smart contract platforms selected for analysis. Specifically, the following sections will focus on their basic design parameters, hardware/capital requirements for network participants, factors that affect decentralization, blockchain architecture, platform performance, on-chain and ecosystem data, as well as the organizations and funding behind them.

Technical Overview

There are innumerable design decisions that endow individual blockchains with their own set of unique properties. Key among them is their node network composition and different approaches towards decentralization.

Nodes and Consensus

“The cloud is just someone else’s computer” is a popular meme.

Taking the above as inspiration, a blockchain is just a distributed network of “nodes” executing instructions contained within a specific blockchain platform’s software.

The takeaway here is that nodes are the physical computers that comprise a blockchain network. Nodes contain the full (or a curtailed) history of all transactions, along with every consensus rule governing the blockchain. Nodes may participate in the network by producing new blocks, validating them, or broadcasting new transactions to the network.

Reliable propagation of blocks in a distributed network of nodes requires a robust consensus mechanism that (ideally) always produces global agreement on the current state of the blockchain. Here, the consensus mechanism refers to a collection of rules encoded in the blockchain algorithm that: 1) offers Sybil attack resistance and 2) creates an incentive structure where it’s profitable to be an honest block producer and costly to be a malicious one. Sybil attack, in this instance, refers to a security threat where one entity attempts to take control over a blockchain network simply by creating multiple nodes.

Today's most popular blockchains use various iterations of consensus mechanisms that rely primarily on PoW or PoS for Sybil attack resistance. PoW (part of Bitcoin's algorithm) requires nodes to compete using computational power to earn the right to produce a new block (and collect block rewards + fees). Fraudulent blocks proposed in a PoW blockchain that violate consensus rules will likely get rejected by the network, leaving the bad actor with only the cost of wasted electricity.

For PoS, validators (nodes with the capacity to produce new blocks) are required to lock in (or "stake") a certain amount of tokens native to each PoS chain. There are various mechanisms that PoS protocols use to disincentivize malicious/incompetent behavior. For example, some or all of this staked capital may be confiscated ("slashed") in case of validator misbehavior. Readers are encouraged to refer here for further details on blockchain consensus mechanisms.

Nearly every new L1 blockchain offering in the market has implemented some iteration of a PoS consensus mechanism. Moreover, all of the fastest-growing L1s since 2020 have been based on PoS, including every smart contract chain selected for analysis in this report.

The number and geographical distribution of nodes operated by independent entities are critical factors that determine the degree of decentralization of a blockchain. Next, we take a look at how different chains compare on different proxy measures of decentralization.

Decentralization

Blockchains may be likened to "inefficient databases." While mostly true, we accept this inefficiency to ensure decentralization – enabling credible neutrality, immutability, censorship resistance, and permissionless access for anyone with an internet connection.

The difficulty in blockchain scalability can be boiled down to what is commonly referred to as the "blockchain (or scalability) trilemma," popularized by Vitalik Buterin. The trilemma posits that a blockchain can only have two of the three following properties – scalability, decentralization and security. Optimizing for decentralization, for example, will inevitably lead to degrees of tradeoffs on the other properties. Indeed, this is a limitation that has proven to be a significant technical barrier, especially for established blockchain architectures (e.g., Bitcoin).

Traditional enterprise-scale databases that dominate the internet today operate across a handful of centralized data centers with very high compute availability and network bandwidth. Although this optimizes for cost and throughput and may aid in composability of transactions, it is at the cost of critical factors (neutrality, immutability, censorship-resistance, and permissionless access) that make blockchains special to begin with.

The design and architecture of L1 blockchains is thus a careful exercise in compromise. The quote “there are no solutions, there are only trade-offs” from economist Thomas Sowell, may just as well be apt for some blockchain architectures.

Assessing whether a blockchain is decentralized or not ultimately depends on how the evaluator defines decentralization. While there is no universally agreed definition for decentralization, most would agree there is a spectrum with multiple layers ranging from the distribution of the blockchain’s physical infrastructure to the social communities supporting it. One useful and quantifiable way to get an idea of where a chain lies on that spectrum is to analyze its nodes – the actual hardware running that chain’s blockchain software – and the entities operating those nodes.

Nodes serve several critical functions:

1. They vote on and validate blocks of transactions
2. They communicate with other nodes to come to an agreement about the state of the blockchain
3. They store that state history as a universal source of truth
4. They make up the endpoints of the network by which users can access and use the applications built on the network

Different types of nodes serve different functions:

1. Validator nodes participate in consensus to finalize transactions and agree on the state of the blockchain
2. Archival nodes store everything kept in full nodes and build an archive of historical states
3. Light nodes only store a small portion of block data that can be used to reference associated block data stored by full nodes

Decentralization is maximized when:

1. Nodes are numerous and dispersed in terms of both geography and network control
2. The hardware required to run a node is accessible and produced by many different independent manufacturers
3. There are no incentives for node entities to form cartels or collude in any way
4. The financial stake used to secure the network is widely distributed

Here, we focus on PoS validators (we define here as nodes with the capacity for block production in PoS networks) because they are directly related to how difficult it would be to halt or subvert the network. The key components of validator node decentralization concern the hardware and financial requirements to run a validator and the distribution of the total financial stake controlling the network. In brief, there are three key questions to ask:

- What are the computational requirements to run an individual validator node?
- How much financial stake is required to enter the active validator set?
- How much would it cost to control the network?

Hardware Requirements

Let's look at the computational requirements to operate a validator by chain. All else equal, lower hardware requirements lower the barrier to entry for directly participating in consensus, thus encouraging larger and more distributed validator sets.

Hardware Requirements to Run a Validator Node

Platform	CPU Physical Cores	RAM (GB)	Disk (GB)	Bandwidth (Mbps)
Algorand	2	4	100	100
Avalanche	4	17.2	200	30
BNB Chain	16	64	2,000	10
Cardano	4	10	24	10
Cosmos Hub	4	32	500-2,000	NA
Ethereum	4	16	500	25
Near	8	24	1,000	NA
Polkadot	4	16	1,000	500
Solana	12	128	1,500-2,000	NA
Tron	16	32	1,500	100

Notes: (1) Requirements are likely to change materially over time. (2) Some protocols recommend more RAM for better performance (e.g., Ethereum recommends 32 GB and Solana recommends 256 GB). (3) Requirements do not include additional hardware required to run failover node clusters. (3) All protocols recommend fast SSD disks.
Data as of 12/7/2022
Sources: BlockDaemon, developer documentation

THE BLOCK · Research

Note that while lower hardware requirements are generally an indicator of greater decentralization capacity, they also translate it to less computational power per validator. Given the tradeoffs, some platforms may require higher hardware requirements to achieve higher TPS at the sacrifice of ease of decentralization.

The costs and operational difficulties associated with higher hardware requirements may incentivize a large number of validating entities to seek out cloud service providers to host their validator nodes. The consequence is that a large number of PoS validators may end up being run out of the hosted data centers controlled by a small number of entities (as discussed later).

Financial Requirements

Beyond hardware decentralization factors, we can also gauge decentralization by examining the financial requirements to run a validator node. Below, we look at the minimum staking requirements to run a validator node and the relative ease of liquifying the validator stake in terms of unbonding period. A lower minimum stake encourages decentralization by reducing the upfront investment required to enter the validator set.

Staking Requirements to Run a Validator Node

Platform	Capped Validator Set?	Cost Basis	Native Unit Requirement (A)	Native Unit Price (B)	Minimum Stake ($USD) (C = A*B)	Unbonding Period (Days)	Slashing
Algorand	No	Platform	0.1 ALGO	$ 0.23	$ 0.02	0	No
Avalanche	No	Platform	2,000 AVAX	$ 13.46	$ 26,920	21	No
BNB Chain[2]	Yes (41)	Market	270,320 BNB	$ 287.58	$ 77,738,626	7	Yes
Cardano[3]	No	Platform	100,000 ADA	$ 0.32	$ 32,000	0	No
Cosmos Hub	Yes (175)	Market	80,470 ATOM	$ 9.97	$ 802,286	21	Yes
Ethereum	No	Platform	32 ETH	$ 1,255.95	$ 40,190	~27 hours (36 days if slashed)	Yes
NEAR[4]	No	Platform	20,625 NEAR	$ 1.77	$ 36,506	2	No
Polkadot	Yes (297)	Market	1,887,389 DOT	$ 5.41	$ 10,210,774	28	Yes
Solana[5]	No	Platform	33 SOL	$ 13.96	$ 461	2	Yes
Tron[6]	Yes (27)	Market	738,501,144	$ 0.05	$ 39,140,561	3	No

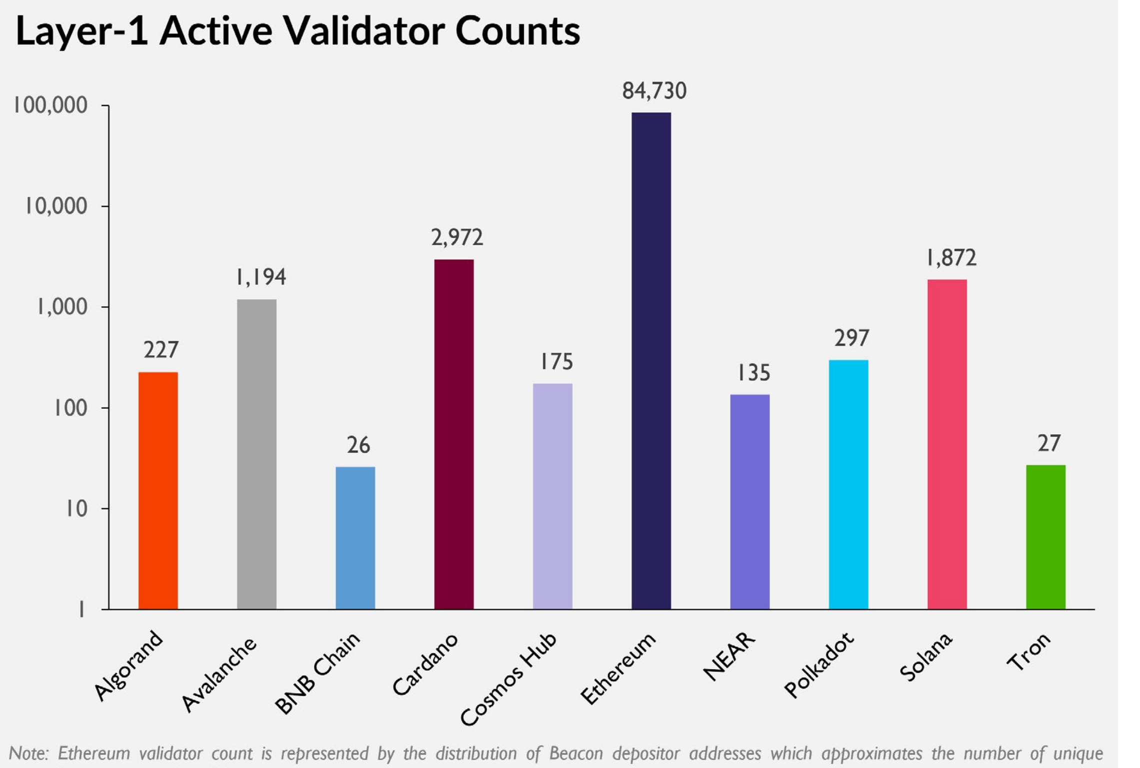
Notes:
(1) Represents the minimum stake to enter the validator set including any stake attributable to delegation.
(2) Top-26 active validators out of 44 validator candidates, the native unit requirement here is based on the 26th highest stake as of 12/7/2022.
(3) While there is no minimum native unit requirement to pledge in setting up a Cardano staking pool (validator node), the staking pool operator must pledge a stake to make their pool attractive. Based on current active pools, we estimated that minimum pledge to be ~100,000 ADA.
(4) NEAR native unit requirement minimum is either 67,000 or above the ""seat price"" which was 98,956 NEAR as of 12/7/2022.
(5) Solana validators need sufficient SOL to cover voting costs (~1.1 SOL/day). Accordingly, the native unit requirement depends on staking duration, which we estimated to be ~30 days.
(6) Tron validators must possess a minimum of 9,999 TRON to enter elections, and then rank in the top-27 stakers to produce blocks. The estimated unit requirement here is based on the 27th highest stake as of 12/7/2022.
Data as of 12/7/2022
Source: Developer documentation, block explorers, Figment, BlockDaemon, CoinMarketCap

THE BLOCK · Research

In instances where there is no cap on the total number of validators, platforms define the minimum level of stake necessary to become a validator. In other cases, where the protocol governance places a limit on how many validators are accepted into the active set, the minimum stake required to become a validator is dictated by market competition and approximated as the stake of the active validator with the least stake.

Most notably, the estimated minimum stake to be an active validator varies significantly by network – with cost basis (platform vs. market) being one of the key differentiators. The market competition to validate for L1s with capped validator sets (e.g., BNB Chain, Tron) drives high costs to run a validator node. For example, while it is prohibitively expensive to be an active validator for Tron at over $46M, the upfront investment required to validate for Ethereum (~$40K), Avalanche (~$30K), or Solana (~$1K) is more accessible to retail consumers. And the cost to be a validator for Algorand is universally accessible at less than a dollar, owing to their tiny native unit requirement.

We also note that protocols that combine a relatively low financial barrier to entry and an uncapped validator set have the highest number of active validators:



Note: Ethereum validator count is represented by the distribution of Beacon depositor addresses which approximates the number of unique controlling entities in the validator set.
Data as of 12/7/2022
Source: Block explorers

Comparing these validator counts to the validator counts from last year for the L1s with uncapped validator sets, we can get a sense of how much these different L1s decentralization improved or worsened in terms of this metric.

- Algorand decreased 31% from 331 (May 2021) to 227 (December 2022) validators
- Avalanche increased 22.0% from 978 (May 2021) to 1,194 (December 2022)
- Ethereum increased 177% from 30,594 (June 2021) to 84,730 (December 2022)
- Solana saw the largest increase of 223% from 579 (June 2021) to 1,872 (December 2022)

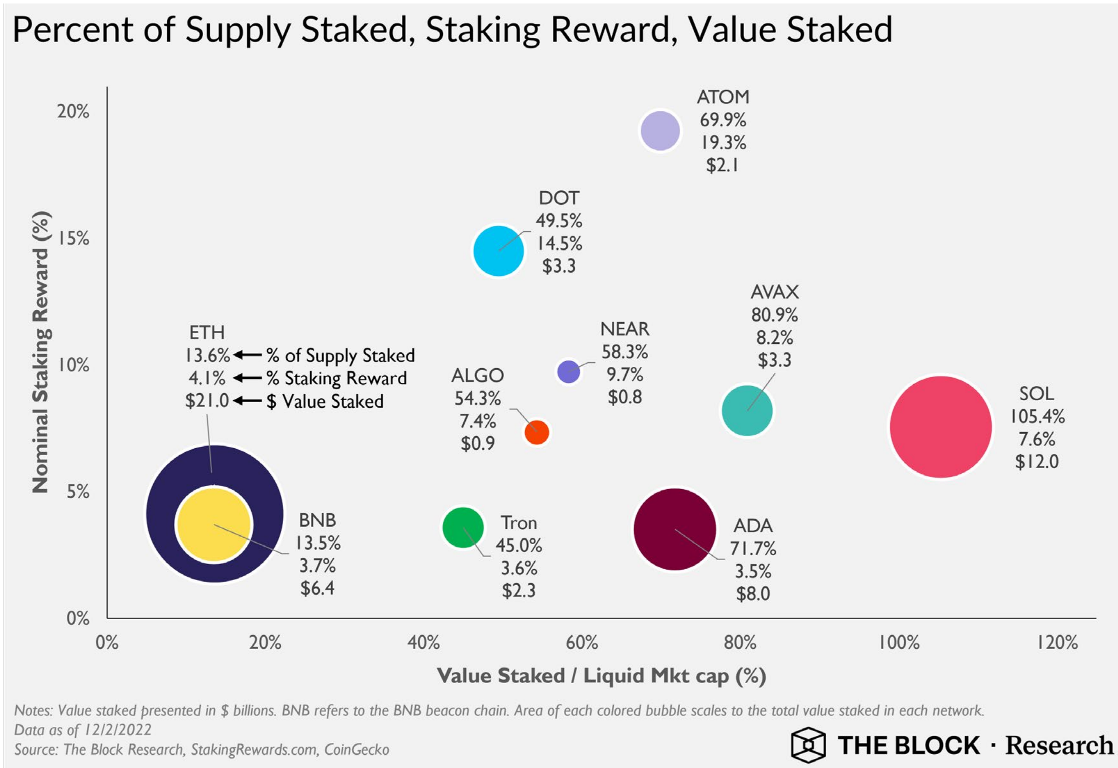
Note that while higher numbers are generally a good sign for decentralization, it's not clear what count of active validators is "sufficient" and that number will vary per use case. Also, it's possible to game these numbers when a single entity operates multiple validators that appear as unique entities.

The devil is in the details. As might be expected, where financial barriers to entry (e.g., minimum stake to enter capped validator sets) are high, it is more likely to see large organizations running the validators than individuals (e.g., see the top-26 stakers in the BNB validator leaderboard). However, even when financial barriers are relatively low (e.g, minimum stake to enter uncapped validator sets), the large majority of the network is secured mostly by validator pools operated by large organizations (e.g., see Ethereum's validator distribution by pool here). It seems that stake still gravitates to a few large and publicly known validators as it's too complicated or costly for individuals to run their own validators. At this point, people would rather trust a reputable validator with low fees than run their own validator.

When evaluating a PoS network's decentralization, one should keep in mind how many of these large validator pools collectively control more than a third of the total stake, as this "superminority" may collude to censor or halt the network. For example, even if Protocol X has 1,000 individual validators, there is still a centralization concern if Pool A controls 250 of them and Pool B controls 150. If these two pools joined, they would collectively possess enough stake to stop the network from reaching consensus.

Staking Statistics

Let's discuss how much value is at stake to get a sense of the overall security of different PoS networks. To do this, we need to take a look at staking statistics such as the percentage of native tokens staked per L1 and how much value that equates to in dollar terms.



First, we can see significant differences in the total amount of value staked across each network. Average staked value is ~$6B, ranging from a low of ~$0.8B for the Near network, to a high of $21B for the Ethereum network (as of 12/2/22). As mentioned before, this total value accrual is crucial in determining the overall degree of security within each PoS network. Despite Ethereum's percentage-of-supply staked being relatively low (13.6%), its staked security (measured strictly by the volume of capital staked) is greater than all the other L1s observed.

Beyond the gross USD value staked, normalizing the number of native tokens staked with total circulating token supply provides some insight into how much security capacity of a PoS network is being utilized. The percentage of circulating supply that is staked across networks ranges from a low of ~13% for the BNB token, all the way up to ~105% for the SOL token. Greater than 100% for this metric suggests that locked token supply (that may be in part earmarked for founders, employees, investors, support foundation(s), service providers, etc.) is staked and earning inflationary rewards. Across the 10 focal networks of this report, an average of ~56% of the circulating supply was staked, at the time of writing. This metric will vary depending on a variety of factors including staking rewards, lockup duration, unbonding duration, and the ease of staking and unstaking (as discussed later).

We also see that staking reward varies between 3.5% and 19% nominal APR for Cardano's ADA and Cosmos hub's ATOM, respectively. The average staking APR across the 10 networks highlighted in this report is 8.2%. Staking yields may change significantly based on a number of factors, such as network demand/usage, as discussed in later sections. All else equal, high staking rewards may attract new users in the short term but adversely affects long-term token scarcity.

Limitations of Staking Statistics to Measure Decentralization

While the analysis above provides some indication for the degree of staking participation and amount of staked capital across different networks, it isn't currently possible to pinpoint the number of independent entities running these validators and their legal jurisdictions. Even if the network stake is distributed across a large number of discrete validators, it's possible that one or a few entities are delegating most of this stake. The following are some general factors to consider that relate to network decentralization.

Infrastructure centralization: There are signs of node centralization across multiple networks where some DApps coming offline tend to correlate with reported outages from cloud services. Blockchain infrastructure service providers (i.e., node rentals, managed blockchain integration) are thought to make up an appreciable portion of all nodes in some networks. For example, Infura operated 5% to 10% of all Ethereum full nodes to service 13 billion queries per day and supported 70% of the top Ethereum DApps – according to estimates in 2018. More recent estimates indicate that >55% of all Ethereum nodes currently run on hardware owned and operated by professional hosting providers.

Node/validator centralization may have an outsized effect on the security of the entire network. For example, Hetzner Online GmbH, which hosts ~14% of Ethereum nodes, announced that "...even if you just run one node, we consider it a violation of our ToS [terms of service]." More recently, an estimated 1000 Solana validators have lost server access due to the same company, Hetzner, blocking all Solana-related activity on its servers. This is potentially a major development where ~20% of total network stake and ~40% of Solana's validators (unknown number of independent operators) may be affected by Hetzner's unilateral decision.

Staked capital centralization: Validators select the transactions to be included in a block. Thus, centralization of block-producing validators along with their staked capital can present enormous challenges to the neutrality, permissionless and censorship-resistant properties of a PoS network. This is an important point of consideration as DeFi currently has ~$42 billion USD locked in value across dominant smart-contract blockchains, as of writing.

We will discuss Ethereum as a case study below, but these concerns may apply to most of the popular PoS chains today.

Staked ETH Custody?

Firm/Protocol	Custody Type	HQ	ETH Staked(1) (%)
Lido	LSD	N/A	27%
Rocket Pool	LSD	N/A	2%
Coinbase	Exchange	USA	12%
Kraken	Exchange	USA	7%
Binance	Exchange	N/A	6%
Staked.us	Staking service	USA	3%
Bitcoin Suisse	Staking service	Switzerland	2%

Notes: Sorted by custody type. (1) Relative to the total of ~16M ETH staked. LSD - liquid staking derivative.
Data as of 12/2/22.
Source: The Block Research & Beaconcha.in.

THE BLOCK · Research

Currently, ~13.6% (15.5M ETH) of all circulating ETH is staked. Non-custodial liquid staking protocols or derivatives (LSD), as well as exchanges and professional staking operators offering custodial staking options, have become immensely popular due to their accessibility and ease of use.

For the Ethereum network, the top 7 identifiable entities control >60% of all staked ETH. Specifically, the Lido DAO controls ~4.6M ETH on the beacon chain, or 27% of all staked ETH, as of writing. Although it is important to note that Lido's stake pool is composed of many individual/enterprise validator operators. Delegated stake can also be withdrawn at will in applicable PoS chains (an unbonding period may be applicable). However, in Ethereum's case, staked ETH is locked for an indeterminate amount of time based on several factors.

Lido's stETH liquid token enjoys wide integration from other DApps in multiple L1 ecosystems, making Lido the front-runner in LSDs by a wide margin. The current dominance of Lido supports the argument that LSD services could be a "winner-takes all" market. If true, the overwhelming dominance of any individual LSD protocol may leave the entire network more open to hostile capture. In Lido's case, it may be through its DAO governance structure where just the top 50 LDO token holders (including Lido treasury) collectively own >81% of all LDO in circulation (out of ~22.5k total holders) on the Ethereum L1 chain.

Regulatory uncertainty: On August 8th 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash (TC), a mixing/anonymizing protocol in the Ethereum ecosystem. The implications could be wide reaching. US-regulated entities operating Ethereum validators such as exchanges that currently custody >22% of staked ETH ("Staked ETH Custody" table) may be required by law to censor all transactions and addresses having any association with TC. As mentioned, an estimated 70% of all new blocks produced in Ethereum L1 are classified as "OFAC-compliant."

OFAC's decision is controversial, to say the least – court challenges and political scrutiny are expected. Although OFAC's announcement is currently limited to TC on Ethereum, most other blockchains (both PoS & PoW) can be targeted if the standard for such sanctions indeed boils down to censoring open-source code. OFAC's decision has sent ripples across the entire digital asset ecosystem, increasing interest in methods that advance censorship-resistance and privacy. More recently, the complete collapse of FTX and its subsidiaries has captured the ire of the public, legislative and regulatory communities. The fall of FTX and other previously well-regarded crypto-native companies are developing stories that are beyond the scope of this report, but are likely to have long-term consequences for the adoption/use of digital assets.

