BINANCE RESEARCH

Ethereum:

Beyond The Merge

Moulik Nagesh

Table of Contents

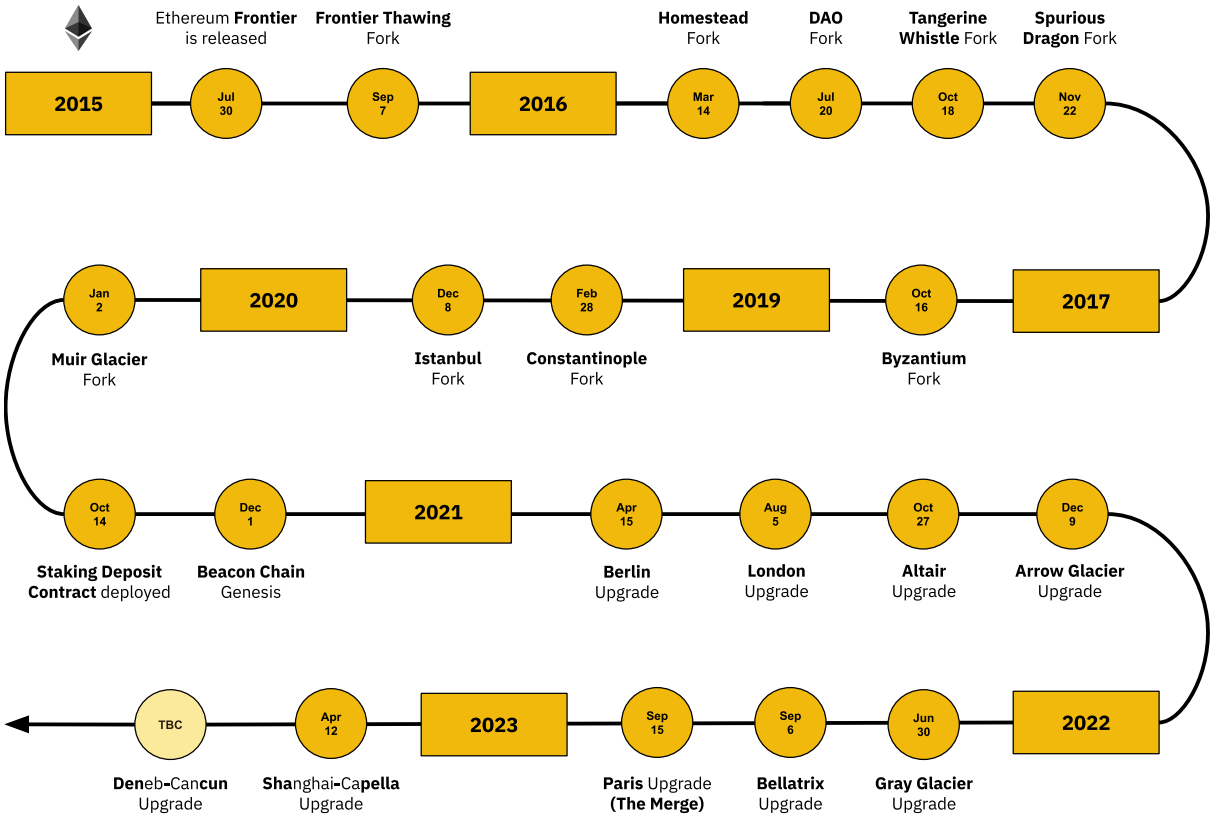
1 Key Takeaways

- While Ethereum's transition to Proof-of-Stake was a significant milestone, it remains just one of many important upgrades to come. A key focus of Ethereum's roadmap is to scale computational throughput without compromising on decentralized validation.
- Layer-2s are seen as the most expedient route to scalability, aligning with the roll-up centric vision. Notably, Layer-2s continue to gain traction, as mainnet data publishing fees reach record heights in 2023, increasing by 257.7% YTD.
- Danksharding is how Ethereum becomes a truly scalable, unified settlement and Data Availability layer. In particular, Proto-Danksharding (EIP-4844) serves as a precursor to Danksharding and introduces blob-carrying transactions, a dedicated storage space for Data Availability.
- Blobs are based on a multi-dimensional EIP-1559 fee market where there are two resources, gas and blobs, with separate floating gas prices and limits. The use of blobs unlocks several material benefits for Layer-2s, offering a more cost-effective solution than the current calldata space rollups utilize.
- The path to Danksharding also includes key components such as Data Availability Sampling, KZG Commitments, and Proposer-builder Separation. All paths lead to the endgame of centralized block production with decentralized trustless block validation.
- Verkle trees are a critical step on the path to statelessness. These data structures enable nodes to validate blocks without having to store the entire state database.
- High disk space requirements serve as a barrier to universal node access, undermining decentralization. History expiry (EIP-4444) and state expiry are designed to minimize historical data storage burden and eliminate technical debt.
- Other notable upgrades that refine Ethereum's architecture include Single Slot Finality, Distributed Validator Technology, Secret Leader Election and recently, Account Abstraction.

2 Setting The Scene

Launched in 2015, Ethereum revolutionized the blockchain industry by **creating a global settlement layer**. Despite inspiring the creation of many well-funded, competing smart contract blockchains, Ethereum remains a leader in the space. It boasts the most extensive developer community and a diverse range of decentralized applications ("dapps"). **Currently, the platform holds over US$21B[(1)] in total value locked ("TVL") and ranks second only to Bitcoin, with a market cap just shy of US$200B[(2)].** Figure 1 below captures several notable milestones of Ethereum in recent years, each contributing significantly to its growth while improving scalability, security, and decentralization. **With Ethereum continuing to gain influence in a fundamentally important Layer-1 ("L1") ecosystem, it isn't surprising why the crypto community is increasingly curious about the roadmap and future of the largest L1**. After all, any alterations to the largest L1 are likely to have a profound impact and initiate ripple effects across broader crypto markets.

