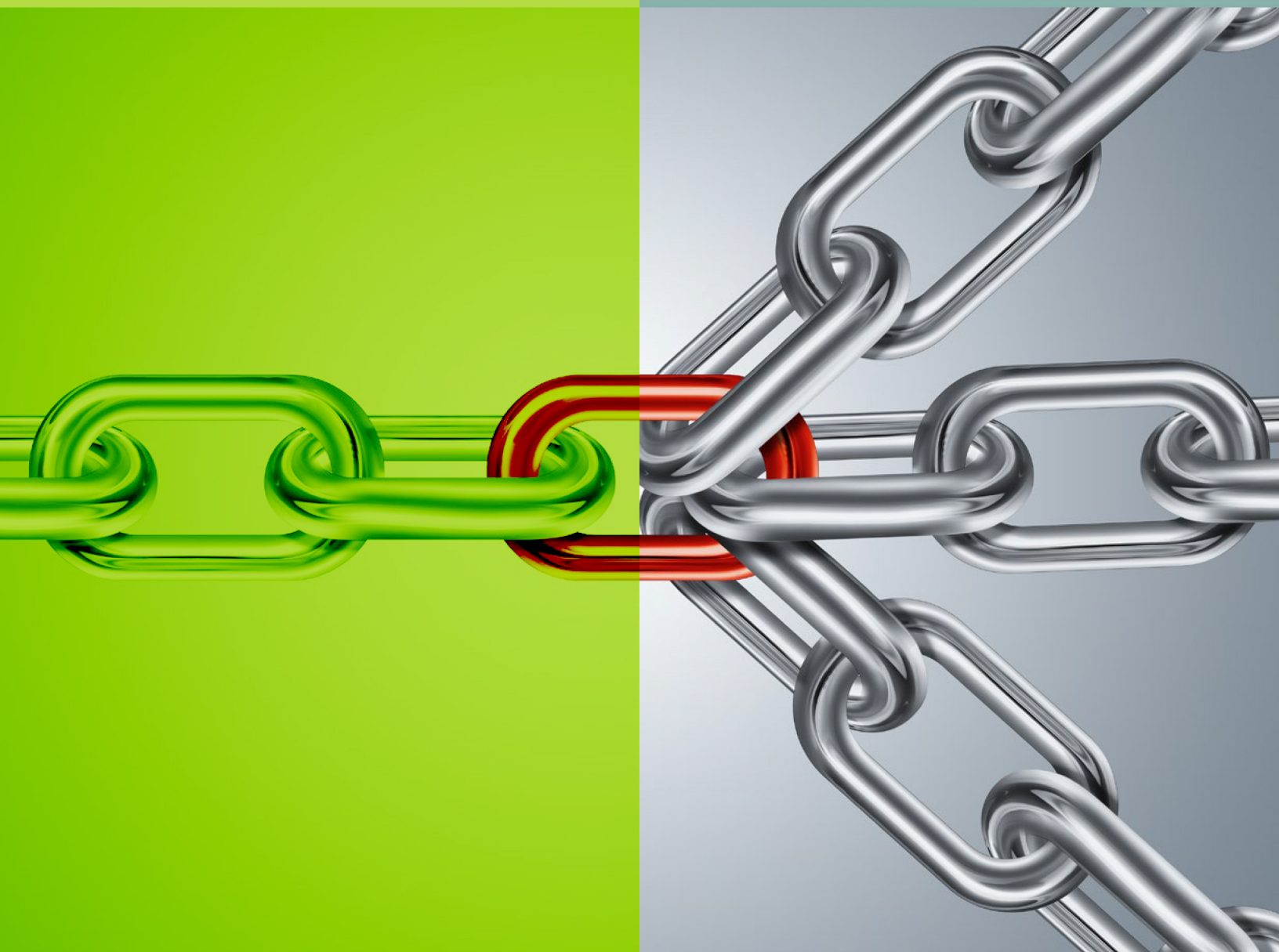


Layer-1 Platforms: *A Framework for Comparison*



COMMISSIONED BY

 Algorand



PUBLISHED ON 08/11/2021

Introduction

Decentralization. Scalability. Security. They are words that are thrown around a lot in the blockchain discourse. But what do they really mean? And how should they be used to analyze different blockchain networks?

Over ten years after the advent of Bitcoin, the quest for answers continues.

Bitcoin has thrown a monkey wrench into how we think about money. It is radically transforming our notion of who controls it, how it is controlled, and who can use it. It is bringing the revolutionary power of decentralized computing to life and its digital cash network has settled and secured trillions of dollars in value.

But Bitcoin is one part, albeit a very important part, of a broader emerging decentralized economy. And if its introduction of digital cash unlocked the door to this economy, Ethereum's smart contracts are kicking it wide open. They unleashed the power of blockchain technology beyond payments to any application imaginable. To date, we have caught glimpses of the impact of its technology. Foremost, in the financial sphere with the rapid growth of stablecoins and the explosion of activity across decentralized exchanges and lending protocols. Secondly, in the cultural sphere with the widespread adoption and rise of non-fungible tokens (NFTs).

And who knows what new applications will emerge next year. Or the year after that.

But the story doesn't stop at Ethereum.

Dozens of smart contracting platforms have launched in tandem with Ethereum's rise. Some are seeking to offer an easily adoptable alternative to Ethereum and challenge its status as the de-facto platform for launching decentralized applications. Others are taking a different approach centered on giving developers the highest level of flexibility in building their own blockchains and creating infrastructure to facilitate cross-blockchain communication.

Introduction

They span platforms that very much embody the decentralized ethos of Ethereum to others that are pushing the limits of what minimal level of decentralization users will accept. They are making bold technical design choices primarily aimed at delivering scalability; a feature that Ethereum has historically lacked.

The breakneck pace of development and competition amongst these platforms is not slowing down anytime soon.

Why are we writing this report?

While this emerging decentralized economy has seen exponential, albeit lumpy, growth over the past years, we have only scratched the surface in terms of discovering what experiences smart contracting platforms are capable of delivering. As use cases evolve and application development accelerates, platforms are poised to support ecosystems orders of magnitudes larger than those we have seen to date. Nonetheless, they already compose a material portion of the investable crypto landscape today.

The Investable Crypto Landscape



Source: The Block Research, Messari, Factset; Market caps as of 6/30/21. Private market investments not included. Images not shown to scale.

With each passing year, the likelihood of a “one blockchain to rule them all” outcome fades further and further into the rearview. But analyzing these platforms continues to be a challenging task. Objec-

Introduction

tive and digestible comparisons amongst them are few and far between. The lack of standards for discussing and analyzing them causes headaches. Having a framework for comparing these platforms will be important for years to come.

How we are structuring this report

Analyzing smart contracting platforms outside of the context of Ethereum is difficult. Analyzing Ethereum outside the context of Bitcoin is equally difficult. So, the report starts with an introduction to Bitcoin, what it introduced, and the prospect for use cases outside of payments on its platform. It then provides an introduction to smart contract platforms, what they are used for, and dives into the current state of Ethereum.

With this background, we analyze a select set of platforms. We compare and contrast them across their technical designs, their blockchain and ecosystem data, and the individuals and organizations behind them. Finally, we use these comparisons to draw insights into what the future of the broader smart contracting platform landscape could look like.

Commissioned by



Algorand Inc. - Algorand builds technology that accelerates the convergence between decentralized and traditional finance by enabling the simple creation of next-generation financial products, protocols, and exchange of value. Founded by Turing Award-winning cryptographer Silvio Micali, Algorand's platform is designed to handle the volume of transactions needed for Decentralized Finance (DeFi), financial institutions, and governments to smoothly transition into the Future of Finance (FutureFi).



The Algorand Foundation - The Algorand Foundation is dedicated to fulfilling the global promise of blockchain technology by leveraging the Algorand protocol. With core beliefs in the establishment of an open, public and permissionless blockchain, the Algorand Foundation has a vision for an inclusive ecosystem that provides an opportunity for everyone to harness the potential of an equitable and truly borderless economy.



Author
Andrew Cahill

[Twitter](#)
[LinkedIn](#)

Acknowledgments

We would like to thank Algorand Inc. and the Algorand Foundation for commissioning this research report and making its production possible.

We are also grateful to those that shared their perspectives and were interviewed for this report including individuals across the following organizations:

- Algorand Inc. and Algorand Foundation (Algorand) – Keli Callaghan, Paul Riegler, David Markley, Stephen Duignan
- Ava Labs (Avalanche) – Kevin Sekniqi, Lydia Chiu, John Nahas, Eric Kang
- Binance (Binance Smart Chain) – Samsul Karim
- Tendermint, Interchain Foundation, Informal Systems, Sikka (Cosmos) – Peng Zhong, Billy Rennekamp, Ethan Buchman, Sunny Agrawal
- Parity Technologies and Web 3 Foundation (Polkadot) – Peter Mauric, Joe Petrowski
- Solana Labs (Solana) – Anatoly Yakovenko, Raj Gokal, Ben Sparango

Finally, we thank everyone at The Block who helped with its production including Larry Cermak, Mika Honkasalo, and Igor Igamberdiev. Additionally, we thank Aleksander Hamid for designing the report. The author, Andrew Cahill, has holdings in the following tokens mentioned in the report: ALGO, ATOM, BTC, and ETH.

Introduction

Bitcoin Origins

There are many unknowns regarding Bitcoin's pseudonymous creator(s), Satoshi Nakamoto. But a few certainties can be gleaned. Satoshi was not living in a vacuum. And Bitcoin was not conceived out of thin air.

Anonymous digital cash and pseudonymous reputation systems were being designed in the 1980s. Proof of Work, a core design feature of Bitcoin, was introduced as an anti-spam measure in the 1990s. And, at the highest level, Satoshi put the two together to create Bitcoin in 2008.

The Bitcoin network is best described in a few select words.

It is censorship-resistant and decentralized. Bitcoin is not owned by any single entity. While governments can enact legislation prohibiting mining or transacting in Bitcoin, there is no universal "off switch" for the network as it is operated by a global, distributed base of computers.

It is permissionless. Anyone can send, receive, and hold bitcoins ("BTC") from virtually anywhere on a 24/7 basis. Anyone willing to invest in computer hardware can contribute to securing the network through mining.

It is pseudonymous. The closest thing to identifiable people on the network are strings of alphanumeric characters which in some cases, can be mapped to certain individuals, but in other situations represent groups of individuals or corporations.

It is secure. Bitcoin miners are economically incentivized to secure the Bitcoin network and they earn BTC in return for doing so. BTC's disinflationary issuance schedule introduced a new-found model for bootstrapping network security and has allowed the network to achieve a high level of security early in its life.

Beyond BTC: Omni Layer and USDT

Bitcoin's most prominent use case to date has been settling and storing value with its native asset, BTC. But its programming lan-

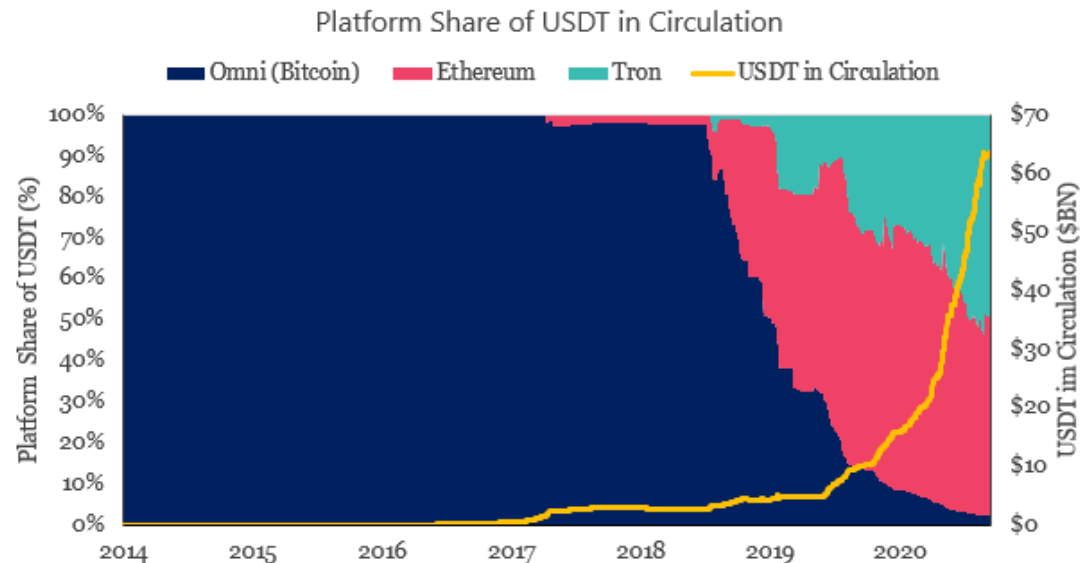
Introduction

guage, Script, allows for more complex transactions. Multi-signature functionality can be used to restrict access of funds until a certain number of distinct entities, such as two out of three, sign or approve transactions. Data storage functionality allows users to write up to 80 bytes worth of data onto the Bitcoin blockchain and use it as an immutable data ledger.

Accordingly, decentralized securities trading, property rights, and self-sovereign identity were all concepts being explored in the Bitcoin community as early as 2011.

Founded in 2012, the Omni protocol (originally named Mastercoin) has been one of the most prominent users of Bitcoin's capabilities as an immutable ledger. It created a protocol for asset issuance using Bitcoin's data storage capabilities and has facilitated the creation of hundreds of assets directly on the Bitcoin ledger.

Tether's stablecoin, USDT, is the most prominent asset issued using Omni. USDT is backed by a basket of assets that help it achieve a peg to the value of the US Dollar. Among other use cases, traders rely on it as a stable asset to park funds in on exchanges that do not support traditional currencies.



Source: The Block Research, Coin Metrics

Introduction

“At Tether, we truly care for Omni, since it was the first protocol that made Tether possible, and it also relies on Bitcoin security. But we had to give traders what they were asking for”

— Paolo Ardoino, CTO at Tether

While USDT was historically issued exclusively on Omni for ~3 years, it started making its way onto Ethereum in 2018 and onto another smart contract platform, Tron in 2020. It has also been issued on several other platforms including Algorand, Avalanche, Solana, and EOS. As of today, only about 2% of the ~\$63BN worth of USDT in circulation resides on the Bitcoin blockchain.

Not all USDT are created equal

USDT is backed by the same basket of assets regardless of where it is issued. Nevertheless, it inherits the performance and security characteristics of whichever blockchain it is issued on and user experience can vary widely on a chain-by-chain basis.

So, there are multiple reasons why USDT has become less popular on Omni:

- i. The cost to transact in USDT on Omni is high relative to other chains as it necessitates effecting data storage transactions on the Bitcoin blockchain.
- ii. Confirmation times, or the amount of time before USDT transactions are considered final, are high on Omni due to Bitcoin’s 10-minute block time and probabilistic finality.
- iii. Ecosystem growth on other chains is driving demand for USDT on their respective chains.

So, yes, USDT can be issued and transacted with on the Bitcoin blockchain. But the more appropriate question to ask is: “does it really need to be”. The numbers are speaking for themselves. Smart contract platforms with lower fees and faster confirmation times, albeit with different security profiles, are becoming a more popular venue for USDT.

Beyond Payments: Sidechains and Smart Contracts

More generally speaking, changes to the Bitcoin software have historically and will likely continue to be handled very conservatively. Bitcoin does not rapidly adapt to the new demands of the market.

Introduction

For instance, the Taproot upgrade, which is expected to take effect in November 2021 is the first major Bitcoin software upgrade in over four years.

Given this conservatism and the relatively limited set of programmability within Bitcoin software, the concept of creating auxiliary blockchains, referred to as sidechains, was being researched in depth as early as 2014. These separate chains typically aim to enhance performance and provide a higher level of customizability than the core platform, in this case, Bitcoin. They also leverage the core platform's established security profile to varying degrees. Rootstock ("RSK") is one example of these sidechains.

RSK leverages the security mechanisms of Bitcoin through a process called merge mining. Through merge mining, miners who are dedicating computing (hashing) power to securing the main Bitcoin blockchain can opt-in to mining a secondary chain, in this case, the RSK sidechain, and earn transaction fees generated on RSK. During this process, data from blocks mined on the RSK sidechain is periodically hashed and inserted into the blocks of the primary blockchain. Currently, the RSK sidechain is being merge mined by around 40% of the hashing power on Bitcoin.

RSK also "re-uses" BTC as an asset on its sidechain. The network has a two-way peg mechanism whereby BTC is exchanged for RSK Smart Bitcoin (RBTC) on a 1:1 basis. This is facilitated by "pegging-in" BTC by sending it to a multi-signature wallet on the Bitcoin blockchain and minting RBTC on RSK. RBTC can then be "pegged-out" from RSK to BTC on Bitcoin when nodes running the RSK pegging module, RSK PowPeg, validate the withdrawal request. This allows RSK to leverage BTC in a more flexible environment but introduces reliance on node infrastructure independent of the Bitcoin network to facilitate these pegging processes.

What can be built on RSK?

The RSK blockchain is compatible with the Ethereum Virtual Machine ("EVM") which executes transactions on the Ethereum blockchain.

Introduction

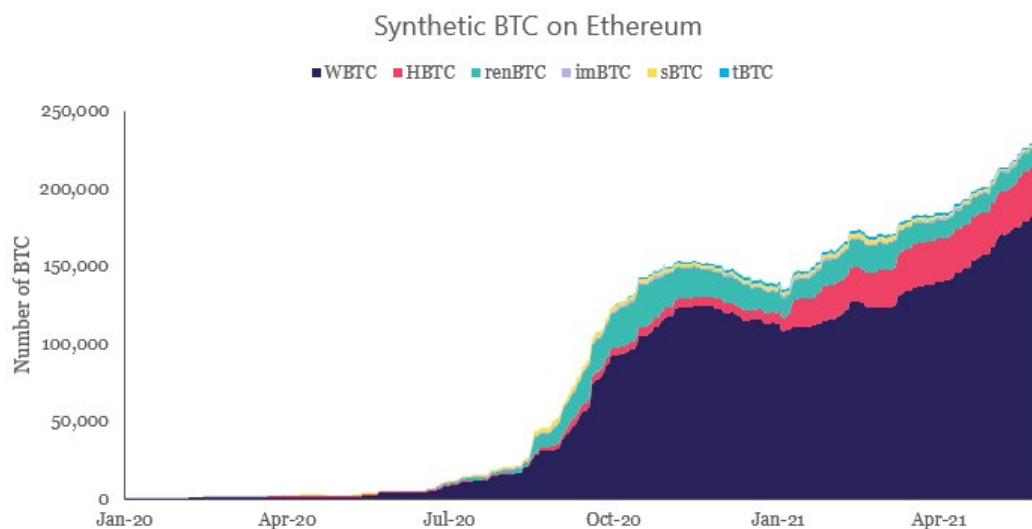
Hence, any applications supported on Ethereum can theoretically be built on RSK.

Launched in December of 2020, Sovryn is one of the more prominent projects building on RSK. The protocol is aiming to bring many of the decentralized finance (“DeFi”) functions such as decentralized exchange and lending, to the Bitcoin ecosystem by employing RSK smart contracts. While it has seen some adoption since its launch, other platforms such as Ethereum and Binance Smart Chain are supporting DeFi ecosystems orders of magnitude larger than what RSK has achieved to date.

Ethereum as a Bitcoin sidechain

In one sense, Ethereum has been Bitcoin’s biggest sidechain to date. While it does not leverage Bitcoin’s security framework, it is the biggest venue for “re-using” BTC in a more flexible environment with smart contracts.

