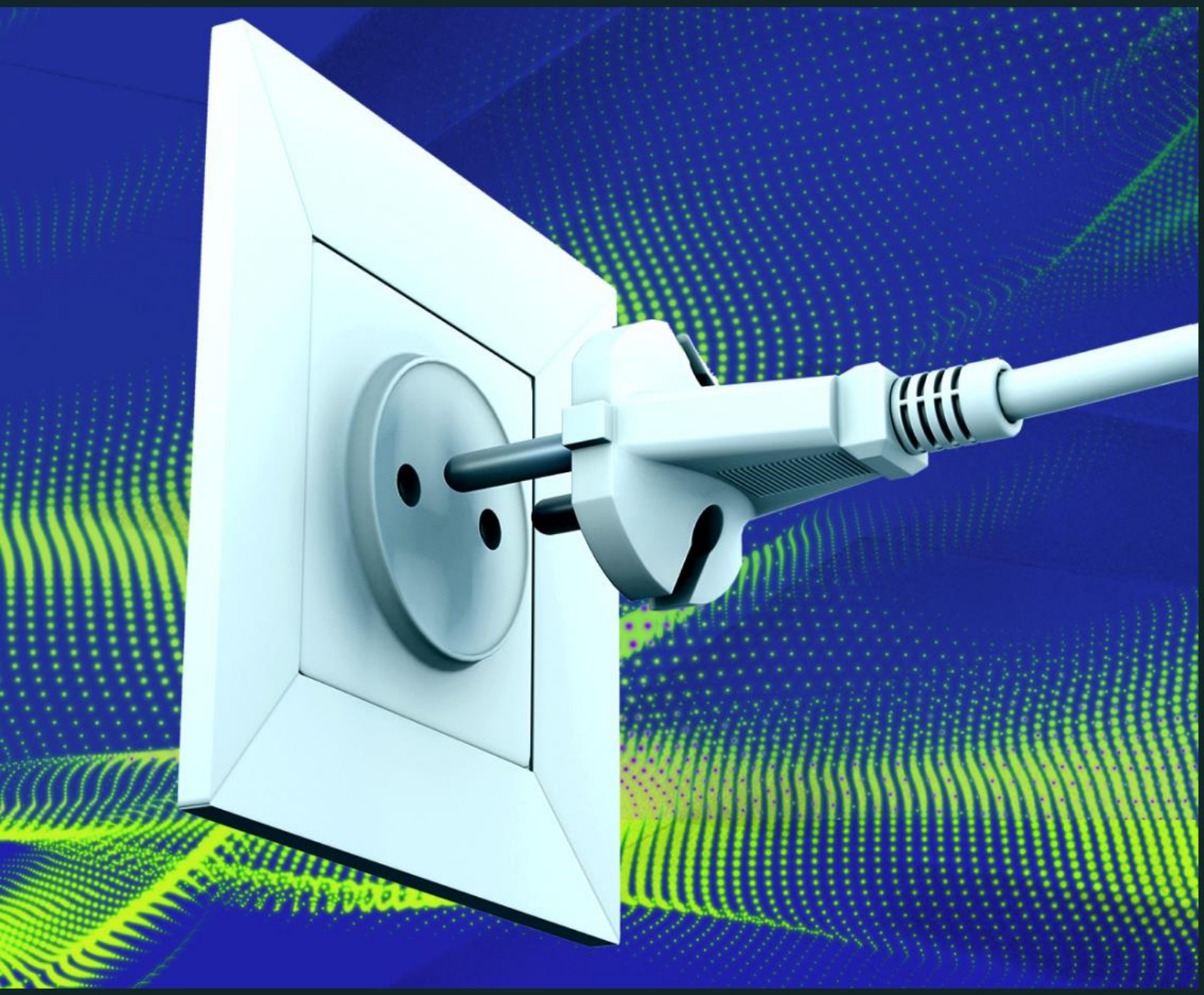
THE BLOCK · Research

Blockchain Compute & Staking: Powering the Decentralized Economy



COMMISSIONED BY W3BCLOUD™

Commissioned by

W3BCLOUD™ (pronounced Web3Cloud) is a leading infrastructure provider powering Web3. We believe everything that can be decentralized will be decentralized, and we provide robust infrastructure required to scale these decentralized protocols and their applications. In short, we are the AWS of Web 3, providing enterprise grade infrastructure that is optimized for the next generation of the Internet.

Researched by The Block Research

The Block is an information services company founded in 2018. Its research arm, The Block Research, analyzes an array of industries including digital assets, fintech, and financial services.

Contact

Email: research@theblockcrypto.com
Twitter: @theblockres

Authors

Dipankar Dutta, Research Analyst
Twitter: @dipdutta06

Table of Contents

Section 1: Introduction

The internet relies on seamless communication between a network of computers located across the globe. Connected devices use standardized protocols (e.g. TCP/IP) that define exact instructions for packaging/unpacking information as it is exchanged between a sender and receiver. The development and universal adoption of TCP/IP, the domain name system (DNS), encryption (e.g. HTTPS), local area communication (e.g. WiFi) and many other standardized specifications and open-source software/protocols have allowed the internet to be the free and open "information highway" that we know today.

In addition to the above, extensive capital investments in physical infrastructure were necessary to scale internet access to the masses. Physical infrastructure includes wired (e.g. telephone lines, fiber optic cables, etc.) and wireless (e.g. cell towers, communication satellites, etc.) hardware that enable end-users to connect their devices to an internet service provider (ISP). Moreover, sophisticated data centers distributed across the globe satisfy the compute and storage requirements for complex applications that users rely on worldwide.

Several parallels can be drawn between the mass-adoption trajectory of the internet and what we refer to as blockchain technologies today. The first is its collaborative development trajectory starting from the 1980's amongst a small circle of independent enthusiasts.[1] Another is the significant set of challenges that blockchain technology must overcome to enable robust functionality and real-world use cases for potentially billions of concurrent users interacting with complex applications.

Scaling blockchain-enabled applications will require innovations both at the protocol-level of blockchain algorithms as well as, their supporting physical infrastructure composed of custom hardware/software distributed globally. This process may be similar to how custom microchip-based processors, related software, databases and server structures in the 1990's laid the foundation for modern data centers powering the internet.

Software that underpins a blockchain network is a critical component of its infrastructure. Development, maintenance and distribution of these blockchain clients can range from being fully open source (e.g. Bitcoin), to being controlled by private institutions with defined development roadmaps (e.g. Solana, Cardano, Polkadot, etc.). Although outside of the focus of this report, development and

[1] JH, Larrier. A Brief History of Blockchain. Technologies and AI. 2021.

fundraising activities for a range of blockchain projects across this spectrum can be found in The Block's Layer-1[2] and Layer 2[3] reports.

This report provides a high-level overview of, 1) the computational and financial requirements to participate in blockchain networks and, 2) the service-based entities focused on simplifying access to compute and staking for entities interacting with blockchains.

Why the Consensus Mechanism Matters

In the most basic terms, a blockchain network is made up of computers connected by the internet running the same set of instructions to continuously add new data (blocks) to a permanent distributed database (blockchain). Reliable propagation of blocks within a distributed network requires a consensus mechanism that allows global agreement on the current state of the blockchain. Here, compute requirements for individual network participants are determined by their specific role(s) within the various types of consensus mechanisms that govern each chain.

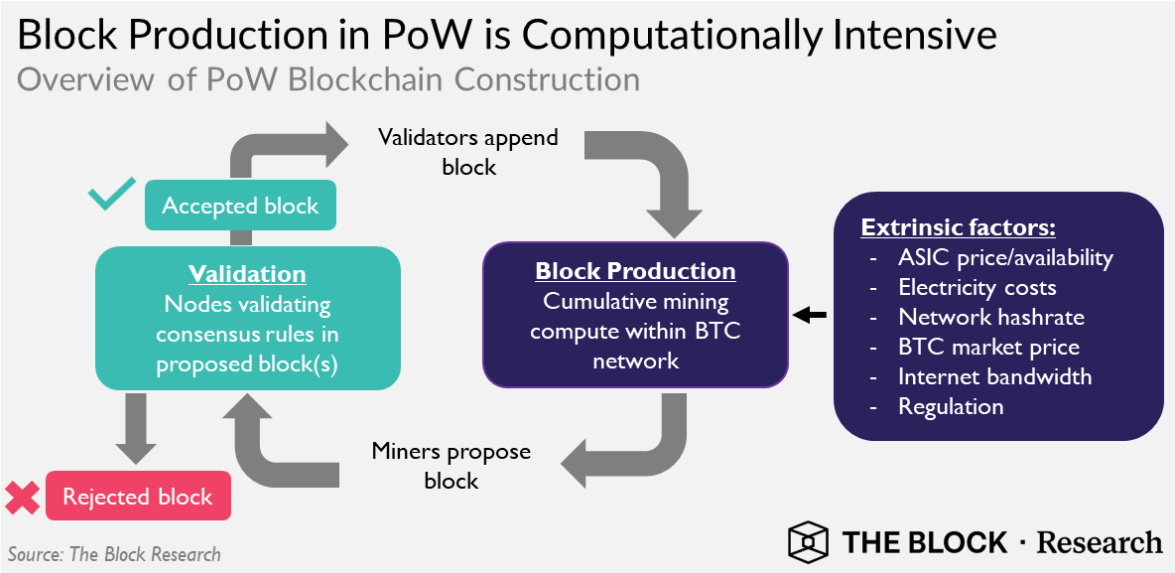
Consensus mechanisms that incorporate proof-of-work (PoW) have dominated the digital asset space. As of writing, >56% of the digital asset market capitalization is composed of PoW chains (Bitcoin, Ethereum, Litecoin, etc.). However, this dominance has been on a significant downtrend in the past years with the emergence of proof-of-stake (PoS) consensus mechanisms preferred by newer blockchains entering the market (e.g. Solana, Cardano, Polkadot, etc.). In fact, the second largest blockchain by market capitalization, Ethereum, is expected to transition from PoW to PoS through what is known as the "merge" – widely considered as one of the most significant events in the history of the digital asset class.