Figure 1: Timeline of major milestones, forks and updates to the Ethereum blockchain



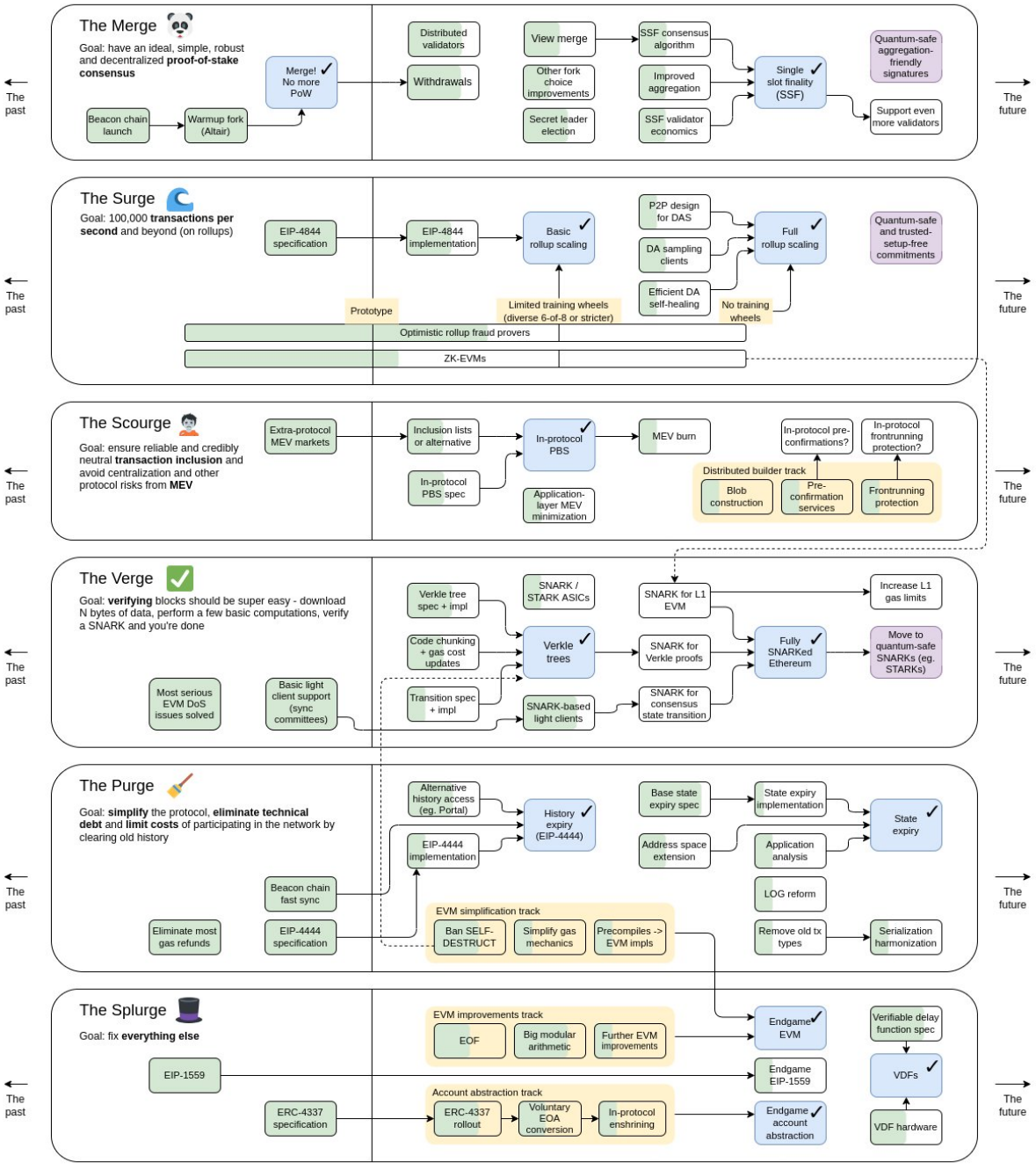
Source: ethereum.org, Binance Research

Today, Ethereum's roadmap is well-documented and openly shared, enhancing transparency and providing a future-oriented framework for ecosystem participants. The roadmap is also structured in alignment with its co-founder Vitalik Buterin's vision, which delineates the path forward through six succinct phases: The Merge, The Surge, The

Scourge, The Verge, The Purge, and The Splurge[3]. Each of these phases is projected to have a transformative effect on the broader blockchain landscape.

The Merge was undoubtedly a watershed moment in blockchain history. However, Ethereum's shift from a Proof-of-Work ("PoW") to a Proof-of-Stake ("PoS") consensus mechanism is **merely one of many important strategic upgrades.** A key focus of the development roadmap is to improve scalability, specifically Layer-2 ("L2") rollups, to fulfill Ethereum's overarching objective: **scaling computational throughput without compromising on decentralized validation**.

Figure 2: Ethereum's Roadmap is categorized into distinct and non-sequential phases



Source: ethereum.org, Binance Research

Importantly, these upgrades are being developed in parallel, not sequentially, with each phase having its own specific goal and thematic focus. According to Vitalik Buterin, **after the culmination of these upgrades, Ethereum can be considered fully developed** and capable of processing an impressive 100K transactions per second ("TPS")[4].

Figure 3: Each phase in Ethereum's roadmap serves a function that centers around a particular theme

	Phase	Description
🐼	The Merge	Transition of Ethereum's consensus mechanism from PoW to PoS.
🌊	The Surge	Improvements related to scalability starting with the introduction of Proto-Danksharding, which ensures sufficient Data Availability for rollup networks.
🧛	The Scrouge	Upgrades focused on censorship resistance, decentralization, and protocol risks stemming from MEV.
✅	The Verge	Introduction of statelessness through the transition from Merkle Trees to Verkle Trees, making it easier to verify blocks.
🧹	The Purge	Simplification of the protocol by reducing historical data storage and eliminating technical debt.
🎩	The Splurge	Upgrades that don't fit into the aforementioned categories, including Account Abstraction, Verifiable Delay Functions, and EVM improvements.