Upwards of 245,000 synthetic BTC (assets whose value is tied to BTC and issued on Ethereum through similar pegging mechanisms), worth ~\$8.5BN, have been ported to the Ethereum blockchain. This far exceeds the current amount of BTC that can be ported onto RSK as its PowPeg is currently capped at 3,000 BTC.



Source: Alchemy

Nonetheless, the quantity of BTC that has been ported over to Ethereum is a powerful signal of the value and network effects that BTC possesses. BTC represents a several hundred-billion-dollar pool of capital. To date, it has seen widespread adoption as a store of value asset but yield generating strategies directly within its ecosystem and security framework have been limited. The evolution of projects like Sovryn will provide insight into how much value sidechains such as RSK can deliver within the Bitcoin ecosystem. Whether or not RSK and other sidechains can become a contender in the smart contract landscape will likely be determined by the success of what is built on top of them.



II

Introduction to Smart Contract Platforms

Smart Contracts Defined

The basic idea of smart contracts, according to their initial proposer, Nick Szabo is that "many kinds of contractual causes (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make a breach of contract expensive (if designed, sometimes prohibitively so) for the breacher.

Why work within the confines of the Bitcoin ecosystem at all when you can start from scratch? The most successful "start from scratch" blockchain to date has been Ethereum. In contrast to Bitcoin's limited base layer programmability, Ethereum launched with customizability and programmability as a first principle. It introduced smart contracts, which had been proposed as early as the 1990s, and expanded the reach of blockchain technology to an unbound number of disciplines, not just payments.

What are smart contracts?

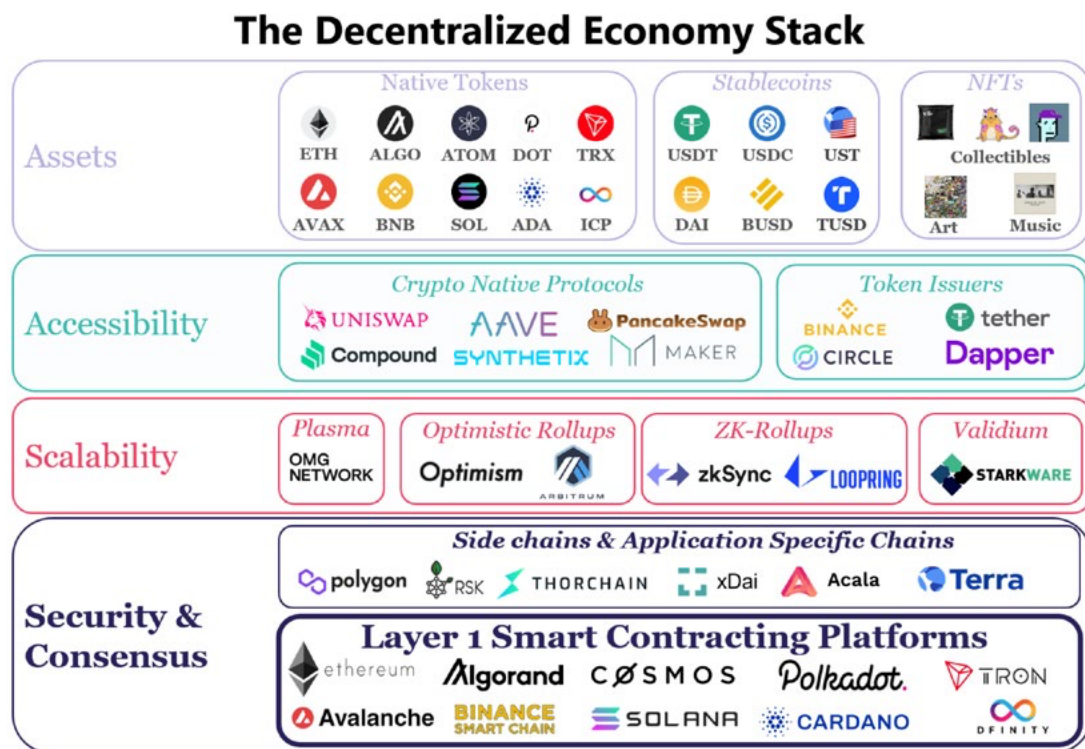
In today's vernacular, smart contracts refer to computer programs that are deployed and executed on blockchain networks. They are being used to facilitate all kinds of functions from decentralized asset exchange to decentralized lending to blockchain-based asset issuance and tokenization. They were initially proposed by computer scientist and cryptographer Nick Szabo in the 1990s. He called vending machines a "primitive ancestor of smart contracts," since they take coins and dispense a product and the correct change according to the displayed price.

Smart contracts execute under a predefined set of conditions and once they are deployed to a blockchain, they cannot be "undeployed". Anyone with the technical expertise to code them can deploy them. And theoretically, anyone with sufficient funds to cover transaction fees can interact with them once they are deployed.

What are smart contracting platforms?

Smart contract platforms, unironically, provide a venue for deploying smart contracts and decentralized applications. They are owned, operated, and secured by distributed bases of token holders and computer hardware operators which makes them difficult to censor and provides for their 24/7 operation. They serve as the base security layer of this emerging "decentralized economy stack" presented below. And everything that is built on top of them inherits their security, performance, and censorship-resistance characteristics.

Introduction to Smart Contract Platforms



Source: The Block Research

Defining the Layers of the Decentralized Economy Stack

Layer 1 Smart Contracting Platforms are the topic of this report. They set the rules for how networks are secured and how they come to agreement on the state of the blockchain(s). They span general-purpose blockchains such as Ethereum which provide a platform for launching applications deployed as smart contracts to Polkadot which resembles a “Layer 0” platform as it provides developers a security framework for deploying their own Layer 1 blockchains.

Sidechains and Application-Specific Chains such as RSK, are blockchains with distinct consensus processes and security profiles from Layer 1s. Application-specific chains are one example of blockchains that are deployed under the development framework of a Layer 1 platform such as Cosmos, yet nonetheless have independent security models.

Scalability solutions are typically referred to as Layer 2 solutions. They aim to enhance the performance of Layer 1 platforms by offloading transaction execution onto separate chains. They leverage the security frameworks of their underlying Layer 1s to varying degrees and when they rely heavily on their own security frameworks rather than those of their related Layer 1 platform, they qualify as sidechains.

Crypto Native Protocols and Token Issuing Companies are the “gas guzzlers” that consume the computational resources of Layer 1 platforms and scaling solutions. They allow users to tap into the decentralized economy by building blockchain based products and services. Crypto native protocols exist as smart contracts on blockchains and are typically owned and governed by online blockchain communities. Token issuers are one example of traditional companies that leverage Layer 1 platforms for asset issuance among other use cases.

Blockchain-based assets are issued on top of Layer 1 platforms. Native tokens are used to secure Layer 1 networks, pay transaction fees on them, and in some cases grant holders a degree of say in platform governance. Stablecoins and NFTs are two examples of the many types of assets that are being issued on top of Layer 1s.

How do Layer 1 platforms provide security?




Layer 1 networks need to provide security in an environment where anyone, with good or bad intentions, can participate in operating the network. Sybil resistance mechanisms are how they achieve this security. They create incentive structures that aim to prevent one or few “malicious” entities from being able to temporarily subvert or stall the network for their own gain to the detriment of other network participants.

To date, there have been three major sybil resistance mechanisms employed: Proof of Work (PoW), Proof of Stake (PoS), and to a lesser extent, Proof of Authority (PoA). They all typically aim to achieve security by:

- i. Encouraging participants to come to consensus (agreement) on the state of the blockchain through a competitive process
- ii. Rewarding some or all participants for coming to agreement
- iii. Punishing participants that make efforts to stall the network from reaching agreement or for more directly trying to subvert it

The table below provides an overview of these different mechanisms and how they are operationalized.

Introduction to Smart Contract Platforms

Sybil Resistance Mechanisms Overview			
Mechanism	Competition	How to compete	Punishment for misbehavior
 Proof-of-Work (PoW)	Computational work	Perform computational work to solve mathematical puzzles first	Proposing an invalid block after solving the puzzle does not earn rewards and results in unrecovered energy costs
 Proof-of-Stake (PoS)	Financial stake	Put financial stake at risk to gain a larger share of network rewards	If a node goes offline or signs invalid transactions, it risks losing the financial stake it put at risk through slashing and can be excluded from consensus
 Proof-of-Authority (PoA)	Reputation	Undergo authentication process to gain the right to participate in the network	If a node goes offline or signs invalid transactions, it can be excluded from consensus and face other penalties imposed by the consortium of approved validators

Source: The Block Research, CoinDesk

To date, the majority of activity in the greater blockchain ecosystem has been secured by PoW blockchains such as Bitcoin and Ethereum. In these networks, computational work must be performed to earn rewards, and security is typically quantified by measuring how difficult it is to obtain 51% of the total computing power on the network. Once one or few entities accumulate 51% of this computing power, they are capable of censoring the network and intentionally excluding transactions or, in some cases, double spending coins.

The vast majority of smart contract platforms employ PoS or some variation of it. In these networks, economic incentives surrounding staking are employed to achieve security. Security is often quantified by how difficult it is to obtain 33% of the aggregate financial stake being used to secure the network. Once one or few entities accumulate 33% of the stake in a PoS network, they are capable of censoring the network and can stall it from coming to agreement.

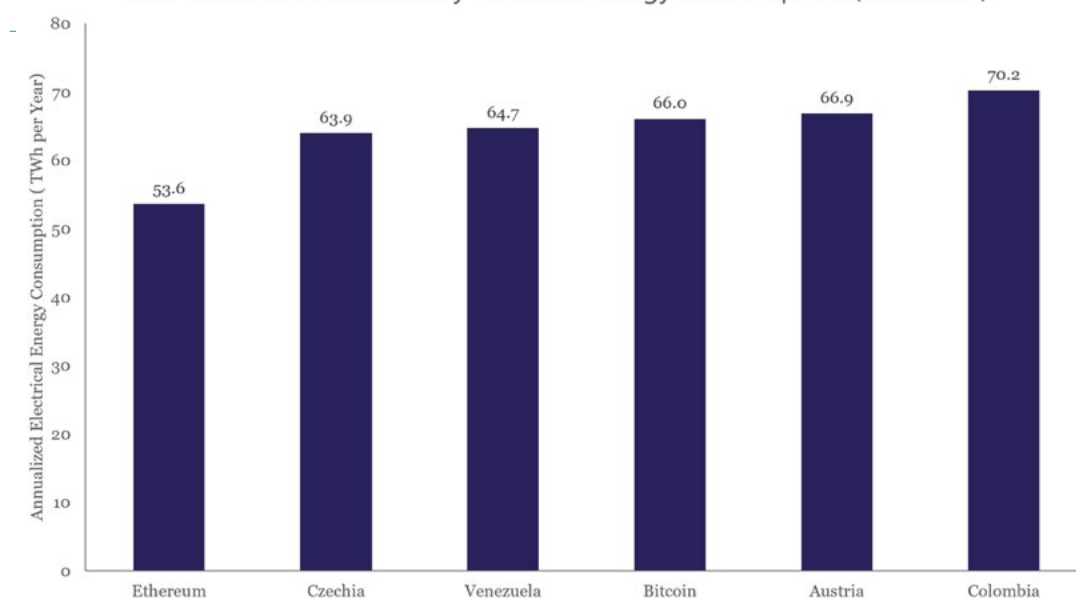
In summary, computational power defines network influence in PoW and financial capital defines network influence in PoS. This divergence has important implications for one of the most hotly debated topics in the blockchain discourse: energy consumption.

Sybil resistance and sustainability

PoW is by far the most energy-intensive sybil resistance mechanism. Performing more computational work in PoW networks translates to a higher likelihood of gaining rewards from block subsidies and transaction fees. So, it is not surprising that miners have competed to perform

more work to earn more rewards; especially as BTC and ETH's prices have risen over the past years and increased the value of these rewards.

PoW Blockchains vs Country Electrical Energy Consumption (Estimated)



Source: Cambridge Center for Alternative Finance, Digiconimist; Estimates as of 6/30/2021. Estimates subject to large fluctuations as they are calculated by annualizing current levels.

How much electricity do Bitcoin and Ethereum actually consume?

The Cambridge Center for Alternative Finance estimated that Bitcoin accounted for ~0.30% of global electrical energy consumption as of the end of June 2021. As seen in the chart above, Bitcoin and Ethereum's estimated electricity consumption are both in the range of small nation-states.

Nonetheless, the topic of energy consumption for PoW blockchains has layers of nuance and complexity.

Energy sources, opportunity costs, and security

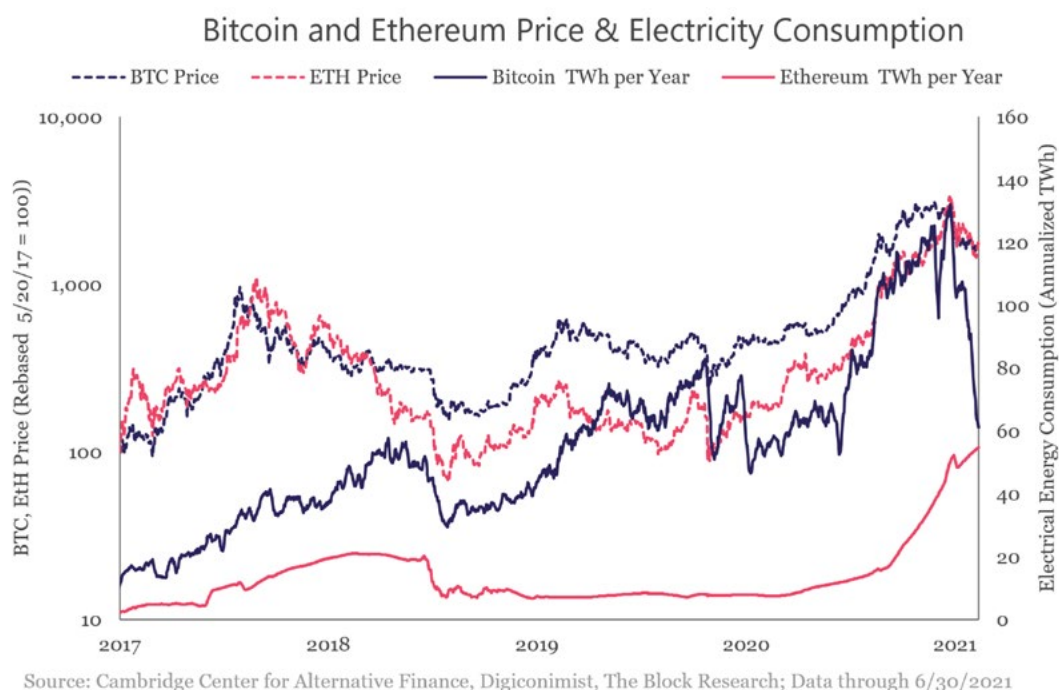
Electrical energy consumption and carbon footprint are not synonymous. Electricity is generated from several different energy sources such as coal, natural gas, hydro, and solar power that all have different carbon footprints. Estimating the total carbon footprint of a PoW network necessitates pinpointing the mix of energy sources employed by the operators of these networks.

Additionally, the opportunity cost of using energy to secure PoW networks is an important consideration. In some instances, PoW mining is being used to monetize energy that would otherwise be stranded and potentially never put to productive use. In other instances, there is a case to be made that PoW mining is competing with other “more legitimate” uses of energy and pushing up the cost of energy across certain regions.

Blockchain security is also an important consideration. All else equal, more electricity being dedicated to mining PoW chains makes them harder to attack and increases their censorship resistance. PoW chains with very low levels of electricity consumption have consistently been exploited in attacks and are less secure environments for deploying applications.

What is the outlook for energy consumption for PoW chains?

Ethereum’s energy consumption will be significantly reduced when its network transitions to PoS, which is estimated to happen some-time within the next 18 months.



"The mechanics of measuring the environmental impact of a global decentralized and widely used blockchain are nuanced and complex. That's why we are teaming up with ClimateTrade to continue and double-down on our eco-conscious efforts...We find it crucial to operate at a carbon-negative level"

—
Silvio Micali, Founder at Algorand

How much energy Bitcoin and other PoW blockchains will consume in the future will be impacted by several factors. The future price of their native assets, their issuance schedules, the efficiency of mining equipment, where mining is concentrated geographically, and execution or lack thereof on initiatives to move to more sustainable energy sources are all variables that need to be considered.

Historically, higher prices of native assets, such as BTC and ETH, have raised the breakeven cost for mining and, with a lag, resulted in increased electricity consumption. But whether this relationship will persist in the future is dependent on the intersection of the factors mentioned above.

Is the electricity consumption worth it?

Whether or not Bitcoin and Ethereum, or any other PoW chains, are worth their energy consumption depends on how the services provided by their networks are valued.

To those who think that PoW blockchains, and Bitcoin, in particular, provide critical financial access to individuals, it is a worthy consideration for energy use. In that case, comparing the energy consumption of these PoW chains to use cases that they are potentially absorbing or providing superior alternatives to is the appropriate analysis. The resources required to extract gold, run payments and banking infrastructure, or more broadly, the costs suffered by individuals living under hyperinflationary monetary regimes could all serve as appropriate measuring sticks.

To those who think PoW chains solely serve as arenas for excessive speculation or are used extensively for money laundering, they do not provide value and are a wasteful use of energy.

Finally, there are many who think PoW networks provide valuable services yet view current levels of energy consumption as unacceptable. Some are taking initiatives to increase reliance on renewable

sources of energy for PoW mining. Others are employing less energy intensive sybil resistance mechanisms such as PoS.

How much less electricity do PoS networks consume?

Given that participants in PoS networks compete on accumulating financial stake rather than performing computational work, they consume far less electricity than their PoW counterparts. The Ethereum Foundation estimates that Ethereum's move from PoW to PoS will result in a 99.8% reduction in its network's electricity consumption. This is a good starting point for quantifying just how much less energy PoS networks consume.

Additionally, PoS networks such as Algorand are pushing the pace of blockchain sustainability even further. Algorand has committed to being carbon negative and is purchasing carbon offsets for the energy consumption of its entire network. It will do so by employing a sustainability oracle that periodically notarizes the network's carbon footprint on-chain and purchases carbon credits, which are tradable as blockchain-based assets, from partner ClimateTrade.

III

The Current State of Ethereum

The Current State of Ethereum

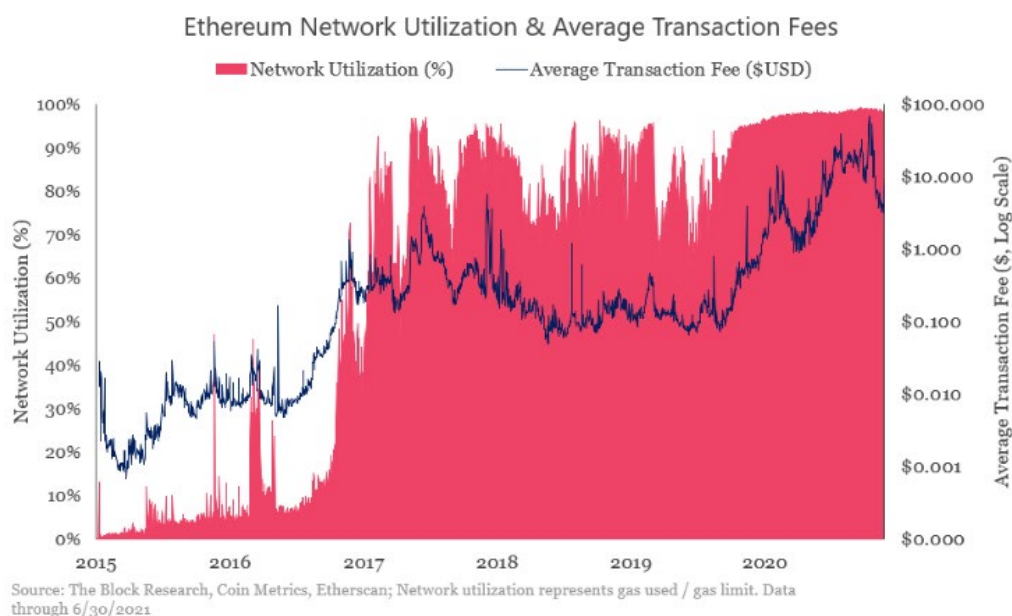
Ethereum is the first major smart contracting platform. To date, it has seen the highest level of adoption and usage. And while the broader smart contracting platform landscape is rapidly evolving, developments within the Ethereum ecosystem have repercussions for the entire crypto market.