Blockchain Network Architecture

In the early to mid-2010's, the concept that all transactions may one day be executed on one blockchain was relatively common. Today, it appears more likely that multiple chains with a wide array of specifications, each housing an ecosystem of compatible applications and blockchains, may be what is required to scale and deliver the decentralized internet.

Generalized Chains vs Application-Specific Chains

This vision of a multichain future laid the foundation for Cosmos in 2016. As described in their whitepaper titled "A Network of Distributed Ledgers," the basic premise was that different applications may have wildly different blockchain specification requirements. Thus, instead of an ecosystem reliant on a single-threaded blockchain with fixed attributes, Cosmos' approach was the introduction of the Cosmos software development kit (SDK), which enabled anyone to fine-tune the exact design and deploy their own app chain. What's more, is that all blockchains developed with the Cosmos SDK have native tooling for cross-chain coordination and messaging – in other words, built-in interoperability for any chain configured with the Cosmos SDK.

The multichain approach appears to be gaining traction across a wide range of major players in the industry. The Avalanche/Cosmos/Polkadot chains, for example, are often referred to as "network of networks" or "blockchain of blockchains." It is important to note there are some significant differences to how each of these multichain ecosystems are architected – principal among which is the approach towards network security.

Multi-chain: (Pretty Much) Everyone's Doing It

Network (Asset)	Mkt Cap ($ billion)	Scaling Approach	Chains Employed[1]
Ethereum (ETH)	$ 154.1	Multi-chain	Beacon Chain, Data Shards, Layer-2 Networks
BNB Chain (BNB)	$ 47.3	Multi-chain	BNB Chain Layer-1, Sidechains, ZK-Rollups
Cardano (ADA)	$ 11.1	Multi-chain	Cardano Layer-1, Hydra (Layer-2 Network)
Solana (SOL	$ 4.9	Single-chain	Solana Layer-1
Polkadot (DOT)	$ 6.6	Multi-chain	Relay Chain, Parachains
Polygon (MATIC)	$ 8.2	Multi-chain	Polygon PoS Sidechain, Layer-2 Networks, Avail (Data Availability)
Tron (TRX)	$ 5.0	Multi-chain	Tron Layer-1, DAppChain (Sidechains)
Avalanche (AVAX)	$ 4.1	Multi-chain	Avalanche Primary Network (P-chain, X-Chain, C-Chain), Subnets
Ethereum Classic (ETC)	$ 2.7	Single-chain	Ethereum Classic Layer-1
Cosmos (ATOM)	$ 3.0	Multi-chain	Comos Hub, Zones

Notes: (i) Represents current and planned network architecture at time of writing
Data as of 12/2/2022
Source: The Block Research & CoinGecko

THE BLOCK · Research

Overall Frameworks for Network Security in Multichain Ecosystems

One generalized method for building security in a multichain ecosystem is a single "base" chain acting as the settlement layer connected to an ecosystem of L2 (and even layer-3; L3) blockchains that may use rollups or other scaling technologies (discussed in more detail later). In return, all associated L2/L3 chains inherit the security guarantees of the underlying base-layer chain. This, in essence, ensures shared security for every chain in the ecosystem associated with the base layer (e.g., the Ethereum L1 and its rollup-centric scaling solutions such as Arbitrum).

A second general approach to security is a fully sovereign application-chain model where every chain is its own settlement layer, has its own set of validators, and does not rely on any other base layer chain. This is possible in the Cosmos and Avalanche ecosystems, although there are (or expected to be available) options for sovereign blockchains deploying in these ecosystems to incentivize and/or, purchase security from within. Since the total amount of capital available to be staked in any ecosystem is finite, the ability of sovereign chains to acquire adequate security during their early-growth phase may be one potential challenge.

Regardless of which security approach becomes dominant for multichain interoperable ecosystems in the future, there is interest from developers to deploy DApps in these ecosystems. For example, dYdX is a popular central limit order book (CLOB) exchange that was built on the StarkEx ZK-rollup for Ethereum and routinely handles >$500M USD in daily trading volume. Permissionless CLOB exchanges like dYdX require very high transaction throughput at low cost to ensure price efficiency, liquidity, and profitability for market-makers. This is in contrast with the need for blockchain validators who require a minimum amount of transaction fees to ensure reliable execution and security for the network.

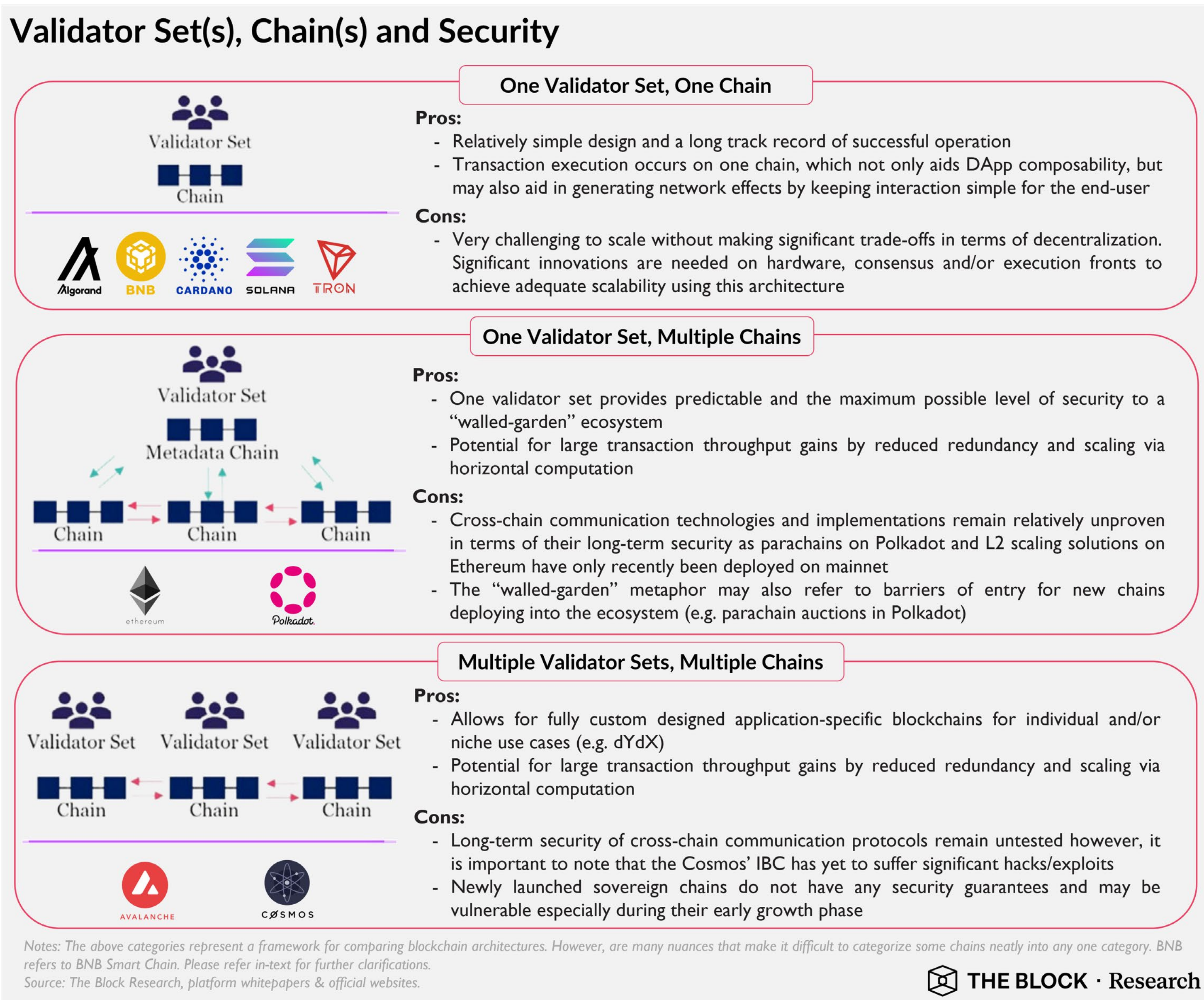
Given dYdX's myriad of unique challenges, full stack optimization from the bottom up was a necessity to deliver their application. dYdX has recently announced a move to the Cosmos ecosystem enabled by the Cosmos SDK that allows sufficient flexibility in developing an application-specific blockchain that satisfies their design goals.

Validator Roles in Blockchain Ecosystems

The architecture of a blockchain network can be categorized by looking at three general characteristics: 1) the number of chains supported, 2) how the available validator set is responsible for securing the ecosystem as a whole, and 3) modular implementation. This relates to the generalized versus application-specific chains (app chain) concept. Currently there are three broad approaches:

1. **One Validator Set, One Chain**: Historically, the most common approach where a single threaded generalized chain is directly connected to all DApps in the ecosystem and is responsible for the security (at minimum) of all transactions (e.g., Solana and Cardano)
2. **One Validator Set, Multiple Chains**: A single settlement layer responsible for security along with an ecosystem of L2 and app chains creating a hierarchical, tree-like architecture (e.g., Polkadot)

3. **Multiple Validator Sets, Multiple Chains**: The idea of an ecosystem made of fully-sovereign app blockchains, each responsible for their own security and execution. There is no "one central chain" for any function thus, it is expected that some chains will be more secure than others (e.g., Cosmos)



Although the generalized categories above represent a useful framework for comparing blockchain architectures, there are several nuances that make it difficult to categorize some chains neatly into any one category, especially when considering future roadmaps for some projects. The readers should be aware of the following:

- Algorand is expected to have Co-Chain functionality aimed to create interoperable, private & permissioned blockchains that interact with the public Algorand chain.
- Cardano and BNB Chain are both open to L2 & sidechain-based scaling solutions in the future, similar to Ethereum
- Near was among the first chains to implement a multi-year roadmap for sharding (splitting a blockchain into pieces or shards and storing those pieces in different places)
- The Tron foundation has launched the DAppChain, a side project for the Tron mainnet
- Ethereum's ecosystem includes L2s, sidechains, and future roadmap includes sharding and other improvements as mentioned in Section 2
- Avalanche's Primary Network and Cosmos' Atom Hub both have their own validator sets for their security. By default, any new blockchains launched in each of these ecosystems must provide their own means of security. However, as mentioned, there are (or will be) means to incentivize and/or, purchase security from within their respective ecosystems.
- There are multiple validators sets that secure subnets comprising the Avalanche ecosystem. However, every subnet validator must also validate the Primary Network. In other words, although the Primary Network may not directly secure subnets, subnet validators do contribute to the security of the Primary Network.

Another important differentiating factor to consider is how the Polkadot relay chain interacts with its parachains. In short, the relay chain aims to be a "Layer-zero" (L0) blockchain, serving as a basis for protocols, or "parachains" like Acala and Moonbeam to safely interoperate. Polkadot's hub-and-spoke approach where all validators validate all parachains may provide a more secure alternative to the problematic cross-chain "bridges" that are currently employed to transfer and receive data between completely independent blockchains. As mentioned earlier, the Polkadot relay chain will be referred to as a L1 for the purposes of this report.

> *"... when we talk about Layer Zero, what we mostly mean is that like Polkadot itself provides context to a bunch of layer ones... [parachains] are independent chains that are 99% sovereign. They have their own tokens... own governance models [and] they can choose when to upgrade"* – Joe Petrowski, Web3 Foundation (interview by The Block, October 2022)

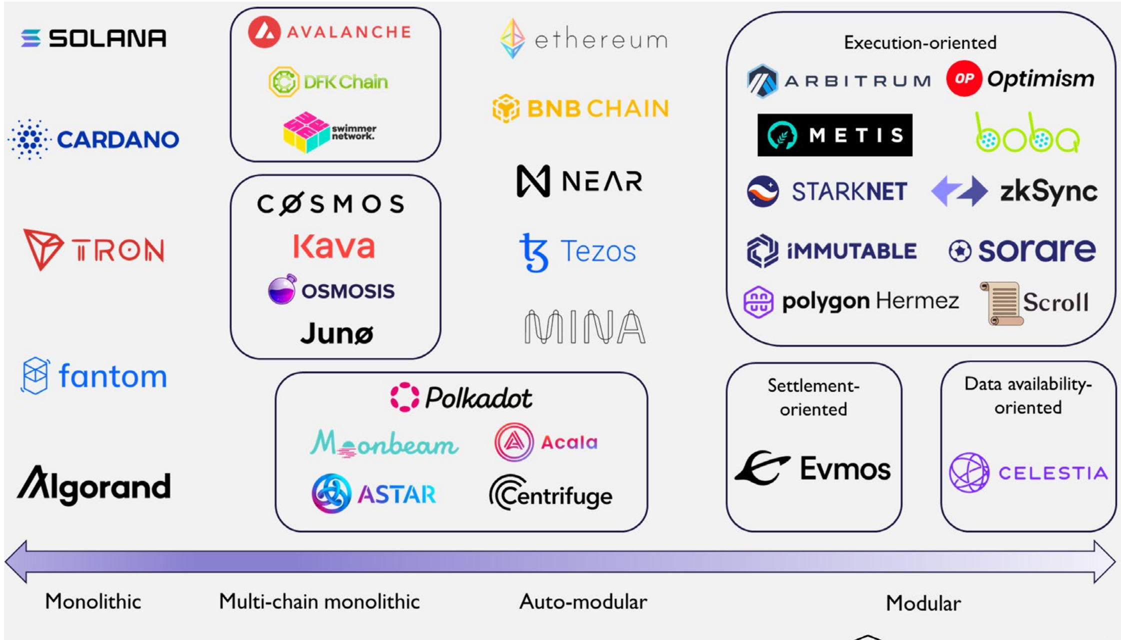
In all, the multitude of above approaches towards security for multichain ecosystems may present an opportunity for a robust validator economy/marketplace for independent operators.

Monolithic vs. Modular Architecture

The use of multiple chains and different validator setups also relates to the concepts of blockchain modularity and task chains, but in a different way from how it relates to app chains.

While both app chains and task chains may require their own validator sets, it doesn't mean they are the same thing. While app chains are typically built using the software stack of a multichain L1 platform to serve specific applications (e.g., dYdX chain built using Cosmos SDK), task chains are built to serve specific blockchain functions. They can be used in an application-specific or application-general context (e.g., Celestia general-purpose data availability layer and general-purpose rollups). Furthermore, their aims are different: app chains are built to serve a specific application while task chains are built for simplification and outsourcing.

The degree to which different L1s utilize in-protocol or third-party task chains to offload execution or other blockchain functions varies much more than ever before. Until recently, all chains took a monolithic "do-it-all" approach, but now most major networks are (re)positioning toward a "divide-and-conquer" approach. The L1 landscape has evolved into a continuum, with different protocols being more monolithic (e.g., Solana) or more modular (e.g., Ethereum, Celestia).



Source: The Block Research

To understand why once-purely-monolithic L1s may be shifting toward more modular designs, let's consider the pros and cons of each approach.

Modular Designs: Pros and Cons

Modular chains are chains that handle a subset of the main blockchain duties while outsourcing the rest to other protocols. While there are various ways to categorize these duties, the following four-layer model popularized by Celestia is useful for understanding how blockchain modularization can work:

Layer	Responsibilities
Execution	o Execute transactions o Produce new state commitments
Settlement	o Establish transaction correctness (finality) o Facilitate communication across execution layers
Consensus	o Reach agreement on transaction ordering
Data Availability	o Attest to availability of transaction data o Provide transaction data on demand

Source: The Block Research
THE BLOCK · Research

Modular designs in one way or another outsource some of these layers to different chains, with the main advantage being the freedom from constraints associated with trying to do everything on one chain.

Pros

- **Scalability**: When Vitalik proposed the "blockchain trilemma" idea, he noted that it applies only "if you stick to 'simple' techniques" – excluding advanced techniques such as sharding and rollups. But, now we've seen the potential of modularizing execution with rollups, which can increase scalability while preserving decentralization and security by relying on Ethereum for data availability, consensus, and settlement. While there is still the challenge of sequencer centralization, popular rollup protocols plan to progressively decentralize and phase out centralized sequencers as the systems mature. As for sharding, protocols like Near demonstrate the potential of sharding for scalability. Together, such protocols demonstrate that distributing execution resources is a powerful scaling strategy.
- **Simplicity**: By being responsible for only a subset of blockchain duties, a modular chain can be much easier to build and deploy. Proponents argue that it should be as easy to deploy a modular blockchain as it is to deploy a smart contract. No one involved in building a modular chain needs to know everything about the whole stack, allowing efficient devops that don't require individuals with comprehensive blockchain knowledge. For example, developers can focus solely on execution without worrying about how to get security right (e.g., distribution of tokens in PoS; distribution of miners in PoW).
- **Flexibility**: By moving away from a shared hosting provider, modular chains have more degrees of freedom when it comes to tradeoffs and design decisions. For example, modular chains can leverage the resources of distributed execution environments, as in the case of Ethereum, when it is used only for security and data availability while outsourcing execution to rollups. In this case, Ethereum only needs to validate off-chain execution and guarantee the availability of off-chain data. Likewise, a scalability-optimized rollup (execution layer) benefits from the security properties of whichever parent chain it chooses.

Cons

- **Complexity**: Modular blockchains introduce a new level of complexity, as different modules need a way to communicate efficiently and securely. For instance, Ethereum's plan for sharding (estimated shipment in 2023) relies on complex mechanisms (i.e., randomly-sampled attestation committees; data availability sampling) to verify the availability of high volumes of data without requiring any single node to download all the data. Likewise, execution layers like optimistic rollups (e.g., Arbitrum, Optimism) require dispute resolution mechanisms to validate fraud proofs, detect fraudulent transactions, and dissuade bad behavior. Validity rollups (e.g., zkSync, Starkware, Aztec), on the other hand, require validity proofs to prove that state changes included in the proof are valid. Without these measures, the security layer (e.g., Ethereum) cannot be confident about the validity of the off-chain state transitions.

- **Security**: Modular blockchains rely on the security of the modules they outsource work to as well as the interoperability protocols that link the modules. If one protocol in this mesh of protocols fails, it could bring about systemic failure. For example, bridge protocols have a notorious history of exploits due to both programmatic and human error. Also, rollups rely on the security properties of whichever parent they are tied to. Each module and each link between modules presents potential insecurities to the system as a whole.

- **Division**: Modularity means that blockchain transactions have to go through multiple separate systems, with each system introducing different communities, network participants, fee systems, token economics, and so forth. The division of systems may create inefficiencies and security vulnerabilities that pose a risk to long-term stability. Furthermore, dependence means that the global network can't be spun up by a single smart contract, restricting some use cases.

Monolithic Designs: Pros and Cons

A monolithic chain is one where nodes are responsible for all blockchain duties – data availability, consensus, settlement, and execution. While modular chains attempt to break down a blockchain system into simpler modules, a monolithic chain attempts to build a global shared computer à la the original vision of Ethereum as a "world computer."

Pros

- **Composability:** Perhaps the main benefit of monolithic designs is that the network doesn't need to be split, making composability (the "LEGO block" feature of blockchains) easier. In other words, it is easier for different DApps to talk with each other when they are all on one monolithic network. When a network is split into modules, complications may be introduced that introduce risks or limit certain use cases. For example, transaction asynchronicity in a sharded network may stymie flash loan strategies that require borrowing and lending within a single transaction. Or, one DApp may wish to build upon another DApp in a secure monolithic environment, but that latter DApp has introduced potentially systemic risks by utilizing a centralized modular chain.
- **Security**: A global shared computer means that a monolithic design enforces its own security. Nodes can see all transactions executed on-chain, validate them, and agree upon their ordering. There is no issue of dependence where one chain must trust another chain for security. There is also no data availability problem, since all transaction data is stored redundantly across nodes that operate both execution and security functions. In contrast, in a modular system, an off-chain execution layer (e.g., L2 rollups) could hide transactions but still be validated if there is no way to know about the hidden transactions (e.g., due to data unavailability).
- **Familiarity**: Currently, developers may find it simpler to design and implement monolithic designs, as there are years of learning history working with monolithic designs (e.g., all modern operating systems

are based in monolithic designs). Modular designs are much more experimental and may present unwanted risk and guesswork in the design process.

- **Token Value**: By handling many duties within one system, the native token of monolithic blockchains has many opportunities to be useful, accrue value, and attract network participation. In contrast, native tokens of modular chains may have fewer possible applications, and thus less opportunity to accrue value and attract network participants.

Cons

- **Scalability**: Scalability is constrained by the resources of a shared hosting provider. The nodes in the network may limit scalability due to storage and bandwidth constraints, and measures to increase scalability by increasing data throughput (e.g., block expansions, block time reductions) impose costly hardware requirements that may drive increased centralization and security risks. Also, having every node process transactions (i.e., redundant re-execution) causes network congestion that limits throughput and drives up gas prices.

- **Limited choices**: What can be deployed on a monolithic blockchain is limited by the execution environment of that system and its shared smart contract platform. In contrast, apps using modular systems could have a wide range of choices in terms of how to derive security and what environments to execute transactions. However, apps built on monolithic chains have the advantage of being able to call resources across the whole network with a smart contract if needed.

- **Storage issues**: Storing transaction data on-chain means that monolithic blockchains have increasing data requirements over time. To deal with this issue, blockchains with large historical datasets like Bitcoin and Ethereum already support block file pruning to reduce disk requirements. EIP-4444 proposes to force Ethereum clients to stop serving historical block data older than one year on the p2p layer. The problem is that large blockchains mean higher hardware requirements – again, more centralization pressure. In contrast, in a modular design, historical data could be stored off-chain (e.g., Filecoin/IPFS) and data availability could be handled by a modular chain specifically designed for it (e.g., Celestia).

Regarding where any given chain lies on the monolithic-modular spectrum, we group network architectures into four categories ranging from fully monolithic to fully modular:

Monolithic: A blockchain that handles all four core blockchain duties – data availability, consensus, settlement, and execution – without outsourcing to any third-party blockchains.

Pseudo-modular: A monolithic blockchain that doesn't rely on outsourcing blockchain duties, but splits the single network into multiple parts (e.g., Polkadot), with subnetworks that are bound and dependent on the single network.

Proto-modular: A monolithic blockchain that outsources at least one component of the stack to a modular blockchain (e.g., Ethereum outsourcing execution to rollups while retaining the ability to handle execution itself).

Modular: A blockchain built for handling a specific task(s): data availability, consensus, settlement, or execution. Modular blockchains cannot handle all of these blockchain duties by themselves (e.g., Celestia).

Note that a blockchain's network classification here is likely to change with protocol upgrades and ecosystem developments.

Other Notable Blockchain Design Criteria

Validator selection process: Block production normally occurs within a subset(s) of the validator pool available in a PoS network. How block-producing validators are selected can vary significantly across networks. This selection process may be purely random (Algorand) or in some cases, the users may vote for specific validators using their native tokens to bias the selection process (delegated proof of stake; dPoS). This process for periodically sampling a smaller set of validators for block production reduces the communication overhead between nodes, thereby accelerating consensus. The PoS networks highlighted in this report all comprise a pool of nodes with the capacity to produce blocks (validators) for block production

Finality: Finality refers to the length of time users must wait before there is reasonable assurance that their transactions are final. Finality is dependent on a consensus mechanism and may be probabilistic or deterministic. For example, the Nakamoto consensus in pre-Merge Ethereum requires enough subsequent blocks to be constructed such that the likelihood of an invalidated transaction later becomes negligible. In contrast, consensus mechanisms that have deterministic finality rely on specified fault-tolerance thresholds where transaction finality is often achieved when two-thirds of the active validator set testify to a block's validity.

The number of nodes in a network can also affect the time to transaction finality. For example, new Bitcoin blocks must reach all nodes after they are validated, where each node must broadcast the new state to all of its peers. On average, a Bitcoin node takes an estimated 12.6 seconds to see a newly mined block. On that front, Avalanche's novel Snowball consensus mechanism uses a "repeated random subsampling" that aims to maintain transaction finality speeds regardless of the number of validators in the network.