Source: ethereum.org, Binance Research

It is worth noting that although Ethereum hasn't formally adopted this category-based terminology, opting instead for a more user-centric approach, the vision remains the same as per Vitalik Buterin's classification. In the sections that follow, we'll explore the key initiatives within each of these roadmap categories in greater detail. To begin, we first introduce Ethereum's transition to PoS, examining its implications and expected outcomes. We will then move on to what lies beyond The Merge, exploring some of the key subsequent phases outlined in the roadmap.

3 The Merge

Similar to Bitcoin, Ethereum originally ran on a PoW consensus mechanism, enabling a distributed network of anonymous participants to reach an agreement on transaction validation and blockchain entries. **Ethereum, however, had always envisioned a shift to a PoS mechanism**. In this system, block producers - referred to as validators under PoS as opposed to miners under PoW - operate full nodes, stake the native token of the protocol, and propose or verify blocks based on a set selection process. **September 15, 2022 marked a historic milestone for Ethereum with the implementation of The Merge**[5]. Vitalik Buterin himself has commented on the importance of this event, going as far as stating that **The Merge brings the network's development to approximately 55% completion**[6].

In a nutshell, **The Merge signifies Ethereum's conversion to a PoS system**, unfolding through two key upgrades: Bellatrix and Paris, which incorporated the Ethereum Improvement Proposals ("EIPs") of EIP-3675 and EIP-4399. **The Merge involved the joining of Ethereum's original execution layer ("EL") with its newly established PoS consensus layer ("CL"), known as the Beacon Chain**.

The Merge introduced some key modifications that network participants need to be aware of. **One significant change was the requirement for full nodes to operate both an EL and a CL client**. Prior to The Merge, a single EL client could manage all tasks related to transactions and blocks. After The Merge, EL and CL clients each maintain their own peer-to-peer networks. **While the CL client handles block gossip, attestations, and slashings, the EL client continues to manage transaction execution and state maintenance**. These two clients interact via the Engine API, jointly constituting a complete post-Merge Ethereum node[7].

Ultimately, The Merge served as a monumental step toward fulfilling Ethereum's vision for a highly decentralized, scalable, secure, and sustainable network. The following are some of the key benefits unlocked by the upgrade[8]:

- **Reduced energy consumption:** By eliminating the need for energy-intensive mining, The Merge **decreased Ethereum's energy consumption, in some estimates, by up to 99.95%**. This marked one of the most significant **decarbonization efforts in history, reducing worldwide electricity consumption by 0.2%**[9]**.** What's more, in an era where ESG concerns are rising, Ethereum's transition to PoS is certainly **attractive for ESG-conscious institutions looking to gain exposure** in the digital asset market.

- **Lower barriers to entry:** **The need for specialized hardware has been lowered,** making it **easier for users to participate as validators** and contribute to network security from their homes.

- **Lower net issuance of ETH:** The Merge brought substantial changes to Ethereum's monetary policy. It significantly **curtailed the issuance of new ETH tokens by eliminating miner rewards, which constituted a large portion of daily ETH issuance**. Post-Merge, **daily ETH issuance plummeted by approximately 88.7%, resulting in a gross annualized issuance rate of about 0.52% of the total supply**[10]. In some instances, **net issuance could even become deflationary** due to gas fees being burned under EIP-1559.

- **Reduced block times:** **The average time to create a block has been reduced from 13.3 seconds to a consistent 12 seconds**, assuming no empty slots are present.

- **Improved crypto-economic security:** The transition to PoS **increases the financial cost of launching attacks against the network** and **reduces the risk of Sybil attacks**.

- **Stronger finality:** The network now offers **more robust finality assurances**, underpinned by slashing and other validator penalties.

- **Introduction of yield:** The introduction of **meaningful staking yields**; Validators also **accrue transaction priority fees** and have additional opportunities to **capture Miner Extractable Value ("MEV")**.

Even though we are past The Merge itself, several on-going developments on the roadmap remain important to consider. For instance, the network has since rolled out additional upgrades, **notably the Capella and the concurrent Shanghai upgrades**. **One important feature arising from these subsequent upgrades was in EIP-4895, which formally enabled withdrawals of staked Ethereum ("ETH")**. Although these particular upgrades fall outside the purview of this report, for more details, we direct readers to our earlier report, Ethereum's Shanghai Upgrade: By The Charts.

Distributed Validator Technology

While Distributed Validator Technology ("DVT") is not an in-protocol development, its introduction marks another significant stride for the Ethereum network[11]. **Traditionally, running an Ethereum node has been a technically demanding solo venture that mandates a 32 ETH stake**. While platforms like Lido offer alternative staking options, these come at the cost of decentralization. **DVT aims to tackle this by enhancing the performance and risk profile of validators, while also fostering greater decentralization**.

Instead of individually staking 32 ETH, **DVT allows for a collaborative approach where multiple parties can pool varying amounts of ETH to jointly operate a node**. An important component of DVT is **multi-party computation ("MPC"), a system that lets participants share a single private key, which is much like a multi-signature wallet ("multisig")**, to collectively act as a distributed validator. **DVT not only enhances the resilience of node validation** - by allowing validators to substitute for each other in case of hardware failure - **but also strengthens security**. The shared private keys under DVT architecture make it **more challenging for attackers to exploit the system**.

Although DVT brings improvements to the network, it also has its own set of challenges that need attention.