To say a lot is going on in the Ethereum ecosystem would be an understatement. Its network is routinely facilitating the transfer of tens of billions of dollars of value daily. Over \$50BN of value is currently sitting in smart contracts on its network to facilitate decentralized asset exchange, lending, insurance, and payments among other use cases. And on the technical front, an array of solutions are being developed to tackle the biggest challenge facing its community: scalability.

Ethereum's Scalability Challenge

Ethereum's scalability challenge is not a new phenomenon.

The advent of CryptoKitties NFTs and the activity surrounding them gave us a glimpse of the scalability limitations of the platform as early as 2017. But this time around, the explosion of DeFi activity is driving a more pronounced and sustained increase in fees that has brought these limitations center stage.



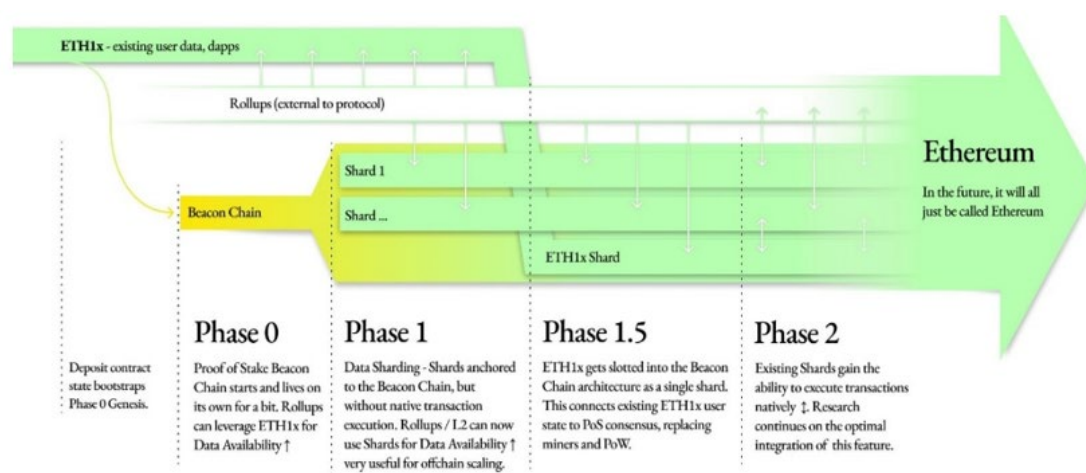
The Current State of Ethereum

According to data from Coin Metrics, the average fee a user paid to execute a transaction on Ethereum was around \$0.08 at the start of 2020. It has been as high as \$68.00 on certain days over the past year. And depending on the type of transaction being executed, many have cost in the hundreds of dollars. Wow.

For some users, high fees have gone from being an inconvenience to an outright deterrent to transacting on the Ethereum platform. Many have started exploring the greener pastures of other platforms that offer similar applications with lower transaction fees, albeit with different and oftentimes inferior security profiles. On the development side, applications have begun deploying their technologies on Ethereum Layer 2 scaling solutions and sidechains to provide users lower transaction fees while still leveraging Ethereum's established decentralization and security characteristics to varying degrees.

Ethereum's Technical Roadmap

To overcome these scalability challenges and provide better user experiences, while also not compromising on the network's decentralization, there are several development initiatives underway in the Ethereum community. The visualization below by Trenton Van Epps captures the concurrent and intertwined nature of the technical roadmap.

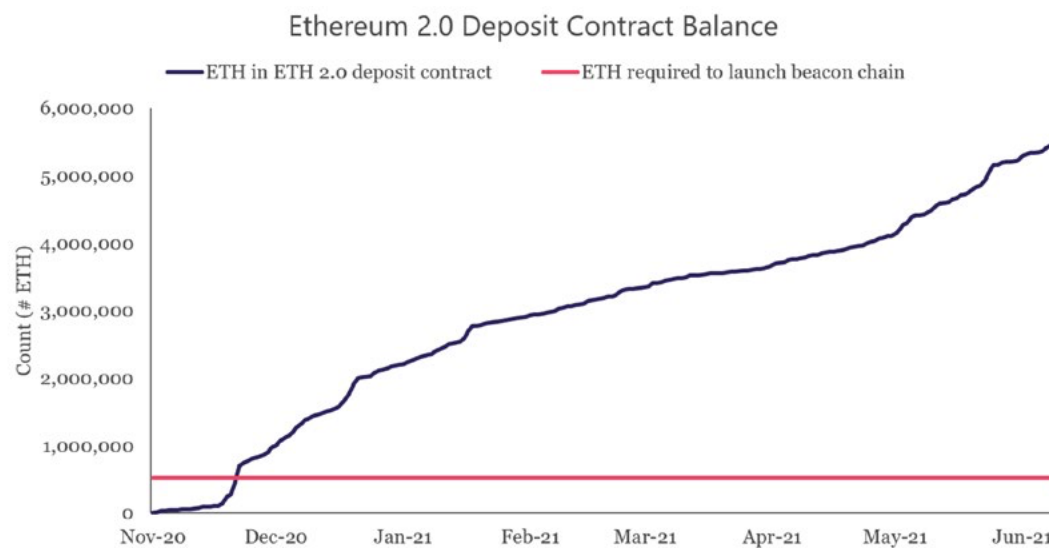


Source: Trenton Van Epps; Given recent progress in layer 2 scaling solution research and development, Phase 1.5 has since been prioritized over phase 1

The Current State of Ethereum

The roadmap can be broken down into two workstreams:

- i. Scaling at Layer 2, which does not require any changes to the underlying base Ethereum layer
- ii. Scaling at Layer 1, which, at a minimum, involves changing the network's sybil resistance mechanism from PoW to PoS, and changing its architecture from a single blockchain to a multi-chain network, referred to as Ethereum 2.0



Source: The Block Research, Ethersean

Phase 0 marked the preliminary launch of the Ethereum 2.0 network. Ethereum 2.0's architecture will consist of a beacon chain and 64 homogenous chains referred to as shards. The beacon chain will manage organizing the network's validator set into committees and nominating block proposers for each of these respective committees. It will also serve as an anchor point on which the shards register their states to facilitate cross-shard communication. The beacon chain officially went live in December 2020 after the network reached 16,384 validators who had collectively staked 524,288 ETH.

Phase 1 will kick off the data sharding of the Ethereum network. This is when the 64 homogenous shard chains will be formed. While these shards will not perform transaction execution initially, they will

The Current State of Ethereum

"The Ethereum ecosystem is likely to be all-in on rollups (plus some plasma and channels) as a scaling strategy for the near and mid-term future"

—

Vitalik Buterin, Ethereum Co-Founder

increase the amount of data the Ethereum network is capable of storing and deliver performance gains in connection with Layer 2 scaling solutions. While Phase 1 was originally slated to occur before “the merge” which is described below, it has since been postponed until after the merge.

Phase 1.5, also referred to as “the merge”, will mark the Ethereum network’s official move from PoW to PoS. In this phase, the Ethereum network in its current state will be ported over to Ethereum 2.0 as a shard. The merge is slated to happen over the coming 6 to 18 months according to estimates from the Ethereum Foundation.

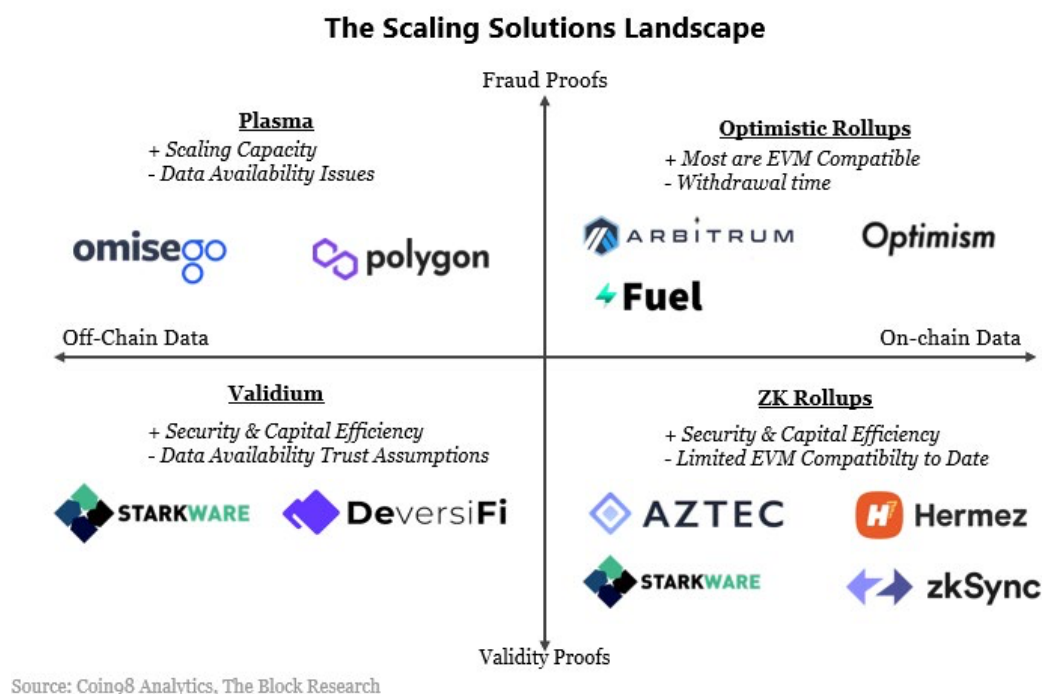
Phase 2.0 would mark the final phase of the Ethereum network upgrade and take transaction execution into the shards of the Ethereum 2.0 network. It is still uncertain whether phase 2.0 will happen or if the future will be “roll-up-centric”. If the future is indeed roll-up-centric, the Ethereum 2.0 network will solely be used for security and data availability rather than transaction execution.

The scaling solutions patchwork

Irrespective of the changes to the Ethereum 2.0 data structure, a patchwork of different scaling solutions are being employed to enhance the performance of the Ethereum network in its current, single chain state. They all aim to offload transaction execution from the main Ethereum blockchain and increase scalability, but they do so in a diverse range of ways. Notably, these scaling solutions are not specific to Ethereum and could be adopted across other networks.

Key considerations for analyzing these scaling solutions include: (i) to what degree they inherit the security and network effects of their underlying Layer 1 and (ii) whether they impose additional requirements on users that are more stringent than what is expected on the base layer. The graphic below outlines four of the more popular approaches.

The Current State of Ethereum



Rollups

Rollups are solutions that perform transaction execution outside Layer 1 but make transaction data available on Layer 1.

In optimistic rollups, batches of transaction data are posted to the main chain and presumed to be valid (optimistic) but can be challenged. Theoretically, anyone can challenge them by submitting a claim, also known as fraud proof, to prove that a batch committed to the chain contained invalid state transitions. If the fraud proof is valid, these invalid state transitions would be rolled back. Additionally, the proof publisher would be entitled to collateral (bonds) posted by the sequencers who batch the data. Thus, there is an economic incentive for users to monitor the validity of this transaction data.

Batches posted to the main chain can be disputed for several days (typically 1 week) during which funds on these Layer 2s cannot be withdrawn back to the main chain which could create a challenge from a usability perspective. However, several projects are working on providing liquidity to Layer 2 users to bridge this withdrawal period. Importantly, existing smart contract languages are supported in optimistic rollups, which allows for existing applications to easily be ported over to these solutions.

The Current State of Ethereum

Zero-knowledge rollups are similar to optimistic rollups in that they post all transaction data onto the main chain. However, they use zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) to validate transactions. Once these validation proofs are completed and posted to the main chain, all the transactions included in them are considered final. The computational power required to generate these proofs by the Layer 2 nodes is higher than optimistic rollups as they are cryptographically intensive. Implementations with Ethereum compatible smart contract support are a subject of active research and development but some have made significant steps towards Ethereum compatibility.

Validium and Plasma

Validium works very similar to ZK rollups except data is stored off-chain. Since transaction data is not published on-chain, this introduces new trust assumptions as users must trust an operator to make data available when it is needed. This is typically achieved through a committee of known entities who stake their business reputation on being reliable data providers. If an L2 node operator stops servicing withdrawal requests, this committee will make its copy of the data publicly available.

Plasma users, on the other hand, do not have to trust operators and always have the option to retrieve their funds, even in cases where operators are malicious or uncooperative. While Plasma generated much excitement in the Ethereum community upon its introduction, it introduced several complications. The combination of new data availability attack vectors, the need for users to monitor transactions to detect malicious behavior, and concerns around data capacity on the main chain should many users try to exit plasma chains simultaneously has stifled deployment of Plasma solutions.

What does this patchwork mean for Ethereum?

Over the near to medium term, rollups are expected to be the most popular scaling solution. Many of them are just being implemented today for the first time. Given how far away the advent of a full-fledged Ethereum 2.0 is, they are likely here to stay.

The Current State of Ethereum

Optimistic rollups, given that they effectively allow developers to “copy and paste” their Ethereum applications onto a Layer 2 have seen the most attention and adoption thus far. Some of the leading applications on the Ethereum mainnet such as Uniswap and Synthetix have already started deploying their applications on Optimistic rollup solutions. Likewise, ZK rollups and Validium solutions, while they have limited support for general-purpose smart contracting to date, are also actively being deployed.

What will happen to composability, one of the biggest drivers behind Ethereum’s network effect and growth, remains to be seen. Composability allows anyone in a network to easily build on top of and around existing products and services to devise new use cases; use cases that many did not know were possible until they were invented. Not only has this fueled innovation and growth on the Ethereum network, but it has allowed users a high degree of freedom in being able to affect relatively complex transactions under one security framework, on one chain, and with relative ease.

Layer 2 solutions, while they will undoubtedly enhance user experience through lower fees, come with the possibility of separate execution environments. And in a scenario where several competing solutions are adopted, this composability that has been so central to the Ethereum network could become fragmented.

To date, there has been a high level of indecisiveness on the deployment side as application developers wait and see which Layer 2 solutions gain adoption before deciding which platform to deploy on. Whether or not there will be convergence amongst one or a few Layer 2s will be an important development going forward. It has implications for not just the network effects of the larger Ethereum ecosystem, but the broader smart contract platform landscape.

IV

Framework for Layer One Platform Comparison

Framework for Layer One Platform Comparison

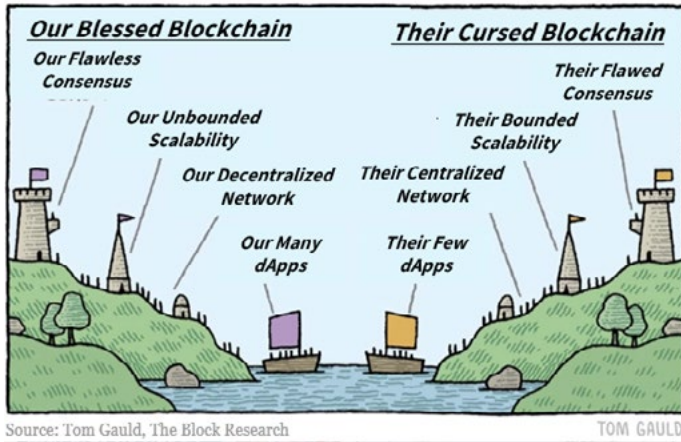
While Ethereum is the largest Layer 1 platform, dozens of platforms have emerged over the past years. Some are rapidly innovating and bringing new consensus algorithms, blockchain architectures, and execution environments. Others have brought very little innovation and would pass as “zombie” chains that have had very little active development for the past few years. Below are the top 30 of these platforms sorted by market capitalization.

Top 30 Smart Contract Platforms by Market Cap									
Count	Platform	Sybil Resistance	Native Token	Price	Market Cap (\$MM)	Percent Chg. 7 Day	Percent Chg. 30 Day	Percent Chg. YTD	
1	Ethereum / Ethereum 2.0	PoW / PoS	ETH	\$ 2,143.35	\$ 247,816	7.6%	-21.8%	189.9%	
2	Binance Smart Chain	PoA / dPos	BNB	\$ 283.05	\$ 44,195	-2.8%	-18.5%	661.1%	
3	Cardano	PoS	ADA	\$ 1.33	\$ 41,434	4.7%	-24.6%	647.1%	
4	Polkadot	PoS	DOT	\$ 15.57	\$ 14,867	-2.7%	-34.0%	85.2%	
5	Solana	PoS	SOL	\$ 32.43	\$ 8,864	4.4%	-1.9%	1641.8%	
6	Ethereum Classic	PoW	ETC	\$ 53.63	\$ 6,605	31.1%	-23.8%	841.1%	
7	Internet Computer	PoA / PoS	ICP	\$ 46.28	\$ 6,270	19.4%	-60.7%	-90.6%	
8	VeChain	PoA	VET	\$ 0.09	\$ 5,457	10.0%	-33.5%	338.8%	
9	TRON	dPoS	TRX	\$ 0.07	\$ 4,506	11.6%	-15.8%	140.8%	
10	EOS	dPoS	EOS	\$ 3.93	\$ 3,735	6.1%	-41.2%	47.5%	
11	Algorand	PoS	ALGO	\$ 0.86	\$ 2,627	1.9%	-9.4%	112.6%	
12	Cosmos	PoS	ATOM	\$ 11.37	\$ 2,464	16.8%	-19.6%	91.1%	
13	NEO	PoA	NEO	\$ 34.75	\$ 2,422	2.0%	-38.9%	135.7%	
14	Tezos	PoS	XTZ	\$ 2.80	\$ 2,378	4.0%	-22.4%	39.0%	
15	Avalanche	PoS	AVAX	\$ 11.25	\$ 1,933	-2.2%	-38.3%	205.6%	
16	Waves	PoS	WAVES	\$ 16.88	\$ 1,780	25.8%	19.0%	175.1%	
17	Kusama	PoS	KSM	\$ 201.86	\$ 1,664	-4.5%	-47.5%	179.7%	
18	Hedera Hashgraph	PoS	HBAR	\$ 0.18	\$ 1,573	-2.3%	-23.7%	439.9%	
19	Elrond	PoS	EGLD	\$ 80.52	\$ 1,414	22.4%	-22.5%	226.8%	
20	NEM	PoI	XEM	\$ 0.12	\$ 1,099	7.4%	-37.9%	-45.5%	
21	Zilliqa	PoW / PoS	ZIL	\$ 0.08	\$ 936	10.1%	-30.0%	2.6%	
22	Stacks	PoX	STX	\$ 0.75	\$ 864	15.5%	-25.1%	74.7%	
23	NEAR Protocol	PoS	NEAR	\$ 1.98	\$ 810	-8.8%	-41.7%	44.0%	
24	Celo	PoS	CELO	\$ 3.01	\$ 744	35.2%	-12.4%	109.4%	
25	Horizen	PoW	ZEN	\$ 63.83	\$ 711	-6.7%	-41.4%	435.6%	
26	Qtum	PoS	QTUM	\$ 7.02	\$ 685	18.1%	-43.9%	206.5%	
27	Harmony	PoS	ONE	\$ 0.06	\$ 641	5.3%	-38.4%	1374.5%	
28	Ontology	PoS	ONT	\$ 0.70	\$ 607	10.5%	-39.4%	54.1%	
29	Fantom	PoS	FTM	\$ 0.22	\$ 558	-10.3%	-31.0%	1177.5%	
30	Flow	PoS	FLOW	\$ 8.74	\$ 370	4.4%	-36.0%	24.7%	

Source: Messari, The Block Research; Data as of 6/30/2021

Nearly 6 years after the inception of Ethereum, comparing and analyzing these different platforms remains challenging.