The following sections briefly discuss the basic functionality of "layer-1" (L1) PoW and PoS blockchains (sections 2 & 3, respectively) to inform our discussion of compute requirements for each. Here, L1 refer to blockchain networks that can validate and finalize transactions without relying on a different chain. We will also discuss current efforts to scale blockchain transaction throughput (section 4) and end with our concluding thoughts.

[2] Layer 1 Platforms: A framework for Comparisons. The Block. 2021.
[3] Layer-2 Scaling Solutions: A Framework for Comparisons. The Block. 2022.

Section 2: Proof-of-Work Blockchain Infrastructure

The implementation of PoW used in Bitcoin was the first to address several fundamental challenges in achieving consensus in a distributed computer network – the Byzantine Generals' problem and Sybil resistance.[4] PoW requires an investment in real-world costs such as electricity, compute hardware and related infrastructure (lumped together as extrinsic factors in figure below), that penalize network participants for behaving dishonestly.



Nodes are the individual participants in a blockchain network. They are (usually) equipped with the entire blockchain ledger history and participate in the consensus mechanism by producing new blocks, validating them and/or broadcasting new transactions to the network. Terminology is inconsistent across the industry, but PoW node compute requirements can be divided further into two entities. The first are the "mining nodes" with the primary function of competing using computational power to "mine" (produce) new blocks and capture fees plus the mining reward.

The second are nodes that only validate whether blocks proposed by mining entities meet the consensus rules. We shall refer to this subset as "consensus nodes." Bitcoin consensus nodes (not involved in mining new blocks) require relatively minimal computational power, storage, bandwidth and technical expertise – a new dedicated device costs roughly $250. There are no economic incentives to operate a consensus node other than ideological reasons to help secure the network. There are ~14,000 total reachable nodes operating in the Bitcoin network as of writing. They are a mixture of both consensus and mining nodes.

[4] I. Chohan, et. al. The Double Spending Problem and Cryptocurrencies. SSRN. 2021.

Mining Landscape for PoW Chains

The block production process begins with mining nodes selecting a set of transactions to include in a block from a pool of pending transactions (usually based on fees). Bitcoin mining entities then compete using computational power available to each by performing iterative SHA-256, a deterministic hashing calculation to generate a "nonce" that satisfies the current difficulty setting of the algorithm. There are several hashing algorithms currently implemented across various PoW chains (e.g. Bitcoin, Ethereum, Litecoin and Monero; Table 1). Once a block is mined that satisfies the consensus rules, it is broadcast to the network to be validated and included in the blockchain. A more detailed explanation of the PoW consensus mechanism can be found here.[5]

Computational power dedicated to popular PoW networks has increased significantly on a year-over-year basis. This demonstrates robust capital commitments in infrastructure as well as, operation and management (O&M) due to favorable monetary incentives for miners. Conversely, less popular PoW chains (i.e. Bitcoin Cash) have failed to maintain a long-term uptrend in hashrate over their lifetime due to a confluence of factors that include lower rates of adoption and other extrinsic factors (as identified in the figure above).

Table 1	Market Cap (billion USD)	Block Time (s)	Block Reward (in-kind)	Hash Algorithm	Processor Type[2]	Total Network Hashpower (Ph/s)	Hashrate Efficiency (Mh/W)[3]
BTC	405	600	6.25	SHA-256	ASIC	200,000	47,619
Ethereum[1]	149	15	2	Ethash	ASIC/GPU	0.9	2.0
Dogecoin[1,4]	9.3	60	10,000	Scrypt	ASIC/GPU	0.4	0.9
Litecoin[4]	3.6	150	12.5	Scrypt	ASIC/GPU	0.4	0.9
Monero	2.3	120	0.74	RandomX	CPU/GPU	0.0000024	0.0001
Ethereum Classic	2.2	15	2.56	Etchash	ASIC/GPU	0.024	2.0
Bitcoin Cash	2.1	600	6.25	SHA-256	ASIC	1,053	47,619
Bitcoin SV	1	600	6.27	SHA-256	ASIC	509	47,619
Zcash	0.8	75	5	Equihash	ASIC/GPU	0.000013	0.0003

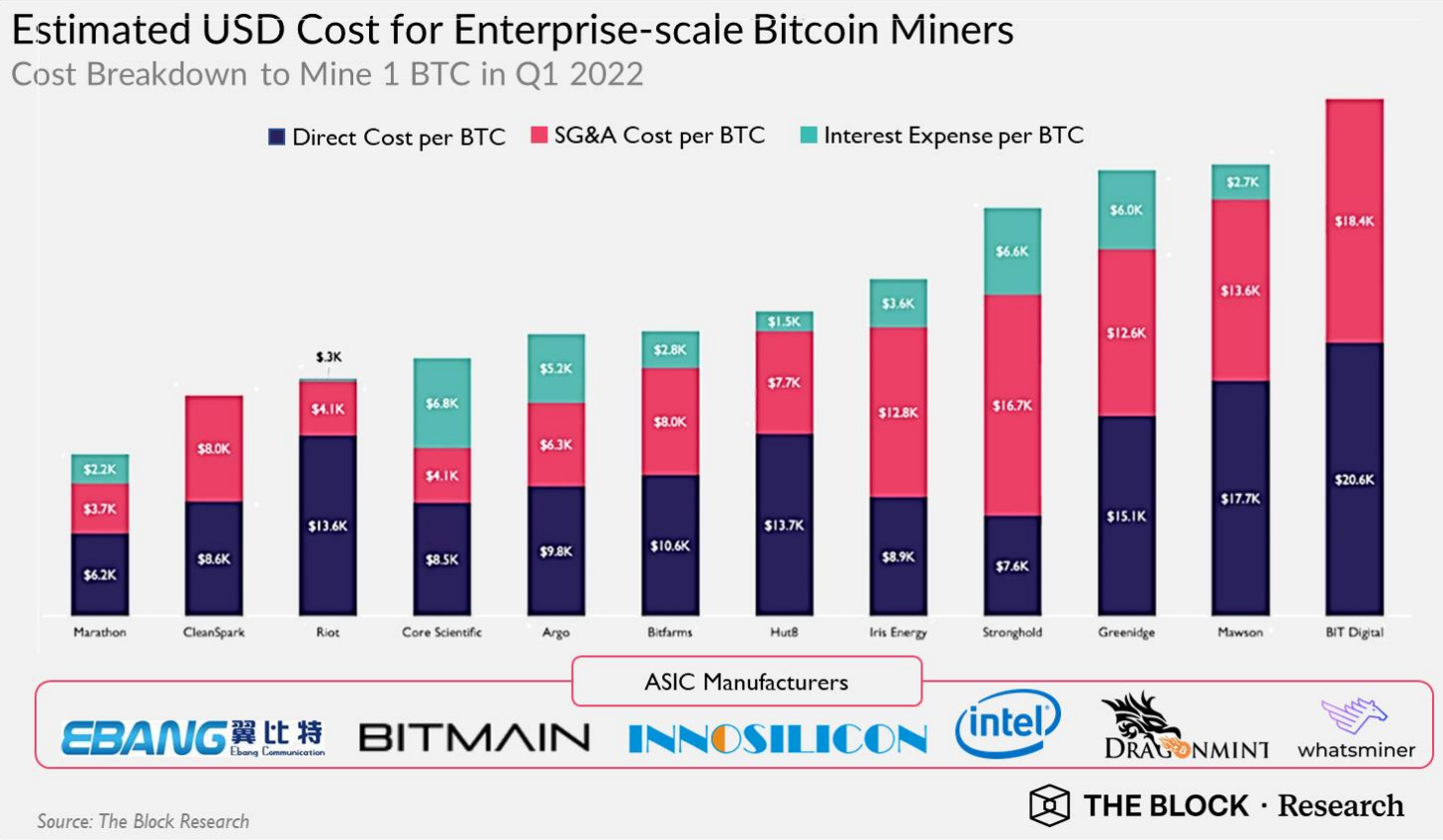
[1]Slated to transition to proof-of-stake; [2]Used by professional miners; [3]For compatible state-of-the-art processor in megahash/watt (Mh/W); [4] Litecoin & Dogecoin are merge-mined; **AISC** - application-specific integrated circuit; **GPU** - graphics processing unit; **CPU** - central processing unit; Accurate as of 7/25/2022; Sources: f2pool.com & minerstat.com