- **Additional vulnerabilities:** Incorporating a DVT node **introduces an additional component that may be susceptible to faults or vulnerabilities**, adding another layer of risk.
- **Increased costs:** By distributing the validator role across several parties, DVT **requires more nodes for its operation, potentially leading to higher operating costs.**
- **Higher latency:** The **use of a consensus protocol among the multiple nodes** in DVT could **introduce higher latency** into the system.

By lowering the financial entry barrier, **DVT democratizes access to Ethereum's validator landscape**. **This is particularly significant for individuals and small DAOs, given that it enables them to participate without requiring huge sums of capital**. In doing so, DVT has the potential to dilute the concentrated staking power currently seen in platforms like Lido and centralized exchanges ("CEXes"). **Innovative projects such as Obol and ssv.network have emerged to leverage the advantages offered by DVT**. Moving forward, we expect DVT to **proliferate use cases across solo staking, staking pools, and staking-as-a-service ("SaaS")** and consequently **impact the market composition of Ethereum's staking industry**.

Figure 4: Though nascent, several DVT-based protocols are progressing toward launch this year

	Obol	ssv.network
Client Software	Middleware clients run in parallel with a standard validator client.	Custom validator client built with the go-eth2 client library.
Token	-	SSV
Stage	**Alpha release**; Integrate Obol into staking applications.	**Limited launch**; Introduce a complete set of verified operators.

Source: Project Documentations, Binance Research

Secret Leader Election

In current PoS consensus models, **the identity of block proposers for each of the 32 slots at the beginning of every epoch is publicly known**, making it possible to pinpoint their network locations. This leaves the door open for **bad actors to launch Denial-of-Service ("DOS") attacks** on the known block proposers in an attempt to halt block production. Such a tactic would enable the attacker to extract rewards that instead should have been distributed across multiple slots. **Not only does this pose security risks but it is also likely to disproportionately affect smaller, less secure participants, leading to centralization concerns**.

While there are various approaches to counteract this, including DVT and secret non-single leader election ("SnSLE"), the most promising solution seems to be secret single leader election ("SSLE")[12]. **Put simply, SSLE aims to address this vulnerability by keeping the identity of each slot's proposer hidden until they actually propose a block**. Although **the exact details of its implementation are still under research**, the prevailing discussion involves using various validator shuffling techniques to maintain anonymity until a block is officially proposed.

Single Slot Finality

Single Slot Finality ("SSF") represents another substantial upgrade to the Ethereum network. **SSF aims to drastically reduce Ethereum's block finality time to just one slot, down from the current 64 to 95 slots (roughly 15 minutes)**[13]. Today, achieving finality -

ensuring a block is permanently part of the blockchain - **results in long wait times** for transaction confirmations, which has proven to be **inefficient for dapps that rely on high transaction throughput**. This time lag also exposes the network to short reorgs, potentially creating vulnerabilities around block censorship and MEV extraction. While speeding up the finality process would address these issues, it also places greater computational demands on the validating nodes, impacting network participation. **Therefore, there is a balance to be struck among computational overhead, level of decentralization, and the speed at which finality is reached**.

To make SSF a reality, a **significant overhaul of the existing PoS system** would be required first. In particular, **three critical challenges must be resolved** before SSF can be implemented: **the development of a precise consensus algorithm, the optimization of signature aggregation processes, and determining the best approach to validator participation and economics**. For an in-depth look into these aspects, Vitalik Buterin's blog post offers substantial detail on this topic. As of now, **SSF remains in the research phase and isn't expected to be rolled out for several years**, likely after other major upgrades such as Danksharding and Verkle trees.

As we look back, while The Merge has been a transformative shift in Ethereum's architectural landscape, it is just one element of a broader, more comprehensive roadmap. Subsequent phases of Ethereum's development are closely linked to the outcomes of The Merge. For instance, the transition to PoS lays the groundwork for critical enhancements like Danksharding by facilitating the separation of proposers and builders, which is key to increasing network speed in later upgrades. We will now turn our attention to the other parts of Ethereum's multifaceted roadmap.