The technical jargon surrounding them causes headaches. Most analysis on them is written by individuals and entities that, while extremely knowledgeable and informed, have vested interests in the success of one platform or the other. This makes digestible and objective comparisons between platforms few and far between. In



this section, we aim to cut through some of that noise by stacking up several platforms side by side.

The platforms we compare are Algorand, Avalanche, Binance Smart Chain (BSC), Cosmos, Ethereum/Ethereum 2.0, Polkadot, and Solana. The categories we compare them across are technical design, on-chain and ecosystem data, native token design, and key ecosystem members and fundraising histories. Collectively,

this gives us a “look under the hood” at how these platforms differ.

Our selection of individual platforms is qualitative. It comprises a range of platforms with differing levels of ecosystem growth and maturity, different approaches to scaling, and different approaches towards decentralization. The combination of these factors makes them a useful sample set for drawing conclusions about the broader smart contract platform landscape. Inclusion or exclusion of platforms from our sample set does not constitute support or disapproval.

Technical Design & Performance

There are many ways to construct a decentralized network.

Getting a large, distributed base of computers to agree on many transactions quickly and with a high level of security is no small feat. Add in the fact that theoretically anyone, including actors intentionally trying to subvert the network, can participate and it makes sense why there are so many platforms taking so many different approaches.

Decentralization

Decentralization is the core technical design feature that sets blockchain technology apart from its centralized counterparts. It is a key consideration for any network that refers to itself as a blockchain. But assessing whether a blockchain network is decentralized or not ultimately depends on how the assessor defines decentralization.

While there is no universal definition for decentralization, it can be thought of as a spectrum. Pinpointing where on this spectrum different projects lie is best achieved by analyzing one of the core stakeholders in decentralized networks: nodes.

What are nodes?

Nodes are the “boots on the ground” of blockchain networks. They are the physical computer hardware that runs their respective platform’s blockchain software.

They serve several critical functions:

- i. They vote on and validate blocks of transactions
- ii. They communicate with other nodes to agree on the state of the blockchain
- iii. They store the history (state) of the blockchain as a universal source of truth
- iv. They are the endpoints of the network that enable users to access and interact with applications built on the network.

Different classes of them perform different functions, but a few distinctions are common:

- i. Validator nodes participate in consensus to finalize transactions and agree on the state of the blockchain
- ii. Archival nodes typically store the entire state of the blockchain
- iii. Light nodes only store a small portion of the state of the blockchain

The categories are not mutually exclusive. Some validator nodes are light nodes while others are archival nodes. For the sake of analyzing decentralization, the number and distribution of validator nodes that participate directly in consensus provides useful context.

Decentralization as a spectrum

Given that there is no universal definition for decentralization, the spectrum is best described at the extremes.

At one end is “decentralized bliss”:

- There are millions or billions of independent nodes geographically dispersed across the globe

- The hardware needed to run a node is accessible and produced by many different independent manufacturers
- None of the individuals running the nodes have any intention to form cartels or collude in any way
- The financial stake (native tokens) used to secure the network is widely distributed

At the other end is “centralized dystopia”:

- There are one or few nodes geographically concentrated in one datacenter
- The hardware needed to run a node is difficult to source and only produced by one manufacturer
- The individual(s) running the nodes should be expected to collude into a few small groups that, if combined, can easily constitute a large enough share of the network to subvert it for their own benefit
- The financial stake (native tokens) used to secure the network is narrowly held

Decentralization as a journey



Source: www.kinesophy.com, The Block Research

Building out a distributed base of validator nodes does not happen overnight. And the goalpost for what constitutes decentralization will continue to move.

But striving to achieve decentralization should be a persistent and mission-critical goal for communities building blockchain infrastructure. It is how security and censorship resistance are achieved and it has far-reaching consequences for entire ecosystems.

How can decentralization be assessed?

Decentralization can be assessed by trying to answer two questions:

- i. What are the requirements to run a validator node?
- ii. How distributed is the current validator set?

Answering the first question gives us a sense of the flavor of decentralization that the platform is capable of delivering. Answering the second question provides insight into how these requirements are being reflected in market data.

The requirements to run a node can be broken down into:

- i. The computational requirements to run a validator node
- ii. The minimum financial stake required to enter the validator set.

Validator Node Hardware Specs			
Platform	CPU Cores	RAM (GB)	Disk space (GB)
Algorand	2	4	100
Avalanche	2	4	200
BSC	8	16	1000
Cosmos	4	16	500
Ethereum 2.0	4	8	500
Polkadot	8	32	500
Solana	12	128	2000

Source: BlockDaemon, Platform Websites; Represents estimated values as of June 2021. Requirements are likely to change materially over time. Requirements do not include additional hardware required to run failover nodes.

While PoS networks are substantially less computationally intensive than their PoW counterparts, they nonetheless require upfront and ongoing spend on computer infrastructure to run blockchain software. Depending on how networks are structured, requirements can vary substantially. They span inexpensive consumer-grade hardware such as Raspberry Pis and laptops that cost around \$100 to \$1,000 to industrial-grade hardware setups that cost

thousands of dollars and require substantial recurring maintenance spend. The table nearby outlines the required specifications for the platforms in our sample set.

All else equal, lower hardware requirements lower the barrier to entry for directly participating in consensus and are conducive to building out larger and more distributed validator sets.

"Do we need to optimize so that every chain can run on a Raspberry Pi? My answer is: no."

—
Anatoly Yakovenko, CEO
at Solana

Nonetheless, hardware is also an important consideration for platform performance. For example, on a single chain with the same number of validators, identical sybil resistance mechanisms, identical consensus processes, and identical

execution engines, a network with more performant hardware will be able to process more transactions in a set amount of time. Hence, while the computational requirements to run a node are a consid-

eration for decentralization, they are one of several variables that impact platform performance.

In addition to procuring hardware to run blockchain software, validators in PoS networks are typically required to “lock-up” a minimum amount of financial stake to enter the validator set. As displayed in the table below, requirements vary substantially on a network-to-network basis.

Minimum stake to run a validator node ⁽¹⁾							
Platform	Capped Validator Set?	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	\$0.9	\$ 0.1	0	No
Avalanche	No	Platform	2,000 AVAX	\$11.3	\$ 22,500	21	No
BSC	Yes (21)	Market	518,211 BNB	\$288.2	\$ 149,363,957	7	Yes
Cosmos	Yes (125)	Market	65,022 ATOM	\$11.4	\$ 741,251	21	Yes
Ethereum 2.0 ⁽²⁾	No	Platform	32 ETH	\$2153.7	\$ 68,918	TBD	Yes
Polkadot	Yes (297)	Market	1,740,000 DOT	\$15.6	\$ 27,144,000	28	Yes
Solana ⁽³⁾	No	Platform	34 SOL	\$32.5	\$ 1,110	2	Yes

Source: The Block Research, Figment; (1) Represents the minimum stake to enter the validator set inclusive of any stake attributable to delegation. (2) ETH deposits made to the ETH 2 deposit contract cannot be unbonded until the merge of Ethereum into ETH 2.0, thus the effective unbonding period is uncertain. After the merge, it is expected to range from one day to three weeks. (3) Validators on Solana need sufficient SOL to cover voting costs (estimated at 1.1 SOL per day). Accordingly minimum stake requirements for Solana depends on staking duration, which we estimated to be a minimum of 30 days; Data as of 6/30/2021

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 platform places a limit on how many validators are accepted into the active set, the minimum stake required to become a validator is dictated by the market and approximated as the stake of the active validator with the least stake.

In addition to these financial requirements, there are other important considerations for joining the validator set. The risk of having stake forfeited (slashed) and how long validators and delegators typically need to have their tokens staked before they can remove them (unbond) are two of the major considerations.

Slashing

Slashing is a mechanism built into most PoS networks designed to explicitly discourage validator misbehavior and incentivize security, availability, and network participation. The two main misbehav-

iors that incur slashing are downtime (if your validator goes offline) and double signing (submitting conflicting votes on blocks). Penalties for these actions vary on a platform-by-platform basis, but they can result in temporary or permanent removal from the validator set and forfeiting some or all the stake that was “locked up”. Penalties for double signing are typically much larger than downtime penalties. Algorand and Avalanche do not have slashing built into their networks and thus rely on the implicit byzantine fault-tolerant properties of their networks to discourage these behaviors.

"Without decentralization, we remain in the financial system that already exists today: exclusive and secretive."

—
Silvio Micali, Founder at Algorand

Overall, the combination of these hardware requirements, minimum stake requirements, and parameters on slashing and unbonding paint a picture of how easy it is to participate in consensus. Of the platforms analyzed, Algorand has some of the lowest hardware and stake require-

ments, does not impose slashing, and has no unbonding period, thus making it the easiest to participate in consensus. On the other hand, Binance Smart Chain has relatively high hardware requirements, the highest minimum stake requirements, and its network currently caps its validator set at 21. The combination of these factors makes its network the most restrictive in terms of participating in consensus.

Assessing Decentralization

The requirements to run a validator provide insight into what the composition of the validator set could look like. The actual number and the distribution of stake amongst these validator nodes provide quantitative estimates of their current levels of decentralization. The table below provides an overview of some of the most important metrics for analyzing the state of these networks.

Layer 1 Platform Stake Distribution ⁽¹⁾							
Platform	Total Staked (\$MM)	Validator Count (Unique Est.)	Herfindahl Score	<u>Per Validator</u>			
				Min. Staked	Max. Staked	Med. Stake	Avg. Stake
Algorand	\$ 2,809	331	329	0.00%	10.68%	0.00%	0.30%
Avalanche	\$ 3,711	978	78	0.00%	1.54%	0.00%	0.10%
BSC	\$ 4,388	21	477	4.48%	5.45%	4.67%	4.76%
Cosmos Hub	\$ 2,913	125	287	0.03%	6.90%	0.30%	0.81%
ETH 2.0 ⁽²⁾	\$ 12,621	30594	221	0.00%	13.76%	0.00%	0.00%
Polkadot ⁽³⁾	\$ 16,139	212	139	0.26%	6.52%	0.32%	0.47%
Solana	\$ 14,114	579	120	0.00%	4.83%	0.06%	0.17%

Source: The Block Research, Block explorers; (1) Stake distribution data as of 5/25/2021 (Algorand), 5/28/2021 (Avalanche), 6/7/2021 (BSC, Cosmos Hub, Solana) and 6/8/2021 (Eth 2.0, Polkadot); (2) ETH 2.0 stake distribution represents distribution of ETH1 deposit contract balances which are closest approximation to unique controlling entities in validator set. (3) Polkadot stake distribution represents distribution of estimated unique validators (212 of 297 total active validators)

Comparing the aggregate financial stake being used to secure these networks is a valuable starting point for assessing network security. Abstracting away the complexities that the actual distribution of stake introduces, networks that have more financial stake securing them have higher attack difficulty as an attacker would need to expend more financial resources to accumulate the required stake to censor the network.

Comparing the number of validators that a network currently has is the most simplistic method for assessing decentralization. While they may not always map to one distinct entity, they are proxies for the number of independent decision-makers in the ecosystem. Having more independent validators is conducive to a higher level of decentralization.

Analyzing the distribution of validators and their respective financial stake provides a second degree of insight into a network's level of decentralization. The Herfindahl score (the sum of the squares of each validator's stake for each respective network) approximates the distribution of the network's validator set. The lower the score, the more distributed the validator set is.

Quantifying Decentralization

In PoS, 33% is the most important number for assessing blockchain security and liveness. PoS networks reach agreement and transactions are finalized when 2/3 or 66% of the aggregate financial stake in the network agree that a block or a series of blocks are final. So,

Framework for Layer One Platform Comparison

anyone that can accumulate 33% of the total value staked on the network can censor it and prevent it from finalizing transactions and coming to agreement. Depending on the consensus algorithm of the individual network, this could result in the network stopping (i.e. ceasing to produce blocks until it gets 66% agreement on the block) or continuing to produce blocks, but not reaching final agreement on the content of the blocks.

In the table below, we calculate the minimum number of validators that account for 33% of the aggregate value staked on the network. This is one way of quantifying how difficult the network would be to attack.

How many validators does it take to control 1/3 of the aggregate stake of a network? ⁽¹⁾															
Sorted by	Algorand		Avalanche		BSC		Cosmos Hub		Ethereum 2.0 ⁽²⁾		Polkadot ⁽³⁾		Solana		
Validator #	Stake %	Cumulative	Stake %	Cumulative	Stake %	Cumulative	Stake %	Cumulative	Stake %	Cumulative	Stake %	Cumulative	Stake %	Cumulative	
1	10.7%	10.7%	1.5%	1.5%	5.5%	5.5%	6.9%	6.9%	13.8%	13.8%	6.5%	6.5%	4.8%	4.8%	
2	8.6%	19.3%	1.5%	3.1%	5.1%	10.6%	6.7%	13.6%	2.1%	15.9%	4.6%	11.2%	4.0%	8.8%	
3	2.9%	22.2%	1.5%	4.6%	5.1%	15.7%	5.4%	19.0%	1.5%	17.4%	3.8%	15.0%	3.8%	12.6%	
4	2.8%	25.0%	1.5%	6.1%	5.0%	20.7%	4.9%	23.9%	1.5%	18.9%	3.2%	18.2%	3.0%	15.5%	
5	2.8%	27.9%	1.5%	7.7%	5.0%	25.8%	4.6%	28.5%	1.3%	20.1%	2.9%	21.1%	2.5%	18.0%	
6	2.8%	30.6%	1.5%	9.2%	4.8%	30.6%	4.5%	33.0%	1.0%	21.2%	2.3%	23.4%	2.2%	20.2%	
7	2.3%	32.9%	1.5%	10.8%	4.8%	35.4%	3.5%	36.5%	0.9%	22.1%	1.9%	25.3%	1.9%	22.1%	
8	2.1%	35.0%	1.5%	12.3%	4.8%	40.2%	3.2%	39.8%	0.9%	23.0%	1.9%	27.1%	1.7%	23.8%	
9	1.9%	36.9%	1.5%	13.8%	4.7%	44.9%	3.1%	42.8%	0.9%	23.9%	1.0%	28.1%	1.6%	25.4%	
10	1.9%	38.9%	1.5%	15.4%	4.7%	49.6%	2.6%	45.4%	0.8%	24.8%	1.0%	29.1%	1.5%	26.9%	
11	1.9%	40.8%	1.5%	16.9%	4.7%	54.2%	2.3%	47.7%	0.8%	25.6%	0.9%	29.9%	1.4%	28.3%	
12	1.9%	42.7%	1.5%	18.4%	4.7%	58.9%	2.2%	50.0%	0.8%	26.4%	0.7%	30.7%	1.4%	29.6%	
13	1.9%	44.7%	1.5%	20.0%	4.6%	63.5%	2.1%	52.1%	0.8%	27.2%	0.7%	31.4%	1.3%	31.0%	
14	1.9%	46.6%	1.5%	21.5%	4.6%	68.1%	2.1%	54.1%	0.7%	27.9%	0.7%	32.0%	1.2%	32.2%	
15	1.9%	48.5%	1.5%	23.0%	4.6%	72.7%	1.9%	56.0%	0.7%	28.6%	0.7%	32.7%	1.1%	33.2%	
16	1.9%	50.5%	1.4%	24.5%	4.6%	77.3%	1.8%	57.9%	0.6%	29.2%	0.7%	33.4%	1.0%	34.3%	
17	1.8%	52.2%	1.3%	25.7%	4.6%	81.9%	1.8%	59.7%	0.6%	29.8%	0.7%	34.1%	1.0%	35.2%	
18	1.8%	54.0%	1.3%	27.0%	4.6%	86.4%	1.7%	61.4%	0.6%	30.4%	0.7%	34.8%	1.0%	36.2%	
19	1.8%	55.8%	1.2%	28.2%	4.5%	91.0%	1.7%	63.1%	0.6%	31.0%	0.7%	35.4%	1.0%	37.2%	
20	1.8%	57.6%	1.0%	29.2%	4.5%	95.5%	1.7%	64.8%	0.6%	31.6%	0.7%	36.1%	0.9%	38.1%	
21	1.7%	59.3%	0.9%	30.1%	4.5%	100.0%	1.4%	66.3%	0.6%	32.2%	0.7%	36.8%	0.9%	39.0%	
22	1.7%	61.0%	0.9%	31.0%			1.3%	67.6%	0.6%	32.8%	0.7%	37.5%	0.9%	39.9%	
23	1.7%	62.8%	0.9%	31.9%			1.3%	68.9%	0.6%	33.4%	0.7%	38.2%	0.9%	40.8%	
24	1.7%	64.5%	0.9%	32.8%			1.3%	70.1%	0.6%	34.0%	0.7%	38.8%	0.9%	41.7%	
25	1.7%	66.2%	0.9%	33.6%			1.0%	71.1%	0.6%	34.6%	0.7%	39.5%	0.9%	42.6%	

Source: The Block Research, Block explorers; (1) Stake distribution data as of 5/25/2021 (Algorand), 5/28/2021 (Avalanche), 6/7/2021 (BSC, Cosmos Hub, Solana) and 6/8/2021 (Eth 2.0, Polkadot); (2) ETH 2.0 stake distribution represents distribution of ETH1 deposit contract balances which are closest approximation to unique controlling entities in validator set. Polkadot stake distribution represents distribution of estimated unique validators (212 of 297 total active validators)

Considerations for quantifying decentralization

While the analysis above contains some adjustments to most closely approximate the distribution of “unique controlling entities” within each validator set, pinpointing who actually runs these validators, and what their relation to one another is challenging. Additionally,

the degree to which these validators source their stake through delegation adds another degree of complexity to the equation. Even if stake is distributed across a wide base of validators, one or few entities could potentially be delegating the majority of this stake, thus making validator shares of stake a less reliable metric.

Additionally, the data presented above is as of a certain point in time and collected over several weeks. Tracking it over time within and across networks would provide the best insight into the evolution of decentralization for these networks.