Strong demand from PoW mining entities for computational power have also incentivized chip manufacturers to optimize their designs specifically for hashing functions. A few manufacturers have since risen from the periphery to compete and deliver modular computational units offering the optimal balance between

[5] Antonopoulos, AI. Mastering Bitcoin: Programming the Open Blockchain. 2017.

energy efficiency, hashrate, reliability and cost. This has led to specialized application-specific integrated circuit (ASIC) designs that are highly efficient at performing specific hashing calculations – relative to more general-purpose computing units such as, central processing units (CPU) and graphics processing units (GPU).[6] Varying hardware requirements across hashing algorithms significantly affect hashrate efficiency (Table 1). Thus, total network hashrate is expected to vary across networks where the magnitude of total hashpower alone is not a reflection of its security guarantees.

For the Bitcoin network, introduction of ASICs along with intense competition between mining entities mean that successful Bitcoin mining operations all tend to look the same today – highly capitalized entities with optimized O&M, ability to source the most advanced hardware, lowest cost energy, while operating in a stable jurisdiction. PoW mining is thus a dynamic landscape that is difficult to enter and navigate, making it a very high churn industry. The figure below represents the estimated operational cost for mining Bitcoin across some the largest mining entities as of Q1 2022. As a reference, the market price for BTC ranged between $32.9k and $47.8k USD during this period.



[6] 1. Cho, H. ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols. IEEE Access. 2018.

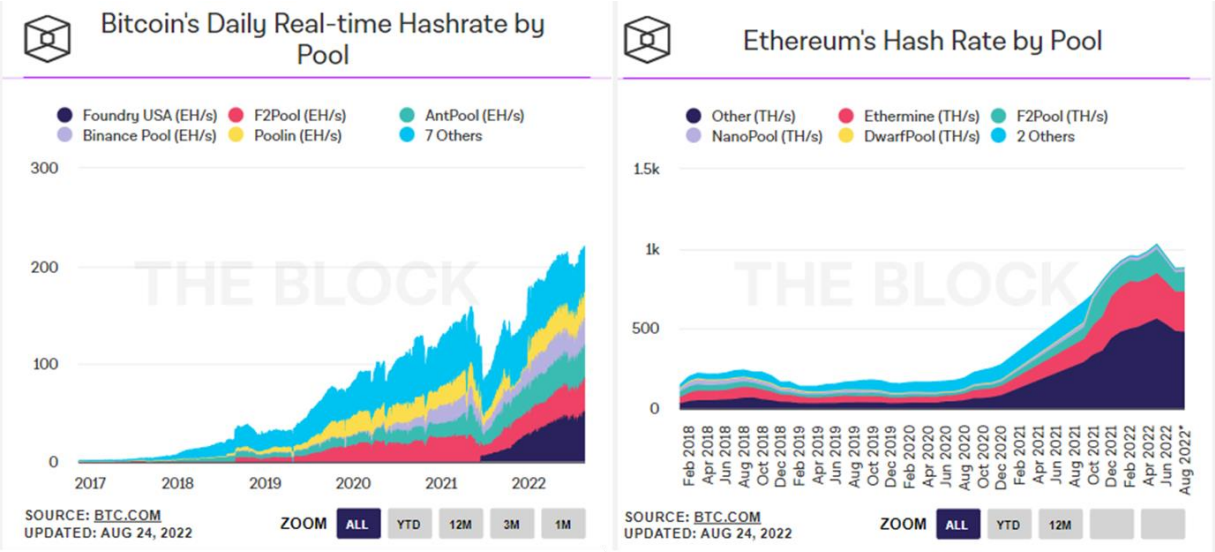
PoW Infrastructure Service Providers

In the early days of PoW networks, the mining market was dominated by individuals mining on home computers. At this time, "solo-mining" was the norm where each entity was competing with a small number (relative to today) of peers using comparable hardware. The growth of the Bitcoin network and more importantly, the market value of BTC, has not only attracted professional mining operators, but also a small class of investors that treat ASIC miners like yield-producing commodities. Both these market participants have led to the rise of multiple niche PoW-based service providers.

Mining Pools

News articles about solo-miners miraculously mining a new Bitcoin block to receive mining rewards worth multiples (in USD) of their rig is akin to winning the lottery. Long-term PoW miner profitability is based on probabilities directly related to the compute hashpower they control. Thus, it is also highly likely for a sufficiently small miner to never mine a new block through its operational lifespan.

Entities known as "mining pools" were thus devised for continuous and predictable flow of block rewards for miners. Mining pools can be thought of as a coalition between two or more mining entities with an appointed "pool manager" as the block reward recipient. If an entity within the pool successfully mines a new block, the pool manager receives the associated block reward and distributes it to all mining entities.[7] Reward distribution is based on previously agreed upon rules and is usually proportional to the compute power each miner contributes to the pool.



[7] I. Chatzigiannis, et. al. Diversification across mining pools: optimal mining strategies under PoW. Journal of Cybersecurity. 2022.

Mining pools dominate all PoW networks today. The top 5 mining pools make up ~80% and ~45% and of the Bitcoin and Ethereum global hashrates, respectively. Concentration of hashpower in mining pools is often used to criticize PoW mining centralization, which is generally not well-supported. Pools are usually permissionless and the hashpower is not "owned" by any pool operator. Rather it is voluntarily supplied by many independent participants that are incentivized to redirect their hashpower elsewhere when there is foul play. Pools however may make miner collusion easier, in principle.

Miner hosting & Co-localization Services

As the concept of digital assets propagates through popular culture, so does the prospect (allure even?) of mining and potentially generating a new source of income among retail participants. ASICs also have robust secondary market dynamics where global participants not only speculate on future AISC prices, but also may demand the ASICs in their custody to generate income while under their control. There are many such reasons why several services are competing for market share to provide turn-key hosting solutions that involve PoW mining.

Some providers cater to demand for remote O&M of ASICs supplied by third parties in jurisdictions with favorable economic conditions (e.g. electricity costs). These services can be classified as mining hosting services where prominent companies in the US include Frontier Mining and Compass Mining. In the hosting sector, Compute North completed a notable $85M USD series C raise in February 2022.

Other examples include plug-and-play modular mining units that in principle, could be co-located with wasted or stranded energy. This is a developing industry niche where notable operators include Great American Mining and Blockstream, largely targeting the oil and gas producer sector. Blockstream completed a $210M USD series B raise in August 2021. Crusoe Energy Systems completed a second notable $350M USD series C raise in April 2022.

Ethereum's transition to PoS from PoW in what's known as the "merge" is one of the most anticipated events in the history of the digital asset class. Details regarding the merge (scheduled for September 19th, 2022), are outside the scope of this document. However, given that for the month of July 2022, total mining revenue for Ethereum was $620M USD (versus $597M for Bitcoin), an interesting question that remains is: what will the miners do after the difficulty bomb?

There is no precedence for an event like the merge. Chain fork(s) (e.g. "EthereumPoW" with the token, ETHW) that continue using PoW consensus are expected. However, the fate of these forks are (arguably) sealed as several prominent decentralized applications (DApps), data oracles and centralized stablecoin issuers have publicly announced their support for the "official" PoS Ethereum chain. Current Ethereum miners may decide to migrate their hashpower to EthereumPoW, to a different PoW chain or, decide to liquidate their hardware.

Considerations for PoW Compute Decentralization

The open, trustless, censorship-resistant and permissionless nature of the most popular blockchains (e.g. Bitcoin and Ethereum) arise from their degree of decentralization. The term "blockchain trilemma" coined by Ethereum co-founder, Vitalik Buterin describes a simple relationship between blockchain decentralization, scalability and security – you can choose two and must compromise on the third.

Thus far, this trilemma has proven itself to be a fundamental technical barrier. New entrants in the market may begin with advertising novel technologies to go around it. Most simply test the minimal amount of decentralization the market will accept towards achieving scalability and minimizing transaction costs. The controversial concept of centralized-decentralized finance (CeDeFi) has also been proposed.