> *"... classical consensus can't scale past [a certain number] of nodes... Avalanche is decidedly different because it maintains its sub-second finality at [~1200] validators... and there's* ***no reason that [validator count] can't continue to grow orders of magnitude without sacrificing the [time to] finality.****"* – Luigi Donorio Demeo, Ava Labs (The Block interview, November 2022)

Safety vs. Liveness: For consensus mechanisms that favor safety, inability to establish consensus will cause the network to suspend block production until a predetermined portion of the validators are able to come to an agreement. On the other hand, networks that favor liveness will continue block production to execute transactions that won't achieve finality until they are provably audited. Algorand, Solana and Cosmos are examples of networks that favor safety over liveness, whereas Ethereum and Polkadot favor liveness. Readers are encouraged to refer to The Block's 2021 L1 landscape report for more details on the above concepts.

Comparison of Network Architectures

What is clear from this discussion is that the L1 landscape today comprises a variegated set of blockchain architectures. Currently, there is no single approach that has proven better than the rest, but we can at least notice that a lot of chains are shifting toward modularity – most likely in an effort to scale without losing security and decentralization. The table below summarizes some of the more significant design parameters for each of the L1s selected for comparison. Note that the following is a representation of how each L1 is currently implemented and does not include planned upgrades.

The combination of all the design choices for a blockchain under the hood will determine its performance in the real world. Transaction throughput and the time to finality are two critical factors for quantifying blockchain performance. We discussed transaction finality earlier, as the time needed for a transaction to be considered irreversible. Transaction throughput is the number of transactions a network can process in a given period of time, commonly measured in transactions per second (TPS).

TPS measurements on a network's public mainnet give the highest confidence in its capabilities. There are large differences in recorded mainnet TPS across the networks selected for analysis, ranging from Cardano at ~16 TPS to Solana at ~100,000 TPS. However, there are some caveats to these numbers depending on the specifics of a network. For example, Cardano's EUTXO model allows for batching of transactions, meaning real-world TPS may be significantly higher than 16. Similarly, Solana's consensus mechanism requires voting messaging between validators, which means its real-world TPS values may be overstated unless only the "non-vote" transactions are counted.

There is also significant room for increased scalability for some of these networks. As mentioned earlier, Ethereum is expected to achieve ~4,000

Design of Selected Smart Contract Platforms

Platform	Sybil Resistance	Consensus Algorithm	Network Architecture	Modularity	Security(1)	VM / Language	Block Time (s)
Algorand	PoS	Pure-PoS	One Validator Set, One Chain	Pseudo-modular	Global	Algorand VM (TEAL, Reach)	5
Avalanche (C-Chain)	PoS	Snowball	Multiple Validator Sets, Multiple Chains	Pseudo-modular	Variable	AVM (Go), Athereum-EVM	2[2]
BNB Smart Chain	PoA/dPoS	Proof of Staked Authority	One Validator Set, One Chain	Pseudo-modular	Global	EVM (Solidity, Vyper)	3
Cardano	dPoS	Ouroboros	One Validator Set, One Chain	Monolithic	Global	(Plutus)	20
Cosmos Atom Hub	PoS	Tendermint BFT	Multiple Validator Sets, Multiple Chains	Pseudo-modular	Variable	WebAssembly / Cosmos SDK	7
Ethereum L1	PoS	Gasper	One Validator Set, Multiple Chains	Proto-modular	Shared	EVM (Solidity, Vyper)	12
Near	PoS	Nightshade	Multi-chain (Shards)	Pseudo-modular	Global	NearVM(Rust) Aurora-EVM	1.25
Polkadot (Relay Chain)	PoS	Grandpa/Babe	One Validator Set, Multiple Chains	Pseudo-modular	Shared	WebAssembly, Substrate	6
Solana	PoS	Tower BFT	One Validator Set, One Chain	Monolithic	Global	Sealevel (Rust)	0.4
Tron	dPos	dPos	One Validator Set, One Chain	Pseudo-modular	Global	TVM (Solidity, Vyper)	3

Notes: The above is a representation of how each L1 is currently implemented and does not include planned upgrades. Actual block times across all networks could vary substantially depending on network usage dynamics. Blockchain design parameters across the Ethereum, Avalanche, Polkadot and Cosmos multichain ecosystems is expected to vary greatly depending on the specific characteristics within each L2, subnet, parachain or, zone, respectively. PoS - proof-of-stake, PoA - proof-of-authority, dPoS - delegated PoS.

(1) Security on each Zone and Subnet for the Cosmos and Avalanche ecosystems, respectively, is labeled as "variable" because security can either be provided independently by each sovereign chain or leased from other entities in the ecosystem.

(2) Avalanche C-Chain allows asynchronous block issuance that targets every 2 seconds but varies depending on several factors such as the number of transactions waiting to be included in a block.

Source: The Block Research, platform whitepapers & websites.

Data as of 12/1/22.

THE BLOCK · Research

TPS with rollup-centric scaling in its current state. Estimates for network performance under idealized (testnet) conditions are also often published. Testnet transaction throughput provides medium assurance for a network's potential performance. However, it must be noted that testnets by definition abstract away the intricacies of a public environment, and thus are likely to overestimate performance in comparison to mainnet.

Qualitative estimates from a project's development community provide the lowest level of assurance on the production capabilities of a platform. However, theoretical estimates for some architectures that are yet to be tested in a production environment (e.g. Ethereum data sharding) often represent the best available data point. Quantitative analysis for smart-contract platform performance is beyond the scope of this report and readers are encouraged to refer to The Block's dedicated report on blockchain settlement for further details on this topic.

Solana's Network Outages

Solana has suffered a series of outages over the past year or so. In September 2021, block congestion (peaking at ~400K TPS) caused the network to go offline for about 17 hours. Similarly, in May 2022, Solana Mainnet Beta lost consensus after being flooded by inbound transactions (~4M TPS, surpassing 100 Gbps, according to Solana), requiring a validator cluster restart. In June 2022, the network ceased producing blocks for about four hours as a result of stalled consensus caused by a bug in the durable nonce transactions feature. Moreover, the network showed degraded performance in January, March, April, and May.

What's going on? The biggest issue is that Solana has faced some of the highest demand of any L1 blockchain (>1M TPS). And sometimes the protocol is not prepared for such extreme conditions. For example, in the September 2021 event, a mechanism was not in place for prioritizing network-critical messaging during the unexpected deluge of transaction requests.

Note however, that issues handling extremely high volumes is not only a Solana issue. Solana just happens to be the chain that handles high volumes regularly. Also, Solana is known to roll out upgrades in beta to speed up development. Other popular chains, including Ethereum and Avalanche, have faced network slowdowns during periods of extreme usage, though such occurrences are relatively rare.

> *"Blockchains are complex things, **built by human beings, but run by machines**. An issue that was small enough to bypass during an initial inspection **can snowball as a network grows**."* – Patrick O'Grady, Engineer at Ava Labs (Medium, February 2021)

However, Ethereum's liveness failure issues are not about bugs or transaction overload per se, but rather its transaction fees soaring during periods of extremely high volume. Buterin himself once said that "$50 fees should IMO count as a de-facto liveness failure." Then, one can argue that the Ethereum network has been "down" for a large portion of potential users for several extended periods of time.

What is Solana doing about it? As for bugs causing failure in edge cases, this is something Solana acknowledges shouldn't happen. And, they are in the process of shipping new network upgrades to try to prevent these situations. For example, their new QUIC-based networking technology should make the network and validators more resistant to spam (e.g., to prevent degraded performance from spam attacks like that which happened back in January). Also, Firedancer, a second Solana client could provide a long-term fix, according to Solana co-founder Anatoly Yakovenko. For more information on Solana's network upgrades, see this report's section on Major Technical & Ecosystem Updates.

On other fronts, Solana notes the tradeoffs of any PoS system, which is that if they get into a place where they can't recover themselves, they require human (validator) intervention. While it's not ideal, it is one of the tradeoffs to the security granted by PoS systems, and it can happen to any PoS system (e.g., it happened to Ethereum's PoS in testnet too).

> *"The default state of Solana **when it runs into something it can't resolve is to not continue advancing.** The network design chooses **security over liveliness** intentionally. [To keep the state safe] when the chain can't reach consensus, don't try to keep going, **wait for human intervention.**"* – Austin Federa, Head of Communications at Solana Foundation (The Block Interview, October 2022)

On-Chain Data

Ecosystem maps are often designed to look flashy, but the value they provide may be limited. Most deployed DApps have little-to-no user traffic (or maybe they're mostly bots) and long-term viability of select DApps is uncertain as the ability of their individual founders and team members to implement their development roadmaps is not guaranteed. In this report, we instead focus on metrics that quantify the health and growth of the L1 ecosystem as a whole. To that end, we extracted data for the following critical metrics: 1) daily active wallet addresses, 2) daily transaction counts, 3) daily total transacted value, 4) average daily fee paid per transaction, 5) daily aggregate fees paid by users and, 6) total value locked (TVL) across DeFi applications in each respective ecosystems.

L1 ecosystems and their architectures are becoming increasingly more diverse as mentioned above (e.g., generalized vs. multichain as well as, monolithic vs. modular). Moreover, many of these chains have also announced roadmaps that may include significant alterations to their architectures moving forward (e.g., Ethereum's roadmap). It is thus a difficult task to separate these ecosystems into discrete categories.

Thus, for each of the above critical metrics, we assessed the core asset for each L1 ecosystem, which includes ETH, DOT, AVAX, and ATOM for Ethereum L1, Polkadot, Avalanche and Cosmos, respectively. We acknowledge this is not a comprehensive look at these multichain ecosystems, but these core ecosystem assets arguably serve as a relevant proxy for the growth of their respective ecosystems. For example, DOT tokens are required to be bonded for every parachain auction, and AVAX staking is required for all validators in the Avalanche ecosystem. Although value accrual mechanisms for the ATOM token have previously been unclear, the recently announced roadmap for ATOM 2.0, may ensure the sustained significance of the Cosmos Hub and the ATOM token within the ecosystem.

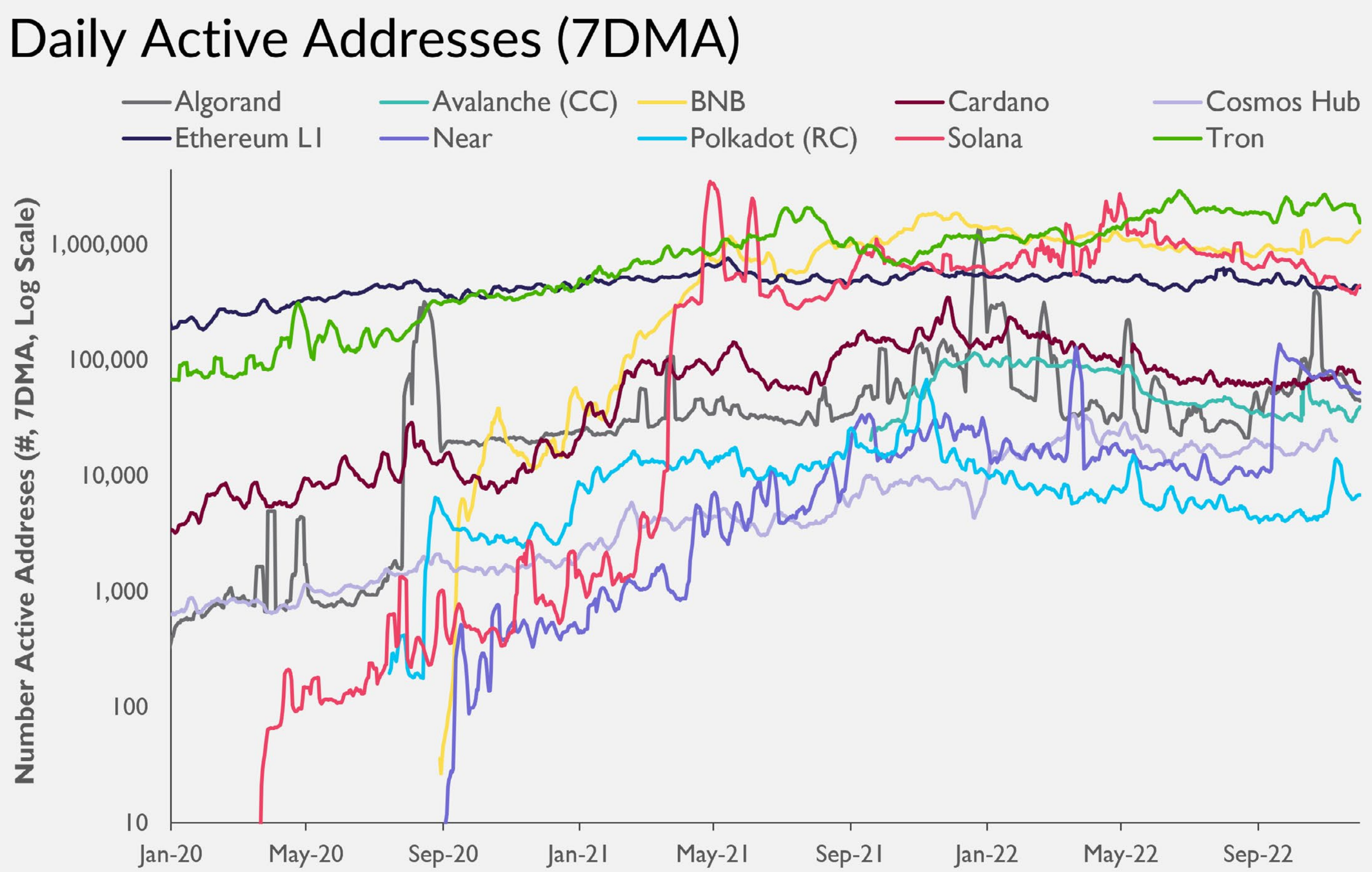
Additionally, we also present data comparing a sample of blockchains constituting the Avalanche (DFK & Swimmer subnets), Cosmos (Axelar & Osmosis), Ethereum (Arbitrum, Optimism & Polygon) and Polkadot (Acala

& Moonbeam) multichain ecosystems. It is worth noting that Polygon's PoS chain (native token MATIC), sometimes referred to as a "commit chain," has its own independent validator set, where staked/delegated MATIC is managed on Ethereum L1 mainnet. Polygon PoS chain also periodically commits network checkpoints to Ethereum L1, leveraging its security guarantees to some degree. Thus, Polygon PoS chain has properties of both a side-chain and an Ethereum L2 scaling solution. For the purposes of this document, we considered the Polygon PoS chain as a component of Ethereum's ecosystem.

> *"We think of [scaling Ethereum] as a whole spectrum. On the left extreme of the spectrum are fully sovereign chains with simple bridges to Ethereum... i**n the middle you will find something like Polygon PoS**... it checkpoints to Ethereum but that checkpoint contains less information [than a layer-2] ... On the right extreme you will find the pure layer-2s [rollups] which are actually putting both their data and the dispute resolution related to the data on Ethereum"* – Sandeep Nailwal, Co-Founder at Polygon Technology (Bankless Podcast, November 2021)

Active Addresses

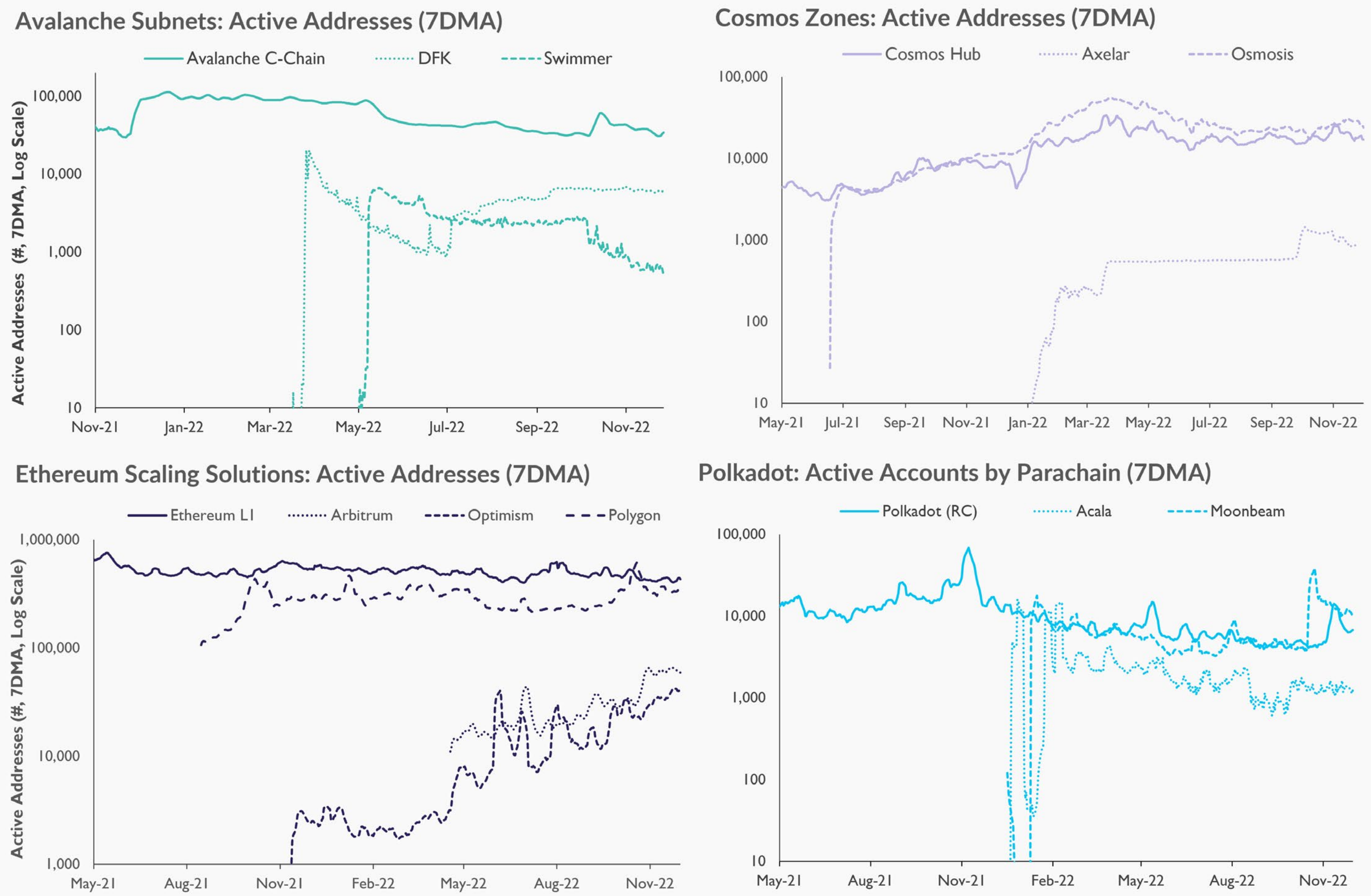
Daily active addresses indicate the total number of unique addresses that were involved in a transaction in the network that day either as a source or a destination. Depending on the underlying protocol, these transactions may involve block signatures, claiming staking rewards, voting, account creation, and other actions. Since active addresses are less sensitive to network stress tests, they are a common proxy for the number of users on a blockchain. However, we should also note that active addresses can be manipulated on blockchains, where address creation and/or transaction costs are inexpensive or free. Thus, it may not be possible to know exactly what percentage of daily active addresses are bots, especially in some low-cost chains.



Notes: Data represents 7-day simple moving average (DMA). Active addresses is the sum count of unique addresses that was either a destination or, source of a ledger change for each day. All parties in a ledger change action (source and destination) are counted. Individual addresses are not double-counted if previously active in the same day. BNB refers to BNB Smart Chain. Data from multi-chain ecosystems refer only to the Cosmos ATOM hub, Avalanche C-chain (CC), Polkadot Relay chain (RC) and Ethereum L1.
Data through 12/1/22
Source: The Block Research, Subscan, Coinmetrics & Gokustats.
THE BLOCK · Research

We can see an overall uptrend in active addresses across these L1s during the measured period, which slows down around the beginning of 2022. Also, while Ethereum is still dominant in terms of number of active addresses, other chains have started catching up. Notably, in the middle of the bull run last year, Solana and BNB Smart Chain (BNB) saw exponential growth in number of daily active addresses, meeting and, at times, exceeding the number of daily active addresses on Ethereum. Between October 1 to 10, Solana had on average ~35% more daily active addresses (666,118) than Ethereum (492,255) while BNB Chain had ~86% more daily active addresses (853,054).The Tron ecosystem has seen sustained growth in active addresses starting from ~70k in Jan, 2020 to about ~2.5M as of writing, the highest among the 10 networks compared in this report.

Multichain Ecosystems – Are they Getting Any Traction?



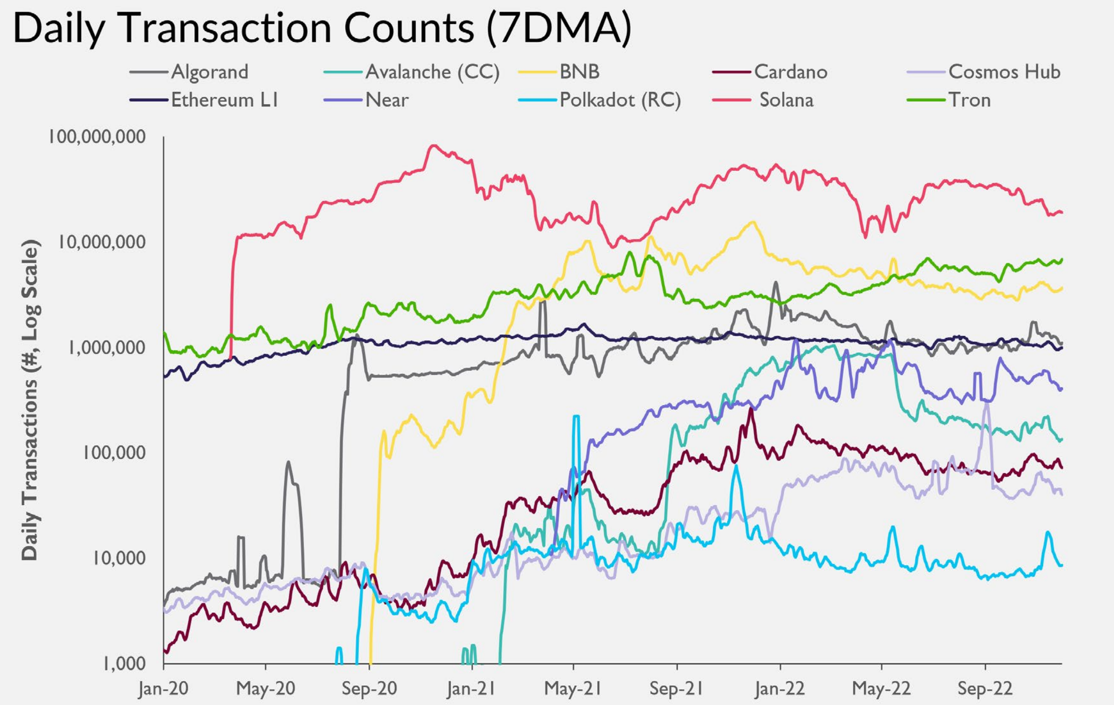
Notes: Data represents 7-day simple moving average (DMA). Data presented for a sample of hubs, parachains, subnets and L2s for the Cosmos, Polkadot, Avalanche and Ethereum ecosystems, respectively. Polkadot Relay chain (RC) and Acala data represents the "daily active account" as reported by Subscan.io. Whereas data for Moonbean represents unique addresses that were active on the network as a sender or receiver as reported by Moonscan.io
Data through 12/1/22
Source: The Block Research, Coinmetrics, Subnets.avax.network, Subscan.io, Moonscan.io & Gokustats.

THE BLOCK · Research

There are signs of sustained usage across the various multichain ecosystems discussed in this report, as seen in the figure above highlighting a sample set of chains within each. For example, the Osmosis chain (dominant DEX in the Cosmos ecosystem) has had consistently greater unique daily active addresses since November 2021, relative to the Cosmos ATOM hub. It is also interesting to see a sustained growth in daily active addresses and interest for the L2 scaling solutions, Arbitrum and Optimism, in the Ethereum ecosystem, despite the recent market downturn from early 2022.