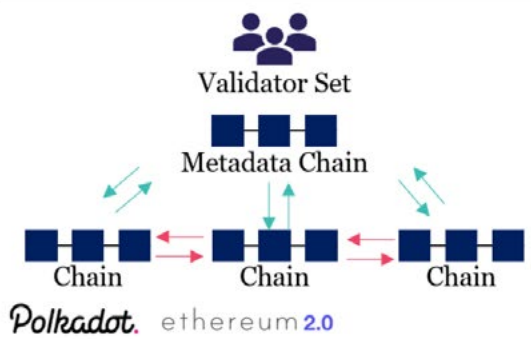
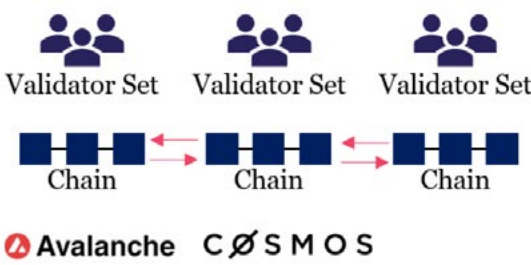
Nonetheless, the analysis above does provide some insights for the outlook for the decentralization of these platforms. For example, the stake securing Binance Smart Chain's network is fairly evenly distributed across all 21 of its validators, but only 7 validators account for over 33% of the active stake of the network. Barring any changes to Binance Smart Chain's platform that would increase the size of its active validator set, the prospects for higher levels of decentralization on its platform are limited. This stands in contrast to other platforms analyzed that support larger and in many cases uncapped validator sets, which will allow them to achieve higher levels of decentralization as more validators enter the set and stake becomes more distributed.

Network Architecture

While decentralization is an important factor, it does not exist in isolation. Performance and usability are also important considerations for these networks. How networks are structured helps shed light on the intertwined nature of all of these attributes.

Structure is most easily assessed by examining how security is provisioned and where transaction execution takes place. In the table below, we identify three distinct network structures: (i) networks with one validator set and one blockchain, (ii) networks with one validator set and multiple blockchains, and (iii) networks with multiple validator sets and multiple blockchains. Additionally, we highlight some of the most apparent tradeoffs associated with each of them.

Framework for Layer One Platform Comparison

Network Architecture	
One Validator Set, One Chain	
 <p>Validator Set</p> <p>Chain</p> <p>Algorand BINANCE SMART CHAIN ethereum SOLANA</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Battle tested method with simple design that is proven to work • Execution occurs on one chain and is conducive to composability and generating network effects <p>Cons:</p> <ul style="list-style-type: none"> • Layer 1s such as Ethereum have been unable to scale on one chain. Thus, scaling requires tradeoffs or innovation on hardware, consensus, and/or execution engine fronts
One Validator Set, Multiple Chains	
 <p>Validator Set</p> <p>Metadata Chain</p> <p>Chain Chain Chain</p> <p>Polkadot ethereum 2.0</p>	<p>Pros:</p> <ul style="list-style-type: none"> • One validator set provides predictable level of security to “walled garden” ecosystem • Potential for large throughput gains by reduced redundancy and horizontal computation <p>Cons:</p> <ul style="list-style-type: none"> • Interchain communication largely untested in a production environment • Introduces higher level of complexity and could break composability of applications under the same security framework that reside on different chains
Multiple Validator Sets, Multiple Chains ⁽¹⁾	
 <p>Validator Set Validator Set Validator Set</p> <p>Chain Chain Chain</p> <p>Avalanche CØSMOS</p>	<p>Pros:</p> <ul style="list-style-type: none"> • Allows for highest level of customizability for individual and application specific chains • Potential for large throughput gains by reduced redundancy and horizontal computation <p>Cons:</p> <ul style="list-style-type: none"> • Interchain communication largely untested in a production environment; similar composability concerns as networks with one validator set and multiple chains • No formal security guarantees provided to chains with their own distinct validator sets

Source: The Block Research; ⁽¹⁾ Avalanche and Cosmos both offer their own “one validator set” security models within their respective networks (Primary Network, Cosmos Hub). Nonetheless, they provide frameworks for developers to launch their own chains with independent validator sets. Additionally, established validator sets on the Primary Network and Cosmos Hub can secure multiple chains within their respective ecosystems.

One Validator Set, One Chain

Employing one validator set and one blockchain is the most battle-tested architecture. Algorand, Binance Smart Chain, Ethereum, and Solana are all currently employing this strategy. Abstracting from layer 2 scaling solutions, all transactions in these networks are executed on one chain under one security framework. This is conducive to generating network effects within their ecosystems as all applications on the chain can easily interact with other applications on a synchronous basis.

One Validator Set, Multiple Chains

Ethereum 2.0, and Polkadot are examples of platforms employing one shared validator set that validates multiple chains within a “walled garden” ecosystem.

In the case of Ethereum 2.0, its metadata chain is the beacon chain and other chains represent its 64 homogenous shard chains. More detail on the structure of the Ethereum network can be found in section 3 of this report.

"Substrate's actual reason is to be the antithesis of block-chain maximalism... the whole point of Substrate is to make making new chains really, really easy."

— Gavin Wood, Founder at Parity Technologies

In the case of Polkadot, its metadata chain is the relay chain and ~100 heterogeneous parachains are slated to be used for transaction execution. In contrast to Ethereum 2.0 where applications are deployed using smart contracts, Parity Technologies' Substrate framework is designed to allow developers to deploy application-specific blockchains or other Layer 1 platforms referred to as parachains. While these parachains rely on the security and finality guarantees of the global Polkadot validator set, they have their own native tokens and are optimizing for certain use cases. Parachain slots are secured through competitive auction processes whereby candidates are required to bond a certain amount of DOT tokens to effectively rent their parachain slots.

Multiple Validator Sets, Multiple Chains

Cosmos and Avalanche are examples of platforms that can support multiple validator sets and multiple chains. Both networks provide frameworks that allow for blockchains to be created and interconnected. They also allow developers the highest level of customizability for designing their own chains with their own security models.

To date, the majority of the activity with the Avalanche ecosystem has occurred within its the Primary Network which spans one validator set that currently validates three separate blockchains: (i) a platform chain that coordinates validators, keeps track of active subnets, and allows for the creation of new subnets, (ii) an exchange chain which is a decentralized acyclical graph (DAG) that enables the creation of new

assets, exchange of assets and cross-subnet transfer, and (iii) a contracts chain which is an Ethereum compatible linear blockchain.

To date, the Cosmos Network has seen the most activity within Zones, or chains that were launched using Cosmos SDK, but maintain their own validator sets and native tokens. Dozens of chains securing billions of dollars in value have been deployed using Cosmos SDK technology including Binance Chain (not to be confused with Binance Smart Chain), Terra, and Thorchain. While they retain their own validator sets, there is a possibility that Cosmos Hub validators will serve as validators of other Zones should governance processes dictate.

Cross-chain communication both within and across multi-chain ecosystems will become an increasingly important consideration that we discuss in the final section of this report.

Sybil resistance and consensus

Sybil resistance and consensus mechanisms lie at the heart of all blockchain networks. They determine how networks are secured and how they reach agreement on the state of the blockchain.

Sybil Resistance and Consensus Overview					
Platform	Sybil Resistance	Consensus Algorithm	Finality type	Priority	Chain Re-orgs
Algorand	PoS	Pure Proof of Stake	Deterministic	Safety	Not Possible
Avalanche ⁽¹⁾	PoS	Avalanche	Probabilistic	Safety	Not Possible
BSC	PoA / dPoS	Proof of Staked Authority	Deterministic	Liveness	Possible
Cosmos Hub	PoS	Tendermint BFT	Deterministic	Safety	Not Possible
Ethereum	PoW	Nakamoto	Probabilistic	Liveness	Frequent
Ethereum 2.0	PoS	Gaspar	Deterministic	Liveness	Possible
Polkadot	PoS	Grandpa/Babe	Deterministic	Liveness	Possible
Solana	PoS	Tower BFT	Deterministic	Liveness	Possible

Source: The Block Research, Platform websites; (1) Avalanche consensus represents consensus for its DAG. Finality type, prioritization and chain re-orgs could differ for its linear blockchains

Sybil Resistance

With the exception of Ethereum, all of the platforms in our sample set employ some variation of PoS whereby security is achieved by having distributed bases of token holders stake their native tokens. Nonetheless, they have subtle differences.

Particularly, in the case of networks with capped validator sets, they have different parameters around how validators are elected into the active set. Through delegation, token holders who are not operating computer hardware can participate in consensus by assigning their tokens to active validator nodes. Delegation processes span those where delegation is facilitated at the protocol level and facilitated through on-chain processes to others where delegation is conducted off-chain through third party staking pools and staking as a service providers.

Consensus

Blockchain networks are inherently redundant. The truth, or the state of their ledgers, is maintained locally on individual nodes. The global network truth is formed through internode communication which is operationalized by consensus algorithms. While the ins and outs of each algorithm are highly technical, there are several distinctions that help differentiate them.

Probabilistic vs Deterministic Finality

Finality defines how long users typically have to wait until there's a reasonable guarantee their executed transactions cannot be "rolled back". Consensus protocols provide two main types of finality: probabilistic and deterministic.

In probabilistic finality arrangements like Ethereum's Nakamoto consensus, once a block is propagated, several additional blocks need to be built on top of it such that the probability of a longer chain forming, which would invalidate said block, is sufficiently low. Participants in these networks typically agree to a "rule of thumb" number of blocks that need to pass before transactions are considered final. Importantly, networks with probabilistic finality can reach consensus without full knowledge of the total active set of miners/validators.

In deterministic finality arrangements, there is a notion of validator identity. While networks have different fault-tolerance thresholds, finality is typically irrevocably achieved when $2/3$ of the active validator set attest to the validity of a block(s).

Favoring safety over liveness

Algorand and Cosmos achieve finality in lock-step with block production and favor safety over liveness. If these networks are not capable of reaching consensus, they cease producing new blocks until $\frac{2}{3}$ of the network reaches agreement on the latest block. In Avalanche consensus, transactions are grouped into vertices. If a vertex includes conflicting transactions, all transactions in it are rejected and re-issued for execution. Thus, when transactions on any of these safety favoring networks are executed, they are considered final.

Favoring liveness over safety

In contrast to platforms that favor safety, platforms favoring liveness decouple block propagation from finality. These chains execute transactions optimistically and finalize them after they have been sufficiently and provably audited.

For example, in Ethereum 2.0, leaders propagate shard blocks within their respective committees that are periodically linked back to the beacon chain and finalized by beacon chain committees. In Polkadot, the network's Blind Assignment for Blockchain Extension (BABE) coordinates block propagation and leader selection. Through Polkadot's GHOST-based Recursive Ancestor Deriving Prefix Agreement (GRANDPA) finality gadget, validators reach agreement on the state of chains rather than individual blocks. Solana's Proof of History (PoH) works as a "clock before consensus" in that each validator runs a sequential hashing function that generates a data structure to provide guarantees on time and order of events. Leaders in Solana rotate based on a predetermined schedule and the blocks they propagate are finalized by the network's Tower BFT consensus algorithm.

If these liveness favoring networks are not capable of coming to agreement on a block, they will continue to propagate new blocks and execute transactions but will not achieve finality.

Chain reorgs

Reorganizations or roll-backs of previously executed transactions are not feasible for networks that favor safety. Any violation of sin-

gle block finality would require that more than $\frac{1}{3}$ of the validator set be slashed (if the network supports slashing). Accordingly, only in rare instances, (i.e. If an attacker caused two conflicting blocks to be finalized by controlling 67% of the stake), would these chains be reorganized through social intervention.

On the other hand, networks favoring liveness make progress when the network is unstable and tolerate partitions in their networks that could cause reorgs before finality is reached. Nonetheless, these networks employ checkpointing schemes whereby transactions that occurred before a certain point in time (i.e. such as ~12 minutes or two epochs prior in Ethereum 2.0) cannot be reorged.

For PoW networks, small reorgs are a frequent occurrence as multiple proposers can and do broadcast blocks at the same height that can result in temporary partitions of these networks.

In addition to the previously mentioned factors, consensus algorithms share several commonalities that are worth exploring.

Random sampling or partitioning of the validator set

In Algorand's Pure Proof of Stake consensus, a committee and a leader are randomly selected from the global validator set via a verifiably random function (VRF), and consensus is achieved within these committees that are rotated each block. In Avalanche's Avalanche consensus for its directed acyclic graphs ("DAG"), nodes repeatedly perform their own random samples of the network and periodically update their states until the majority of the network is in agreement. In Ethereum 2.0, validators will be randomly sorted into committees that reach consensus within their respective shards.

In all these scenarios, consensus is periodically reached within subsets of the global node base which nonetheless inherit the decentralization characteristics of the broader set, provided that it is sufficiently large. This results in lower communication overhead between nodes and thus speeds up consensus.

Capping the size of the validator set

Binance Smart Chain, Cosmos, and Polkadot all currently cap their validator sets at 21, 125, and ~300, respectively. In contrast to other networks that employ sampling strategies, these networks reduce communication overhead by design. Cosmos's Tendermint consensus was designed as early as 2014 and has become one of the most popular consensus algorithms employed across several leading chains.

Assessing platform performance

While consensus algorithms are a critical component of how networks operate, they also impact one of their most important attributes: performance. Performance is best measured through two metrics: throughput levels and finality.

Throughput defines how many transactions a network can handle in a set amount of time and is typically measured in transactions per second (TPS). Finality defines how long a user typically needs to wait until there is a reasonable assurance that their transactions will not be rolled back.

Platform Performance Estimates					
Platform	TPS	Figure Source	Certainty Level	Block Time (sec)	Finality Time (sec)
Algorand	1,100	Mainnet Results	High	4.5	4.5
Binance Smart Chain	220	Mainnet Results	High	3	35
Ethereum	20	Mainnet Results	High	13	78
Solana	50,000	Testnet Results	Medium	0.4	2
Avalanche ⁽¹⁾	4,500	Testnet Results	Medium	-	2
Cosmos Hub	4,000	Testnet Results	Medium	7	7
Ethereum 2.0	100,000	Developer Estimate	Low	12	768
Polkadot	100,000	Developer Estimate	Low	6	12 - 60

Source: The Block Research, Platform Websites, Testnet Results; (1) Avalanche figures represent estimates for its DAG. Actual throughput and finality times could vary substantially depending on which chain transactions are executed on. Please see commentary below for a detailed explanation of the complexities behind these estimates.

Mainnet Results

How many transactions per second a network has processed on its mainnet provides the highest degree of certainty of its capabilities. Ethereum and Binance Smart Chain have achieved ~20 TPS and ~220 TPS in a live production environment, respectively. Algorand has

achieved ~1,100+ TPS in a production environment, although these transactions represent asset transfers which are less computationally intensive than smart contract transactions. Accordingly, this throughput level is likely overstated on an apples-to-apples basis compared to Binance Smart Chain and Ethereum mainnet results.

While these throughput levels have been achieved to date, there is a potential for much higher throughput on these platforms. With rollups, Ethereum community members have estimated that ~4,800 TPS is achievable on the network in its current state. Likewise, developer estimates of maximum throughput, with certain technical changes, are estimated at ~46,000 for Algorand and ~1,000 for Binance Smart Chain.

Testnet Results

Testnet throughput levels provide a moderate degree of certainty into how many transactions a network is capable of processing in a production environment. They are performed in controlled environments that abstract away many of the complexities and risks associated with public blockchains and thus likely overstate performance compared to live mainnet results. Nonetheless, they are a useful metric.

Avalanche has achieved upwards of 4,500 TPS in a testnet environment with 2,000 nodes. Avalanche's Primary Network is currently composed of three separate chains with distinct consensus algorithms which achieve different throughput levels. Accordingly, these estimates of 4,500 TPS likely refer to its lightweight X-Chain which is structured as a Directed Acyclic Graph (DAG) and facilitates asset creation and exchange. Throughput levels achievable on its Ethereum compatible C-Chain, which facilitates smart contracting transactions, are likely materially lower than these testnet levels.

Cosmos Hub employs Tendermint consensus. In testnet simulations with 64 nodes, Tendermint has regularly processed around 4,000 TPS. Cosmos Hub's validator set is currently comprised of 125 nodes. Hence, communication overhead in a production environment is likely higher and testnet levels could be slightly overstated.

Solana has achieved approximately 50,000 TPS in a testnet environment. However, its execution engine does not delineate between messages such as votes cast in consensus (which nonetheless require payment of transaction fees) and more typical peer-to-peer value transfers and smart contract transactions. Hence, testnet levels are likely overstated compared to other platforms due to how transactions are defined. Additionally, this throughput was achieved with about 200 nodes which is about 1/3 of the nodes currently on its mainnet, and communication overhead in a production environment is likely higher.

Developer estimates

Developer estimates provide the lowest level of certainty of a platform's capabilities in production. Nonetheless, given that the multi-chain, shared security structures employed by Ethereum 2.0 and Polkadot have never been employed in production environments before, they are the best estimates we have.

Ethereum Foundation researchers estimate that the move to Ethereum 2.0 (with transaction execution in shards) would result in 100,000 TPS. Likewise, Polkadot community members have estimated the platform's throughput in the range from 100,000 to as high as 1 million transactions per second.

Considerations for assessing throughput and finality

As many networks have not achieved their theoretical TPS limits in live production environments, it is difficult to pinpoint what their maximum levels are. Even for networks that have reached these maximum levels, the technical changes they are making have important implications for throughput levels in the future.

Additionally, the definition of what constitutes a transaction can vary widely across networks and creates challenges for comparison. Some transactions represent computationally intensive smart contracting interactions. Others represent simple value transfer transactions. And some represent votes or messages that are recorded in conjunction with the network's consensus process.

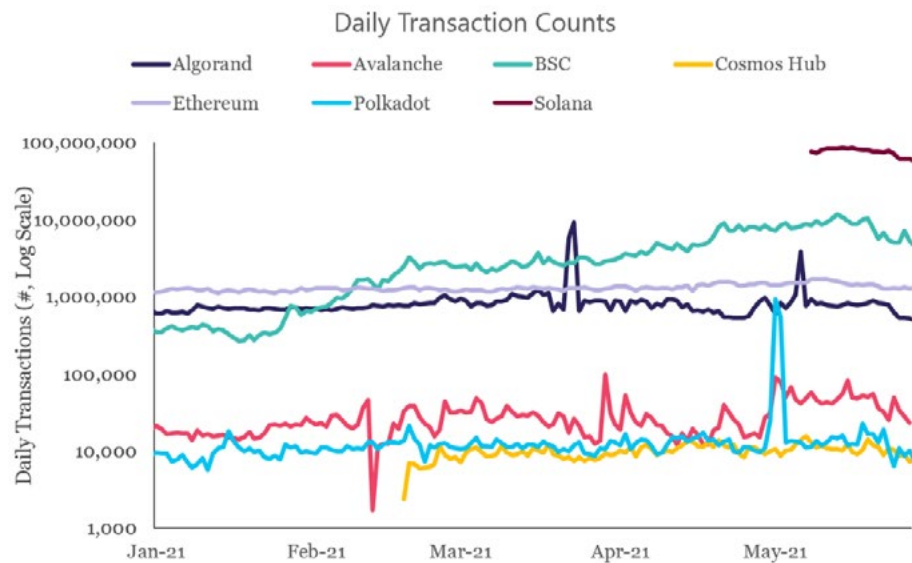
Layer 2 solutions will add another layer of complexity to assessing throughput and finality for Layer 1 platforms. Depending on how transactions are executed on these Layer 2 solutions and finalized on Layer 1 platforms, there could be material impacts on throughput and finality times that are not reflected in the data above.

4.2 On-Chain and Ecosystem Data

Irrespective of their theoretical capabilities, on-chain data provides a look at what blockchain networks have actually achieved in live environments. How this data is evolving both within and across ecosystems can provide valuable insight into the state of these networks.

In this section, we present five series of blockchain data for the networks in our sample set. The data series we present are (i) daily transaction counts, (ii) daily transacted value, (iii) average fees per transaction, (iv) daily aggregate fees, and (v) total value locked in decentralized finance (if applicable).