Beyond the potential of inherent centralization at the protocol level, there may also be concerns related to the centralization of the hardware underpinning these blockchains. Single entities that dominate critical pieces of infrastructure of an ecosystem represent bottlenecks and single point(s) of failure.

There are significant centralization concerns for the PoW network infrastructure. Looking just at the Bitcoin network, there is a limited number of dominant ASIC manufacturers that are concentrated geographically in China. Secondly, these manufacturers largely supply a handful of mining operators, which as mentioned in section 2, tend to be large corporate entities.

Thus, both supply and operation of Bitcoin's hashrate infrastructure, crucial for the security of its consensus mechanism, maybe be susceptible to mal/over-regulatory shocks in individual jurisdictions, local supply-chain disruptions, and/or financial collapse of individual mining companies or ASIC manufacturers. The degree of threat these concerns pose to the network is debatable. However, they are real.

In May 2021, China instituted a ban on all PoW mining and transactions of digital assets. Hashrate across every PoW chain dropped significantly as Chinese mining operations began to bring their hashpower offline. At the time, Bitcoin mining operations were highly concentrated in China – peak to trough, total mining hashrate dropped by more than 50% in two months by July 2021 for Bitcoin. To address the mono/oligopolistic structures prevalent in PoW mining, ASIC-resistant hashing algorithms (e.g. Monero's RandomX) have been proposed, but remain unproven as of yet.

Further concerns for PoW network security relate to maintaining a long-term economic incentive structure for the mining entities. A prominent criticism for Bitcoin is thus its 21 million hard cap and its block rewards reducing by 50% ever 4 years. The assumption is that at some point, transaction fees on Bitcoin L1 alone will be sufficient to incentivize miners to provide adequate security for the network.

> "*In a few decades when the reward gets too small, the* ***transaction fee will become the main compensation for nodes****. I'm sure that in 20 years there will either be very large transaction volume or no volume*." – Satoshi Nakamoto, founder, Bitcoin (Bitcointalk.org, February 2010)

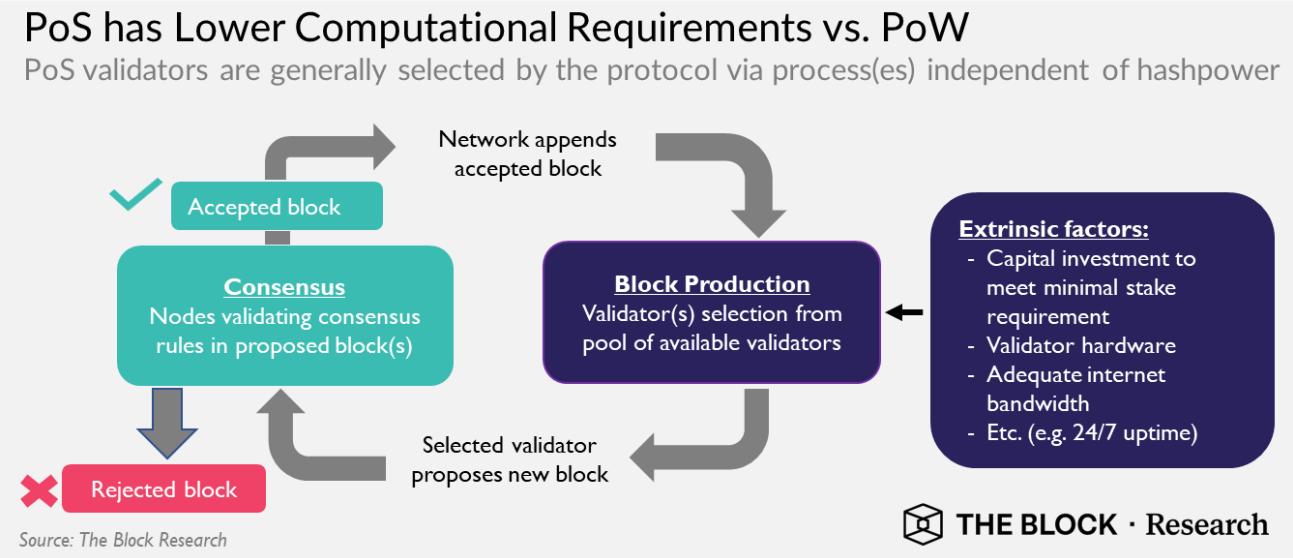
Although outside of the scope of this document, there is a healthy ongoing debate about the long-term sustainability of Bitcoin's security model.[8,9] It is difficult to predict what the Bitcoin blockspace market may look like years from now because it requires assumptions about network adoption, transaction volume and development/adoption of future technical advances. PoW networks with infinite token tail emissions for block rewards may in theory address these concerns, but it is unclear as of now if such a design is an absolute necessity.

[8] Alden, L. Bitcoin: Fee-Based Security Modeling. 2021.

[9] Hasu, et. al. A model for Bitcoin's security and the declining block subsidy. 2019.

Section 3: Proof-of-Stake Blockchain Infrastructure

Proof-of-stake (PoS) is currently the second most dominant blockchain consensus mechanism with the first known implementation being Peercoin in 2012. A core feature of any distributed consensus mechanism is that it is much more profitable to simply be an honest participant rather than a malicious one. For PoW, fraudulent blocks that get rejected by the network leave the bad actor with only the cost of wasted electricity. For PoS, it's risk of loss (or "slashing") of "staked" capital in the form of tokens native to the blockchain required to run a validator.



A validator in a PoS chain serves a similar purpose to what was described earlier as nodes for PoW chains – they are the functional units responsible for proposing and validating new blocks in a PoS chain. Thus, validators must also contain full/curtailed history of all transactions along with the consensus rules governing the chain.

A key difference with the PoS consensus mechanism is the process by which block production is initiated. For PoW, any mining node can earn the right to propose a new block if they show the proof of work by generating a valid nonce. In PoS, a validator is usually nominated by the protocol using various mechanisms to propose the next block. This validator selection mechanism may be purely random, or in some cases, users may vote for specific validators using their coins to bias the selection process (delegated proof of stake; DPoS).[10] As such, PoS validators do not usually employ any energy-intensive brute-force compute.

[10] I. Sun, et.al. DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. Procedia Computer Science. 2021.

In any case, the selected validator formats available pending transactions, which are either accepted or rejected by the network based on the consensus rules. As mentioned earlier, validators are required to lock in (or "stake") a certain number of tokens native to each chain. The protocol disincentivizes malicious/incompetent behavior by confiscating and burning ("slashing") some/all the deposited stake. Readers are encouraged to refer here for further details on PoS chains.[11]

The PoS consensus mechanisms have been proposed as a solution for many of the disadvantages found in PoW blockchains. Principally, unsustainable/high energy usage, low transaction throughput, poor scalability, high barrier to entry for PoW mining entities, among others.

It remains to be seen whether PoS can live up these expectations in the long run. However, nearly every new L1 blockchain offering in the market has chosen to implement some iteration of a PoS consensus mechanism. Moreover, the fastest growing L1 chains since 2020 have all been PoS L1s, notable examples include (in order of market capitalization): BNB chain, Cardano, Solana, Polkadot, Avalanche and others.

Validator Landscape for PoS L1 Blockchains

The above is a simplified outline of PoS consensus. In reality, there are significant differences in design choices between PoS chains that endow each with their own set of unique properties, advantages and disadvantages. Some PoS chains have implemented a traditional blockchain structure with a single chain and an associated security framework (e.g. Cardano & Solana). Others have more complex multi-chain architectures that rely on the security guarantees of the base L1 chain (e.g. Polkadot). Further still, a second way of approaching blockchain interoperability is a multi-chain ecosystem with each chain having an independent security profile (e.g. Cosmos). Details regarding the specifics of these design architectures is out of the scope of this report, please refer to The Block's Layer-1 report for more details.[12]

In short, PoS nodes can be classified into four categories – validation (participation) nodes, read/write nodes, sentry (proxy) nodes and relay nodes. Details about differences between them can be found in The Block's data infrastructure report.[13] This section will discuss the validator requirements for the most popular PoS L1

[11] I. Xiao, et. al. A Survey of Distributed Consensus Protocols for Blockchain Networks. IEEE Commun. Surv. Tutorials. 2020.

[12] Layer 1 Platforms: A framework for Comparisons. The Block. 2021.

[13] The State of Digital Asset Data Infrastructure Landscape. The Block. 2021.

chains. These requirements can be divided into two major categories, hardware and connectivity (Table 2) as well as, staking requirements (Table 3).

Requisite hardware components for PoS L1 chains are usually available off-the-shelf (as opposed to ASICs for Bitcoin mining; Table 2). However, given the composability and transaction speed/finality guarantees that some contemporary PoS blockchains advertise, validator uptime and reachability are critical factors.