Daily Transaction Counts

Daily transactions represent the number of transactions processed by each chain on a given day. Depending on how a network defines a transaction, these values can vary substantially and range from thousands of transactions to tens of millions.

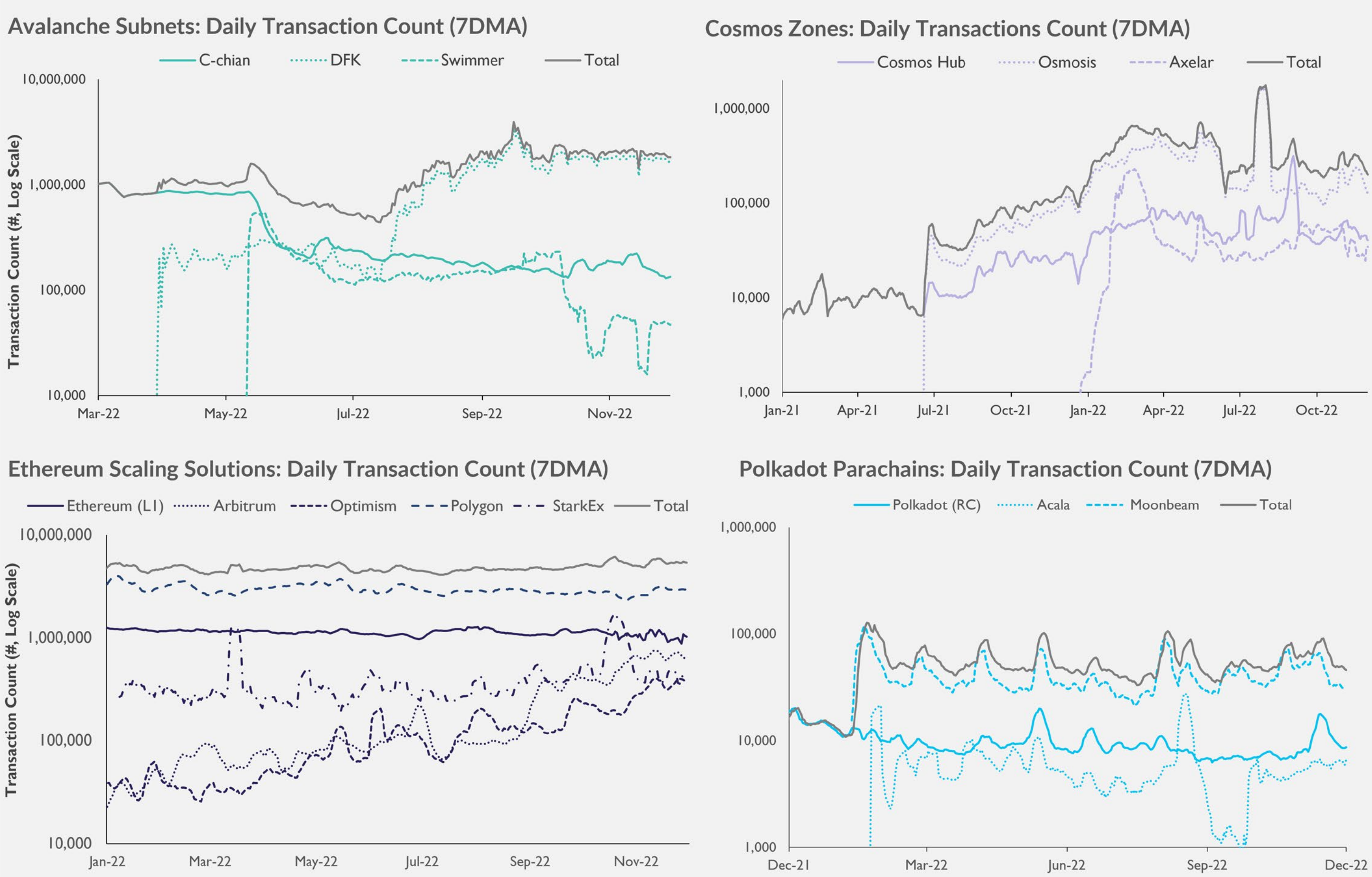


Notes: Data represents 7-day simple moving average (DMA). BNB refers to BNB Smart Chain. Data from multi-chain ecosystems refer only to the Cosmos ATOM hub, Avalanche C-chain (CC), Polkadot Relay chain (RC) and Ethereum L1. Polkadot RC data represents the "daily extrinsic number" as reported by subscan.io
Data through 12/1/22
Source: The Block Research, Gokustats, Subscan & Coinmetrics.

Here, we see the volatile nature of transaction counts over time in alt-L1s when compared to Ethereum, where daily counts have remained steady for the past two years. There is also a noticeable uptrend among several chains during 2021 bull market conditions – including Cardano, Near and BNB Chain. Whereas the 2022 bear market conditions may have produced a general decrease in daily transactions across a few of the ecosystems. Notable exceptions include two of the key players in the multichain ecosystems: Cosmos and Avalanche. For example, from January to September 2022, daily transaction counts in the Cosmos Hub increased ~34% from 50,662 to 67,727, on average, and Avalanche C-Chain daily transaction counts increased ~195% from 769,165 to 2,270,247, on average.

One approach for scaling a multichain ecosystem is the offloading of transaction processing/execution to related chains, thereby improving overall ecosystem throughput. In the figure below, we see an example in the Avalanche ecosystem where throughput may be maintained by diverting high-volume transactions to its subnets and away from the C-Chain. The DeFi Kingdoms (DFK) and Swimmer Network subnets together have accounted for the majority of Avalanche transactions since August 2022. Similarly, we generally see an increasing trend for transaction counts for chains within the Cosmos ecosystem.

Scalability via Offloading Transactions to Other Chains?



Notes: Data represents 7-day simple moving average (DMA). Data presented for a sample of hubs, parachains, subnets and L2s for the Cosmos, Polkadot, Avalanche and Ethereum ecosystems, respectively. Polkadot and Acala data represents the "daily extrinsic number" as reported on Subscan.io. Whereas data for Moonbean represents total number of on-chain transactions completed as reported by Moonscan.io
Data through 12/1/22
Source: The Block Research, Subnets.avax.network, Subscan.io, Moonscan.io & Gokustats.

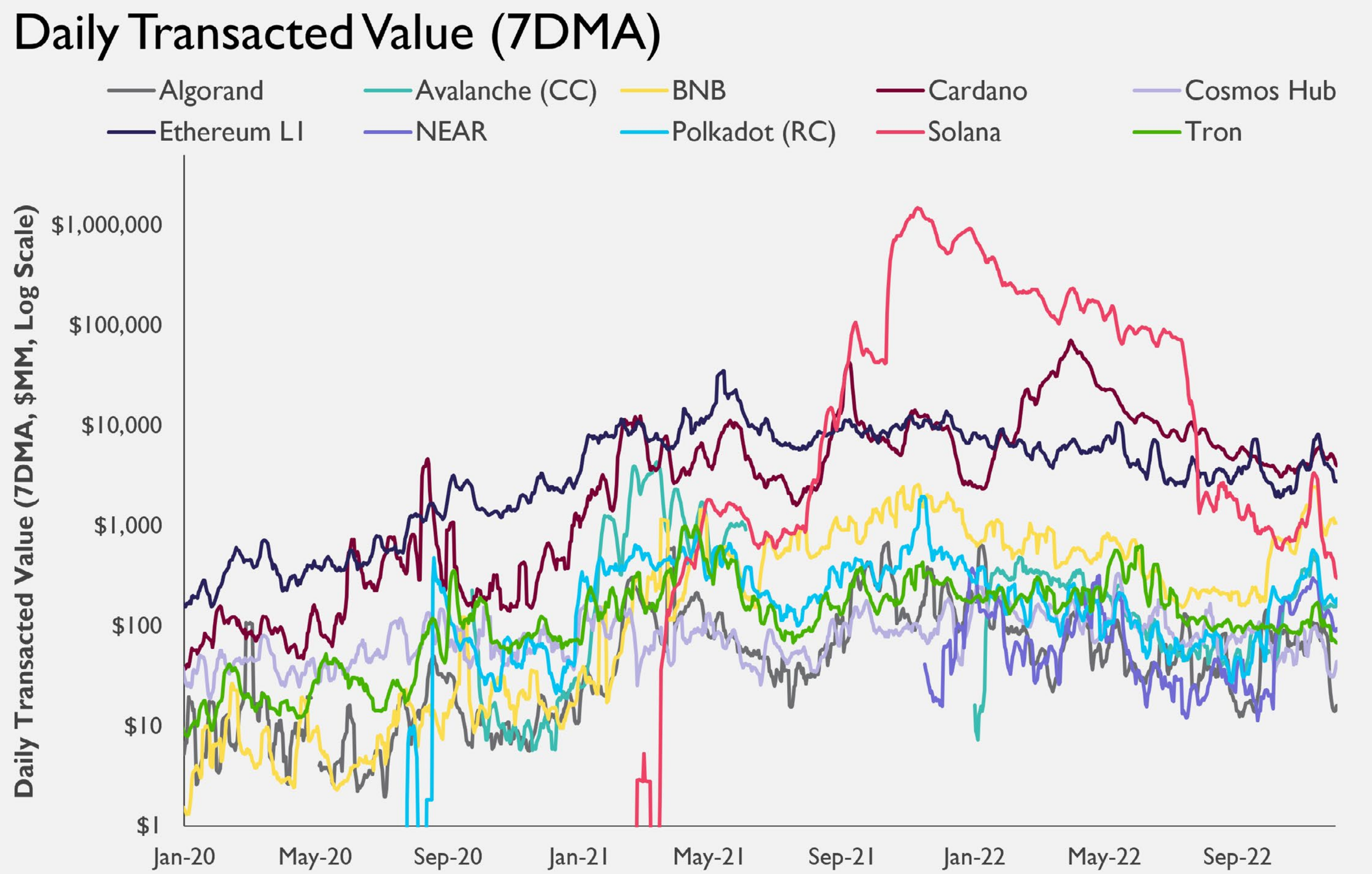
THE BLOCK · Research

Once again, bots may be one reason for the high transaction counts observed, especially in the DFK subnet – ~1.6 million daily transactions and 6,200 active addresses on the DFK Chain correspond to approximately 258 daily transactions per user. However, we do see that the Avalanche ecosystem as a whole was able to successfully process a significant increase in transaction counts since August 2022. Moreover, this increase in throughput did not produce noticeable congestion on the C-Chain where the average fee per transaction remained between $0.09 - $0.13 from August till as of writing in October (as shown later).

Ethereum's L1 has been processing ~1.2 million transactions per day as its network has essentially reached maximum capacity. Both Arbitrum and Optimistic L2s have processed ~10,000 to ~100,000 transactions, whereas StarkWare's StarkEx instances have collectively been processing ~100,000 to ~1,000,000 transactions per day. Polygon's PoS chain is the most widely adopted sidechain as of writing, significantly surpassing Ethereum L1's daily transaction counts. The data also shows a steady increase in the total number of transactions processed by the Ethereum ecosystem since the deployment of its L2 scaling solutions. Ultimately, it remains to be seen how Avalanche subnets, including the C-Chain and other multichain ecosystems like Polkadot and Cosmos will compare against rollup-centric scaling and high-performance L1s (e.g., Solana) with varying architectures for scalability.

Daily Transacted Value

Daily transacted value is the total value in USD that was transacted in an L1's native token on a daily basis. It does not include payment volumes of assets issued on top of these platforms such as, stablecoins and other tokens. Thus, the market price of each protocol's native token significantly affects the values in this chart. For instance, in a bear market, these charts will show depressed USD values even if the network activity levels remained constant.

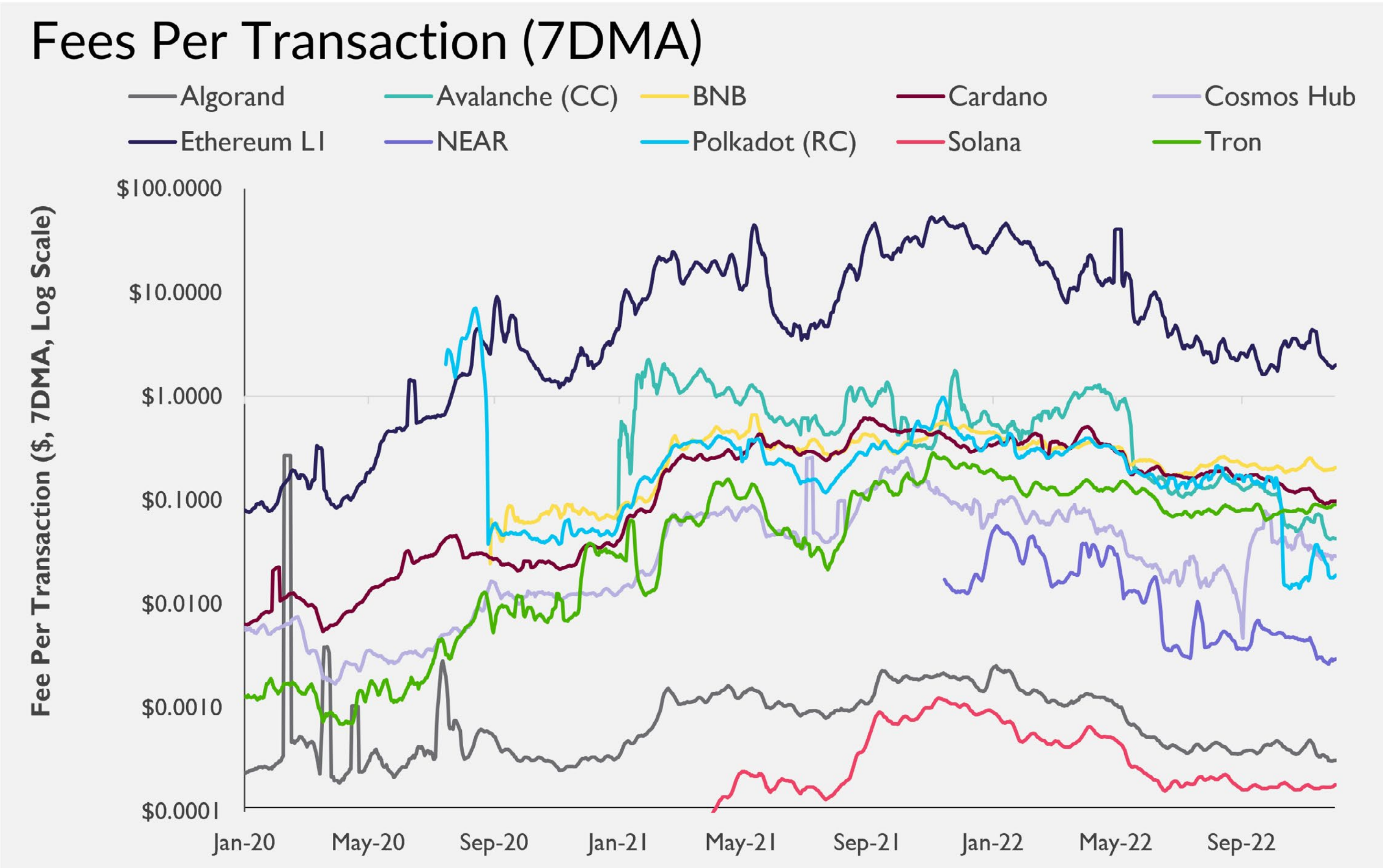


Notes: Data represents a 7-day simple moving average (DMA) presented in millions of USD. Data from multi-chain ecosystems refer only to the Cosmos ATOM hub, Avalanche C-chain (CC), Polkadot Relay chain (RC) and Ethereum L1. BNB refers to BNB Smart Chain.
Data as of 12/1/22
Source: The Block Research, Coinmarketcap, Coinmetrics, Atomscan

While billions of dollars worth of Ether are transacted on the Ethereum network currently, other networks are routinely transferring tens to hundreds of millions of value in their native tokens each day.

Average Fee / Transaction

Fees per transaction represent the average cost to effect a transaction on a given network. Fees paid on an individual transaction vary as a function of network demand and the computational resources ("gas") consumed by an individual transaction.

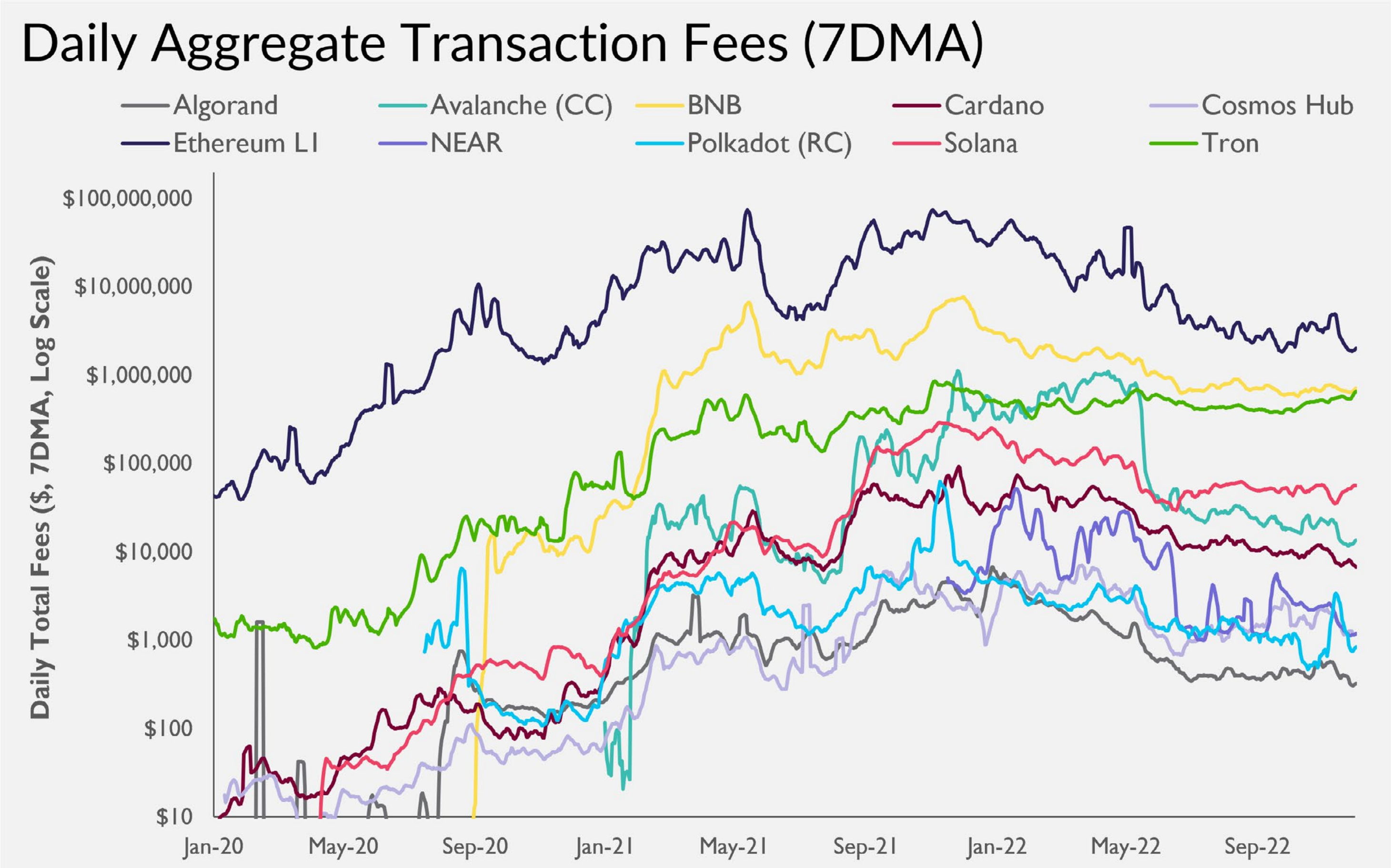


Notes: Data represents a 7-day simple moving average (DMA). Data from multi-chain ecosystems refer only to the Cosmos ATOM hub, Avalanche C-chain (CC), Polkadot Relay chain (RC) and Ethereum L1. BNB refers to BNB Smart Chain.
Data through 12/2/22
Source: The Block Research

Here, we see a general pattern of transaction fees increasing during bull market conditions and decreasing in bear market conditions. We also see great variation in transaction fees between chains, with L1s like Solana and Algorand that prioritize low-cost transactions costing several orders of magnitude less than Ethereum.

Daily Aggregate Fees

Daily aggregate transaction fees are the total amount of fees paid to effect transactions on a given network in a given day. This metric gives us a look into daily on-chain revenue. While Ethereum and BNB Chain have generated millions of dollars worth of fees daily at several periods during the observed period, most other platforms observed were generating hundreds to tens of thousands of dollars daily (e.g., Algorand and Near).

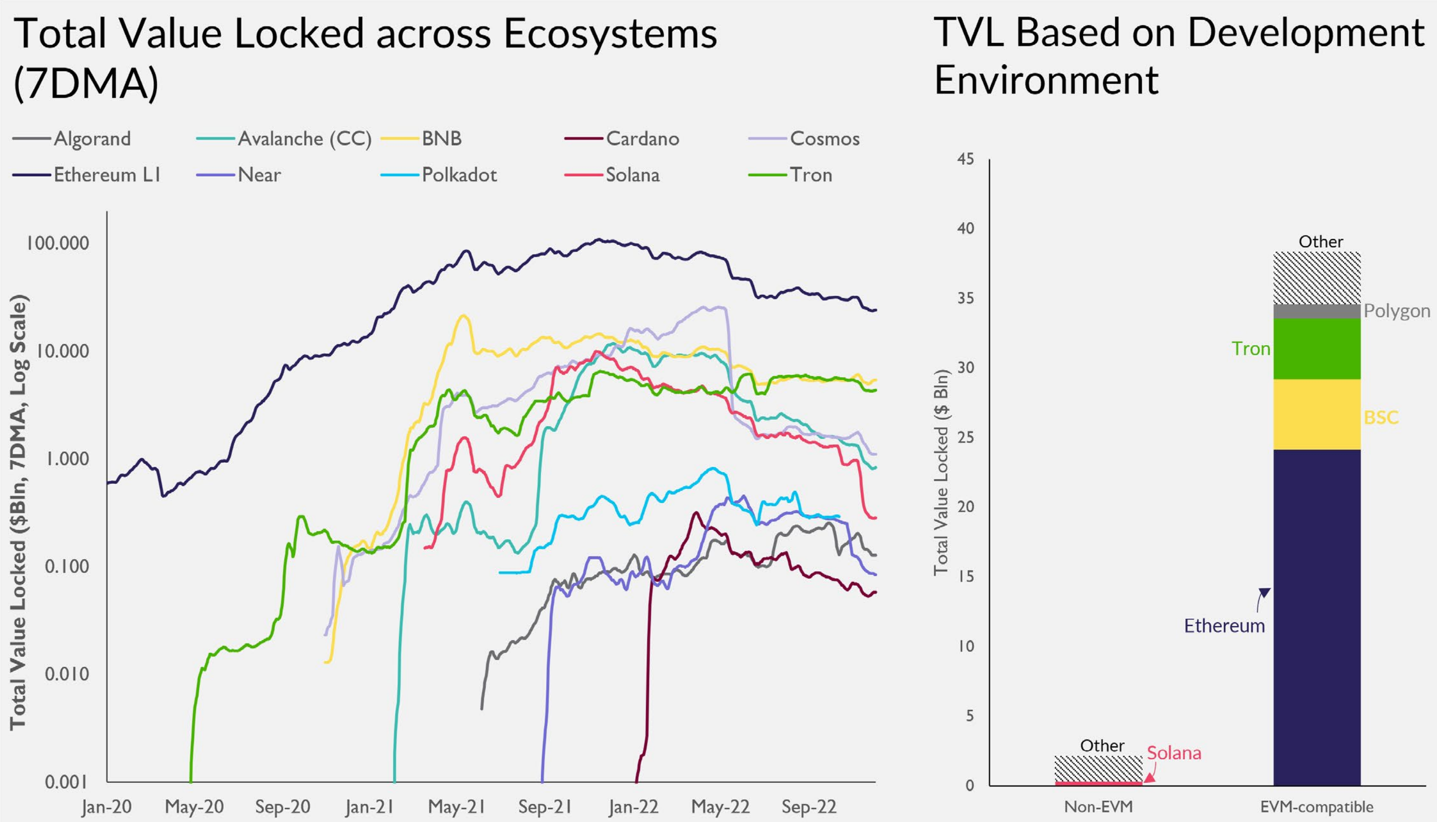


Notes: Data represents a 7-day simple moving average (DMA). Data from multi-chain ecosystems refer only to the Cosmos ATOM hub, Avalanche C-chain (CC), Polkadot Relay chain (RC) and Ethereum L1. BNB refers to BNB Smart Chain.
Data through 12/2/22.
Source: The Block Research

While gas fees are a burden to the ordinary user, they are useful for preventing spam attacks and securing the network. For example, the limited space of an Ethereum block means that in each block, people compete in an open gas fee market to get their transaction included in a block. It is not economically sensible to spam a network where a spam transaction costs several dollars or more. Transaction fees can also be used to reward validator nodes producing blocks and securing the network state. If transaction fees are tiny (e.g., Solana), the network can similarly reward validator nodes and secure the network via token inflation.