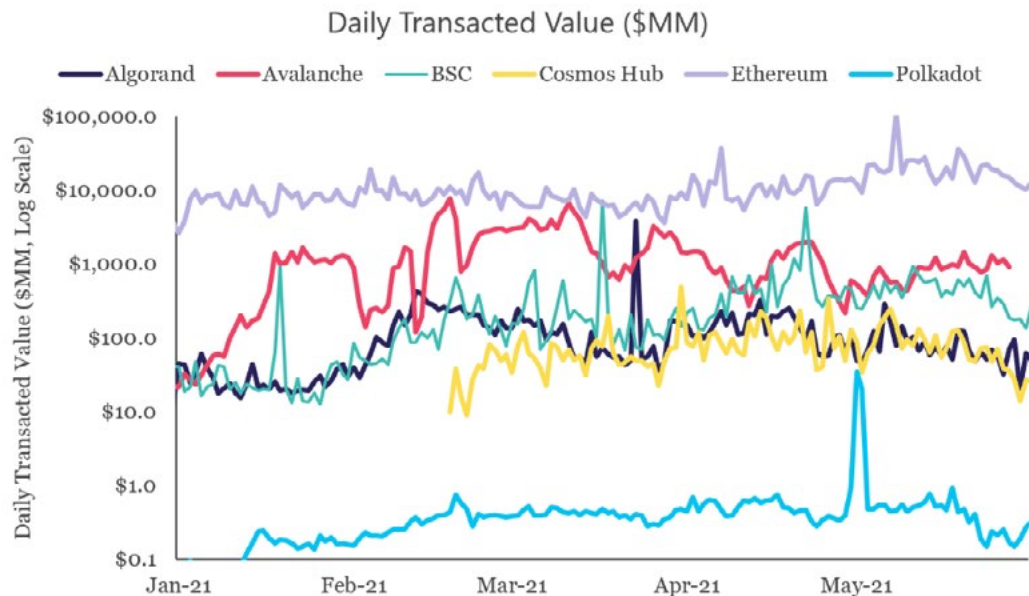
Differences in how on-chain data is tracked and defined across networks create challenges for apples-to-apples comparison. Accordingly, we highlight these instances in the footnotes of the figures.



Source: Coin Metrics, BscScan, Subscan, Platform teams; Solana transaction counts include consensus votes which are not typically included as transactions on other platforms. Polkadot blockchain data represents solely relay chain transactions such as governance messages, transactions related to parachain auctions, and transactions related to participating in staking. Data through 5/31/2021.

Daily transactions represent the number of transactions processed by each chain on any given day. Depending on how transactions are defined across networks, these metrics can vary substantially and range from the tens of millions of transactions to the thousands.

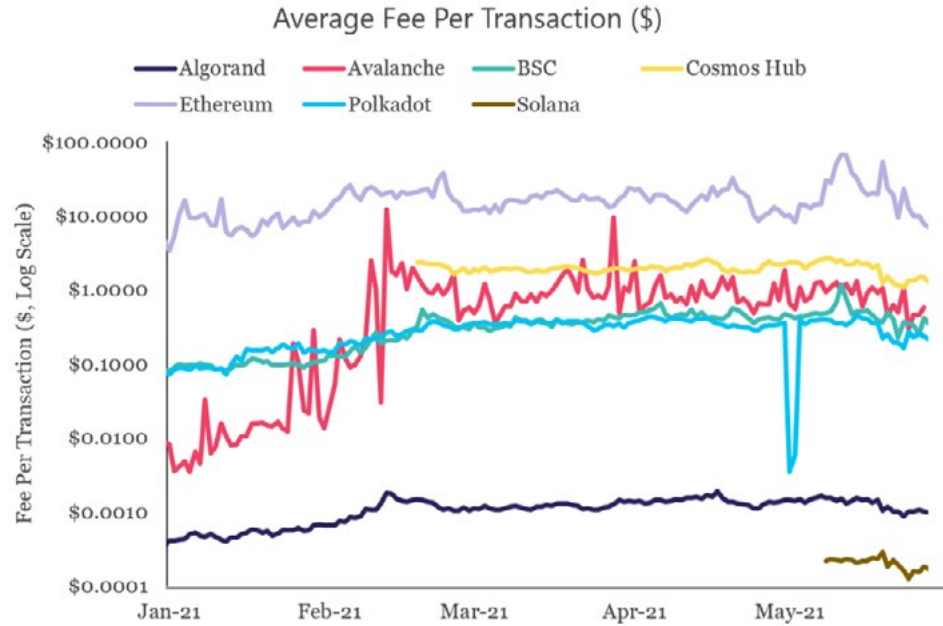
Daily Transacted Value is the total value that was moved in the platform's native token on a daily basis. It does not include payment volumes of assets issued on top of these platforms such as stablecoins. On any given day, tens of billions of dollars of value are transacted on the Ethereum network while other networks are routinely transferring tens of millions to billions of value on any given day.



Source: Coin Metrics, Platform development teams; Polkadot blockchain data represents solely relay chain transactions such as include governance messages, transactions related to parachain auctions, and transactions related to participating in staking. Data through 5/31/2021

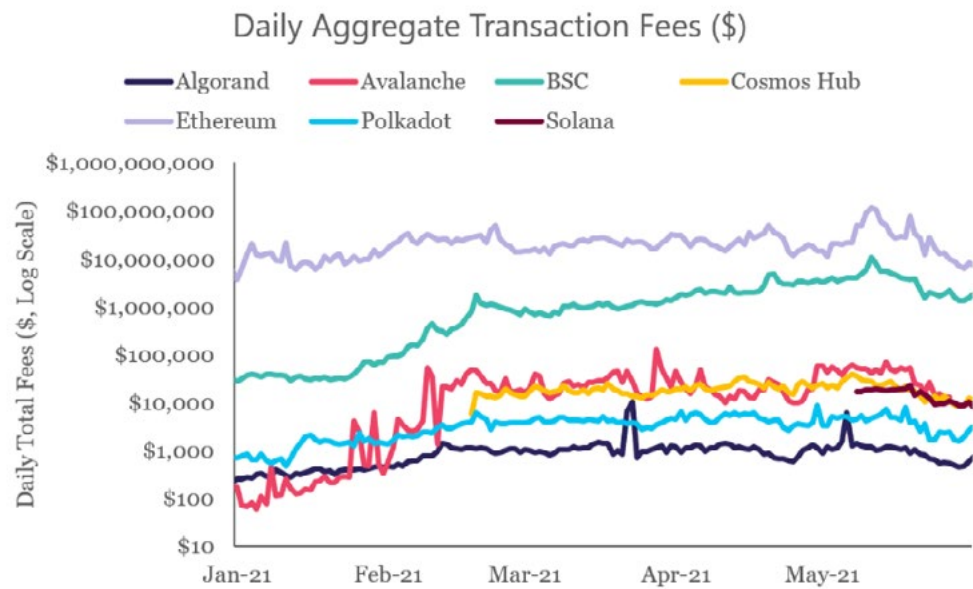
Fees Per Transaction represent how much it costs, on average, to effect a transaction on each of these respective networks. Fees paid on an individual transaction will differ substantially depending on the computational resources ("gas") consumed by the individual transaction. Average fees on Ethereum have risen as high as \$68 over the past year while other chains such as Algorand and Solana are regularly seeing fees as low as one-tenth to one-hundredth of a penny.

Framework for Layer One Platform Comparison



Source: Coin Metrics, BSCscan, Subscan, Platform development teams; Polkadot blockchain data represents solely relay chain transactions such as include governance messages, transactions related to parachain auctions, and transactions related to participating in staking. Data through 5/31/2021.

Daily Aggregate Transaction Fees is the total amount of fees paid to effect transactions on the network in a given day. Ethereum and Binance Smart Chain have generated millions of fees on a given day while most other platforms are generating in the hundreds and thousands of dollars.



Source: Coin Metrics, BSCscan, Subscan; Platform development teams. Polkadot blockchain data represents solely relay chain transactions such as include governance messages, transactions related to parachain auctions, and transactions related to participating in staking. Data through 5/31/2021.

Value Locked in DeFi represents the amount of funds locked in a platform's smart contracts to facilitate DeFi functions such as exchange and lending. The amount of value locked varies substantially based on the capital intensity and efficiency of each of the functions that it is being used to facilitate. Nonetheless, it provides useful insight into the relative size of the DeFi ecosystems across these platforms.

Total Value Locked (TVL) in Decentralized Finance Applications (\$MM)								
Month	Avalanche		Binance Smart Chain		Ethereum		Solana	
	TVL	% Chg	TVL	% Chg	TVL	% Chg	TVL	% Chg
Jan-20					\$ 937	35%		
Feb-20					\$ 983	5%		
Mar-20					\$ 675	-31%		
Apr-20					\$ 939	39%		
May-20					\$ 1,072	14%		
Jun-20					\$ 2,087	95%		
Jul-20					\$ 4,003	92%		
Aug-20					\$ 9,563	139%		
Sep-20					\$ 11,097	16%		
Oct-20			\$ 193		\$ 10,130	-9%		
Nov-20			\$ 247	28%	\$ 12,594	24%		
Dec-20			\$ 394	59%	\$ 16,862	34%		
Jan-21			\$ 916	133%	\$ 30,475	81%		
Feb-21	\$ 107		\$ 7,101	675%	\$ 38,104	25%		
Mar-21	\$ 80	-25%	\$ 13,130	85%	\$ 51,074	34%	\$ 210	
Apr-21	\$ 135	68%	\$ 31,177	137%	\$ 73,528	44%	\$ 1,230	486%
May-21	\$ 165	23%	\$ 14,670	-53%	\$ 56,430	-23%	\$ 975	-21%
Jun-21	\$ 181	9%	\$ 13,860	-6%	\$ 50,430	-11%	\$ 563	-42%

Source: The Block Research, DeFi Pulse, DeFiLama

Ecosystem Data

In addition to on-chain data, trends in community data are useful for estimating the relative size and growth of platform ecosystems. In this section, we provide data on social media followings and estimations of development community size.

Social media followings approximate community size and growth over time. They also provide a quantitative estimation of the reach platform organizations have to promote ecosystem growth initiatives, disseminate educational materials, and make announcements across their respective ecosystems.

Framework for Layer One Platform Comparison



	Algorand	Avalanche	BINANCE SMART CHAIN	COSMOS	ethereum	Polkadot	SOLANA
Handle	@Algorand	@avalancheavax	@BinanceChain	@cosmos	@ethereum	@Polkadot	@Solana
Date	Followers % Chg.	Followers % Chg.	Followers % Chg.	Followers % Chg.	Followers % Chg.	Followers % Chg.	Followers % Chg.
Jan-20	14,198 4%	4,229 11%	52,400 2%	30,127 2%	449,720 0%	33,078 1%	8,885 2%
Feb-20	15,571 10%	4,671 10%	54,265 4%	31,330 4%	452,303 1%	33,863 2%	9,052 2%
Mar-20	16,299 5%	4,908 5%	55,718 3%	31,908 2%	452,605 0%	34,077 1%	9,492 5%
Apr-20	17,123 5%	5,396 10%	58,254 5%	32,755 3%	455,181 1%	34,436 1%	52,545 454%
May-20	18,189 6%	6,318 17%	60,104 3%	33,625 3%	459,215 1%	35,563 3%	51,249 -2%
Jun-20	19,169 5%	7,412 17%	61,941 3%	34,901 4%	462,461 1%	36,644 3%	59,455 16%
Jul-20	21,577 13%	11,213 51%	64,857 5%	37,115 6%	470,518 2%	39,783 9%	81,373 37%
Aug-20	25,700 19%	12,603 12%	69,581 7%	41,384 12%	484,613 3%	56,481 42%	84,822 4%
Sep-20	28,231 10%	17,711 41%	74,135 7%	43,088 4%	492,938 2%	66,111 17%	90,224 6%
Oct-20	29,457 4%	18,969 7%	90,189 22%	44,219 3%	498,736 1%	71,567 8%	91,977 2%
Nov-20	30,651 4%	20,064 6%	95,982 6%	45,398 3%	514,841 3%	77,185 8%	92,239 0%
Dec-20	33,155 8%	22,313 11%	132,906 38%	47,081 4%	547,193 6%	96,576 25%	104,965 14%
Jan-21	41,649 26%	28,487 28%	157,178 18%	52,994 13%	635,751 16%	144,672 50%	109,673 4%
Feb-21	60,071 44%	43,995 54%	219,010 39%	73,714 39%	751,444 18%	201,481 39%	122,809 12%
Mar-21	75,461 26%	58,502 33%	286,306 31%	93,397 27%	850,900 13%	257,279 28%	135,148 10%
Apr-21	101,612 35%	108,244 85%	645,998 26%	151,339 62%	1,260,473 48%	434,060 66%	288,955 14%
May-21	103,910 2%	117,157 8%	685,421 6%	154,519 2%	1,298,248 3%	449,127 3%	302,555 5%
Jun-21	113,572 9%	142,768 22%	775,626 13%	162,472 5%	1,403,575 8%	488,491 9%	345,570 14%

Source: The Block Research, SocialBlade



	Algorand	Avalanche	BINANCE SMART CHAIN	COSMOS	ethereum	Polkadot	SOLANA
Subreddit	r/algorand	r/avax	r/binance	r/cosmosnetwork	r/Ethereum	r/polkadot	r/solana
Date	Members % Chg.	Members % Chg.	Members % Chg.	Members % Chg.	Members % Chg.	Members % Chg.	Members % Chg.
Jan-20	798 6%	5 0%	59,640 1%	8,166 1%	453,533 1%	35 3%	1,706 60%
Feb-20	833 4%	5 0%	61,027 2%	8,330 2%	456,343 1%	35 0%	1,744 2%
Mar-20	856 3%	5 0%	62,315 2%	8,381 1%	459,268 1%	36 3%	1,816 4%
Apr-20	883 3%	21 320%	63,913 3%	8,472 1%	463,443 1%	39 8%	1,890 4%
May-20	914 4%	175 733%	65,316 2%	8,627 2%	467,854 1%	49 26%	1,939 3%
Jun-20	984 8%	441 522%	67,357 3%	8,823 2%	473,149 1%	72 47%	2,088 8%
Jul-20	1,236 26%	570 29%	70,424 5%	9,234 5%	480,491 2%	581 707%	2,319 11%
Aug-20	1,338 8%	773 36%	73,086 4%	9,575 4%	485,763 1%	1,021 76%	2,452 6%
Sep-20	1,404 5%	851 10%	74,873 2%	9,660 1%	489,796 1%	1,291 26%	2,506 2%
Oct-20	1,499 7%	1,086 28%	78,264 5%	9,765 1%	498,513 2%	1,693 31%	2,642 5%
Nov-20	1,629 9%	1,283 18%	83,308 6%	9,945 2%	510,542 2%	2,453 45%	2,779 5%
Dec-20	2,068 27%	1,501 17%	97,687 17%	10,235 3%	543,426 6%	5,834 138%	2,966 7%
Jan-21	7,335 255%	4,327 888%	177,975 82%	18,934 85%	698,355 29%	18,062 210%	4,918 66%
Feb-21	11,307 54%	5,680 31%	215,015 21%	22,172 17%	752,384 8%	23,394 30%	6,348 29%
Mar-21	16,720 48%	6,635 17%	294,704 37%	25,846 17%	829,200 10%	29,138 25%	11,836 86%
Apr-21	23,116 38%	7,684 16%	427,764 45%	28,995 12%	965,621 16%	37,423 28%	19,015 61%
May-21	24,387 5%	7,843 2%	455,114 6%	29,607 2%	986,109 2%	38,804 4%	20,406 7%
Jun-21	27,634 13%	8,306 6%	528,720 16%	31,472 6%	1,027,539 4%	26,894 -31%	25,483 25%

Source: The Block Research, SocialBlade



	Algorand	Avalanche	BINANCE SMART CHAIN	COSMOS	ethereum	Polkadot	SOLANA
Channel	Algorand	Avalanche	Binance	Cosmos	Ethereum	Polkadot	Solana
Date	Subs % Chg.	Subs % Chg.	Subs % Chg.	Subs % Chg.	Subs % Chg.	Subs % Chg.	Subs % Chg.
Jan-20	946 10%	268 8%	12,700 3%	1,820 6%	56,100 0%	1,070 11%	403 2%
Feb-20	1,080 14%	285 6%	13,100 3%	1,880 3%	56,100 0%	1,130 6%	422 5%
Mar-20	1,210 12%	313 10%	14,600 11%	1,920 2%	56,000 0%	1,170 4%	451 7%
Apr-20	1,310 8%	368 18%	17,700 21%	1,990 4%	56,000 0%	1,340 15%	724 61%
May-20	1,430 9%	440 20%	21,000 19%	2,060 4%	56,100 0%	1,650 23%	809 12%
Jun-20	1,550 8%	562 28%	23,500 12%	2,190 6%	56,200 0%	2,010 22%	861 6%
Jul-20	1,730 12%	704 25%	26,800 14%	2,390 9%	56,400 0%	2,740 36%	969 13%
Aug-20	1,990 15%	779 11%	30,700 15%	2,640 10%	56,500 0%	6,090 122%	1,220 26%
Sep-20	2,160 9%	1,020 31%	37,900 23%	2,800 6%	56,600 0%	7,460 22%	1,380 13%
Oct-20	2,250 4%	1,150 13%	43,700 15%	2,940 5%	56,700 0%	8,060 8%	1,500 9%
Nov-20	2,430 8%	1,390 21%	53,000 21%	3,030 3%	56,900 0%	8,820 9%	1,630 9%
Dec-20	2,670 10%	1,610 16%	89,600 69%	3,150 4%	57,100 0%	9,810 11%	1,730 6%
Jan-21	3,160 18%	2,070 29%	109,000 22%	3,370 7%	58,200 2%	14,000 43%	1,880 9%
Feb-21	4,310 36%	2,850 38%	137,000 26%	4,040 20%	59,300 2%	17,900 28%	2,280 21%
Mar-21	5,430 26%	3,520 24%	168,000 23%	4,440 10%	60,400 2%	20,600 15%	2,600 14%
Apr-21	6,700 23%	4,450 26%	247,000 47%	5,100 15%	64,100 6%	36,900 79%	11,400 338%
May-21	6,850 2%	4,540 2%	255,000 3%	5,160 1%	64,600 1%	28,000 -24%	11,600 2%
Jun-21	7,380 8%	4,780 5%	279,000 9%	5,520 7%	65,800 2%	29,600 6%	12,600 9%

Source: The Block Research, SocialBlade

Development Community

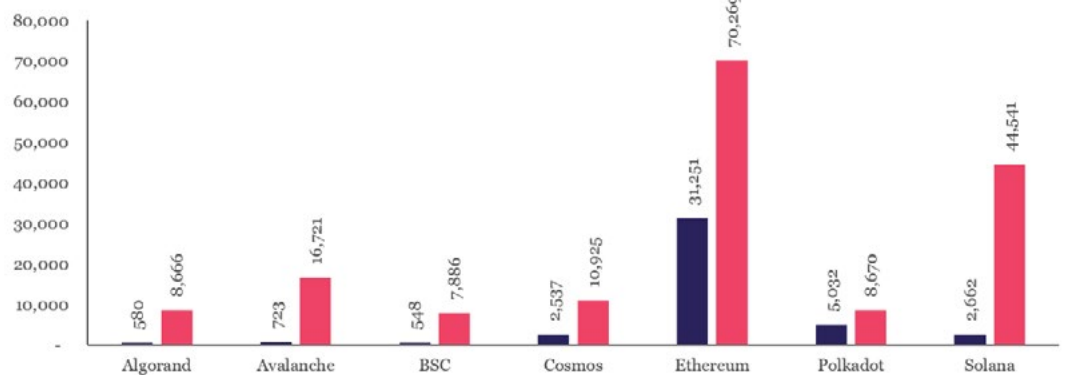
Developer time is a relatively expensive resource. If platforms have high levels of developer engagement it is a positive sign that the community is confident in the prospects of the project and could be an indicator that the project will be shipping more features or improvements. Blockchain development activity is heavily skewed towards Ethereum today, partly due to the platform's longevity. But development communities outside of Ethereum are already substantial as evidenced by the Github and Discord data below.