Table 2	Ethereum[1]	BNB Chain[3,4]	Cardano	Solana	Polkadot[3]	Avalanche	Near[3]
CPU (# cores)	4	16	4	16	4	8	8
RAM (GB)	8	64	16	256	64	16	16
Storage (GB)	2,000	2,000	256	2,000	1,000	1,000	1,000
Blocktime (s)	12	3	20	0.8	6	~1	1.1
Est. Bandwidth (Mbps)	50	100	100	1,000	50	50	50
Current Validator count	400,000[2]	21	3,180	1,878	297	1,238	100
Software Clients	Various	BSC Full Node	Cardano Node	Solana Tool Suite	Polkadot	AvalancheGo	NEAR-CLI

[1]For Ethereum beacon chain; [2]Represents the number of unique signing keys, number of unique/independent validators are unknown but almost certainly lower; [3]There is either a limit on the total number of validators, or only privileged entities can run validators on these networks. [4]Binance chain and Binance smart chain was rebranded into "Build and Build" (BNB) chain. Sources: official protocol documentation & The Block Research as of 7/25/2022

Many PoS protocols thus enforce slashing penalties to not only penalize malicious behavior (breaking consensus rules), but also for what may otherwise just be bad luck (e.g. unplanned internet/power outage). Multiple geographically distributed nodes are often clustered for redundancy to protect staked capital (Table 3) – multiplying O&M resources needed to maintain validators.

Additional validator O&M requirements may include 24/7 uptime, high internet bandwidth, and/or involved monitoring for network connectivity and synchronization issues. High performance PoS networks can run into congestion issues and significant network downtime, the cause of which are usually related to distributed denial-of-service (DDoS) attacks.

Table 3	Ethereum[1]	BNB Chain	Cardano	Solana	Polkadot	Avalanche	NEAR
Min. Native Token Stake	32	10,000	500	0.027[4]	Dynamic[6]	2000	>67,000
Min. Capital Lockup (USD)	$43,200	$2,500,000	$250	$2	Dynamic[6]	$50,000	$251,250
Unbonding Period (d)	N/A[2]	7[3]	N/A	10	28	N/A[7]	2
Est. Rewards (APR)	2-8%	5-10%	3.5-8%	4.5-8%	8-16%	8-11%	8-14%
Slash (Y/N)	Y	Y	N	Y[5]	Y	N	N

[1]For Ethereum beacon chain; [2]Staked ETH locked up at least until the merge event; [3]Refers to delegated stake; [4]~1.1SOL/day additional for on-chain voting transactions; [5]Long-term slashing rules under exploration; [6]Can be estimated from statistics for current validator set; [7]Stakers must lock tokens for 14-365 days. Sources: official protocol documentation & The Block Research as of 7/25/2022

To summarize – even though the hardware can be sourced from most local electronic retailers, reliably operating a self-hosted PoS validator can be challenging and risky in practice.

The Avalanche and Cardano networks are notable exceptions where there is no risk of slashing. Instead, validator misbehavior results only in loss of their claim to the block reward. Cardano and Avalanche both have a stake delegation system where validators (or stake pool operators) may earn fees by attracting token delegation from other stakers. Validator earnings are therefore related to the total amount of tokens staked, which should incentivize stake pool operators to remain honest and maintain high performance standards. Exact yields for validators and delegators can vary significantly based on parameters specific to a protocol.

Operators may also elect to run PoS full nodes to function as a read/write, sentry (proxy) nodes and/or a relay node. This may be to function as a witness observing the blockchain state, broadcast new transactions and/or allow for applications to interact with the blockchain. Hardware and O&M requirements for all nodes are usually the same as a validator node and generally do not have any staked capital or any of the associated slashing risks.

PoS Infrastructure Service Providers

The market has shown healthy adoption of an assortment of new PoS chains built using bespoke technologies. Interacting with these ecosystems often require a complex array of compute infrastructure and expertise to run nodes and. Some entities (e.g. individual DApp developers) may not have the necessary tooling or resources to be agile in this highly dynamic environment.

There is thus a vibrant software and service-related economy making up the PoS blockchain infrastructure that has matured over the past years. Companies and organizations cater to diverse clientele that include individual token holders looking for simplified staking services, entities looking to interact with various blockchains and organizations that demand digestible blockchain data for their operations.

In simple terms, the first generation of these entities were created to address fundamental challenges in blockchain infrastructure (mining/staking pools), node operation/rentals and blockchain data science. These operators have since grown in complexity, offering a wide variety of services including fully managed backends for blockchain projects. This section will specifically outline the current service offerings that exist to satisfy the growing market demand to simplify staking for PoS networks.

Staking Operators

As mentioned in the previous section, staking of native assets on PoS chains will likely require an assortment of compute infrastructure that includes specialized node(s) that require the appropriate O&M. Here O&M encompass specialized expertise and support tooling for load balancing, failover protection as well as, container, monitoring and alerting to avoid slashing penalties.[14] Some PoS networks also have a high cost of entry and opportunity costs for prospective stakers. As PoS chains began to gain traction post-2018, so did the demand for services that simplify the process of earning yield via staking.

Table 4

Firm / Protocol	Est.	HQ	Funding ($ millions)[1]	Chains Supported[2]	Value Staked ($ millions)[2]	Unique Users[3]
Allnodes	2017	USA	N/A	23	$3,493	31,533
Kraken	2011	USA	Private	8	$1,536	N/A
Binance Staking	2017	N/A	Private	23	$1,511	N/A
InfStones	2018	USA	$66	29	$1,121	34,684
Staked	2018	USA	$4.5	28	$775	22,768
Everstake	2018	Ukraine	Private	27	$757	258,037
Stakefish	2018	Estonia	Private	23	$746	86,555
SwissBorg	2017	Switzerland	$52	19	$664	229,688
Bison Trails	2018	USA	Acquired	13	$628	7,976
Bitcoin Suisse AG	2013	Switzerland	Private	6	$626	839
StakeWise	2018	USA	$2	1	$489	N/A
Attestant	2019	UK	Private	1	$479	N/A
MyCointainer	2018	Estonia	$6	105	$474	232,183
Ankr Liquid Staking	2017	N/A	$27	7	$450	11,823
Guarda Wallet	2017	Estonia	Private	9	$443	5,465
P2P Validator	2018	Cayman Islands	$36	17	$433	16,193
Stakin	2019	Estonia	Private	25	$404	33,727
ChorusOne	2018	Switzerland	$30	20	$308	34,237
HashQuark	2017	Hong Kong	$17	32	$266	2,727
Figment	2018	Canada	$165	26	$251	34,663

[1]Data from crunchbase.com; [2]Data from stakingrewards.com as of July 2022. [3]Total number of users are an estimate, data from stakingrewards.com. Sources also include company website(s), pitchbook and press releases as of July 2022.

[14] The State of Digital Asset Data Infrastructure Landscape. The Block. 2021.

Firms operating staking pools (Table 4) not only manage the infrastructure needs, but also compete to provide access to the plethora of PoS protocols currently in existence. Moreover, new protocols reaching the market often have their own governance mechanisms as well as hardware, connectivity, and O&M needs. These firms manage these back-end requirements to simplify the end user's (e.g. token holders, developers, and other businesses) staking interactions with PoS blockchain networks. In return the end-users agree to pass on a portion of the staking rewards as a fee to the operator.

Liquid Staking Pools

Liquid staking is an evolution in the way stakers interact with the staking operators. Instead of a direct interaction, the stakers deposit their native tokens into a pool managed by a smart contract. In return, the stakers receive a derivative token that represents their proportional share of the underlying stake pool and the yield it generates. The yield is generated by making the token pool available to a group of professional node operators that have usually undergone some selection process.

Liquid staking solutions and their derivative tokens have become increasingly popular as they can be traded or used as collateral on some popular decentralized finance (DeFi) applications. Lido is currently a front-runner in adoption across five L1 PoS chains where it has been deployed – Ethereum, Solana, Kusama, Polygon, and Polkadot. Lido completed a $70M strategic raise in March 2022. Although there are several other protocols of note, as shown above. Lido functions as a decentralized autonomous organization (DAO). Stakers are free to deposit native tokens in practically any amount. The Lido DAO also operates a whitelisting process for the node operators.

Considerations for PoS Compute Decentralization

For PoS chains, we have seen signs of node infrastructure centralization where some DApps coming offline tend to correlate with reported outages from cloud service providers. Infrastructure providers that target developers/businesses to help build out their blockchain-enabled product/service (i.e. node rentals, managed blockchain integration) are thought to make up an appreciable portion of all nodes

in some networks. For example, Infura operated 5% to 10% of all Ethereum full nodes to service 13 billion queries per day and supporting 70% of the top Ethereum DApps – according to estimates in 2018.[15] More recent estimates indicate that >55% of all Ethereum nodes currently run on hardware owned and operated by professional hosting providers. Node centralization may have an outsized effect on the security of the entire network. For example, Hetzner Online GmbH, which hosts ~14% of Ethereum nodes just announced that "…even if you just run one node, we consider it a violation of our ToS [terms of service]."