TVL Data

TVL in DeFi represents the amounts of funds locked in an L1's smart contracts to facilitate DeFi functions such as exchange and lending. TVL varies substantially based on the capital intensity and efficiency of each of the functions that it is being used to facilitate. It is also important to note that there are no widely adopted standards for measuring TVL, where different data aggregators often report significantly different values for the same ecosystem. Moreover, it is now established that TVL data can be manipulated. Nonetheless, this measure can be used to illustrate the relative size of the DeFi ecosystems across different L1s.



Notes: Data represents a 7-day simple moving average (DMA) for time series data in the left panel. Data from Cosmos ecosystem accounts for 14 Cosmos Hubs and 15 Parachains for Polkadot in the left panel. Data represents TVL for C-chain (CC) in the Avalanche ecosystem and for Ethereum L1 in the left panel. BNB refers to BNB Smart Chain. All y-axis values presented in billions of USD. Data through 12/2/22

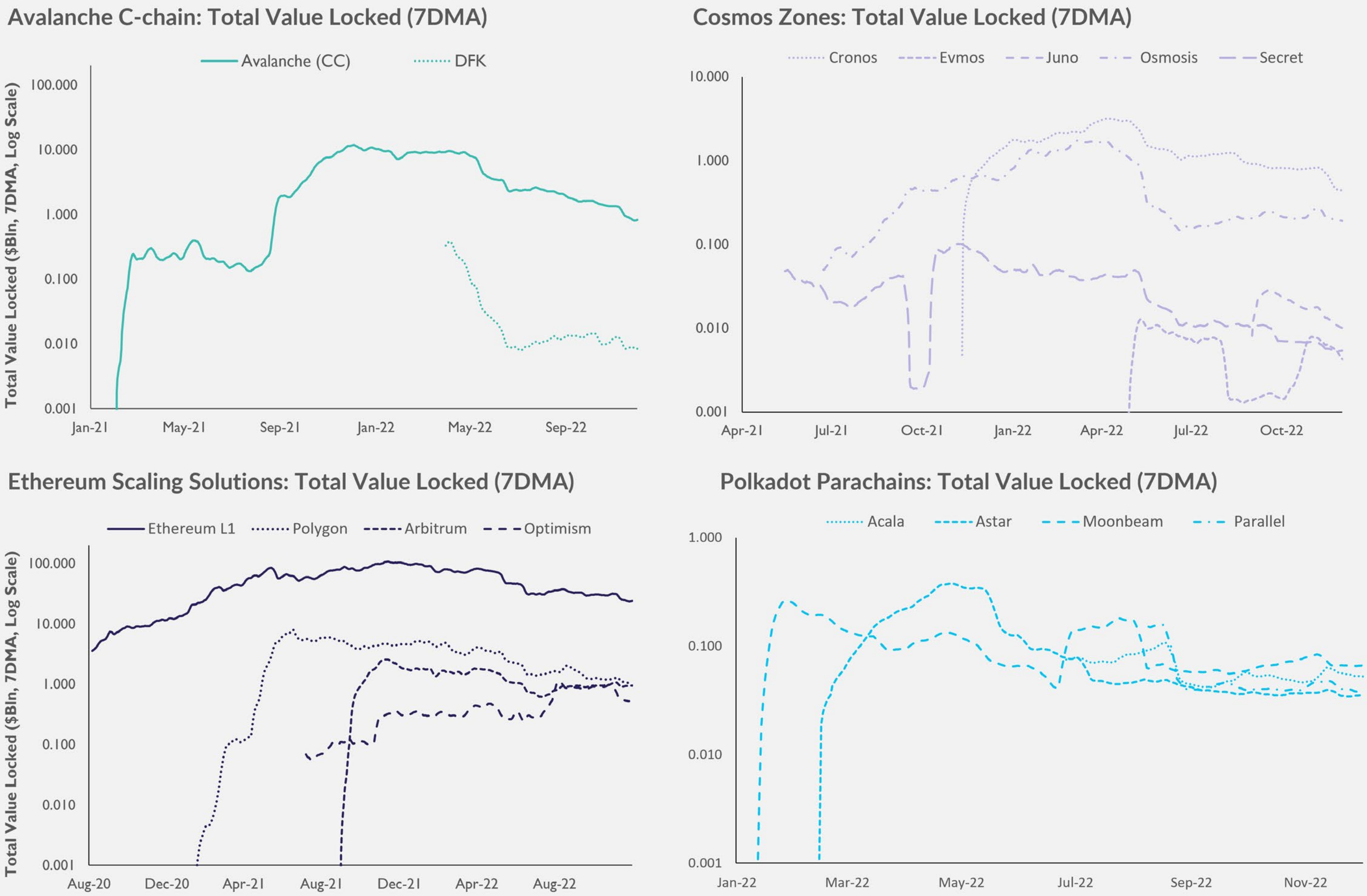
Source: The Block Research, Defillama & Gokustats

THE BLOCK · Research

Here, we can see that Ethereum's TVL is significantly larger than most other L1s, suggesting that its DeFi ecosystem maintains high market confidence and usage despite the high transaction costs in Ethereum L1. However, there is likely to be a relatively high concentration of lost/abandoned capital on Ethereum L1 (due to lost private keys, etc.), however the magnitude of such lost capital is difficult to estimate and compare across ecosystems.

We also see a general decline in TVL across most of the 10 ecosystems presented - TVL in Ethereum L1 decreased from a high of ~$110B USD in November 2021 to ~$32B USD as of writing. This is in part a reflection of the downturn in market conditions affecting the USD value of (nearly) all crypto tokens used in DeFi. Furthermore, the chart on the right shows that EVM-based smart contracts have significant dominance in the DeFi industry, currently holding over tenfold the TVL of non-EVM-based smart contracts.

TVL Growth in Multichain Ecosystems



Notes: Data represents 7-day simple moving average (DMA). Data presented for a sample of hubs, parachains, subnets and sidechain/L2s for the Cosmos, Polkadot, Avalanche and Ethereum ecosystems, respectively.
Data through 12/2/22
Source: The Block Research, Defillama & Gokustats.

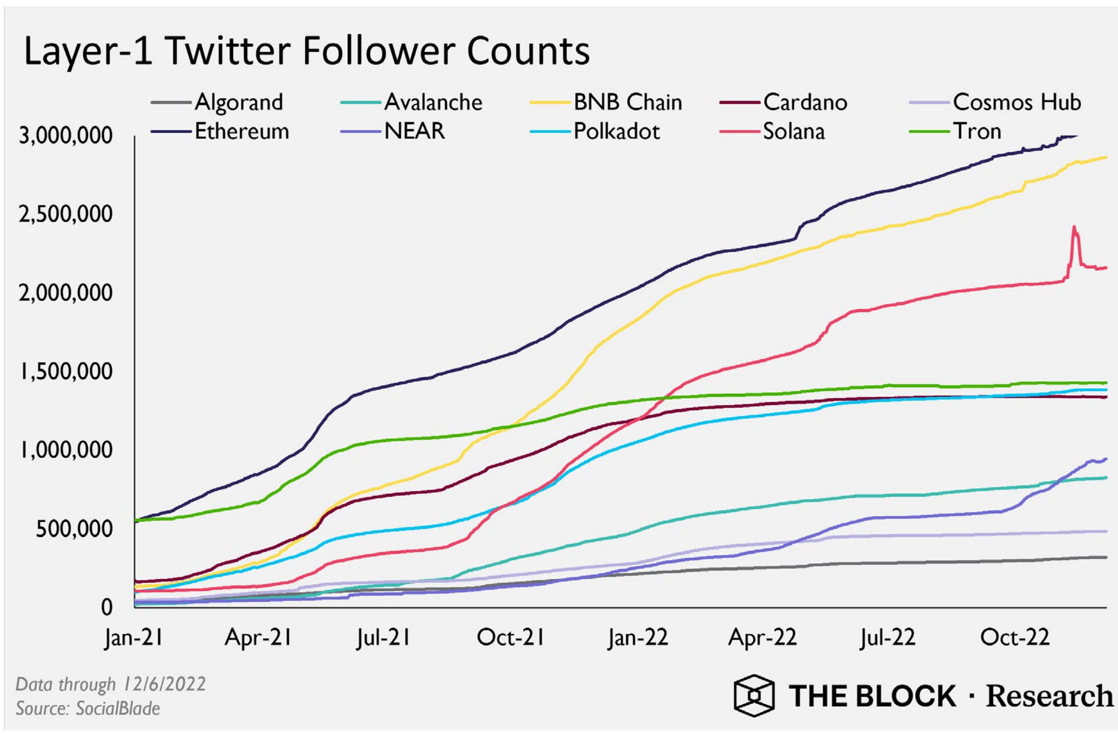
THE BLOCK · Research

Similarly, multichain ecosystems (figure above) have also seen a general downturn in TVL, which as before, is in large part due to the decline in crypto asset values in USD terms. The Ethereum L2s Arbitrum and Optimism, as well as the Juno chain in the Cosmos ecosystem, have the highest TVL at ~$1B USD for each. However, these figures are still relatively small compared to the ~$32B USD currently in Ethereum L1.

Ecosystem Data

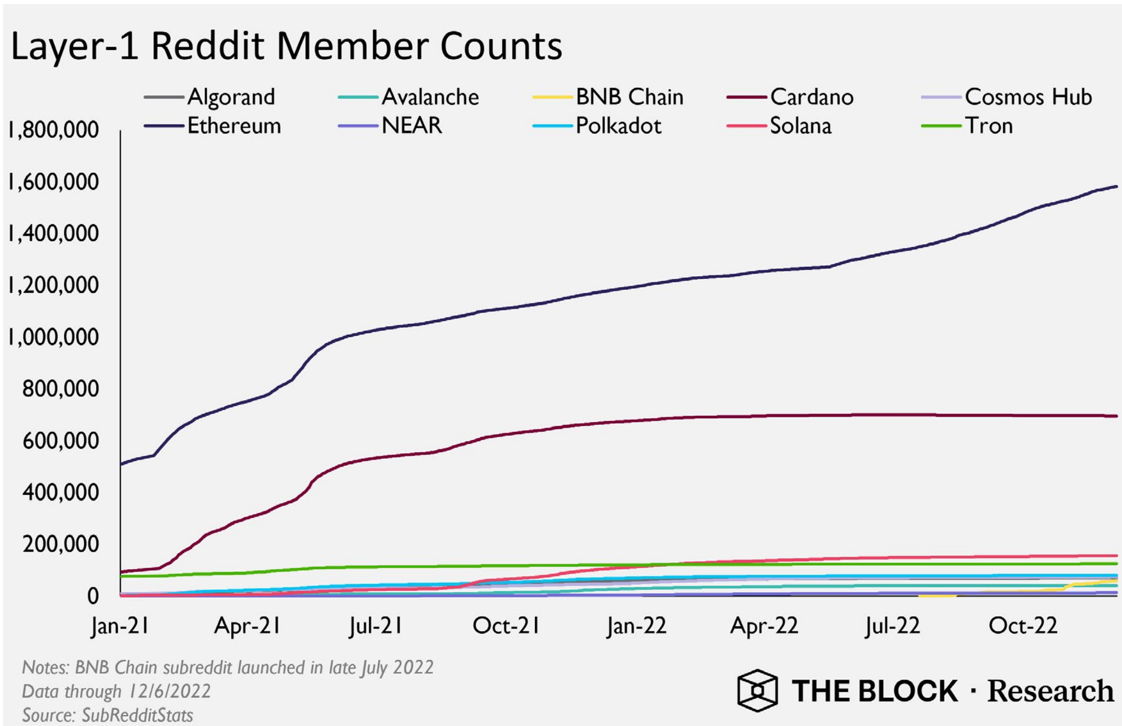
In addition to on-chain data, trends in community data are useful for estimating the relative size and growth of different L1 ecosystems. Next, we take a look at data from Twitter, Reddit, and YouTube to get a sense of different L1's social media followings. Social media followings are both a proxy for community size and growth as well as a quantitative estimate of the reach that different L1s have to share news and announcements, promote growth initiatives, and disseminate educational materials.

Twitter



These data suggest that Twitter users' interest in L1 platforms has kept increasing since the beginning of 2021 to now despite nearly a year-long bear market starting around the end of 2021. The good news is that people still seem interested in L1 platforms, and their respective communities are still growing.

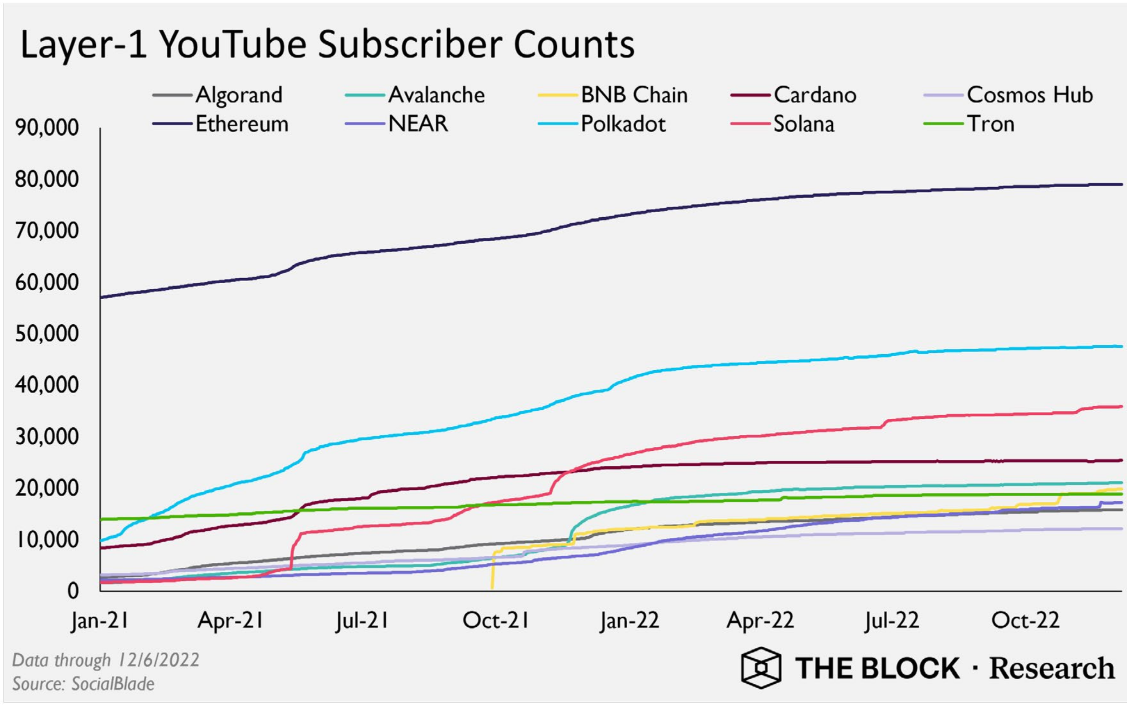
Notably, Solana and BNB Chain saw accelerated growth in their Twitter followings starting around the end of the bull run of 2021 that boosted their follower counts past several other chains – for example, BNB chain surpassing that of Tron, as well as Solana surpassing that of Cardano. Solana also saw a sizable spike in follows/unfollows during the FTX meltdown.



Reddit

While L1s show a fairly even distribution in terms of their Twitter followings, this isn't true about their Reddit member counts. Here, we can see that Ethereum and Cardano have large Reddit communities that dwarf other L1's Reddit communities. That said, Solana saw a boost in Reddit member counts around the end of the 2021 bull run, sending it past Algorand, Cosmos, Polkadot, and Avalanche.

YouTube



While Ethereum also dominates in terms of YouTube subscriber counts, Polkadot and Solana have also amassed an impressive following on this video sharing platform – with Polkadot having 60% the following of Ethereum and Solana having 44% per the latest data presented above.

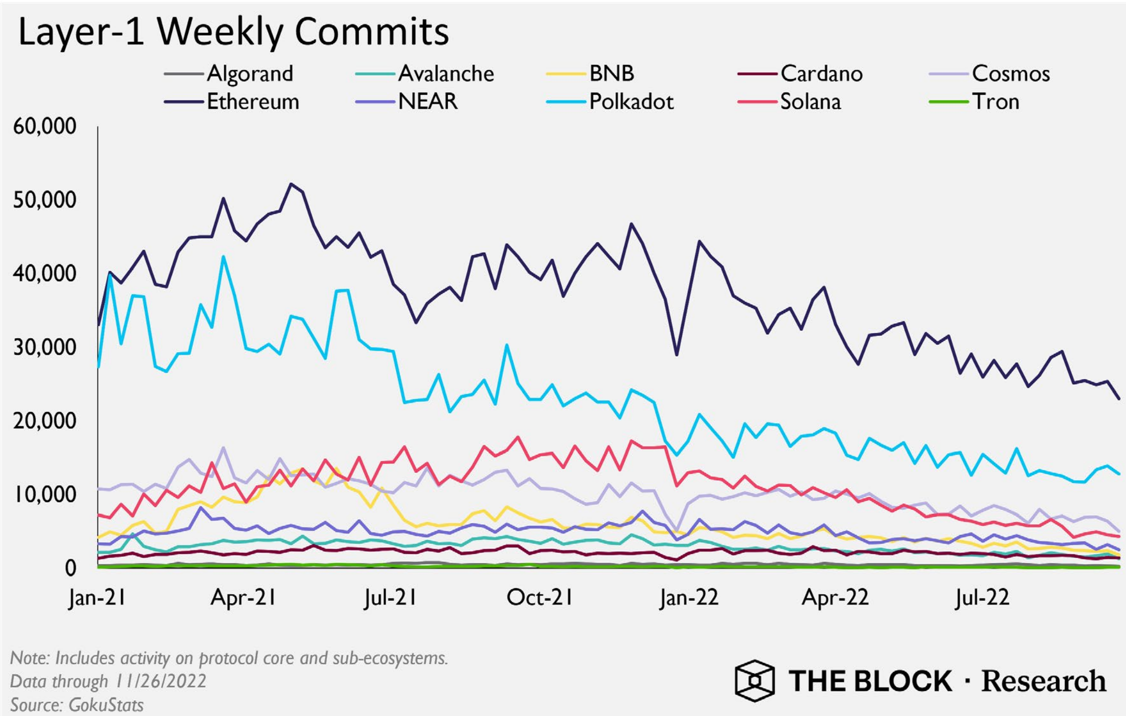
Developer Activity

In January this year, Electric Capital released its in-depth Web3 Developer Report, which provided many insights into what developers were up to in the crypto space during 2021. The report had a generally optimistic tone, showing that web3 developer activity reached all-time highs and grew rapidly in 2021. Here, we provide some updated figures (using Electric Capital's methodology) about two key developer activity metrics – commits to open-source repositories and active developer counts – to get a sense of where things have headed since their report.

A few caveats concerning this methodology:

- We can only track developer activity in public repositories and we can't know how much developer activity is in private repositories.
- The methodology is based on a simple count of repository commits and does not discount possibly negligible or spurious contributions.
- The repositories considered are those indexed by Electric Capital. While they aim to categorize all open source repositories for each protocol and openly accept submissions for missing entries, it is possible that some protocols are more completely indexed than others.

Weekly Commits



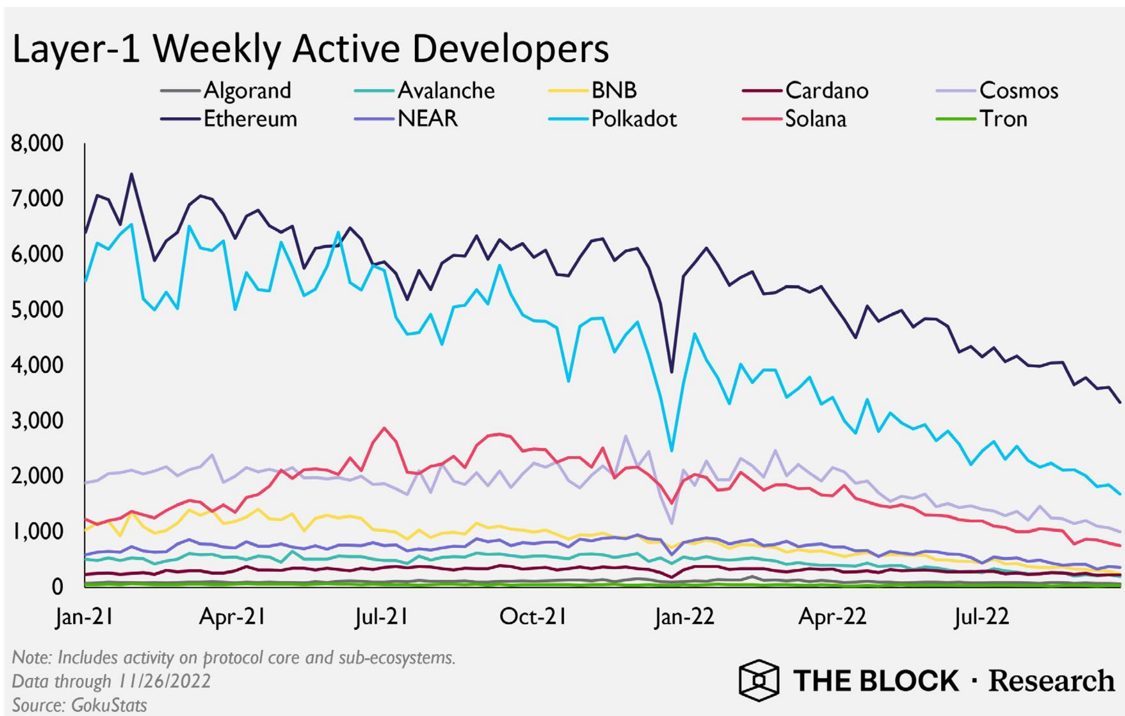
These are the weekly number of commits tagged to open-source repositories associated with an L1 core protocol or its sub-ecosystems. A commit is the smallest unit of work for developers and while there is variance in the size of a commit, it is a useful proxy for developer productivity.

The data here suggest that developer productivity has generally been on the decline since mid-to-late 2021. While most protocols and their sub-ecosystems have received commits in the thousands or several thousands weekly, Tron and Algorand stand out with very low commit counts. During the nearly two-year-long measurement period, neither protocol received more than a few hundred commits in any given week.

To look at developer activity another way, we can also consider the number of weekly active developers.

Weekly Active Developers

Here, we plot the weekly number of active developers tagged to open-source repositories associated with an L1 core protocol or its sub-ecosystems. A developer was considered active if they pushed at least one commit during the week.



The data here more or less mirrors the pattern which we saw with the number of commits. While most of the measured L1s have hundreds (e.g., BNB chain, Cardano, NEAR, Avalanche) or thousands (e.g., Ethereum, Polkadot, Cosmos, Solana) of active developers, Tron and Algorand only had fewer than a hundred active in any given week in the observed period.