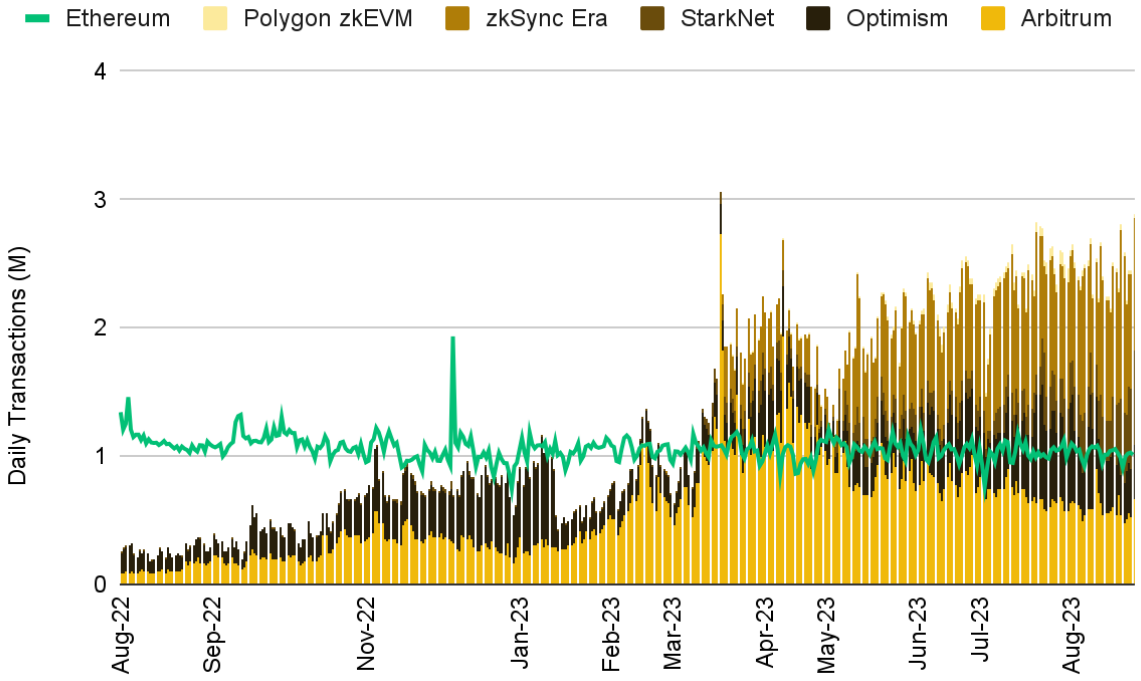
4 The Surge

The Surge targets to solve the age-old problem that has plagued blockchain technology since its inception, that is, the issue of scalability. The question often arises: if traditional financial systems like Visa can handle thousands of TPS, why can't Ethereum achieve similar performance? **The Surge is designed to address this gap by focusing on development paths that substantially boost Ethereum's transaction throughput**. In particular, **Danksharding** **("DS") is how Ethereum becomes a truly scalable blockchain**, but achieving this requires a series of protocol upgrades. Moving forward, we will explore some of these important upgrades.

One of the key rationales for these set of upgrades came in 2020 with the arrival of the rollup-centric roadmap. As the term rollup-centric infers, **the role of rollups in the Ethereum ecosystem has expanded its importance ever since**. In this approach, rollups handle the computational heavy lifting of transaction execution, while the network is

repurposed mainly for ensuring Data Availability ("DA"). **This shift was motivated by the maturity of L2s, which have demonstrated computational advantages in real-world applications and are therefore seen as the most expedient route to scalability**. Supporting this claim, L2s have continued to experience significant growth, with their daily transaction volume even surpassing Ethereum's own in 2023.

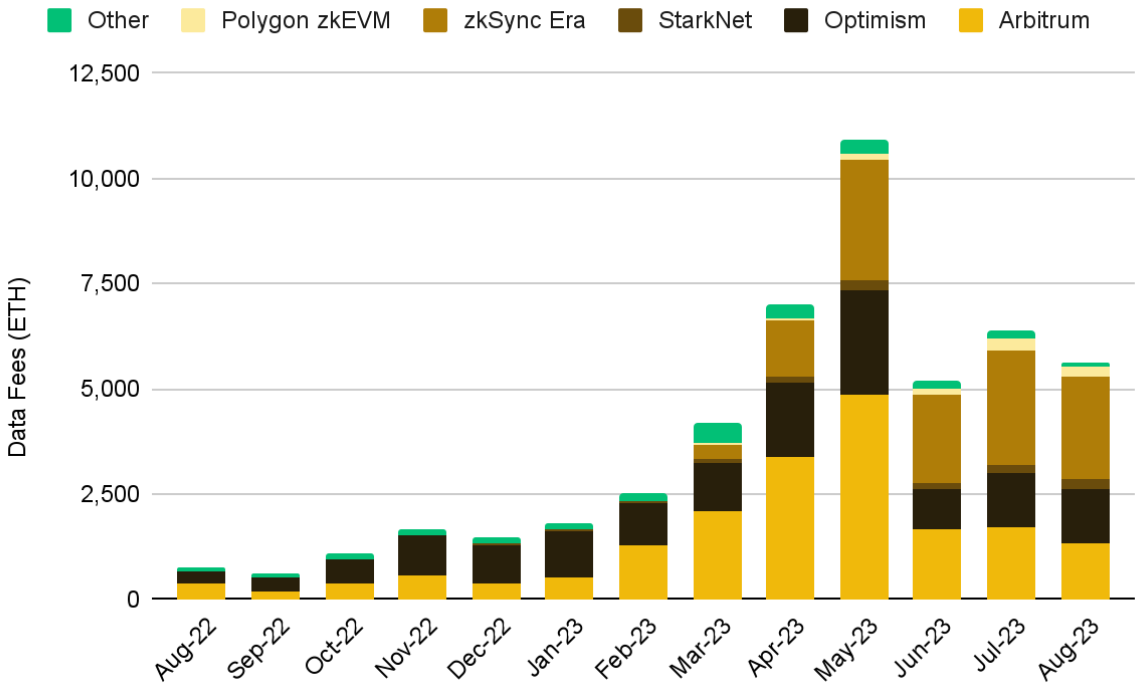
Figure 5: With an over 600% YoY increase in daily transactions, L2s have shown that they are a mainstay in the ecosystem



Source: Artemis, Binance Research, as of August 31, 2023

The shift to a rollup-centric architecture reflects a strategic pivot for Ethereum by **deemphasizing scaling at the base layer** and **repositioning its mainnet to specialize in consensus, settlement, and DA**. This creates a **fertile ground for L2s to engage in free-market competition for transaction execution**. Analyzing this in the context of today's markets, **the approach appears particularly prescient given the rising prominence of L2 rollup technologies in the current landscape**. In fact, L2s have seen a surge in adoption this year, reaching new heights in May, with data publishing fees exceeding 10,500 ETH.