PoS validators select the transactions to be included in a block. Thus, centralization of block-producing PoS validators along with their staked capital can present enormous challenges to the neutrality, permission-less and censorship-resistant properties of a PoS network. This is an important point of consideration as current decentralized finance (DeFi) platforms have ~$90 billion USD locked in value across dominant smart-contract PoS blockchains, as of writing.

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

In anticipation of the "merge" event on September 19th, 2022 (as of writing), ~11.1% (13.3M ETH) of all circulating ETH has been deposited in the ETH2 deposit contract. Non-custodial liquid staking protocols as well as, exchanges and professional staking operators offering custodial staking options have become immensely popular due to their accessibility and ease of use (Table 5).

Table 5

Firm/Protocol	Type	HQ	ETH2 Staked[1] (%)
Lido	LSD	N/A	31.1%
Rocket Pool	LSD	N/A	1.6%
Coinbase	Exchange	USA	14.8%
Kraken	Exchange	USA	8.5%
Binance	Exchange	N/A	6.8%
Staked	Staking operators	USA	2.4%
Bitcoin Suisse	Staking operator	Switzerland	2.2%

[1]Relative to the total of ~13.3M ETH staked on the beacon chain. **LSD** - liquid staking derivative. Source: The Block Research & Etherscan. Data accurate as of 8/10/22.

For Ethereum, the top 7 identifiable entities control >67% of all staked ETH. Specifically, the Lido DAO controls ~4.15M ETH on the beacon chain, or 31% of all staked ETH, as of writing. Delegated stake can be withdrawn at will in applicable PoS chains (an unbonding period may be applicable). However, in Ethereum's case,

[15] Research report: The State of the Digital Asset Data and Infrastructure. The Block. 2020.

staked ETH is locked in at least until the merge event, and for an indeterminant amount on time afterwards based on several factors.

Lido's stETH liquid token enjoys wide integration from other DApps in Ethereum's ecosystem, making Lido the front-runner in liquid staking protocols by a wide margin. The current dominance of Lido (across multiple PoS chains) supports the argument that liquid staking services could be a "winner-takes all" market. If true, overwhelming dominance of any individual protocol may leave the entire network more open to hostile capture. In Lido's case, it may be through its DAO governance structure where the top hundred LDO token holders collectively own >92% of all LDO in circulation (out of ~19k total holders on the Ethereum chain).

On August 8th 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash (TC), a mixing/anonymizing protocol in the Ethereum ecosystem. The implications could be wide reaching. US-regulated entities operating Ethereum validators such as exchanges that currently custody >23.3% of staked ETH (Table 5) may be required by law to censor all transactions and addresses having any association with TC.

OFAC's decision is controversial to say the least – court challenges and political scrutiny are expected. Although OFAC's announcement is currently limited to TC on Ethereum, most other blockchains (PoS or, PoW) can be targeted if the standard for such sanctions indeed boils down to censoring open-source code. OFAC's decision has sent ripples across the entire digital asset ecosystem, increasing interest in methods that advance censorship-resistance and privacy.

To that end, platforms that implement ZK proofs (discussed in more detail in section 4) may help address concerns related to hardware/validator centralization and end-user privacy. Although ZK proofs in principle advance the permission-less nature of blockchains, they may not completely negate the need for hardware decentralization. Censorship-resistance will still be a function of the number and geographical distributions of independent node operators. However, the concept of encouraging everyone to run their own personal nodes may also prove to be practically unrealistic.

Optimization and implementation of ZK proofs is one potential way of reducing the threshold for what some may consider "adequate" in terms of decentralization. One implementation of note is Aztec protocol's "ZK-ZK-rollup" that promises private L2 transactions while leveraging the security guarantees of the Ethereum L1.

> *"In a system that uses cryptographic proofs, you can have a situation where* ***one big machine, with dedicated hardware that need not be trusted by anyone else, can process … [many] transactions*** *and generate a very, very small proof that everyone can trust with perfect certainty."* – Eli Ben-Sasson, Co-Founder and President of StarkWare (Real Vision Podcast, February 2022)

Section 4: Scaling Challenges for Blockchains

Blockchain scaling refers to optimizations for transaction throughput (number of transactions per second), latency (time to final settlement) and cost (fees). There has been a flurry of activity to develop "ETH-killers" – L1 chains that promise to solve Ethereum's scaling constraints and overcome the blockchain trilemma.

In practice, new market L1 chains have found it extremely difficult to overcome the deeply entrenched network effects of developers, programming languages (Solidity & Vyper), the Ethereum Virtual Machine (EVM) execution environment, infrastructure and the capital liquidity that is powering the Ethereum's ecosystem of DApps.

L1 smart contract chains such as, Build and Build (BNB) chain (formerly Binance smart chain; BSC), Avalanche and Fantom have thus chosen to integrate with Solidity/Vyper and EVM, making this transition easier for developers and users alike (e.g. interoperable wallet clients; Metamask). Although Solana has now set a precedent for gaining significant development activity and end-user adoption, despite using a different development environment (Rust programming language and Sealevel as the execution environment).

Solving Ethereum's scalability challenges is not difficult if a protocol is willing to sacrifice decentralization, censorship-resistance and security. For example, BNB chain has demonstrated incredible growth since 2019 given its compatibility with Solidity/EVM that has allowed developers to "copy/paste" applications from Ethereum into its ecosystem. BSC has taken advantage of the lack of network bandwidth and increasing gas costs on the Ethereum network allowing developers to deploy and users to interact with DApps with significantly lower transaction fees.

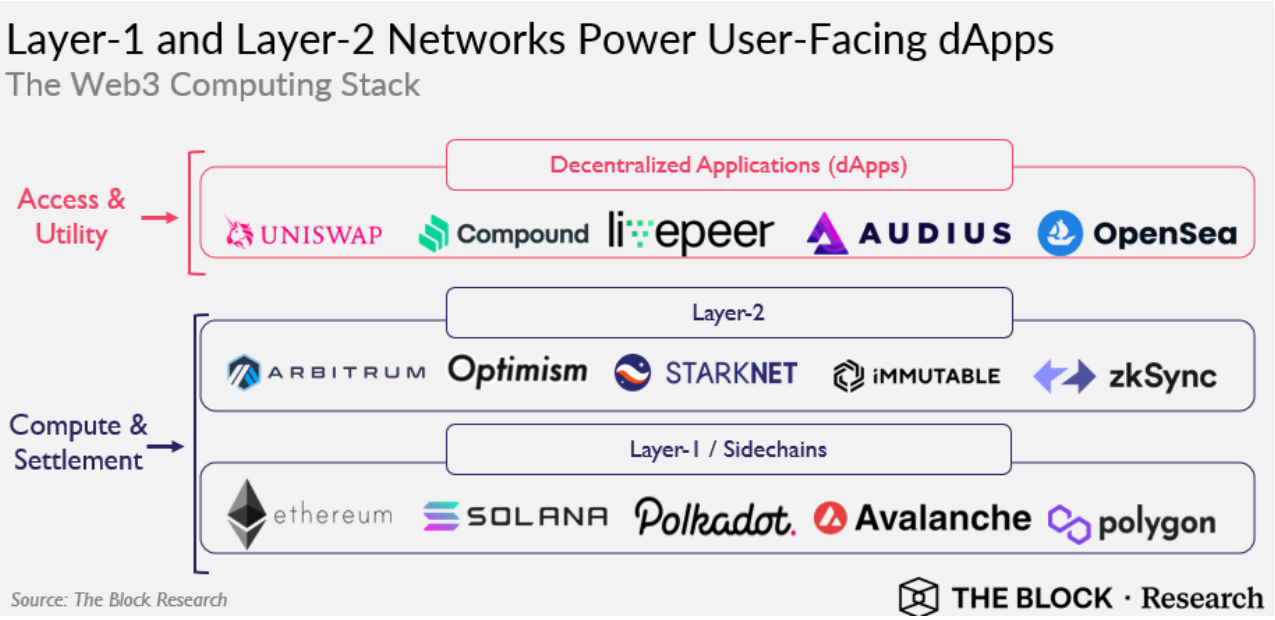
However, BNB chain achieves low transaction fees at the cost of decentralization. The BNB chain adopted a proof of staked authority (PoSA) consensus mechanism that has only 21 validators selected by a centralized authority (Binance) leaving it especially prone to censorship by third parties (e.g. a government). There are many trade-offs that can scale Bitcoin and Ethereum in short order if the community were willing to compromise decentralization and security (i.e. make blocks bigger and more frequent).