GitHub is a code hosting platform for version control and collaboration. "Starred" repositories represent workstreams that users have followed in the past and are one simplistic method for gauging relative levels of developer engagement. Discord is an online chat room primarily used by platform engineers and community participants to discuss core platform technology, coordinate validator and user support, and make announcements.



Developer Community Sizing: Github and Discord

■ Github Stars (Most Starred Repository) ■ Discord Members



Source: GitHub, Discord; Ethereum Discord represents Gitter developer chat; Data as of 6/30/2021

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.

Native tokens sit at the center of all POS networks. They are typically the only tokens eligible for staking and paying transaction fees. And in most cases, they grant holders varying degrees of influence in governance decisions of their respective platforms. The table below provides an overview of these native tokens and what they are used for across platforms.

Native Token Overview									
Token Overview							Use Cases		
Platform	Native Token	Market Cap (\$M)	Capped Supply?	Circ. Supply (% of Tot.)	Staked Supply (\$MM)	Nominal Staking Payout	Staking	Governance	Req. to Pay Tx Fees
Algorand	ALGO	\$3,032	✓	30.9%	\$5,492	6.0%	✓	✓	✓
Avalanche	AVAX	\$2,339	✓	24.0%	\$2,984	9.8%	✓	✓	✓
Binance Smart Chain	BNB	\$51,480	✓	90.0%	\$4,393	12.5%	✓	✓	✓
Cosmos	ATOM	\$2,592			\$2,375	9.0%	✓	✓	
Ethereum 2.0	ETH	\$256,771			\$11,977	4.6%	✓		✓
Polkadot	DOT	\$19,824			\$14,293	13.3%	✓	✓	
Solana	SOL	\$9,760			\$12,296	10.2%	✓	✓	✓

Source: The Block Research, CoinGecko, StakingRewards.com; Data as of 6/30/2021; In certain instances, total staked supply exceeds token market cap as tokens that have not yet been emitted into circulation are being staked by development organizations and foundations. Circulating supply as % of total supply metrics not calculated for tokens with uncapped supply as total supply can change, thus making comparison with capped supply tokens inaccurate.

Defining Native Token Basics

Token supply

Some native tokens have a capped supply whereby no new tokens will be issued after a certain point. For these networks, development organizations typically post detailed schedules outlining when they will be emitted into circulation and for what use. Other platforms do not put a formal limit on their native token's supply and hence there is no formal limit on how many tokens could eventually be issued. Not placing a cap on total supply gives these communities the flexibility to modify token inflation and staking payouts over the longer term. Nonetheless, tokens with uncapped supply come with weaker assurances over the scarcity of the native token as holders have no guarantee on what percentage of total tokens their current holdings could account for in the future.

Staking

Staking payouts compensate holders for using their tokens to participate in securing the network. Networks are bootstrapping their security models by issuing new tokens or transferring those that are currently in circulation to stakers in return for “locking up” their tokens. Actual all-in returns from staking vary substantially from nominal payout rates as native token prices fluctuate and variable token inflation rates reduce or in many cases eliminate real returns. Due to this inflation, nominal staking payouts also represent an implicit tax on token holders who do not stake their tokens and suffer dilution of their stake.

Governance




The debate surrounding on-chain governance has been raging for several years. Different platforms have different approaches to governance that range from informal coordination on online forums and chat rooms to formal voting processes conducted on-chain. Changes to core technical design features, token inflation rates and economics, and how treasury funds are allocated are all examples of decisions that, to varying degrees, are starting to be coordinated through on-chain governance processes.

Transaction fees

Native tokens are generally the only form of payment accepted to cover fees on their respective networks. Exceptions to this rule in our sample set include ATOM and DOT. ATOM can be used to cover Cosmos Hub transaction fees, but several different tokens can also be used to pay fees on the Hub. Additionally, while DOT is required to be bonded to rent parachain slots, Polkadot’s parachains will likely issue their own native tokens that are used to pay transaction fees.

How are transaction fees treated?

Transaction fees have several destinations depending on the platform but are typically paid to validators, burned, or recycled. Most networks employ a strategy whereby a portion of fees are remitted to validators and a portion of the fees are either burned or recycled. The table below provides an overview of how these networks currently treat fees.

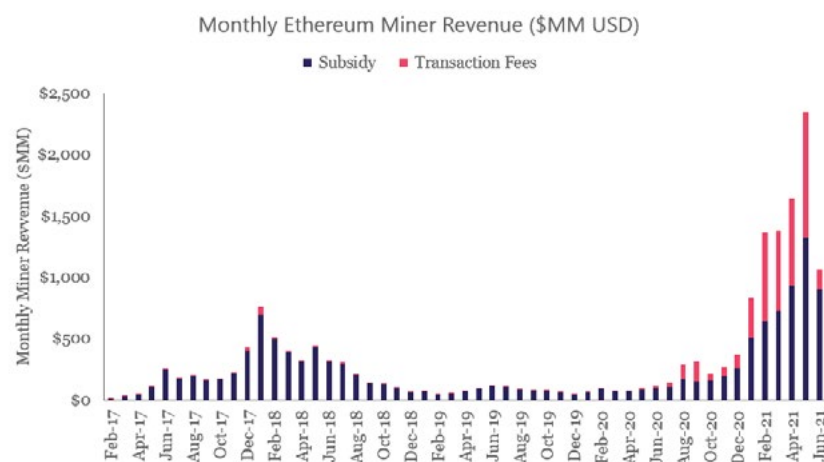
Fee Destination				Fee Destinations Explained	
Platform	Validators	Burn	Recycle		
Algorand			✓	 Pay to Validators/Miners	Transaction fees are paid to the validator/miner who proposed the block or distributed pro-rata to the validator set
Avalanche			✓		
Binance Smart Chain ⁽¹⁾	✓			 Burned	Tokens used to pay transaction fees are permanently removed from circulating supply
Cosmos	✓		✓		
Ethereum (Post EIP-1559)	✓	✓		 Recycle	Transaction fees are temporarily removed from circulation to later be applied to rewards for stakers/miners
Polkadot	✓		✓		
Solana	✓	✓			

Source: The Block Research; (1) Binance Smart Chain native token use relates solely to its function as the native token of BSC ecosystem. In connection with Binance's centralized exchange business, BNB tokens are periodically burned.

Ethereum's EIP 1559: Socializing transaction fee rewards

ETH's token structure was recently overhauled with the introduction of Ethereum Improvement Proposal 1559 (EIP-1559) in August 2021. Among other changes (such as making the network's gas limit more dynamic), the proposal changed the network's fee model such that a portion of the total fees paid by users are burned and permanently removed from circulation rather than paid to miners, or in the case of Ethereum 2.0, validators.

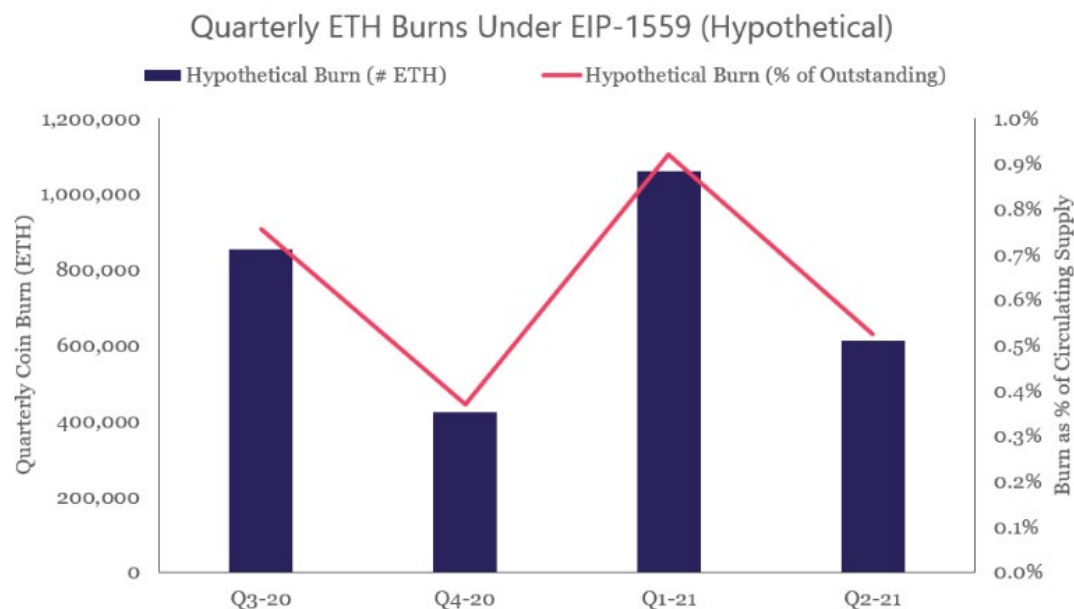
This change is particularly interesting in the case of Ethereum due to the large quantities of transaction fees that it has been generating. Monthly aggregate transaction fees on the network recently surpassed \$1 billion for the first time last May.



Source: The Block Research, Coin Metrics

Under EIP 1559, fees are bifurcated into a base fee and a miner tip. The base fee portion represents the floor for transaction fees and will be burned and permanently removed from supply while the tip will continue to be paid out to miners or validators. Leveraging historical fee data and applying assumptions to what the split of the base fee and the tip are, we can estimate historical hypothetical token burns that would have

occurred had EIP-1559 already been activated. The table below shows these hypothetical burns over the past 4 quarters.



Source: The Block Research, Dune Analytics; Estimated ETH burns assuming tips (non-burnt portions of transaction fees) are 5 gwei

Based on these hypothetical burns, the impact of this proposal could be material. In the quarters analyzed, token burns offset quarterly inflation (ranging from 1.0% to 1.1%) by 0.40% to 0.90%. Nonetheless, several factors will impact whether this proposal will make ETH deflationary and increase its scarcity, as many have posited. The split between base fees and miner tips will ultimately be dependent on the state of the Ethereum network in the future and our estimates used above could be inaccurate. Additionally, Layer 2 scaling solutions and sidechains are already offloading transaction execution off the Ethereum mainnet, and thus aggregate fees on the Ethereum mainnet are likely to continue falling over the coming months. Accordingly, it is highly unlikely that EIP-1559 will make Ethereum's supply deflationary in the near term.

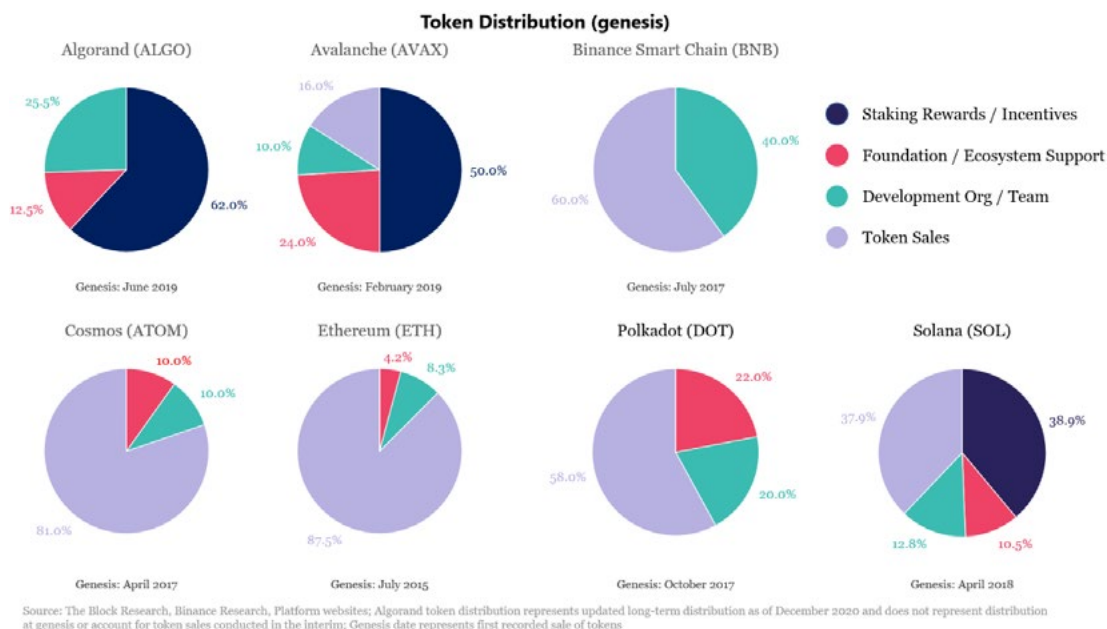
Notably, this burning mechanism is not specific to Ethereum. Solana, for example, also burns transaction fees. Likewise, recycling mechanisms effectively decrease circulating supply which could have material impacts over the long-term should networks generate large

and recurring bases of fee revenue.

Native Token Distribution

Tokens are generally created in initial sales to either venture capital firms or, in some cases, the general public to raise funds to support development. Additionally, there are several other categories for which token supply is typically “earmarked” at the token creation event:

- i. Staking Rewards / Incentives represent tokens slated to be paid out to validators and delegators or emitted in airdrops.
- ii. Foundation / Ecosystem Support tokens are typically reserved for building out infrastructure, securing strategic partnerships, and supporting projects that are looking to deploy apps on these networks.
- iii. Development Organization and Team tokens incentivize developers tasked with developing core platform technology and conducting ongoing research.



Irrespective of how tokens were initially segmented, how they are emitted into circulating supply is an important consideration. Tokens sold to venture capital firms or granted to development team members typically come with vesting periods that introduce them into

circulating supply over several years. Development organizations and foundations typically retain large holdings of native tokens. Some of these organizations publish transparency reports detailing the actions taken with tokens under their custody while others have limited transparency surrounding token holdings and related actions taken.

Why is valuing native tokens challenging?

Some crypto assets, such as DeFi tokens lend themselves well to traditional financial analysis. Native tokens do not. While they have specific use cases within their respective environments, they are issued in censorship-resistant environments and can ultimately be used for whatever users want to use them for.



In the case of PoS networks, they are always used to secure the network through staking. Sometimes they are used as a medium of exchange for transferring value. Other times they are used as a collateral or reserve asset. And in a scenario where one or many of these platforms gain mainstream adoption with billions of active users, it is difficult to predict how their use cases and value capture mechanisms could evolve.

Staking payouts, tokenomic models like EIP-1559, and governance privileges all create incentives for holding tokens over the long term. Nonetheless, the intersection of these features against a backdrop of token inflation, which is necessary to bootstrap platform security, makes valuation a challenging task.

Additionally, native token value has a unique relationship with platform security; especially when it comes to PoS networks. In PoS networks, the aggregate value of staked tokens serves as a proxy for how costly it can be to attack the network. Networks with native tokens that are more valuable, more widely distributed, and more commonly used for staking are more difficult to attack.

All else equal, higher attack difficulty makes platforms more attractive venues for deploying applications which could, in turn, drive more usage and incremental token value. Hence, native token value and platform security are intertwined and there is a potential for positive feedback loops. The opposite effect is also true. If a native token has little to no value, its platform provides weak censorship resistance and security guarantees. And it will most likely not be an attractive venue for deploying applications that could drive incremental token value.

Price performance of native tokens can be found in Appendix A. Appendix B provides an overview of traditional investment products that offer direct exposure to native assets.

Ecosystem Members & Organization Fundraising

While there is no formal executive management team for smart contracting platforms, individuals play a critical role in their operation. They design platforms and tooling, develop applications on top of them, and perform ongoing technical research and development. Certain individuals typically have significant influence over major design decisions of their respective platforms; especially in communities that are in their early growth stages and still developing formalized governance processes.

Pinpointing the most influential individuals within a blockchain ecosystem is an art and not a science. Nonetheless, we make an effort at pinpointing these individuals below. The prior work experience of these individuals and the financial backing of their networks provides context on how these platforms came to life and how their visions could unfold over the future.

Framework for Layer One Platform Comparison

Algorand

Key Ecosystem Members			Select Investors
Dr. Silvio Micali <i>Founder at Algorand</i> <ul style="list-style-type: none"> Faculty member at MIT, Electrical Engineering and Computer Science Department since 1983 Recipient Turing Award (comp-sci), Gödel Prize (theoretical comp-sci) and the RSA prize (cryptography) Co-inventor of probabilistic encryption, Zero-Knowledge Proofs, Verifiable Random Functions 	Steve Kokinos <i>CEO at Algorand</i> <ul style="list-style-type: none"> Serial entrepreneur, most recently Co-Founder and Executive Chairman of Fuze. Co-Founder of BladeLogic, Inc., a recognized leader in the data center automation market Co-Founder and CEO of Web Yes, Inc., an early market leader in the Web hosting 	Massimo Morini <i>Chief Economist at Algorand</i> <ul style="list-style-type: none"> Currently head of Rates and Credit Modelling at IMI bank Teaches Blockchain and Cryptocurrencies at Swiss Finance Institute Lugano Former Advisor and Trainer at the World Bank, the Monetary Authority of Singapore and several private and public financial institutions 	      
     			


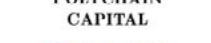










Avalanche

Key Ecosystem Members			Select Investors
Dr. Emin Gün Sirer <i>CEO & Founder at Ava Labs</i> <ul style="list-style-type: none"> Associate Professor (on leave) from Cornell University Creator of first PoW based currency Karma, BitcoinNG, Bitcoin Covenants Author of seminal Bitcoin Selfish Mining Paper 	John Wu <i>President at Ava Labs</i> <ul style="list-style-type: none"> Formerly CEO of the Digital Assets Group at SharesPost; a marketplace for trading private company shares Founder of \$500MM hedge fund, Sureview Capital Portfolio manager at Kingdom Capital and analyst at Tiger Management 	Lee A. Schneider <i>General Counsel at Ava Labs</i> <ul style="list-style-type: none"> Formerly General Counsel at Block.one Co-Founder of Global Blockchain Convergence, an organic collaboration network for people in blockchain and emerging technologies Ex Head of Blockchain, FinTech and Broker-Dealer practices at two major law firms 	     
     			

BINANCE SMART CHAIN


Key Ecosystem Members			Select Investors
Samsul Karim <i>Business & Ecosystem Development at Binance</i> <ul style="list-style-type: none"> Contributor to BSC ecosystem growth initiatives Formerly worked in Business Development at Consensus; an Ethereum development studio Formerly director at Edutech; a tech company serving educational institutions in U.A.E 	Jeff Zhang <i>BSC Community Manager</i> <ul style="list-style-type: none"> Formerly Chief Community Manager in dForce; a DeFi platform on Ethereum and Binance Smart Chain Previously Operations Manager at Cybex; a decentralized exchange forked from BitShares 	Changpeng Zhao <i>CEO at Binance</i> <ul style="list-style-type: none"> CEO of the world's largest crypto exchange, Binance and a key supporter of the Binance Smart Chain Ecosystem Former Partner at Fusion Systems Group Former Head of Development at Blockchain.com and prior experience at Fusion systems and Bloomberg 	 
     			