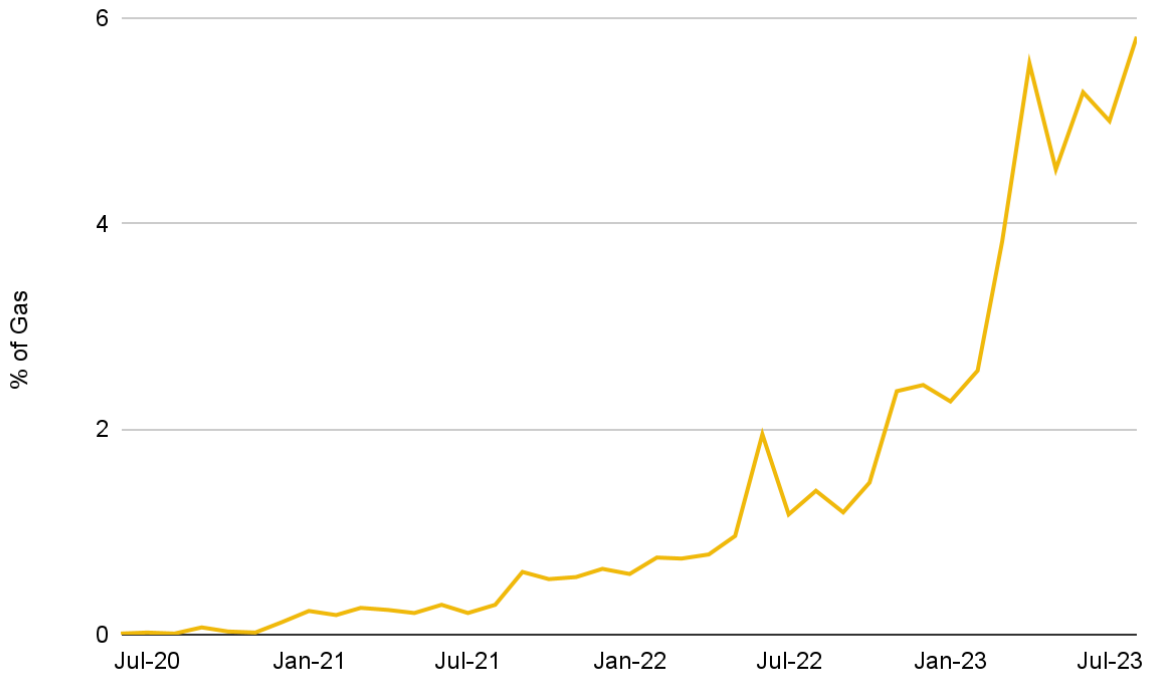
Figure 6: Ethereum L2 mainnet data publishing fees reached record heights in 2023, increasing by over 257.7% YTD



Source: Dune Analytics (@niftytable), The Block Data, Binance Research, as of August 31, 2023

Similarly, **an analysis of gas expenditure for posting L2 data to the Ethereum mainnet reveals an upward trend**. Indeed, much of this growth is **attributed to the ongoing innovations in optimistic rollups and to the launches of zero-knowledge ("ZK") rollups** earlier this year. **L2s have certainly carved out their own market segment** and today are **viable ecosystems for a diverse range of dapps to seamlessly deploy, operate and thrive in**. Coupled with emerging narratives around Layer-3s and Superchains, **the momentum in this sector is likely to persist**. This sets the stage for the eagerly awaited scalability-based upgrades, which are projected to substantially elevate the usability of L2 solutions.

Figure 7: Ethereum L2 percentage of gas spent on L1 Data fees has seen accelerated growth this year, indicating the rising influence of L2s



Source: The Block Data, Binance Research, as of August 31, 2023

Although optimistic and ZK rollups have provided some relief to the scalability challenges, it is undeniably a makeshift solution. **Existing L2s like Arbitrum and Optimism still incur sub-optimal costs, not due to any shortcomings in their own design, but because of the limitations of the L1 architecture upon which they are built**. Even the fastest rollups find themselves bottlenecked at times by the need of submitting extensive data to build consensus on the L1, which is not designed to store this data in an efficient manner.

Figure 8: Snapshot comparison of L2s and Ethereum in the current market

Logo	Name	Rollup type	TPS	Cost to send ETH (US$)	Cost to swap tokens (US$)
	Ethereum	Base Layer	12.02	0.52	2.58
	Arbitrum One	Optimistic	5.00	0.03	0.11
	OP Mainnet	Optimistic	3.23	0.02	0.04

	Polygon zkEVM	Zero Knowledge	0.38	0.02	0.25
	StarkNet	Zero Knowledge	9.01	0.07	0.21
	zkSync Era	Zero Knowledge	13.11	0.06	0.16

Source: l2beat.com, l2fees.info, Binance Research, as of September 3, 2023

The DA issue stems from the current way rollups interact with Ethereum's mainnet; they post their state roots back to Ethereum using calldata for storage, which is neither optimized for rollups nor scalable to meet their needs for DA. This constraint not only **elevates the transaction costs on L2** but also **imposes a considerable load on nodes** that must download this data. Astonishingly, over 90% of transaction fees on rollups are allocated just for these data posting costs[14]. This takes us to EIP-4844, which has been proposed to tackle these challenges and serves as the starting point on the road to DS. While transacting directly on Ethereum will continue to be an option, **the goal is to enable cheaper and faster L2s, expanding Ethereum's capability and versatility**.

Proto-Danksharding (EIP-4844)

The upcoming Deneb-Cancun-combined Dencun hard fork is one of the next highly-anticipated upgrades for Ethereum, **expected to occur by the end of this year** (it's worth noting that there is no confirmed timeline or schedule as of yet, and these details may be subject to change). Although Dencun encompasses a range of updates, the **spotlight falls on EIP-4844, more commonly referred to as Proto-Danksharding ("PDS")**. **PDS serves as a preliminary step toward Ethereum's grand vision of DS**, a long-term solution for scaling. **Instituting full DS presents complexities and challenges**; therefore, the Ethereum community has rallied behind the idea of an intermediate step - PDS - that would offer a subset of DS features, facilitating more immediate scaling gains[15].

Figure 9: A set of proposed EIPs for the upcoming Dencun Hard Fork

Upgrade	Description
EIP-1153	Introduction of transient storage; Add opcodes for manipulating state that behaves identically to storage but is discarded after every transaction.
EIP-4788	Include beacon block roots in the EVM and introduce stateful precompile to improve usability.