The difficulty arises from one basic question – how to achieve scaling without compromising network decentralization?

Leading Blockchain Scaling Solutions

There are intense ongoing efforts to develop technologies that leverage the decentralization/security guarantees of an L1 (e.g. Ethereum) while improving

transaction throughput and cost. Means of achieving the above fall under Layer-2 (L2) scaling solutions.



L2s are complementary blockchains that leverage the security framework of another L1. These L2 solutions have varying degrees of dependence on their related L1 for security. Sidechains are L2 implementations that require the least amount of interaction with an L1, possibly at the cost of security. Development activity so far has largely focused on the Ethereum chain presumably due to its degree of developer and end-user adoption.

L2s aim to improve scalability by allowing users to perform computation and transactions outside of the L1 chain that get batched, compressed and settled later on a L1 chain in some form. Under the hood, there are significant technological differences (e.g. state channels, Validium, Plasma, etc.) between competing L2s and sidechains currently available. These nuances are beyond the scope of this report – readers are encouraged to read The Block's Layer-2 Scaling Solutions report, which includes a framework for comparing the various implementations of scaling solutions currently being proposed.[16]

Here we shall provide an overview of the compute infrastructure requirements for the most widely adopted scaling technologies by usage – sidechains, optimistic and zero-knowledge (ZK) rollups as well as, state channels.

[16] Layer-2 Scaling Solutions: A Framework for Comparisons. The Block. 2022.

> "*The Ethereum ecosystem is likely to be all-in on rollups (plus some plasma and channels) as a scaling strategy for the near and midterm future.*" – Vitalik Buterin, Co-Founder of Ethereum (posted on ethereum-magicians.org October 2020)

Sidechains

Polygon's PoS sidechain with its native token MATIC has become one of the largest Ethereum scaling solutions in the asset class with $1.75b USD TVL in its ecosystem. Polygon periodically records a snapshot of its "state roots" (compressed summary of its blockchain state) to Ethereum L1 as a part of its security framework. Polygon's sidechain currently remains relatively centralized with 100 authorized validators on its network. Although addition of new validators is currently closed, any participant can run a witness node, similar to the L1 PoS chains discussed above.

Recommended system requirements for a Polygon validator are as follows: **CPU:** 16-core; **RAM:** 64GB; **Storage:** 3,000GB; **Bandwidth:** 1,000Mbps.

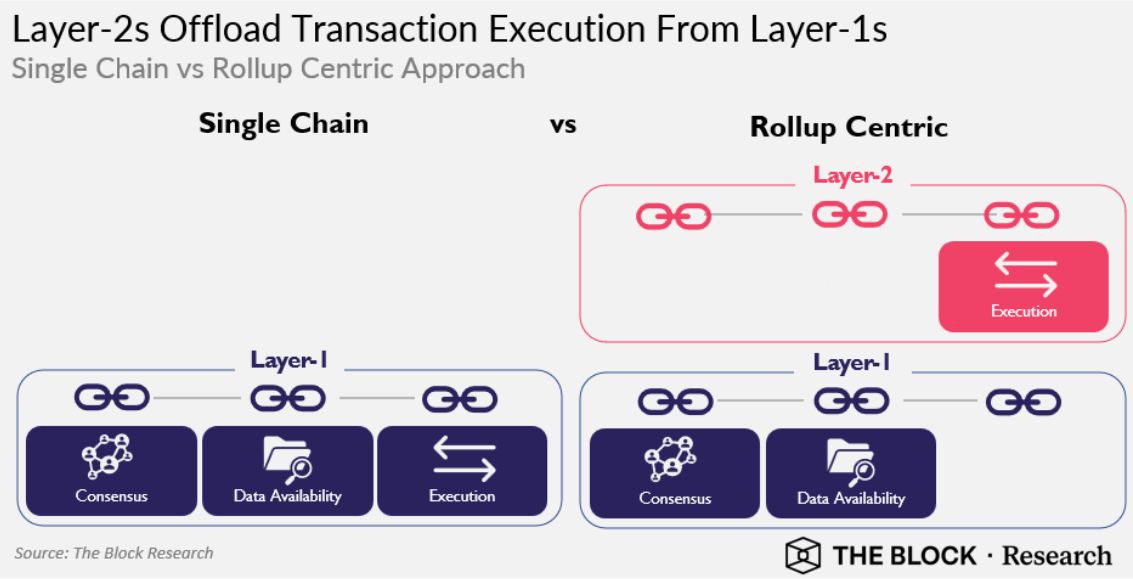
Examples of other sidechains include are Liquid Network and RootStock (RSK). Both Liquid and RSK interact with the Bitcoin network and have failed to gain significant adoption relative to Polygon.

Optimistic Rollups

Arbitrum and Optimism are both optimistic rollups for the Ethereum L1 that are the first and second largest scaling solutions by TVL, respectively. They rely on "sequencers" that act as nodes to receive and execute all transaction requests. Both the Arbitrum and the Optimism networks have effectively one sequencer running for the entire network operated by OP Labs PBC and Offchain Labs, respectively. Although this is the very definition of a centralization risk, sequencer decentralization for both groups are a part of their development roadmaps.

Sequencers wield significant potential influence in all rollup implementation as they store and execute user-submitted transactions locally and post the resulting state roots on the associated L1 chain.[17] Sequencers are incentivized to remain honest via a mechanism that involves a fidelity bond, a dispute period and a second constituent in the consensus mechanism known as "verifiers."

[17] Layer-2 Scaling Solutions: A Framework for Comparisons. The Block. 2022.



Verifiers check the validity of transactions posted on to the L1 chain by sequencers. The fidelity bond refers to capital that sequencers must first lock and risk forfeiting in case of fraud (like the minimum stake requirements in PoS L1 chains). The dispute period refers to the time window verifiers have to spot a fraudulent transaction from a sequencer. Part or all the sequencer's bond may be slashed and awarded to a verifier if they publish a fraud proof within the dispute period. Optimistic rollups assume that verifiers are always available to identify and submit a fraud proof in time.

Due to the nascent state of optimistic rollup implementations, the above security framework is unproven. It is unknown how fidelity bond size and dispute period duration will affect the balance between security (incentivize verifiers) and user-experience (movement of their funds between L1and L2). For more details on the function of sequencers and provers, readers are once again encouraged to refer to The Block's report dedicated to L2 scaling solutions.

From a hardware perspective, sequencers and verifiers run two nodes each, one as an Ethereum L1 full node, the second for the L2 chain of interest. The sequencers must run specialized software that's responsible for bundling and publishing transactions. Sequencers and verifiers are not expected to require highly specialized hardware or ASICs. Requirements are likely to be similar to that of an Ethereum L1 full node.

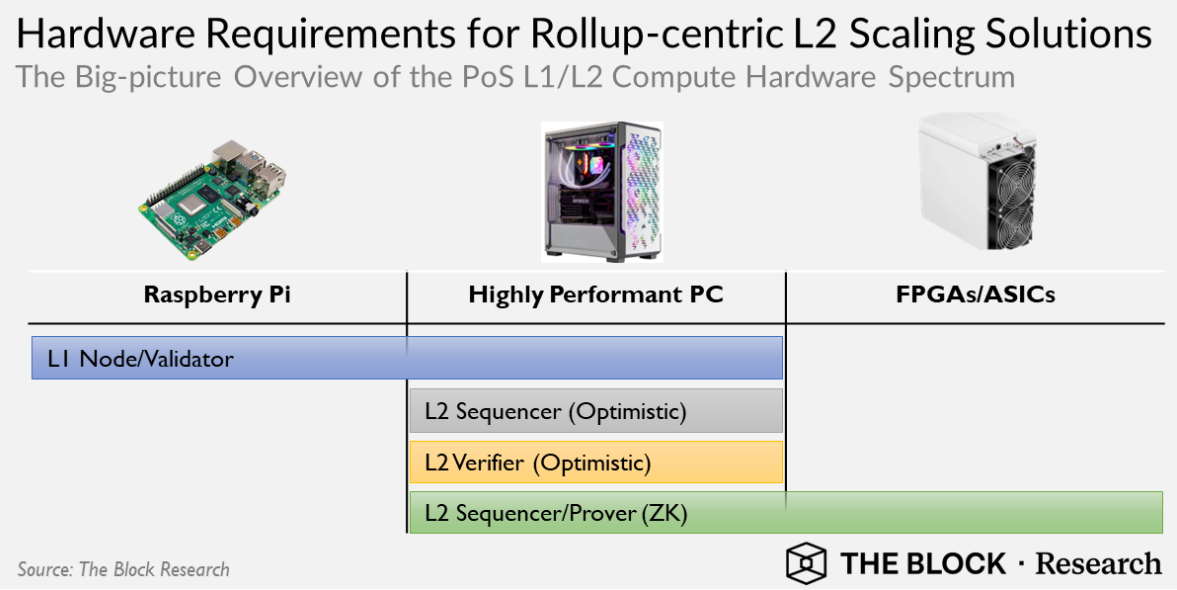
Zero-Knowledge (ZK) Rollups

ZK rollups (like optimistic rollups) also batch transactions but may enable even higher data compression when settling on an L1 (along with some other benefits). One notable added benefit is that ZK rollups eliminate the need for verifiers

entirely. Instead ZK rollups rely on validity proofs that offer mathematical certainty about the proposed state root. This also negates the need for any time constraints for exiting a ZK rollup and transferring funds back onto the associated L1.