COSMOS

Key Ecosystem Members			Select Investors
Ethan Buckman <i>Co-founder at Cosmos</i> <ul style="list-style-type: none"> CEO at Informal Systems, a company focused on bringing verifiability to distributed systems Co-founded Tendermint with Jae Kwon in 2014 pioneering PoS tech and building Tendermint Core Former CTO at Tendermint and remains an active developer in the Cosmos ecosystem 	Peng Zhong <i>CEO & President at Tendermint</i> <ul style="list-style-type: none"> CEO at Tendermint focused on guiding blockchain across the chasm to the mainstream Mentors a team building applications that improve the usability, accessibility, and safety of blockchain for developers and end-users. Advises founders on building sustainable blockchain businesses 	Tess Rinearson <i>VP of Engineering at Interchain</i> <ul style="list-style-type: none"> Prominent Interchain Foundation Council member and active developer in Cosmos ecosystem Led the team at Tendermint responsible for developing Tendermint Core, a BFT consensus engine Worked on multiple storage and protocol problems and was previously a full-stack engineer at Medium 	     
     			

Framework for Layer One Platform Comparison

Key Ecosystem Members			Select Investors
Vitalik Buterin <i>Co-founder of Ethereum</i> <ul style="list-style-type: none"> Author of the Ethereum whitepaper and de-facto leader of the Ethereum community since 2014 Leading blockchain developer, researcher, and industry thought leader Co-creator of Bitcoin Magazine; a Bitcoin news and research publication 	 Danny Ryan <i>ETH 2.0 Researcher at Ethereum Foundation</i> <ul style="list-style-type: none"> Leading coordinator for the Ethereum 2.0 deployment and implementation Former freelance developer who joined the Ethereum Foundation in 2018 Researching proof of stake and sharding for 4+ years 	 Hayden Adams <i>Ethereum Developer</i> <ul style="list-style-type: none"> Founder at Uniswap, the largest decentralized exchange by volume built on Ethereum Uniswap is one of Ethereum's biggest users and has consumed 20%+ of Ethereum's total gas on certain days Previously an engineer at Siemens performing engineering simulations 	 GRAYS SCALE  THREE ARROWS CAPITAL  MULTICOIN CAPITAL  POLYCHAIN CAPITAL  PANTERA
    			

Key Ecosystem Members			Select Investors
Dr. Gavin Wood <i>Founder at Web3 Foundation & Parity Technologies</i> <ul style="list-style-type: none"> Co-founder of Ethereum and former CTO of the Ethereum Foundation Inventor of Solidity smart contract language and authored the Yellow Paper specifying Ethereum's virtual machine Co-Founder at Grid Singularity; an internet based decentralized energy management platform 	 Robert Habermeier <i>Co-Founder of the Polkadot Network</i> <ul style="list-style-type: none"> Core Developer at Parity Technologies and parachain development lead Longtime member of the Rust community and has focused on leveraging the language's features to build performant solutions. Named Thiel Fellow in the class of 2018 	 Peter Czaban <i>Co-Founder of the Polkadot Network</i> <ul style="list-style-type: none"> Formerly Chief Technology Officer at Web3 Foundation Formerly Software Engineer at Parity Technologies Formerly Data Scientist at GYANA; a data science company 	 POLYCHAIN CAPITAL  BLOCKCHANGE  CoinFund  arrington XRP CAPITAL  Outlier Ventures  FABRIC VENTURES
    			

Key Ecosystem Members			Select Investors
Anatoly Yakovenko <i>Co-Founder & CEO at Solana Labs</i> <ul style="list-style-type: none"> Software engineer at Qualcomm for 10+ years building high performance operating systems Software Engineer at Dropbox focused on distributed systems and compression Software Engineer at Mesosphere; a distributed operating system provider 	 Raj Gokal <i>Co-Founder & COO at Solana Labs</i> <ul style="list-style-type: none"> Director of Product at Omada Health; a digital health company Co-Founder at Sano; a healthtech company acquired by One Drop Builder and advisor to technology companies in mental health tech at Stealth 	 Sam Bankman-Fried <i>CEO at FTX & Alameda Research</i> <ul style="list-style-type: none"> CEO at FTX; a leading crypto exchange and creator of Serum, a Solana based decentralized exchange CEO at Alameda Research; a quantitative trading firm focused on cryptocurrencies Formerly trader at Jane Street; a quantitative trading firm 	 MULTICOIN CAPITAL  a16z  POLYCHAIN CAPITAL  CMS  ALAMEDA RESEARCH  CoinFund
     			

Source: The Block Research, LinkedIn, Crunchbase

Company and Foundation Fundraising

While smart contracting platforms are native to the internet, they are typically developed by for-profit companies and supported by related non-profit organizations. These organizations 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 technology and the growth of their respective ecosystems. These organizations and their related fundraising histories are shown in the table below.

Layer 1 Disclosed Funding Rounds				
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	
The Algorand Foundation	Token Sale	6/19/2019	6,000,000	
Total Funding			72,000,000	
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	
Avalanche Foundation	Token Sale	7/22/2020	42,000,000	
Total Funding			60,000,000	
BINANCE				
Binance	Token Sale	7/1/2017	15,000,000	Sequoia, Limitless Crypto Investments, Funcity Capital, Others
Binance	Series A	9/1/2017	10,000,000	
Total Funding			25,000,000	
COSMOS				
Interchain Foundation	Token sale	4/15/2017	17,000,000	Paradigm, Bain Capital, 1confirmation
Tendermint	Series A	3/15/2019	6,000,000	
Total Funding			23,000,000	
ethereum				
EthSuisse	Token sale	8/30/2014	16,000,000	
Total Funding			16,000,000	
Polkadot				
Parity Technologies	Seed	4/23/2016	750,000	Ethereum Foundation
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	
Web3 Foundation / Parity Technologies	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	
Total Funding			335,800,000	A16Z, Polychain Capital, Alameda Research, Coinfund, Others

Source: Crunchbase



V Conclusions & Outlook

Conclusions & Outlook

Comparing different smart contracting platforms requires a multi-disciplinary analysis of their technical design, related blockchain and ecosystem data, and an understanding of the people and organizations behind them. Our analysis of seven of the more active and differentiated platforms serves as a blueprint for comparison. It also provides context for drawing conclusions about the outlook of the broader platform landscape.

Conclusions

As more products and services are delivered on top of smart contract platforms, attempting to quantify decentralization will become an increasingly important task. The requirements to participate in consensus provide insight into what flavor of decentralization platforms are capable of delivering. Market data allows us to make quantitative estimations of real-time levels of decentralization. Nevertheless, the true composition of validator sets is opaque, and thus quantifying decentralization is more of an art than a science.

How networks are architected is one of their biggest differentiating factors. Some are employing the battle-tested one-chain approach and optimizing their networks to provide the highest level of performance. Others are deploying multi-chain frameworks and forging full force into the land of asynchronous networks where cross-chain communication facilitates interaction between and within applications. Both approaches come with their own sets of pros and cons that have implications for their performance, decentralization, and usability characteristics.

Throughput and finality times provide insight into platform performance. They can be sourced from live results, testnet results, and developer estimates which come with differing levels of certainty. On-chain data can serve as a sanity check for comparing actual performance vs theoretical performance but has limitations as many networks have yet to see sufficient adoption to hit theoretical limits. Due to different data tracking methods, examining on-chain metrics over time both within and across networks is necessary for extracting signal.

Conclusions & Outlook

Native tokens sit at the center of all PoS networks. They have a unique and intertwined relationship with their respective networks' security profiles that creates the potential for feedback loops. Tokenomic models such as EIP-1559 provide an early look at what the longer-term value capture mechanisms of these platforms could be. Nonetheless, the combination of incentives for longer-term token holding against a backdrop of token inflation, and in some cases uncapped supply, makes valuing them challenging.

Trends of ecosystem engagement and developer activity are useful for analyzing the growth prospects and the state of platform ecosystems. While these networks are owned and operated by distributed bases of token holders, select individuals will play an important role in the direction of these platforms for years to come; even in instances where they employ on-chain governance.

Outlook

PoS sybil resistance mechanisms have been around for several years now. But Ethereum's move from PoW to PoS is a watershed moment for its network. Tens of billion dollars of value are being transacted on Ethereum on any given day and its move to PoS will significantly alter how the network delivers decentralization and security. On the performance and usability front, rollups and scaling solutions will likely alleviate the congestion on the Ethereum mainnet over the near to medium term and reduce transaction fees. How these solutions will affect Ethereum's composability, which has been central to generating network effects, remains to be seen.

To date, compatibility with the Ethereum development environment (Solidity and the Ethereum Virtual Machine) has allowed many competing platforms to leapfrog the typical obstacles associated with developing applications and tooling for their ecosystems. In particular, Binance Smart Chain's ecosystem growth has largely been attributable to "copy and pasting" applications from Ethereum onto its chain and providing users similar services at lower transaction fees. While this has driven significant adoption of its platform, it has come at the expense of lower security.

Conclusions & Outlook

Blockchain Security

Security is an important consideration at both the base consensus layer and application layer of blockchain ecosystems.

Concerns over the centralization and thus the lack of censorship resistance at the base layer of networks like Binance Smart Chain are well founded. With a small number of nodes and concentrated financial stake, networks like BSC could more easily be censored by a third party such as a government agency and forced out of operation. Hence, networks with low levels of decentralization pose risks to their stakeholders; regardless of whether or not they are aware of it.

On the other hand, security vulnerabilities at the application layer of smart contract platforms are less subtle. As early as 2016, a vulnerability in the DAO smart contract resulted in a \$60MM hack that caused a permanent divide between the Ethereum and Ethereum Classic communities. And just over the past 18 months, applications deployed on Binance Smart Chain and Ethereum have seen upwards of \$400MM worth of value compromised in hacks.

Notably, these application hacks are primarily attributable to developer oversight (missing sanity checks, math logic errors, errors transferring applications across chains, etc...) rather than vulnerabilities with the base layer of these platforms. And there is an element of adverse selection in highlighting Binance Smart Chain and Ethereum as they have seen the most activity and thus have the largest attack surfaces. But as platforms support more economic value, the costs associated with vulnerabilities at the application layer are also set to increase; especially if applications reach mainstream user bases. Accordingly, what development environments platforms support could become a more important consideration going forward.

Development Environment

Ethereum's flagship smart contract language, Solidity, and its execution environment, the Ethereum Virtual Machine, are far from the only frameworks available for deploying decentralized applications. As seen in the table below, many platforms support different smart

Conclusions & Outlook

contracting languages that come with unique attributes. For example, smart contracts on Algorand can be coded in Python and compiled down to lower-level smart contract languages such as Teal. Additionally, languages such as Clarity are “decidable” and provide assurances on how smart contracts will function before they are permanently deployed into live production environments, thus reducing the attack surface of applications.

Supported Languages & Execution Environments		
Platform	Primary Smart Contract Languages	Execution Environment(s) / Runtime
Algorand	Reach, Python (Teal), Clarity	AVM
Avalanche	Solidity / Vyper	EVM
Binance Smart Chain	Solidity / Vyper	EVM
Cosmos	Rust, Solidity / Vyper	WASM, EVM
Ethereum	Solidity / Vyper	EVM
Ethereum 2.0	Solidity / Vyper	EVM
Polkadot	Rust, Solidity / Vyper	WASM, EVM
Solana	Rust	Sealevel

Source: The Block Research

"There's something in the neighborhood of 100,000 developers working on blockchain today. There's close to 20 million (developers) who aren't... Developer experiences need to improve dramatically for mainstream applications to take hold."

—
Steve Kokinos,
CEO at Algorand

Cosmos, Polkadot, and Solana also support coding of smart contracts in more familiar languages such as Rust with different execution environments including WebAssembly (“WASM”) and Sealevel. WASM is a lightweight and platform-independent instruction set standard for web browsers developed by the W3C workgroup that includes Google, Mozilla, and others. Sealevel is Solana’s runtime that allows for parallel processing whereby non-overlapping transactions can be executed concurrently.

Over the near term, this Ethereum-centric development environment appears to be here to stay. Building out platform developer bases and tooling infrastructure does not happen overnight and many competing platforms will continue to offer Ethereum compatible alternatives to bootstrap ecosystem growth. Over

Conclusions & Outlook

the medium term, the evolution of new language constructs and execution environments bears watching. They hold the potential to not only broaden the addressable universe of blockchain developers but also deliver performance gains at the execution level.

Interoperability

The smart contract platform landscape is fragmented across several dimensions.

- i. Layer 1 platforms continue to carve out their own single-chain and multi-chain networks
- ii. Layer 2 solutions are going to take transaction execution off Layer 1 platforms and onto their own chains
- iii. Sidechains with their own security models are being launched

To date, cross-chain asset transfers via bridges such as RSK's Pow-Peg have been the most tangible examples of what interoperability looks like. They have enabled users to port assets across chains and leverage them in different environments.

"Imagine every blockchain right now as a small tribe living on an island in a vast archipelago. So, what IBC enables is the discovery of shipbuilding, which allows these tribes to travel between each other"

Peng Zhong,
CEO at Tendermint

But with the advent of multi-chain networks with sharded states such as Ethereum 2.0 and Polkadot, cross-chain communication will be required not only to agree on the global blockchain state but also to facilitate interaction between applications that reside in one or multiple shards/parachains with other applications in other shards/parachains. Polkadot will employ a Cross-Chain Message Passing (XCMP) protocol for parachains to send arbitrary messages between each other within its ecosystem. If Ethereum does indeed go the route of transaction execution in shards, it would need to employ a similar mechanism to

facilitate cross-shard messaging, although this is likely years away for its network. As these cross-chain communication technologies have not been deployed at scale in production environments, their impending deployments and the associated impact on users bears watching.

Cosmos's Inter-Blockchain Communication Protocol ("IBC") is one of the most detailed specifications for interchain communication to

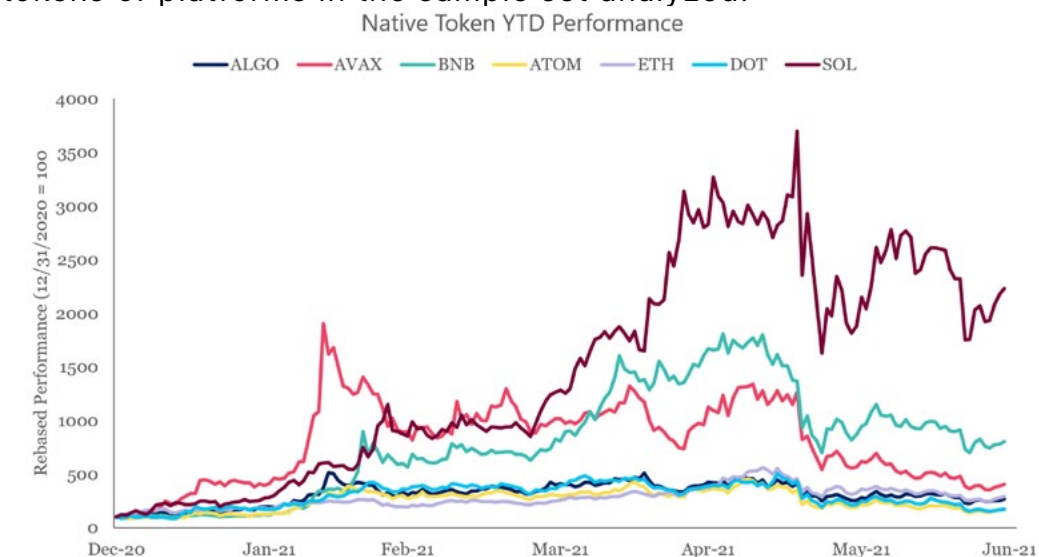
date. At its core, it is a messaging protocol that is often analogized to the TCP/IP layer of the blockchain. IBC is agnostic to the actual content messages which could include fungible token transfers, cross-ledger voting, account delegation, and cross-ledger decentralized exchange order and settlement information. It went live in production earlier this year and could provide insights into the future of interoperability. It is currently being adopted by several zones that leverage Cosmos technology with the potential to be adopted by other chains that reside outside of the Cosmos ecosystem.

Closing thoughts

From different network architectures to different consensus algorithms to different native token designs, there are hundreds of ways to construct a smart contract platform. Based on our analysis of just seven different platforms, the likelihood of a “one chain to rule them all outcome” appears all but impossible. Indeed, the more analytical rigor these platforms are assessed with, the more apparent it becomes that predicting which platform(s) will succeed over the long term is challenging. In many respects, they are very similar. In other respects, they could not be more different.

Appendix:

Figure A: The table below displays YTD performance for the native tokens of platforms in the sample set analyzed.



Source: The Block Research, CoinGecko; Data through 6/30/2021

Conclusions & Outlook

Figure B: The table below provides an overview of traditional investment products that offer exposure to native assets of smart contract platforms.

Traditional Investment Products Offering Exposure to Platform Native Assets								
Product Name	Ticker	Issuer	Holdings	AUM (\$MM)	Expense Ratio (Net)	Inception	Structure	Primary Listing Venue
21Shares Cardano ETP	AADA	21Shares (Amun)	ADA	\$30	2.50%	4/26/2021	ETP	SIX
Osprey Algorand Trust		Osprey	ALGO	\$9	0.00%	5/26/2021	Trust	
21Shares Binance BNB ETP	ABNB	21Shares (Amun)	BNB	\$340	2.50%	10/15/2019	ETP	SIX
21Shares Polkadot ETP	ADOT	21Shares (Amun)	DOT	\$32	2.50%	2/4/2021	ETP	SIX
Osprey Polkadot Trust		Osprey	DOT		0.00%	4/28/2021	Trust	
Grayscale Ethereum Classic Trust	ETCG	Grayscale	ETC	\$651	3.00%	4/24/2017	Trust	OTCQX
21Shares Ethereum ETP	AETH	21Shares (Amun)	ETH	\$215	1.49%	3/5/2019	ETP	SIX
The Ether Fund	QETH.U	3iQ Corp	ETH	\$422	1.95%	12/10/2020	Trust	TSX
3iQ CoinShares Ether ETF	ETHQ	3iQ Corp	ETH	\$182	1.00%	4/23/2021	ETF	TSX
Bitwise Ethereum Fund		Bitwise	ETH		1.50%	12/12/2018	Trust	
BlockFi Ethereum Trust		BlockFi	ETH		1.75%	4/21/2021	Trust	
CI Galaxy Ethereum ETF	ETHX.U	CI Asset Management	ETH	\$365	0.40%	4/16/2021	ETF	TSX
CoinShares Physical Ethereum	ETHE SW	Coinshares	ETH	\$106	1.25%	2/23/2021	ETP	SIX
Ether ETF	ETHR	Evolve	ETH	\$40	0.75%	4/20/2021	ETF	TSX
Grayscale Ethereum Trust	ETHE	Grayscale	ETH	\$6,800	2.50%	12/14/2017	Trust	OTCQX
Purpose Ether ETF	ETHH	Purpose Investments	ETH	\$131	1.00%	4/20/2021	ETF	TSX
Ether Tracker One / Euro	ETHEREUM XBTE	XBT Provider (Coinshares)	ETH	\$1,360	2.50%	10/9/2017	ETP	Nasdaq Stockholm
21Shares Solana ETP	ASOL	21Shares (Amun)	SOL	\$1	2.50%	6/29/2021	ETP	SIX
21Shares Tezos ETP	AXTZ	21Shares (Amun)	XTZ	\$24	2.50%	11/14/2019	ETP	SIX
Grayscale Horizen Trust		Grayscale	ZEN	\$40	2.50%	8/6/2018	Trust	

Source: The Block Research, Company Fact Sheets; AUM as of June 2021. Funds trading on multiple venues have multiple tickers that may not be represented in the chart