It’s notable that Polkadot appears to have relatively high developer activity per number of commits and developer count. It is the only protocol with more than half the number of commits and active developers as Ethereum. On average during the measurement period, the Polkadot ecosystem had 62% of weekly commits and 75% of weekly active developers as Ethereum. Solana and Cosmos also appear to have a lot of developer productivity, with their weekly commits and weekly active developer counts roughly a third of Ethereum’s during the measurement period.

Native Token Overview

Disclaimer: The content in this section does not constitute investment advice. Anyone considering investing should perform their own diligence or consult a financial advisor.

An L1 native token plays crucial roles by ensuring security for the network (via staking), acting as a medium of payment for transaction fees and is used for on-chain coordination and governance in the ecosystem. Thus, the total supply of native tokens over time is an important consideration.

Digital assets have supply dynamics that are distinct from all other asset classes. In this case, native L1 token supply is determined by a combination of factors that may include algorithmic token issuance, stakeholder voting on network governance proposals and even the discretion of the project founders. Another important factor relates to the maximum possible supply of native tokens through time. In cases where total supply is capped, the net token issuance by the protocol should be zero after a specified point. In this scenario, platform development teams generally publish detailed schedules for how and when all tokens will be released, as well as their plans for the long-term sustainability of the network's economic and security models.

Other platforms may not impose any hard limitation on their native token's supply. On one hand, this may provide their communities with the flexibility to alter token inflation, staking payments and other parameters in the protocol, if the need arises. On the other hand, no limits on token supply also means that there are fewer assurances on the long-term scarcity of the native token.

Native Token Distribution at Genesis

There are a wide array of mechanics for initially distributing a supply of native tokens upon network launch. Token distributions at genesis may be labeled a "fair launch," which is loosely defined as a publicly announced token launch of an open-access network without "premined" tokens. Most blockchain network launches however, use significantly more complex initial token distribution strategies that may include airdrops, auctions, direct sales, crowd sales and private sales of premined tokens. Token generation events at genesis for PoS networks have several purposes, primarily they include:

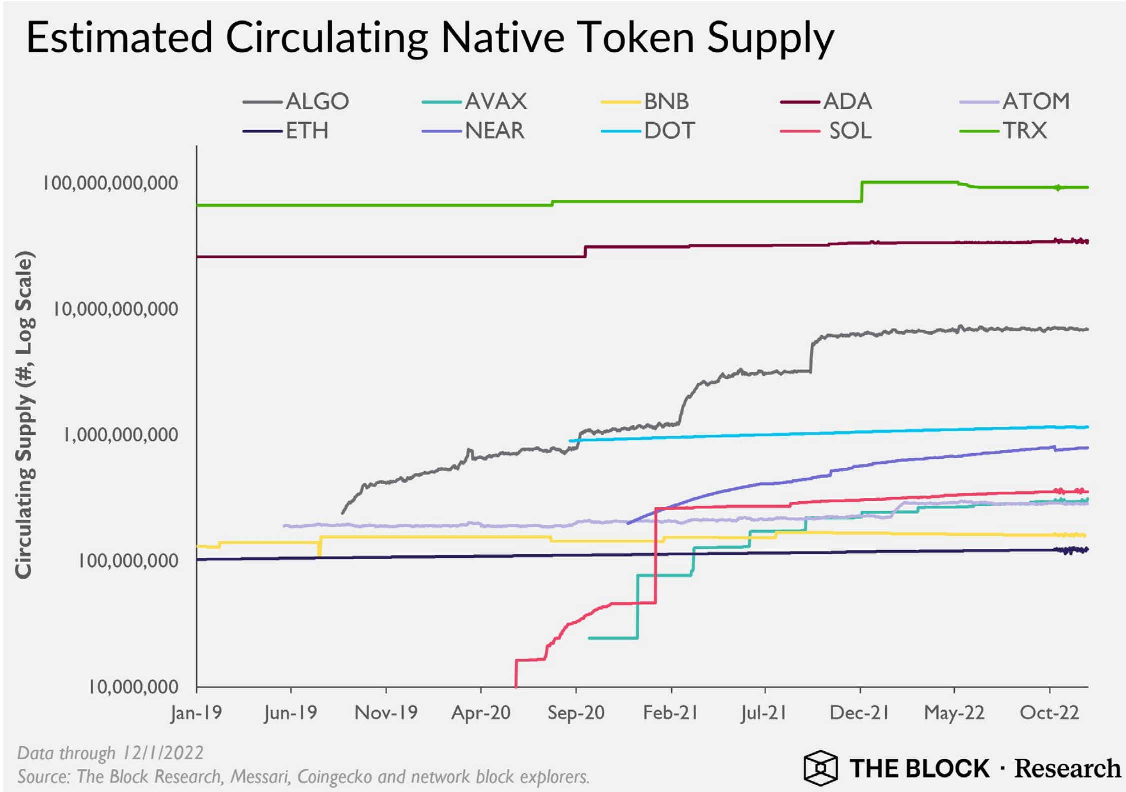
1. Staking Rewards / Incentives: tokens to be distributed to validators and delegators or distributed via airdrops - crucial for "boot-strapping" network security and attracting users
2. Foundation / Ecosystem Support: funds earmarked for infrastructure development, strategic collaborations, and assisting new ecosystem launches on the network
3. Development Organization / Core Team / Early Investors: incentivize developers to produce the fundamental platform technologies, conduct related research, and meet roadmap milestones. This category also includes tokens reserved for early investors

Native Token Circulating Supply Over Time

In addition to token allocation after genesis, how they may enter (or are taken out of) circulation is also an important consideration. Tokens that are sold to venture capital firms or given as incentives to the development team may have vesting periods that make them unavailable to be sold for specified periods of time. Core developers and the project foundation(s) may also own substantial amounts of the native token supply. Some of these actors and organizations publish reports describing their activities and holdings, while others may have limited transparency regarding theirs.

The circulating supply estimates the total "liquid" token supply available to be traded on the open market. It aims to account for known founder/investor token vesting schedules, lockup periods, and known locked project treasury or foundation holdings. Here, liquid supply represents all tokens available on-chain that have no programmatic or known paper-based contractual restrictions. Liquid and circulating supply may differ significantly due to tokens that may be held by project insiders, investors, foundations and other entities that are not subject to being locked on-chain or for them to publicly declare their holdings along with restrictions (e.g., vesting schedules).

Calculating the circulating supply can be challenging in cases where the above details about insider holdings, vesting schedules, paper-based legal contracts, wallet addresses (even ones that belong to non-profit ecosystem support foundations) and other details are not made public. Regardless, the following figure represents the estimated circulating supply of native tokens across the 10 networks selected for this report.



Token Economic Models

In addition to the token supply held by a myriad of entities, there are numerous monetary frameworks used across the industry that also determine the circulating supply. These models may be based on a fixed maximum supply where transaction fees from network usage, premined token emissions and/or secondary token distribution may be used to incentivize validators.

There may also be programmatic or non-programmatic token mint/burn events. Token mints and emissions are often used to incentivize validators and other service providers in the network. Token burns may be used to reduce the outstanding supply either algorithmically or via mechanisms that involve manual intervention, such as the one used previously for the BNB token (now transitioned to an algorithmic burn).

Max Token Supply?

Platform	Native Token	Maximum Supply	Current Circulating Supply
	ALGO	10,000,000,000	7,126,151,070
	AVAX	720,000,000	310,225,936
	BNB	200,000,000	163,276,974
	ADA	45,000,000,000	35,045,020,830
	ATOM	No Cap	292,586,163
	ETH	No Cap	120,521,599
	NEAR	1,000,000,000	834,265,332
	DOT	No Cap	1,179,372,029
	SOL	No Cap	363,962,680
	TRX	No Cap	92,107,389,232

Data through 12/5/2022
Source: Coingecko

THE BLOCK · Research

Moreover, the token mint and burn mechanics can be designed to function fully independently where the total supply of the token may increase or decrease over time deterministically based on a number of specified criteria (e.g., planned time intervals, network conditions such as, transaction throughput, the percent of token supply staked, etc.). Alternatively, mint/burn mechanics may be designed to work together as a system to control supply. For example, the Near protocol is designed to restrict token inflation rate between specified bounds.

Transaction fees can also be an important determinant of circulating supply. Depending on the design of the network, transaction fees may be paid directly to validators, sent to another address to be used for specified purposes, or simply burned to decrease the circulating supply.

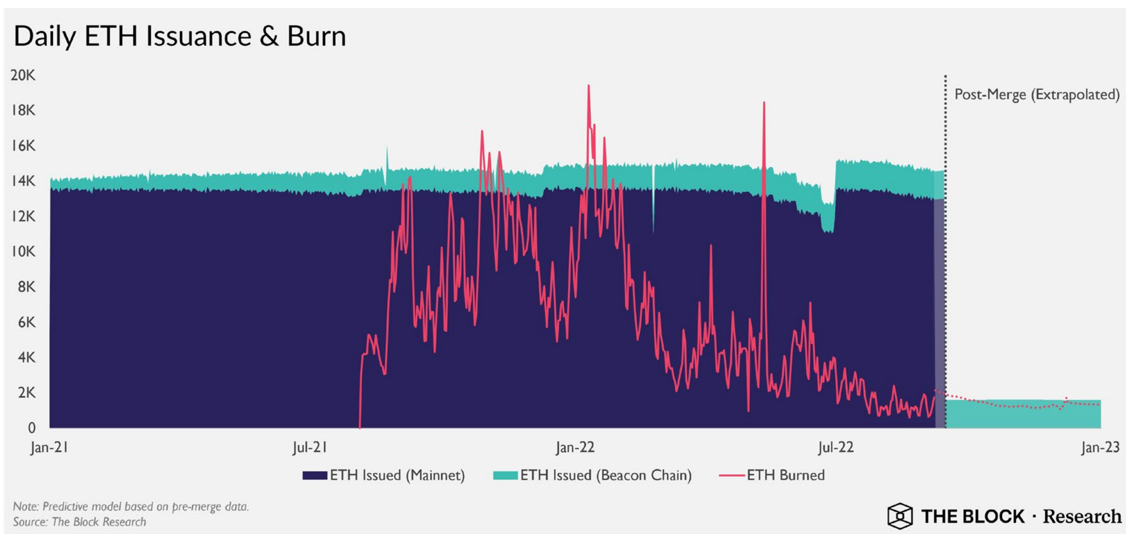
There is also precedence for these token economic models to be changed over time, as observed with Ethereum's Merge event (discussed later). Some L1 ecosystems may set out an explicit expectation for their communities to determine the economic model via governance mechanisms. For example, Algorand's long-term strategy for incentivizing network security will not be determined by its foundation and must be addressed by its community. Algorand has daily transaction fee revenue <$1,000 USD, as of writing.

The Merge's Impact on ETH Issuance

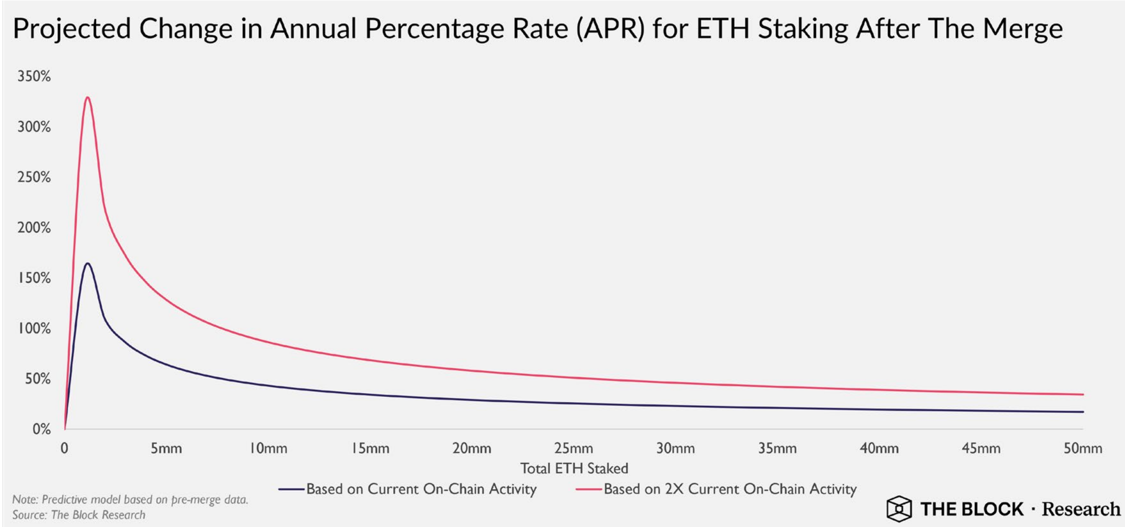
This multiplicity of approaches outlined above (e.g., token allocation at genesis, lockups/vesting schedules, mint/burn mechanics, how transaction fees are treated, etc.) makes it challenging to directly compare the monetary models across different L1s. As a case study, let's look at Ethereum's Merge event that had a significant impact on ETH token economics.

Before The Merge, new ETH was issued from two sources: the execution layer (Mainnet) and the consensus layer (Beacon Chain). Miners producing blocks on Mainnet were rewarded ~13,000 ETH/day while stakers on the Beacon Chain were receiving ~1,600 ETH/day (~10-11% of total issuance). However, The Merge eliminated mining rewards entirely, effectively reducing total ETH issuance by ~90%.

Furthermore, with the inclusion of ETH burns from transaction fees as enacted by the London upgrade, the net emission of ETH is now much more likely to be zero or less post-Merge. It depends on how much is staked and how much network activity there is – for example, if staking issuance is ~1,700 ETH, an average gas price greater than 16 gwei for a given day will offset the staking issuance, effectively making ETH net deflationary for that day.



According to The Block's analysis of post-Merge ETH token economics, the reduction of ETH issuance will increase the probability of daily net-deflationary issuance post-Merge, even when considering the year-to-date (YTD) lows in on-chain volume in August this year. Furthermore, the supply dynamics of ETH and its projected staking yield will be highly dependent on transaction volume as it determines both the amount of gas fees burnt and the amount paid to validators. For example, if total ETH staked is held constant, we could expect validator staking rewards to increase by about 71% if on-chain volume doubles from their current lows.



Company and Foundation Fundraising

While L1 platforms highlighted in this report have permissionless access, they may be developed and maintained by multiple for-profit and nonprofit organizations. These organizations may also tap the capital markets through a combination of equity financing (selling ownership stake in their companies) and token sales (selling the native tokens of their respective blockchain networks) to support the development of platform technologies and the growth of their respective ecosystems, as mentioned above. The table below shows these organizations and their fundraising histories.

Disclosed Funding Rounds

Platform	Related Organization(s)	Type	Date	Amount Raised	Investors
Algorand	Algorand Inc.	Seed Round	2/15/2018	$ 4,000,000	Union Square Ventures, Pillar
	Algorand Inc.	Venture Round	10/24/2018	$ 62,000,000	Union Square Ventures, Polybus, Eterna, NGC, Lemniscap
	The Algorand Foundation	Token Sale	6/19/2019	$ 60,000,000	
	Total Funding			**$ 126,000,000**	
Avalanche	Ava Labs	Series A	2/1/2019	$ 6,000,000	A16Z, Abstract Ventures, MetaStable, Polychain
	Avalanche Foundation	Token Sale	6/25/2020	$ 12,000,000	Bitmain, Galaxy Digital, Initialized Capital, NGC, Dragonfly
	Avalanche Foundation	Token Sale	7/22/2020	$ 42,000,000	
	Avalanche Foundation	Token Sale	9/16/2021	$ 230,000,000	Three Arrows Capital, Polychain Capital, CMS Holdings, Others
	Total Funding			**$ 290,000,000**	
BNB	Binance	Token Sale	7/1/2017	$ 15,000,000	
	Binance	Series A	9/1/2017	$ 10,000,000	Seqouia, Limitless Crypto Investments, Funcity Capital, Others
	Total Funding			**$ 25,000,000**	
Cardano	Cardano Foundation	Token Sale		$ 2,660,000	
	Cardano Foundation	Token Sale		$ 16,490,000	
	Cardano Foundation	Token Sale		$ 14,320,000	
	Cardano Foundation	Token Sale		$ 19,360,000	
	Cardano Foundation	Token sales		$ 26,360,000	
	Total Funding			**$ 26,360,000**	
Cosmos	Interchain Foundation	Token sale	4/15/2017	$ 17,000,000	
	Tendermint	Series A	3/15/2019	$ 6,000,000	Paradigm, Bain Capital, 1confirmation
	Total Funding			**$ 23,000,000**	
ethereum	EthSuisse	Token sale	8/30/2014	$ 16,000,000	
	Total Funding			**$ 16,000,000**	
NEAR	Near Foundation	Token Sale	7/10/2019	$ 12,000,000	MetaStable, Accomplice, Electric Capital, Pantera Capital, Others
	Near Foundation	Token Sale	5/4/2020	$ 21,000,000	Libertus Capital, Blockchange Ventures, a16z, Others
	Near Foundation	Token Sale	1/3/2022	$ 150,000,000	Three Arrows Capital, Mechanism Capital, Others
	Near Foundation	Token Sale	4/6/2022	$ 350,000,000	Tiger Global, Republic Capital, Hashed, Others
	Total Funding			**$ 533,000,000**	
Polkadot	Parity Technologies	Seed	4/23/2016	$ 750,000	
	Web3 Foundation	Token Sale	10/27/2017	$ 145,000,000	
	Web3 Foundation	Token Sale	1/1/2019	$ 60,000,000	
	Parity Technologies	Grant	1/7/2019	$ 5,000,000	Ethereum Foundation
	Web3 Foundation	Token Sale	7/28/2020	$ 43,000,000	
	Total Funding			**$ 253,750,000**	
Solana	Solana Labs	Series A	7/30/2019	$ 20,000,000	Multicoin, Slow Ventures, Rockaway Ventures, Others
	Solana Labs	Token Sale	3/25/2020	$ 1,800,000	
	Solana Labs	Token Sale	6/9/2021	$ 314,000,000	A16Z, Polychain Capital, Alameda Research, Coinfund, Others
	Total Funding			**$ 335,800,000**	
TRON	Tron Foundation/Peiwo Huanle	Token Sale	9/1/2017	$ 70,000,000	
	Total Funding			**$ 70,000,000**	

Source: The Block Research & The Block Pro

THE BLOCK · Research

Major Technical & Ecosystem Updates

As the most dominant smart contract ecosystem, this report has a section dedicated to Ethereum's network architecture, recent updates, and future roadmap while also introducing several important developments in the field as a whole related to blockchain scaling. This section will briefly summarize the major technical updates to each of the ecosystems selected for review in this report.

Algorand

State proofs: The release of state proofs is designed to facilitate easy verification of the Algorand blockchain's state by entities outside of the network. State proofs reduce the number of signatures required to validate that a certain transaction indeed took place in the Algorand ecosystem. The Algorand foundation claims "trustless cross-chain communication." If accurate, cross-chain bridges are one potential beneficiary of this technology that will allow light clients or smart contracts on other chains to verify the state of the Algorand chain with a reduced data packet. State proof may help address decentralization and trust assumption constraints for the current implementation of cross-chain bridges that use "relayers." The Algorand Foundation also claims that state proof introduces quantum security and an increase in performance from 1,200 to 6,000 transactions per second (TPS).

On-chain governance: The Algorand Foundation introduced a community governance model for the Algorand ecosystem in October 2021. Anyone who owns the ALGO token can sign up to be a "Governor" and participate in Algorand governance. Governors are entrusted with allocating cash from the 3.2 billion ALGO Algorand Ecosystem Resource Pool (AERP), valued at around ~$1 billion USD as of writing. This pool of tokens was previously controlled solely by the Algorand Foundation. In order to participate, Governors must commit ALGO for the duration of each three-month quarter that comprises a governance period and vote on every proposal during that period in order to gain governance incentives in the form of ALGO token rewards.

Avalanche

Scalability in the Avalanche network is primarily implemented through subnets that do not ultimately settle on the Avalanche Primary Network. Although this has been effective at diverting high-volume transactions away from the C-Chain network, subnets do not inherit the security provided by Avalanche's Primary Network validators.

Fee burn: The Avalanche network has spent the past year improving its EVM-compatible C-Chain to maintain compatibility with technology and infrastructure designed for the most current EVM version. For instance, the release of Apricot V3 in August 2021 introduced base fees and dynamic fee burning to the Avalanche network.

Patched attack vector: The Ava Labs team announced an urgent upgrade to Apricot V6 in September, which fixed a potential attack vector for DeFi protocols deployed on the Avalanche network. The vulnerability was present in a precompile contract unique to the Avalanche C-Chain meant to optimize gas efficiency.

Core wallet with native bridges: Recently, the Ava Labs team has been working on incorporating functionality for connecting native BTC to the Avalanche C-Chain. BTC bridged via the Avalanche Bridge, BTC.b, is now accepted as collateral on the Aave lending protocol. There is significant interest in expanding the interoperability of the Avalanche network with other chains. The Core wallet (created in-house) is also compatible with other EVM networks.

Optimistic rollup: Boba optimistic rollup was announced in September 2022 as the first L2 chain that would be integrating with Avalanche. This announcement is somewhat unexpected, given the Avalanche team's focus on its subnet technology. Nonetheless, it indicates an ongoing commitment to advancing scaling technologies overall.

Subnet rollouts: The DeFi Kingdoms (DFK) and Swimmer Network subnets have seen significant on-chain activity since launch in early 2022, even in comparison to Avalanche's C-chain. The central limit order book (CLOB) DEX, Dexalot, announced their deployment as a subnet in 2022, paving the way for a CLOB-based decentralized exchange inside the Avalanche ecosystem.

Elastic Subnets: The Banff hard-fork upgrade (in October 2022) provides the ability for subnet creators to allow entities interested in becoming a validator of a subnet by simply staking its token on the P-Chain. Enabling Elastic Validation on a Subnet is at the discretion of the subnet creator(s) and the option to retain the default configuration will remain available for applications that require more control over the validator set. This upgrade is expected to reduce friction for both validators to migrate across subnets, and for subnets to attract new validators. “Banff 1” is a step towards comprehensive interoperability between subnets. Banff-enabled subnets may communicate with others on the Avalanche ecosystem to verify data such as account balances and transaction confirmations without executing a transaction on-chain.

BNB Chain

Name change: The Binance Smart Chain (BSC) team announced a change in branding to the Build-and-Build (BNB) Chain in February 2022 presumably in an attempt to distance the Binance exchange from the blockchain ecosystem. The move comes at a time when Binance and its founder Changpeng Zhao are drawing increased scrutiny from regulators globally. The new BNB chain branding collectively refers to two separate chains known as BNB Beacon Chain (formerly Binance Chain) used for governance and staking BNB, while BNB Smart Chain (BSC, formerly known as Binance Smart Chain) will continue to support DApp activity in the ecosystem.

More decentralization? In the long run, the degree of decentralization of the BNB Chain ecosystem is one of its major concerns, given there are only 26 active validators. This concern recently came to the forefront when the BNB ecosystem was halted for several hours due to a bridge hack/exploit resulting in a drainage of >$100M USD. Recently, BNB Chain developers made a proposal that intends to increase the network's decentralization by increasing the number of validators that can actively participate in block production. By introducing "candidate validators" in BEP 131, two extra validators would be randomly picked from the top 41 validators on the network every 200 blocks, in addition to the 26 validators that now secure the network.

Sharding and app chains: According to the 2022 outlook published by the BNB chain developer community, sharding, EVM parallelization, and implementation of app chains are in store for the BNB chain. This aligns the BNB community closer to the approach taken by Ethereum, Polkadot, Cosmos, and Avalanche. The sidechain component, known as BSC Application SideChain (BAS), will allow developers to build and deploy custom blockchains with built-in cross-chain asset flow for their DApps, while maintaining a connection with BSC to inherit its security guarantees.