For ETH, the most popular ZK rollup implementations include, Loopring, zkSync and Starknet. One prominent barrier for ZK-rollups is its incompatibility with EVM, inhibiting smooth migration of existing Ethereum DApps. However, there have been some significant recent developments on this front from Polygon, Matter Labs and Scroll. From an infrastructure standpoint, ZK rollups require a specific class of participants called "provers" that must generate the validity proofs required for the consensus mechanism.

ZK proofs have been around for quite a while now.[18] ZK-SNARK[19] and ZK-STARK[20] are the two dominant types of proofs that underpin ZK implementations today. Each come with various trade-offs that include compute needed to create and verify the proofs as well as, their (on/off-chain) storage requirements.



Generating ZK proofs is computationally intensive, requiring specialized hardware like field programmable gate arrays (FPGAs) and ASICs. Software to run a provers in the most prominent protocols using ZK proofs such as Loopring, zkSync and

[18] I. Goldwasser, et. al. The Knowledge Complexity of Interactive Proof Systems. SIAM J. Comput. 1989.

[19] N.I. Bitansky, et.al. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. 2012.

[20] I. Ben-Sasson, et.al. M. Scalable, transparent, and post-quantum secure computational integrity. 2018.

StarkNet is currently closed source. Thus, exact hardware requirements for running a verifier across these ZK rollups is not yet published.

Table 6	ZK-Rollup	Validium	Volition
ZK-SNARK	LOOPRING	zkSync 1.0	zkSync 2.0
ZK-STARK	IMMUTABLE X	STARKEx	STARKNET

Source: The Block Research & Chainlink

There are many ongoing experiments surrounding ZK that not only involve the type of validity proof (e.g. STARK vs. SNARK), but also the architecture of the L2 itself. Currently, rollups, validium and volitions are three different L2 ZK architectures. The primary difference between them being varying degrees of off-chain data storage to enhance scalability (possibly at the cost of security). Thus, each of the above implementations is expected to have different supporting compute infrastructure.

The sheer number of projects competing in the ZK-based blockchain space illustrates the level of excitement around ZK-based technologies as a means of scaling while preserving users' privacy. There are significant developments seemingly every other day in this sector. It is thus too early to tell which of the ZK validity proofs and architecture combination(s) the market may adopt.

We also cannot rule out the arrival of further technical advancements that have appreciable effects on end-user adoption and what the supporting hardware infrastructure requirements will look like.

> *"Eventually, a full ZK mining and proving industry will manifest, starting with hobbyists generating proofs in their CPUs, then GPUs, then FPGAs. In contrast to Bitcoin, we anticipate that ASICs could take a long time to see adoption, if ever."* – Georgios Konstantopoulos, CTO at Paradigm ("Hardware Acceleration for Zero Knowledge Proofs", April 2022).

State/Payment Channels

State or, payment channels involve two or more parties locking in an initial amount of value in a contract where subsequent value transfers between said parties are recorded off-chain until the final balances are recorded on-chain once the channel(s) are closed. Bitcoin's lightning network (LN) is the most prominent scaling solution that uses a channel-based architecture. Other state channel-based technologies such as, Raiden Network for Ethereum have been unable to generate a significant user adoption.

Bitcoin LN usability depends on total available liquidity in the network and channel interconnectivity (to facilitate efficient routing). Despite being tested with Litecoin network in 2017, LN is still nascent and usage statistics are difficult to uncover by design. Regardless, there are signs of organic growth in LN capacity over the past two years despite a lack of any token(s) or additional subsidies. El Salvador's adoption of BTC as legal tender and deployment of Chivo (an El Salvadorian state-sponsored custodial LN wallet application) likely aided the recent growth of Bitcoin LN liquidity.

From an infrastructure point of view, any Bitcoin consensus node (see hardware specifications) with the appropriate software (e.g. umbrel) can be LN-enabled where end users can choose to open channels and add liquidity as they see fit. In principle, LN is purported to have the potential for instant transactions with low fees and high throughput.

Section 5: Conclusion

The mass-adoption of blockchains is related to the utility of applications capable of driving such growth. There is no guarantee such applications (possible only via blockchains) with universal mass-market appeal will in fact, exist. However, there have been numerous recent drivers of strong adoption such as, DeFi, non-fungible tokens (NFTs) and play-and-earn (P&E) games. Web3 is another contender as a "killer application" for blockchains. These new potential use cases have caused a boom in interest for blockchain technologies that promise low cost and high throughput transactions.

Infrastructure for scalable blockchain networks depends on the specific role(s) being filled within the consensus mechanism. PoW and PoS are the most prevalent, each with their own unique hardware and operator ecosystems.

The layman's image of PoW is quite negative – a power-hungry waste that pollutes the environment. There are significant efforts dedicated towards decentralization and overall political/regulatory acceptance of PoW. The effectiveness of these remains to be seen. The following are notable factors that will help determine the degree of future investment in the field of PoW infrastructure:

1) Improve decentralization by promoting "open-source" mining hardware with the goal of reducing cost of entry from new chip manufacturers, worldwide.[21] Such designs should also make small-scale mining more feasible. Devices that have multiple applications, such as a PoW miner that can be used as a space heater that may appeal to a larger cross-section of users.

2) Entry of more ASIC chip manufacturers based in stable democracies (e.g. Intel).

3) Public service campaigns where on one end, some groups focus on the environmental dangers of PoW, like the one initiated by an executive of Ripple Labs Inc. (developer of the PoS XRP-ledger) and Greenpeace. On the other end are PoW mining entities branding themselves as energy scavengers seeking out stranded/wasted energy sources. Here co-located PoW facilities may incentivize new renewable energy projects as miners act as a novel load balancer for real-time response to power grid demand. There is one preliminary model that disputes this last claim.[22]

4) Lobbying for regulatory clarity towards PoW at the federal, state and local levels.

[21] Jack Dorsey (CEO, Block) via Twitter

[22] I. Menati, et. al. Modeling and Analysis of Utilizing Cryptocurrency Mining for Demand Flexibility in Electric Energy Systems: A Synthetic Texas Grid Case Study. arXiv. 2022.

PoS consensus mechanisms arguably address some of the disadvantages found in PoW blockchains given their low energy usage and potential for scalability. There is lively debate about the merits of PoS over PoW. The arguments often abstracts into economics, game-theory and resilience against theoretical attack vectors.

Putting philosophy aside, the market clearly favors the PoS landscape (in terms of financial and intellectual capital), as the most promising foundation for building scalable blockchains. There is intense activity in developing L2 scaling solutions, notable among them being implementations of ZK proofs. The following are a few critical factors that will determine future activity in the PoS infrastructure landscape:

1) Continued demand for DApps that follow the "Web3" narrative where current efforts are in restructuring platforms dedicated to social media and publishing rights of original works online (e.g. video, audio and text)

2) Development of novel PoS scaling solutions and the rapidly evolving hardware requirement landscape for each. Current efforts are focused on rollups, specifically those that implement ZK proofs

3) Centralization of PoS node/validator infrastructure is a major concern. However, innovations surrounding ZK proofs may aid (to some degree) in decoupling blockchain decentralization from the number of independent node operators and their geographical distribution

4) Lack of regulatory clarity and designation of individual PoS networks as a "security", rather than a "commodity" is likely to have a significant role in determining both research activity and related infrastructure investments

….

Disclosures

This report is commissioned by W3bcloud. The content of this report contains views and opinions expressed by The Block's analysts which are solely their own opinions, and do not necessarily reflect the opinions of The Block or the organization that commissioned the report.

The Block's analysts may have taken positions in the assets discussed in this report and this statement is to disclose any perceived conflict of interest. Please refer to The Block's Financial Disclosures page for author holdings. This report is for informational purposes only and should not be relied upon as a basis for investment decisions, nor is it offered or intended to be used as legal, tax, investment, financial or other advice. You should conduct your own research and consult independent counsel on the matters discussed within this report. Past performance of any asset is not indicative of future results.