EIP-4844	**Proto-Danksharding.**
EIP-5656	An efficient EVM instruction for copying memory areas.
EIP-6780	Changes to the SELFDESTRUCT opcode; current behavior is preserved only when called in the same transaction as creation.
EIP-7044	Lock validator voluntary exit signatures for perpetuity, improving staking UX.
EIP-7045	Expand attestation slot inclusion range from a rolling window of 1-2 epochs.

Please Note: This table does not comprise an exhaustive list of EIPs.
Source: eips.ethereum.org, Binance Research

EIP-4844 is an instrumental step toward fulfilling Ethereum's scaling roadmap, with a specific focus on **minimizing the operational expenses associated with rollups**. One of the key attributes of EIP-4844 is its capacity to **significantly lower DA costs, which currently constitute a major portion of the L2 overhead**. The proposal aims to accomplish this by **creating a specialized storage space exclusively dedicated to DA, and entirely separate from the main block space**. This is realized through **the introduction of blob-carrying transactions, a novel type of transaction that is temporarily retained by beacon chain nodes**. Put simply, these are data chunks appended to transactions, which not only significantly reduce the DA costs but also pave the way for substantially expanding data storage capacity.

The introduction of blobs promises a seismic shift in how data is stored on the Ethereum network. **Blobs are exceptionally large, averaging around 125KB each, which is significantly larger than a typical Ethereum block**[16]. The use of blobs offers a **more cost-effective solution than the current calldata space** that rollups utilize to post their data on the Ethereum mainnet. Once EIP-4844 comes to fruition, **the calldata mechanism is expected to be largely replaced by these blobs**. Fundamentally, the data space in these blobs is expected to be **used by L2 rollups to better maximize both cost and performance** and hence **accommodate a massive influx of transactions on Ethereum at cheaper rates**. Notably, with the introduction of a tailored data layer, EIP-4844 also serves as an important testing ground for the modular approach to blockchain scaling.

In line with the parameters in EIP-4844, the **pricing for these blobs (in the form of gas fees) will operate under a separate market mechanism** based on the supply and demand of blob storage[17]. This **fee market for blobs will be entirely independent of the demand for block space**. As a result, Ethereum will function with a two-dimensional fee market, consisting of the following:

- **The first dimension** will operate under EIP-1559, which sets the fee market for regular transactions.

- **The second dimension** will introduce a new blob fee market, where the cost of storage is exclusively influenced by the supply and demand for blobs.

This dual fee market structure promises greater flexibility and efficiency in the allocation of network resources, making Ethereum more scalable and cost-effective. What's more, **the introduction of a segregated fee market should yield efficiencies as it separates the economics of DA and transaction execution, allowing each component to be priced according to its specific supply and demand dynamics**. As with any early-stage deployment, the utilization of blobs is anticipated to be relatively modest, even in the context of Ethereum's high network activity. Consequently, the cost associated with blob storage is expected to be several magnitudes lower.

Figure 10: PDS introduces a tailored data layer where blobs get their own distinct fee market with separate floating gas prices and limits

	Target per block	Max per block	Base Fee
Gas	15 million	30 million	Variable
Blob	8	16	Variable

Source: notes.ethereum.org, Binance Research

While PDS is heralded as a significant leap toward Ethereum's scaling roadmap, its nomenclature might be slightly misleading. For instance, **every validator is still required to download all data blobs, verifying their availability**. Thus, the system does not directly implement data sharding in the way some might expect. However, **PDS does introduce a level of forward compatibility, paving the way for a smoother transition to full DS once the architecture for it is finalized**. Nevertheless, the **upgrade represents a critical milestone** in Ethereum's development, **aiming to substantially expand the network's capacity, address pressing usability concerns, and further align Ethereum with its rollup-centric vision**.

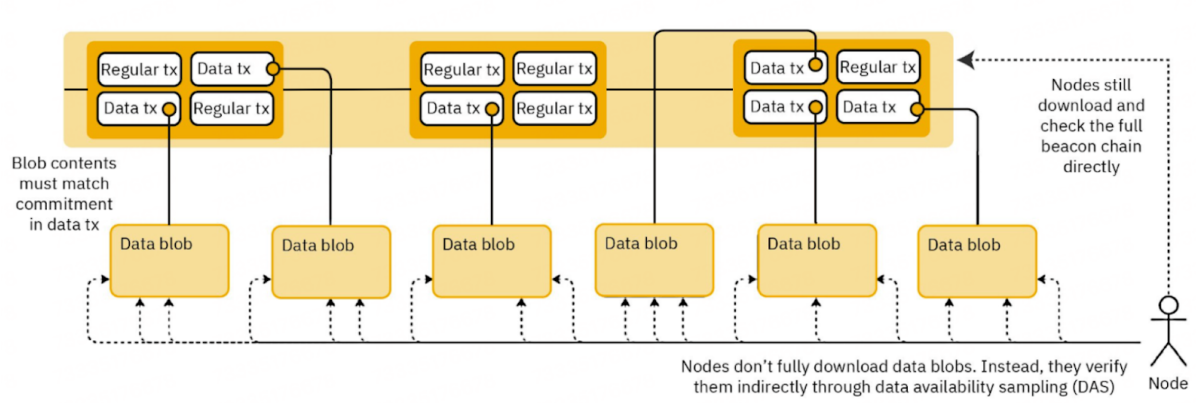
Data Availability Sampling

While the implementation details of full DS are not set in stone, the general idea is simple to understand: **DS distributes the job of checking DA amongst validators**. To do so, DS uses a process known as Data Availability Sampling ("DAS"). **By employing erasure coding techniques, notably Reed-Solomon Codes**, **DAS extends shard data in a way that ensures the availability of the complete dataset if a certain threshold of samples are present**. The technique mathematically guarantees DA as long as more than 50% of the

samples are accessible[18]. **This allows node validators, including light clients, to validate the availability of data without having to download the entire data blob.**

The role of DAS becomes even more critical when considering some of the **challenges** that may arise with the rollout of DS. As Ethereum's adoption continues to grow, so will the number of rollups and the data that these rollups need to process, resulting in a growing data burden on network nodes. **Without effective solutions like DAS,** only those nodes with extensive resources would be able to cope with the increasing data requirements. **By simplifying the validation process and reducing overall data storage needs, DAS not only ensures DA but also fosters decentralization**. **It mitigates centralization risks by reducing the computational burden on individual nodes**, hence encouraging more participants to join and maintain the network.