Cardano

The evolution of Cardano is supposed to occur in distinct phases, or, "eras." Here the priorities (and the era's codename) in chronological order include a foundation (Byron) "of security and correctness," followed by decentralization (Shelley), smart contract capability/expressiveness (Gougen), scalability (Basho), and governance (Voltaire).

Smart contracts & network congestion: Cardano's entry into DeFi was highly anticipated via the implementation of smart contracts through the “Alonzo” hard fork in September 2021. The most anticipated DApp was the SundaeSwap DEX, the first (automated market maker DEX in the ecosystem). However, there were reports of significant network congestion immediately after the update. SundaeSwap's literature before launch also suggested that swaps could "take days to process," which would effectively render the majority of transactions on the DApp untenable as token prices are likely to fluctuate throughout this time frame.

It is important to note that the EUTXO system can theoretically boost throughput by allowing many orders (such as those in an order book) to be bundled into a single transaction, according to the IOHK team. However, such transaction grouping may be challenging to accomplish in practice for some applications, such as traders executing multiple trades quickly to take advantage of transient price fluctuations.

Vasil upgrade: As of late-September 2022, the Cardano network underwent the Vasil upgrade, which was characterized as a step-change in the blockchain's smart contract capabilities. This is largely through upgrades to the Plutus scripting language to add greater efficiency to the EUTXO model to enable faster and more sophisticated DApps. Other efficiency improvements include the reduction of script execution costs and transaction size to improve network speeds.

Cosmos

Failed Atom 2.0 proposal: Cosmos contributors released a new whitepaper in September envisioning a future in which the Cosmos Hub and the ATOM token holders will play an increasingly vital role in delivering valuable functionality to the rest of the ecosystem by leasing security from the Cosmos Hub to other sovereign chains. This concept is comparable to the shared security model being explored in the Polkadot ecosystem and can be considered as an expansion of Interchain Accounts (IA) capabilities discussed later. The update to IA is the concept of Interchain Security (ICS) that was introduced more than a year ago, with the official Cosmos Hub road map forecasting ICS release to be in the first quarter of 2023. As of November 14, 2022, the community voted against the Atom 2.0 proposal. Generally, the Cosmos community is directionally in support of the proposal, however, there are calls for splitting up the sweeping changes in Atom 2.0 into multiple actionable proposals.

Theta upgrade: The Theta upgrade, released in March 2022, brought improvements to interoperability in the Cosmos ecosystem through the IA module. IA allows users to have accounts on a "controller chain" to conduct transactions on a "host chain" using the pre-existing feature, inter-blockchain communication protocol (IBC). IA expanded on existing IBC capabilities by enabling users of sovereign blockchains to submit cross-chain messages to be performed on another chain.

Vega upgrade: The Vega upgrade, completed in December 2021, added the IBC routing capability to the Cosmos Hub, allowing transfers from any chain A to chain C as long as they are both connected to a third chain, B. Through this mechanism, Cosmos chains with high IBC traffic, may earn fees for providing routing services.

Ethereum

EIP-1559: Beyond Ethereum's successful Merge event, as discussed above, the London upgrade in August 2021, which implemented the EIP-1559 proposal via a hard fork is also notable. EIP-1599 has significantly altered Ethereum's monetary policy by implementing a new transaction fee structure that adjusts basic gas fees based on block demand. It also introduced Ethereum's first burn mechanism, where ETH is burned according to Ethereum block space demand. As a result, the total emission rate of ETH has become variable, at times recording net deflationary days amid high network activity.

Near

Near-native algorithmic stablecoin: The Near-native stablecoin, USN, was launched on April 25th and is governed by the Decentral Bank DAO. USN represents the NEAR protocol's entrance into the yield-bearing stablecoin market around the same time as Terra's collapse. USN has a design comparable to Terra's UST, with some key measures taken to avert a UST-like collapse. USN's long-term stability remains to be determined. As of October 24, 2022, Decentral Bank and the NEAR foundation announced that USN became undercollateralized by $40M USD. The NEAR Foundation released a blog post announcing a $40m USD grant for USN holders to redeem their USN on a 1:1 basis with USDT.e. The NEAR foundation also recommended Decentral Bank to dissolve USN operations.

EVM-compatibility: The Aurora chain was created on top of NEAR and enables developers of other EVM chains to release applications for the NEAR ecosystem in a familiar programming environment. The Aurora team also developed the NEAR Rainbow bridge that allows for capital transfers between NEAR, Aurora, and other EVM chains.

Polkadot

Over the past year, the Polkadot team has adopted a somewhat deliberate approach to growth, frequently releasing components of their larger goal in phases. This is represented by the Kusama canary network, which functions as a governance-minimized testnet for core developers and anyone wishing to secure parachain slots on the Polkadot relay chain.

Parachain launches: The introduction of Kusama's first parachain auction in June 2021 was a milestone for the Polkadot ecosystem. It allowed developers to begin deploying apps in a production environment and testing Polkadot's shared security model. Since then, there has been a progressive rollout of parachain auctions to participants. The winners of the first batch of parachain auctions included Moonbeam and Acala. Participants must compete (via DOT token raises through crowd loan auctions) to secure parachain slots in order to begin "leasing" security from the Polkadot relay chain, typically for 96-weeks periods. Auction #29 is ongoing, as of writing.

Cross-chain messaging: XCMP is Polkadot's novel cross-chain message-passing protocol that has seen some delays in development. XCMP not only connects parachains with one another but may also support other L1 ecosystems. Development teams in the Polkadot ecosystem have since started using workarounds such as Horizontal Relay-routed Message Passing (HRMP) - a limited version of XCMP. The Polkadot core team has indicated upcoming updates to the currently implemented Cross-Consensus Message Format (XCM) to add functionality to the cross-chain messaging protocol. However, the much awaited XCMP upgrade is unlikely to occur until at least 2023.

Solana

Network downtime: The most prominent challenge with the Solana network in the recent year or so has been numerous episodes of degraded performance and even network downtime that required coordination between validators to restart the network. There are several reasons for these difficulties. For example, hardware requirements to operate a Solana validator node are the most stringent of all major competing L1s. Solana is also labeled as being in beta and the regularity of updates that contain critical improvements is high relative to more mature networks. These upgrades have occasionally led to increased hardware requirements for enabling new features, causing some validators to underperform for extended durations. In fact, the chronic clock drift issue across early-mid of 2022 was likely due to insufficient response times from lower-tier Solana validators.

More decentralization? The Solana Foundation has launched the **Tour de Sun '22 (TdS22)** program to encourage increased hardware and geographic diversification among validators. This effort includes collaboration with data center operators throughout the world to create a conduit for users who lack the necessary hardware to have access to hosted infrastructure, allowing them to become validators. The TdS22 program is being implemented at a time when U.S. regulators have become more aggressive in enforcing securities laws based on the geographic location of validators. If successful, the introduction of TdS22 could shield validators considered to be inside U.S. jurisdiction and thereby subject to potential SEC enforcement actions.

New validator client: The trading firm, Jump Crypto, announced development efforts for a new Solana validator client that is expected to aid the network's resilience in the case of a client-based attack. Jump also showed interest in proposing significant modifications to Solana's core software, indicating their support for the network's infrastructure in a manner similar to how third-party providers now support Ethereum via RPC endpoints, wallets, node clients, and more.

Reduce spam and add a fee market? One of the primary issues of running a network with low costs is that spamming the network with transactions incurs little to no penalty. One approach to address these issues is a fee market. In early 2022, a framework for a fee market was introduced alongside mainnet version 1.10. Another anticipated update for Solana is the integration of the QUIC client for validators, which is anticipated to enable dynamic screening of malicious bot activity that has historically plagued the network.

Tron

Tron-native algorithmic stablecoin: Tron's team recently released its own native algorithmic stablecoin named USDD or, "decentralized USD." USDD mechanics are closely modeled after Terra's UST that suffered a bank-run resulting in a "death spiral," losing tens of billions USD in value in a matter of hours and days. Currently, only a number of whitelisted institutions, including Alameda Research, Amber Group, Poloniex, and Multichain, can issue USDD. USDD launched with an annual yield of 30% to draw attention and investment (currently 9.37%). Within three weeks of its introduction, USDD in circulation increased to approximately $545 million and is now approximately $800 million. Its long-term stability remains to be seen.

IV Conclusions

Bitcoin was the first decentralized digital medium for exchanging value. The digital asset class as a whole is moving forward with exploring what else can be decentralized using blockchain technologies. Notable current efforts center around data storage, web hosting, social media, and even physical infrastructure, such as internet access. These applications built atop blockchains are thought to enable the new era of the internet that is often termed "Web3." For more information about the web3 stack, we encourage readers to The Block's recent piece, Accessing Web3: Developments and Opportunities.

The ultimate long-term scope for applications blockchain technologies may disrupt is difficult to pin down. However, the imminent need for high-transaction throughput in order for these blockchain-enabled applications to scale and reach the global masses is relatively well accepted.

Novel L1 Designs and Architectures

Blockchains with specific attributes and designs may make it ideal for certain types of applications and inefficient for another. Here, vision, design goals, and even ideological positioning for what a blockchain is "supposed" to do may inform the engineering trade-offs made for specific L1s in order to find unique selling points framed within the blockchain (scalability) trilemma.

However, there is also significant research and development to address the scalability limitations and maybe even challenge the trilemma to some degree. Indeed, the consensus is that the blockchain trilemma can be molded and shaped through further innovations.

> *"The scalability trilemma says that there are three properties that a blockchain tries to have (scalability, security, and decentralization), and that, if you stick to 'simple' techniques, you can only get two of those three."* – Vitalik Buterin ("Why sharding is great," April, 2021)

Technical efforts to scale blockchains generally fall under the following categories:

- **New Layer-1 (L1) technologies**: Incorporate novel technologies (e.g., sharding, zero-knowledge proofs, parallel runtime environments, virtual machine (VM) upgrades, etc.) within monolithic chains to advance and reach a desired compromise between scalability, security, and decentralization (e.g., Ethereum, Solana, Cardano, etc.).
- **Interoperable chains**: An ecosystem of app chains, ideally with high security as well as seamless communication and interaction in-between (e.g., Cosmos, Polkadot, etc.).
- **Sidechain/Layer-2 (L2) solutions**: Connect a new chain to an existing L1 (e.g., Bitcoin or Ethereum) to leverage its security and decentralization guarantees while increasing scalability and/or introducing additional features.
- **Modular approaches**: Multiple task-specific chains that leverage the function of one another to fulfill the core functions of a monolithic blockchain: data availability, consensus, settlement, and execution. A relatively new approach, the modular approach posits that scalability is unlocked when a chain isn't constrained by having to handle all the functions (e.g., Celestia is a pioneer in modular approaches).

While the above innovations have demonstrably increased blockchain scalability to various degrees, there are always associated risks to implementing cutting-edge, unproven tech. In the last year alone, technical vulnerabilities and centralized control over bridges have led to several high-profile bridge exploits totaling over $1B USD cumulatively. At this point, bridges are a demonstrably major area of weakness for blockchain networks that need more work. In pursuing scalability via horizontal scaling or modularity, L1s should be cautious when interacting with third-party bridges or when building their own native bridge infrastructure.

Bridge Exploits

With increasing activity on different L1s, there is a growing demand for chains to be able to talk with each other. For example, a user of Atlas DEX, a cross-chain DEX, may want to bridge Ethereum assets to Solana to transact at higher speeds and lower fees. But, that introduces another layer of systemic complexity in blockchain architecture, with bridge technologies opening up several degrees of freedom in terms of blockchain attack vectors.

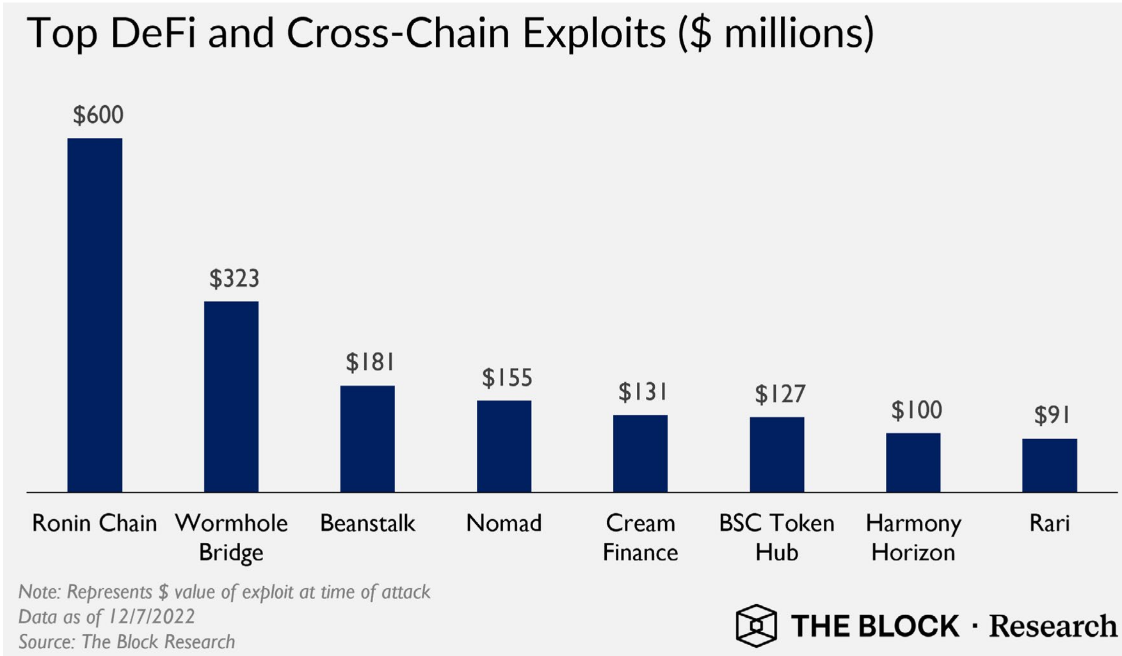
The most popular bridge implementation is the lock-and-mint design. In this design, the original assets are locked in a smart contract on the sending side (e.g., Ethereum) while the receiving network (e.g., Solana) mints a replica of the original token on the other side. That means that Ether bridged to Solana via a lock-and-mint bridge is only a "wrapped" representation of Ether, not Ether itself.

However, weaknesses in this design have been at the center of three of the largest crypto heists in history.

Wormhole: On February 3 this year, Wormhole confirmed that their network was exploited for 120K whETH (Wormhole ETH; equivalent to over $320M USD at the time) a day earlier. The attack exploited unpatched Solana Rust contracts that were manipulated into falsely crediting a 120K ETH deposit on Ethereum, allowing the hacker to mint the equivalent in whETH on Solana. Subsequently, the hacker was able to release a false deposit of 93,750 ETH back on Ethereum over the course of three transactions by burning the equivalent debt in whETH on Solana. The remaining 36,250 whETH were liquidated on Solana into USDC and SOL.

Wormhole could have prevented this attack by patching their Solana Rust contracts or by otherwise validating the hacker's input accounts to identify spoof guardian signatures allowing the false ETH credit.

Within a day, Jump Crypto, which incubated Wormhole, replenished Wormhole's reserves with 120K ETH. Jump is the trading firm that acquired Certus One, the blockchain infrastructure firm behind Wormhole, for an undisclosed amount back in August 2021.



Although Wormhole was rescued in a sense, there are still 93,750 fraudulently unwrapped ETH circulating in the Ethereum ecosystem, as well as 36,250 ETH-equivalent USDC and SOL on the Solana ecosystem.

Ronin: As shown above, the Ronin attack was an even worse exploit than the Wormhole hack in terms of value lost to hackers (purportedly, the North Korean Lazarus group). Again, this was a situation where the typical lock-and-mint bridge design presented a low-hanging fruit for attackers.

In this case, Ronin lost 173,600 ETH and 25.5M USDC worth ~$600M at the time, and all it took was taking control of the majority of nine validator keys securing the Ronin bridge contract, which held billions of dollars at the time. With a bit of spyware, the hackers got a hold of four of those keys from Sky Mavis, then got the last one from the Axie DAO that allowed Sky Mavis to sign transactions on their behalf months earlier.

Unlike the Wormhole attack, the funds drained from the Ronin Bridge were real user funds locked and stolen – there was no fraudulent minting. Sky Mavis – the developers behind both Axie Infinity and the Ronin Bridge – has raised $150M to reimburse the victims.

BSC Token Hub: Most recently, the BSC Token Hub – the official cross-chain bridge protocol in the BNB ecosystem – was at the center of a ~$100M hack that targeted a vulnerability in the BNB network's underlying software that allowed the hacker to forge the merkle proof for a specific block. Leveraging this vulnerability, the hacker fraudulently issued 2M BNB tokens from the BSC Token Hub address, worth around $560M at the time – making the exploit potentially as huge as the Ronin case.

On-chain data showed that the hacker transferred over $100M out to third-party chains, including Ethereum, Avalanche, Polygon, and Arbitrum. The majority of the stolen assets remained in the hacker's wallet on the BNB Chain.

All 26 active BNB Chain validators worked together to salvage any exploited funds that hadn't yet been moved off of the BNB Chain. While they re-enabled the network after about 10 hours, the bridge will remain shut down until the vulnerability is fixed.

Situations like these bridge exploits demonstrate the importance of secure coding practices and in-depth security audits for L1 security. It also highlights how L1 communities need to be especially careful – not to mention knowledgeable – when deciding which third-party protocols to connect with.

DApp Development and Usership

All smart-contract L1 blockchains (to some degree) compete to create a self-sustaining ecosystem of users composed of DApp developers and their end users. Developers (engineers that develop blockchain-enabled applications) are more likely to be interested in the DApp development environment(s), ease of use as well as available funding, and the size of the existing user base before selecting an L1 ecosystem to dedicate their time on. DApp end users, on the other hand, are likely to consider the diversity of DApps available in an ecosystem (along with their usage incentives), transaction cost/throughput as well as, the degree of decentralization and security guarantees of each ecosystem.

Major takeaways for DApp user activity:

- **User adoption trends are a mixed bag**: The data shows leveling off and/or a decrease in active addresses across most ecosystems coinciding with the downturn in the market starting from about November 2021. However, a few individual ecosystems, notably Tron, have defied this trend and have experienced an increasing number of daily active addresses since this time.

  Although the USD values for digital assets are down significantly across the board, interest from the general public is showing resilience as measured by the increasing number of Twitter, Reddit, and YouTube traffic. Lower market prices also mean that the average transacted value on-chain has also decreased significantly, tracing back down to levels observed in early 2021. The same also holds true for TVL allocated to each ecosystem.

- **Low fee transactions are in-demand**: We can loosely see this in the exponential growth of Solana as measured by its overall dominance in active addresses and transaction counts over the past years. Similarly, Tron and BNB Chain are close runner-ups. Interestingly, despite having the highest fees of all ecosystems, transaction counts and active addresses for Ethereum L1 remained among the highest in the asset class. This demonstrates how Ethereum's ecosystem (for a myriad of reasons) is "sticky" enough for a significant number of DApp users to justify paying transaction fees that are orders of magnitude higher than low-cost L1s.

  Despite troubles related to congestion and network outages, Solana consistently maintained some of the highest mainnet transaction throughputs of any ecosystem.

- **Multichain ecosystems are growing but have a long way to go**: User adoption of app chains and L2 scaling solutions, as measured by daily active addresses and transaction counts, shows an increasing trend despite weak market conditions. Specifically, Ethereum L2 scaling solutions have daily transaction counts that have begun to rival those of Ethereum L1. TVL has also grown significantly across multichain ecosystems but has yet to rival that of the current leaders, Ethereum L1, BNB Smart Chain, and Tron. Moreover, Cosmos, Avalanche, and Polkadot all have planned upcoming upgrades focusing on seamless cross-chain interoperability that should aid in the adoption of multichain ecosystems.

Major takeaways for DApp development activity:

- **Decreasing trend in development commits**: The proxies for measuring developer activity in this report show a decreasing trend across all L1s, coinciding with the market downturn starting about November 2021. This trend in developer activity is in contrast with general end-users who (presumably) are more likely to interact with YouTube and Reddit, which both show growth in user engagement over the last two years.

- **Battle of the execution environments?** The execution environment is an important part of blockchain architecture, impacting not only how assets and smart contracts operate but also how users and developers interact with the ecosystem. The perpetual dominance of the EVM-based DApps (as measured by TVL in EVM-compatible chains) is not guaranteed to persist in the long run. There are many emerging EVM alternatives that include Solana's Sealevel runtime, MoveVM, WebAssembly (Wasm), and CairoVM. Specifically, Solana's Sealevel execution environment using the Rust programming language has set a precedent of achieving notable developer/end-user adoption in the past 18 months.

  As mentioned, smart contract exploits are an ongoing issue in the industry. The increasing sophistication of blockchain-enabled applications (e.g., money markets, bridges, DEXs, and more) may also increase the complexity of the code (and attack surface area) in the underlying protocol. Uncovering specific vulnerabilities and assessing overall risks within complex applications and development environments with such broad expressivity can be extremely challenging.

With exploits in mind, the Move programming language and its virtual machine (MoveVM) is a notable new contender in the field. Move was developed by Facebook (now Meta) for their Libra (later changed to Diem) blockchain. Move is expected to address the challenges and risks related to unexpected smart contract execution. The Move language (and its execution environment MoveVM) was specifically created with these concerns in mind. All on-chain assets are defined based on linear logic (as opposed to classical or intuitionistic logic) and have extensive customization of token security and access controls. From the perspective of attracting new developers, the evolution of how the execution environments evolve across ecosystems is an important factor to track.

Outlook & Closing Thoughts

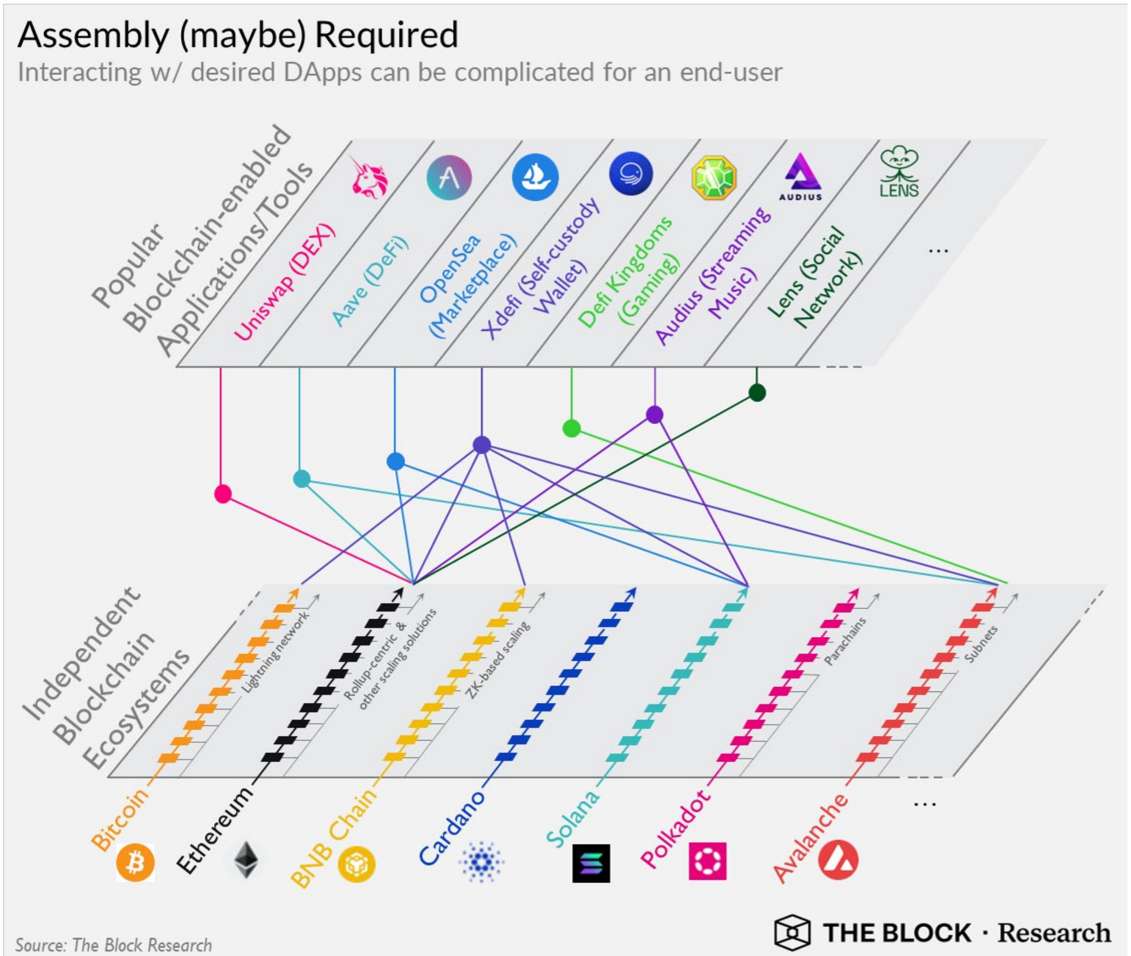
Built atop of the foundation of popular L1 blockchain protocols are a complex set of primitives and consumer-facing DApps. Currently, there are many distinct L1 blockchain ecosystems that secure tens and even hundreds of billions of USD in digital assets.

The keywords to focus on here are: “distinct ecosystems.”

Fragmented L1 Ecosystems

Bespoke technologies, tools, and design choices underpinning each L1 blockchain may produce unique software and hardware dependencies for developers and, to some degree, the end users, as well. DApps development may require specialized expertise in programming environments specific to an L1 blockchain. If these DApps gain some level of acceptance/adoption, it also breeds familiarity within consumers across a known set of DApps that work alongside a specific set of tools (e.g., wallet clients, fiat on/off-ramps, etc.) constrained within an L1 ecosystem.

Moreover, value and information cannot be moved between independent blockchains natively, due to differences that may exist in security frameworks, consensus mechanisms and development environments. This is a fundamental challenge in the industry isolating users and DApps, the effects of which are widespread, ranging from highly fragmented liquidity across dozens of decentralized exchanges to difficult decisions about the choice of an ecosystem that individual DApps developers must make before they deploy.



The figure above illustrates how a sample of popular DApps and tools (e.g., self-custody wallets) have limited compatibility/interoperability across blockchain ecosystems. This forces users to juggle multiple wallets and fiat on/off-ramps, significantly complicating their process of interacting with DApps. This is in stark contrast to how the internet functions today, where such fragmentation of resources and audience is not as much a concern – in a simplified scenario, any website can be made available to anyone with (unrestricted) internet access.

The emerging cross-chain economy and information highway is thus a major effort in the field, as covered in The Block's recent interoperability report, specifically on the topic.

In addition to the fragmentation of audience and liquidity, another factor we cannot ignore is the tribalism that has plagued blockchain networks and their ecosystems. Historically, users and developers have been required to pick and choose between one or a few chains, often creating insular communities that inhibit collaborations across the industry.

> *"We need to collaborate, and we need to work together... I reach out, I talk to other protocols ... learn from them... that's the best way for us in the blockchain industry, to ensure that we have a future together...* ***we're too small for this*** *[vs. traditional finance]"* – Mel McCann, VP of Engineering, Cardano Foundation (The Block interview, October 2022)

Dynamics of L1 Ecosystem Growth

Ethereum has had a significant first-mover advantage and has attracted a network of independent developers with concentrated expertise around Ethereum's development environment – its smart contract computer language, Solidity, and its execution environment, the Ethereum Virtual Machine (EVM). A number of newer L1 smart contract chains (e.g., BNB chain, Avalanche and Fantom) are thus compatible with Solidity and EVM, making the transition easier for both developers and users alike (e.g., interoperable wallet clients; Metamask). As mentioned, there is now intense competition between a wide array of execution environments trying to capture attention from developers.

Looking at DApp end users, there is now a wide range that span retail, technical, professional and institutional (e.g., hedge funds, pension funds, etc.) participants. We may begin to classify their activity by making very broad distinctions based on their: 1) knowledge of new L1s & protocols being deployed, 2) their risk appetite and, 3) their technical competencies (DApp developer) and/or ability to interact with these ecosystems (from private key management for a retail user to, regulatory constraints for an institution).

Most experienced DApps users are likely to be aware of innumerable risk factors such as, "zombie chains," exchange hacks, "rug-pulls," and smart-contract exploits. On the other hand, there are also wild successes of some emergent projects (MATIC's value relative to BTC since mainnet launch) enabling new use-cases for blockchains, along with the rewards of being among the first to try new DApps (UNI, ENS, dYdX airdrops and many others).

Brand new retail users now have access to seamless centralized integrations between fiat on/off-ramps, crypto asset exchanges, and select L1 blockchains (e.g., Binance and BNB chain). Compelling new use cases, such as remittance payments, loyalty programs, gaming (play-and-earn), integrations with professional sporting leagues, fashion, and tradeable art are playing a role in onboarding new users directly into specific L1 ecosystems.

Bootstrap Ecosystem Growth?

With the above factors in mind, we can begin to get an idea of the many interrelated variables that contribute to developing network effects for L1 ecosystems. From a high-level, deployment of innovative/useful DApps correlates with end-user adoption, which correlates with attracting more developers into an ecosystem. This cycle may continue in a positive feedback loop.

New L1 entrants attempt to crystallize an ecosystem not only by innovating on a purely technical level to address fundamental scaling bottlenecks (as discussed in later sections), but also by targeting specific types of users (developers and DApp users alike) who are likely to migrate over to adopt a new ecosystem. These efforts may include developer grants, native token airdrops, incentivized liquidity mining to increase TVL on-chain (e.g., Avalanche Rush), token-based discounts on exchanges, funding developer & community education, strategic partnerships, and others.

Ecosystem funding

Along those lines, many of the prominent L1 networks (e.g., Avalanche, Near, Solana, etc.) have allocated large sums of capital dedicated towards DApp development and ecosystem expansion. The source of the capital is a mix between external investment firms and native token allocations. Even after the drawdown in the digital asset market this year, most of these organizations are expected to have significant capital to be invested across their ecosystems to attract developers and new DApp users over the coming years.

Notable Ecosystem Funds

Announced Date	Platform	Fund Size ($ millions)(1)	Fund Sponsor(s)	Fund Investment Theme
Jun-22	Immutable X	$500	Temasek, Airtree & aothers	Web3, Blockchain Gaming, NFTs
May-22	Flow	$725	A16Z, Venrock & others	Blockchain Gaming, NFTs
Mar-22	Acala (Polkadot parachain)	$250	Hypersphere, Pantera & others	Defi, General Ecosystem Support
Mar-22	Avalanche	$290	The Avalanche Foundation	General Ecosystem Support
Dec-21	Solana	$150	Solana Ventures, Forte, Griffen	Blockchain Gaming
Nov-21	Tron	$1,111	TRON DAO	General Ecosystem Support
Nov-21	Solana	$100	Solana Ventures, Lightspeed, FTX	Blockchain Gaming
Oct-21	Near	$800	NEAR Collective	General Ecosystem Support
Sep-21	Harmony	$300	The Harmony Foundation	General Ecosystem Support
Sep-21	Algorand	$300	Algorand Foundation	Defi
Sep-21	Cardano	$100	EMURGO	DeFi, NFTs

(1) Represents estimated fund size at fund inception
Data through 12/2/2022
Source: Company press releases

THE BLOCK · Research

New Layer-1 Platforms

Solana's approach to scalability stands in contrast to the current popularity of EVM and an overall trend towards modular blockchains and multichain systems. Solana's monolithic architecture relies on a unique consensus mechanism (using PoH) and "Sealevel" runtime were important innovations, introducing parallel transaction processing. Although Solana has had some difficulties with network uptime (as described earlier), its approach of implementing parallel transaction processing in monolithic blockchains has gained significant traction in the developer community.

Aptos and Sui are two separate blockchain projects that have thus captured a lot of attention. They both employ the MoveVM execution environment and parallel transaction processing to claim theoretical TPS figures that are orders of magnitude higher than typical monolithic blockchains using sequential processing (and no sharding). Aptos uses a modified HotStuff consensus protocol they call AptosBFT that optimizes throughput by using the Block-STM parallel execution engine. This consensus mechanism should theoretically also improve the efficiency of validator resource use. Sui on the other hand, uses the Narwhal and Tusk consensus engine where Narwhal is responsible for data availability and Tusk determines the data order.

User adoption for blockchains that implement MoveVM and parallel transaction processing is yet to be determined. Sui is currently on testnet/devnet as of writing whereas, Aptos only recently launched its mainnet. As such, neither of these chains were included for full analysis in this report. Mainnet launch is expected for Sui sometime in 2022. There is significant interest in overall MoveVM-based chains from the public, developers and investors. Aptos has raised $350 million in funding thus far in 2022, whereas Mysten Labs who are developing Sui recently announced that they have raised $300 million.

Long-Term Viability of Low-Fee Ecosystems

Low transaction fees also mean low recurring network revenue available to pay validators. The answer to incentivizing honest validators in the short-term may simply be token inflation through staking rewards. However, this will likely limit long-term value accrual to the native token where token holders indirectly pay for security via inflation. A number of the ecosystems we have discussed in this report generate as little as hundreds or thousands in USD from daily transactions. These include the lowest-fee ecosystems such as Algorand and Near.

There are many ways networks are experimenting to address this issue that include a fee market, as well as complex mint/burn mechanisms that respond to network usage, staking statistics, and others. Multichain ecosystems are experimenting with two primary approaches that include shared/leased security or fully sovereign chains with independent validator sets. How low-fee ecosystems and individual chains transition towards a sustainable long-term security framework (and compromises made on the way there) is an important factor to track.

New Blockchain-Enabled Applications

For a burgeoning smart-contract platform, what comes first? The DApps, or their users? There are good arguments for both, but at some point, a new and disruptive application with mass-market appeal would definitely help the adoption rate (e.g., emergence of play-and-earn games in the past year).

Although DeFi and NFTs are examples of applications that have garnered significant interest from the public, blockchain technology is arguably still in search of its "killer" apps - similar to what social media and online marketplaces mean for the internet's relevance today. There is excitement and capital invested in several verticals that include blockchain architecture (as discussed before), infrastructure (node networks, staking services, etc.), academic research, education programs, and robust ecosystem development funding (mentioned above).

With the above combined with continued acceptance[1] and awareness of the technology from the general public, it's not a stretch to assume that this space will continue attracting developers that are incentivized to discover, and are equipped to build innovative blockchain-enabled "killer" applications over the long-term.

1 The digital asset class has always struggled with legitimacy in the lay public – is it just a medium for gambling and unbridled criminal activity, or are there any real-world uses? The recent collapse of FTX (the third largest crypto exchange) over a matter of days is a developing story and is outside the scope of this report. However, the shocking allegations (e.g. mismanagement, disregard for regulations and the safety of customer funds) behind the downfall of such a crucial institution led by the colloquial "knight in shining armor" founder may have significantly eroded public trust in the asset class.

Disclosures

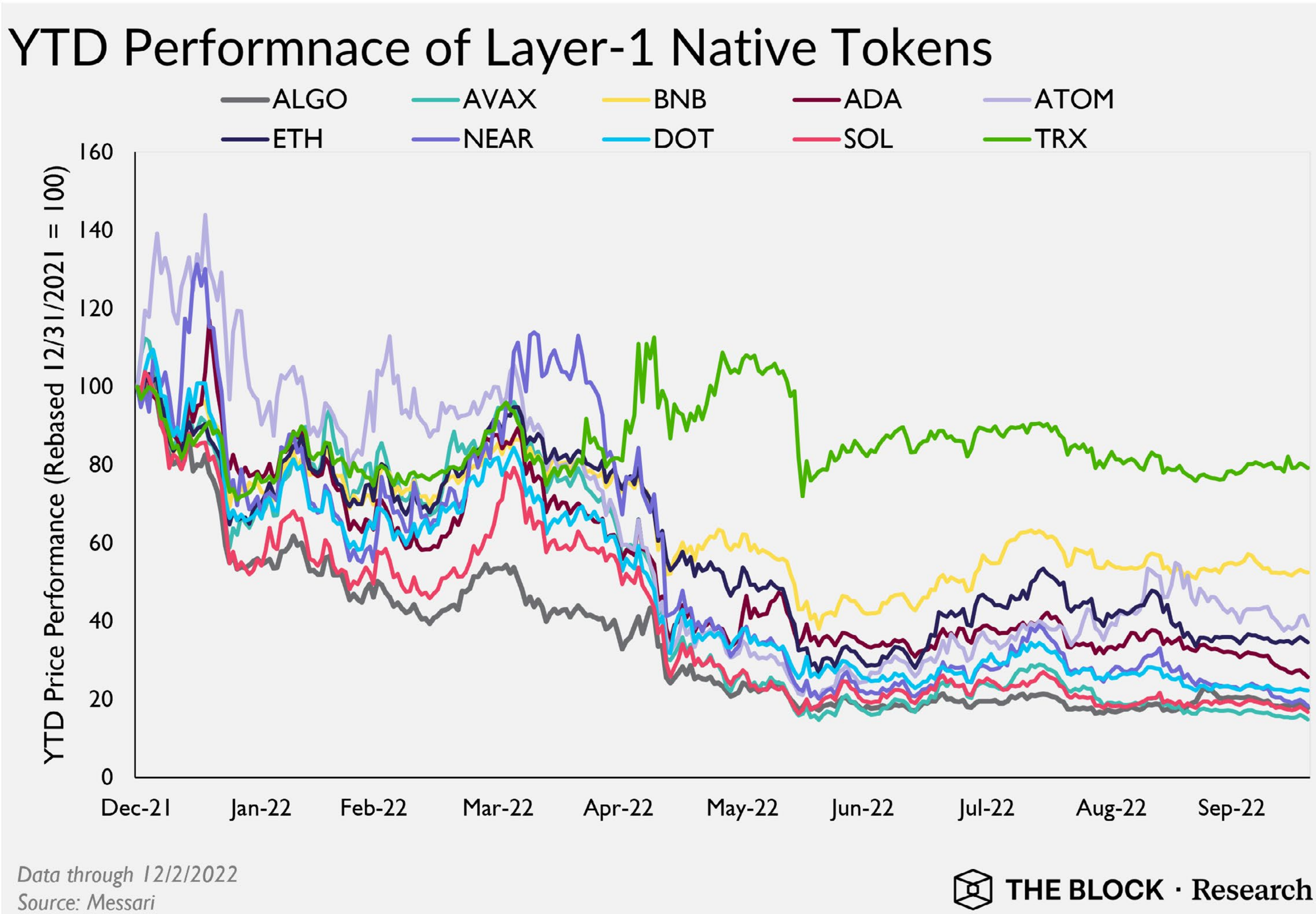
This report is commissioned by Ava Labs and The Solana Foundation. The content of this report contains views and opinions expressed by The Block's analysts which are solely their own opinions, and do not necessarily reflect the opinions of The Block or the organization that commissioned the report. The Block's analysts may have holdings in the assets discussed in this report and this statement is to disclose any perceived conflict of interest. Please refer to The Block's Financial Disclosures page for author holdings.

This report is for informational purposes only and should not be relied upon as a basis for investment decisions, nor is it offered or intended to be used as legal, tax, investment, financial or other advice. You should conduct your own research and consult independent counsel on the matters discussed within this report. Past performance of any asset is not indicative of future results.

Disclaimer: Beginning in 2021, Michael McCaffrey, the former CEO and majority owner of The Block, took a series of loans from founder and former FTX and Alameda CEO Sam Bankman-Fried. McCaffrey resigned from the company in December 2022 after failing to disclose those transactions.

V Appendix

Price Performance of L1 Native Tokens



Overview of Each Focal L1s

Algorand

The Algorand blockchain was launched in 2019 with the native token ALGO, after the project completed a token sale raising over $60M USD. Algorand was the brainchild of Turing award winner, Dr. Silvio Micali. The Algorand Foundation, based in Singapore, was established in 2019 and is responsible for research, development, and fundraising for the Algorand blockchain. The Algorand protocol uses a novel variation of PoS termed, pure-PoS (PPoS) for its consensus mechanism. Algorand has a unique two-tiered blockchain structure, where the base layer manages simpler transactions such as asset swaps and smart contract operations. The second layer processes more complex smart contracts and developmental activity. This separation of processing within the network is thought to increase blockchain efficiency and scalability, according to Algorand.

Avalanche

Avalanche is an open and programmable platform for creating not only decentralized applications, but also custom blockchain networks known as "subnets" for them to operate on. Avalanche was launched in 2020 with the native token AVAX by Ava Labs (a for-profit organization based in New York, USA), founded by Dr. Emin Gün Sirer. The Avalanche network uses a novel consensus protocol (Snowball Algorithm) that aims to optimize scalability, transaction latency and decentralization. The Avalanche network has grown significantly since inception given both its EVM compatibility, as well as popular projects like DeFi Kingdoms launched on their own blockchain subnets using their platform. Avalanche architecture is composed of multiple components that include, C-Chain (executes transactions related to Ethereum-native DApps, and is currently the most-used of the three blockchains), X-Chain (allows for the creation and exchange of new assets built on top of the Avalanche blockchain) and the P-Chain (coordinates Avalanche blockchain's validators and the creation of subnets).

Build-and-Build (BNB) Chain

Binance coin (BNB) was launched alongside an ICO in 2017 (raising $15M USD) on the Ethereum network as an ERC-20 token. BNB utility included discounted trading costs in the Binance centralized exchange (CEX) that also involved quarterly token burns (now transitioned to an algorithmic burn) for a percentage of the token supply. In 2019, Binance launched its own open blockchain initially called Binance Chain, later renamed to BNB Beacon Chain with BNB (BEP-2 standard) as the chain's native token. A blockchain "parallel" to the Beacon chain named Binance Smart Chain (BSC) was activated in 2020 that brought smart-contract functionality and used a proof of staked authority (PoSA) consensus mechanism. As of 2022, the ecosystem underwent another change in nomenclature – both the BNB Beacon Chain and BSC are now both a part of the Build-and-Build (BNB) Chain ecosystem.

Cardano

Cardano was founded by Charles Hoskinson and Jeremy Wood in 2017 with the native token ADA. Development, engineering and fundraising for the Cardano blockchain is conducted by the Cardano Foundation (Swiss non-profit), IOHK (for-profit based in Hong Kong) and Emurgo (Japan). $62 million raised to develop Cardano through ICOs spanning 2015-2017. Cardano is a delegated proof-of-stake (dPoS) blockchain that uses the novel consensus mechanism, Ouroboros. Cardano's development approach is notable due to its emphasis on academic rigor and scientific peer review. In 2020, IOHK published more than 90 academic papers and signed partnerships with global universities. An example outcome of this approach is that Ouroboros is deemed "provably secure" through this review process. Cardano also uses the "extended unspent transaction output" (EUTXO) model similar to Bitcoin's UTXO model, as opposed to Ethereum's account-based transaction model. Cardano's source-code is written in the Haskell programming language that is commonly used in the banking and defense sectors. A downside of Cardano's approach is arguably its slow release of updates relative to other blockchain projects.

Cosmos

Cosmos aims to be the "Internet of blockchain." As the name suggests, its design and architecture reflect the vision of a multichain future from its creators, Jae Kwon and Ethan Buchman. Cosmos whitepaper was published in 2016, and ongoing development is conducted by Tendermint Inc. and the Interchain Foundation (ICF), a Swiss non-profit. Cosmos has the native token ATOM and is powered by a novel PoS consensus mechanism known as Tendermint that uses the IBC for compatibility between blockchains within the Cosmos network. Developers may make use of an open-source framework known as the Cosmos SDK, for building custom blockchains for specific applications. The Cosmos SDK can be used for building public PoS blockchains or permissioned proof-of-authority (PoA) chains optimized for a single application. All chains generated using the SDK are naturally interoperable with one another. The Cosmos ecosystem has seen significant adoption with popular blockchains such as Binance chain, Terra, ThorChain and Cronos that were built using the Cosmos SDK.

Ethereum

Ethereum is the longest operating, most valuable, and most actively used smart-contract blockchain, as of writing. Ethereum was conceived in 2013 by Vitalik Buterin, launched in 2015 after an initial coin offering (ICO) of 72 million ETH (its native token) in an online crowdsale that generated ~$18 million in funding. Notable Ethereum co-founders include Gavin Wood and Charles Hoskinson, both of whom have since released independent blockchain ecosystems with significant market capitalizations (Polkadot and Cardano, respectively). Ethereum's development and maintenance is conducted by the Ethereum Foundation, a Swiss non-profit. Ethereum's general-purpose smart-contract capability has led to the discovery and dissemination of various blockchain-based applications, such as decentralized finance as well as concepts underpinning the Web3 narrative. Ethereum was initially launched as a proof-of-work blockchain. As of September 15th, 2022, Ethereum underwent a successful transition to a proof-of-stake blockchain in a process known as "The Merge." The Merge was the first step in a complex roadmap of planned upgrades that are to follow in the coming years to improve Ethereum's scalability.

Near

The Near protocol was founded in 2018 by Alexander Skidanov and Illya Polosukhin. Near intends to position itself as among the most advanced L1 blockchains in the market with its PoS consensus mechanism called Doomslug that implements state sharding via its Nightshade mechanism. The ultimate vision for Near (native token NEAR) is not only to enable scalability for onboarding billions of users, but also by placing emphasis on user-friendliness for both developers and end users. Near uses its Nightshade sharding mechanism for both processing and storage of data and promises "infinite scalability." Near's claims also include mitigation of slow/expensive transactions due to network congestion through their dynamic re-sharding mechanism to adjust the number of shards based on usage. Near's full functionality and architecture is not yet implemented. Many of these claims are thus not yet verifiable.

Polkadot

Polkadot aims to be an ecosystem of multiple custom blockchains (called parallel chains, or "parachains") with trustless communication, interoperability and scalability, while a "Relay" chain provides security and decentralization guarantees to the ecosystem as a whole. Polkadot's white paper was released by Dr. Gavin Wood in 2016. The Web3 Foundation, a Swiss non-profit, was established to support the research, development and fundraising efforts for Polkadot. Parity Technologies was also founded by Dr. Wood and Jutta Steiner, which maintains Substrate, the development framework for the Polkadot ecosystem. The Polkadot Relay Chain was launched in May 2020 with the native token DOT and subsequently in December 2021 began the process of parachain launches. Parachains are fully customizable via Substrate for any application. All parachains then leverage the Relay chain for their security, finality and voting logic. The Polkadot ecosystem currently consists of two platforms, Polkadot itself and Kasama. Kusama is referred to as Polkadot's "canary network," which is an experimental proving ground for proposed upgrades, new parachains and validating on-chain governance.

Solana

Solana aims to be a high-performance proof-of-stake blockchain with several innovative features that optimize for scalability. Founder Anatoly Yakovenko published Solana's whitepaper in 2017. Novel features for Solana include its proof-of-history timestamp system, Sealevel runtime, Turbine block propagation, and others. Solana Labs is a for-profit entity incorporated in 2018 in the US to support research, development, and fundraising efforts for the Solana Blockchain. Solana Labs began fundraising in Q2 2018 and launched its mainnet beta in March 2020 with the native token, SOL. The founding team has claimed transaction throughput targets of up to 50,000 transactions per second (TPS) for the Solana chain – significantly higher than what is achievable from other monolithic blockchains. Important to note that the Solana chain has experienced several episodes of heavily degraded performance and even network outages in the recent past. However, it must also be noted that Solana is still under beta and is accepted to achieve some of the highest TPS throughputs while delivering high speed, low latency, and inexpensive transactions.

Tron

Tron was launched at the height of the 2017 mania by the polarizing celebrity Justin Sun who had an Asia-focused market strategy for the chain. Development for the Tron blockchain is spearheaded by the Tron Foundation which was originally funded by an initial coin offering (ICO) in 2017. Tron mainnet was launched in May 2018 with the native token TRX. The stated vision is to provide high throughput, scalability, and availability for all applications built atop the Tron chain. Tron is a dPoS blockchain with a 3-layer architecture divided into the storage, core, and application layers. Tron has gained significant attention for its low cost of transactions in comparison to other L1 solutions such as Ethereum.