Figure 11: Node validators are able to verify blocks very efficiently through DAS



Source: eip4844.com, Binance Research

Moreover, it is worthwhile to highlight that the DS roadmap features an ambitious scaling strategy, aiming to eventually expand the target blob storage to 16MB[19]. **While this enlargement in block size poses no challenge for nodes that validate the network - thanks to the efficiency of DAS - it does create a bottleneck for block builders who are responsible for encoding the blob and distributing the data**. As a result, this development does bring its own set of concerns that are important to consider.

In particular, **the increased requirements for block builders could make it harder for a diverse set of participants to partake in the network**, thereby skewing it toward a more centralized framework. **To counteract this issue, an important upgrade known as Proposer-builder Separation would need to be completed first**. This separation aims to balance the computational load between different network participants, thereby preserving the diversity and decentralization that are core to Ethereum's ethos. Further insights into this subject and its significance will be explored later in this report.

KZG Commitments

The challenge in the implementation of DAS and erasure coding lies in guaranteeing that the data is extended correctly and verified for accuracy. This is pivotal as **improperly erasure-coded data would make the blob filled with incorrect or junk data irrecoverable**. Addressing this issue, **KZG commitments serve as the cryptographic assurance that the data has been coded and extended correctly**[20].

KZG (Kate-Zaverucha-Goldberg) commitments employ polynomial commitment schemes to provably commit to certain values[21]. **In other words, while DAS confirms the availability of erasure-coded data, KZG commitments affirm the integrity of the original data**. There are generally two methods to ensure the validity of erasure-coded data: fraud proofs and ZK proofs. **Networks like Celestia use fraud proofs for this purpose, but the Ethereum community has opted for KZG commitments**, more specifically a 2-Dimensional KZG has been proposed. Other notable networks like Polygon Avail also utilize KZG commitments. Below are some of the relative advantages and disadvantages of KZG:

- **Advantages: KZG is lauded for its low latency and assurance of correct erasure coding,** without relying on the honest and synchronization assumptions that are inherent to fraud proofs.
- **Disadvantages: KZG is not quantum-resistant and requires a trusted setup,** which may raise concerns about system integrity. However, **the trusted setup in KZG operates under a 1 of n trust assumption**. This means that it **only requires a single good actor in the total set of participants involved to preserve the integrity of the setup**, making it a more robust choice than it might initially appear.

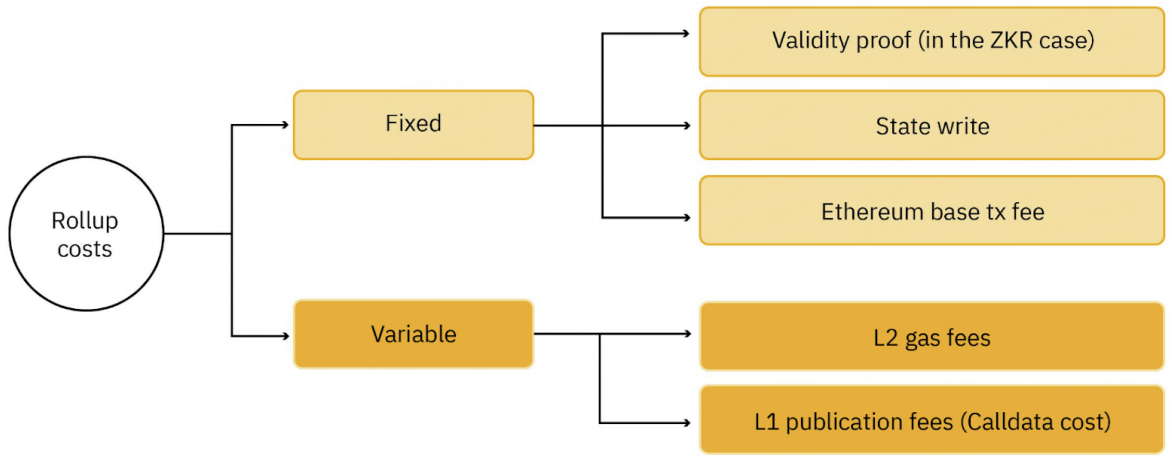
Overall, KZG commitments offer an effective but not entirely flawless solution to the challenges posed by the implementation of DAS and erasure coding in Ethereum's scaling roadmap. Nevertheless, to reach the long-term goal of a fully quantum-proof Ethereum, **the latter stages of the Ethereum roadmap are likely to transition away from KZG to a different commitment scheme that is quantum-resistant and doesn't need a trusted setup**. For more details on this topic, we recommend reading Dankrad Feist's post on KZG Polynomial Commitments.

Impact on Layer-2 Rollups

The introduction of initiatives like **EIP-4844 and DAS aim to significantly improve the scalability and performance of Ethereum**. **These changes will inevitably have a direct impact on L2s**, which have already been carving out their own niche within the ecosystem. To better understand this impact, it's crucial to examine the cost structure associated with using rollups.

The costs related to rollups are usually broken down into fixed and variable costs. Fixed costs include three primary elements: **the state write fee, validity proofs, and the Ethereum base transaction fee**. Variable costs, meanwhile, consist mainly of the **L2 gas fee for processing transactions and the L1 publication fee for storing batch data in Ethereum blocks, commonly known as calldata costs**. Network revenue, generated through gas fees that users pay to the rollup operator when executing transactions, generally cover these costs.

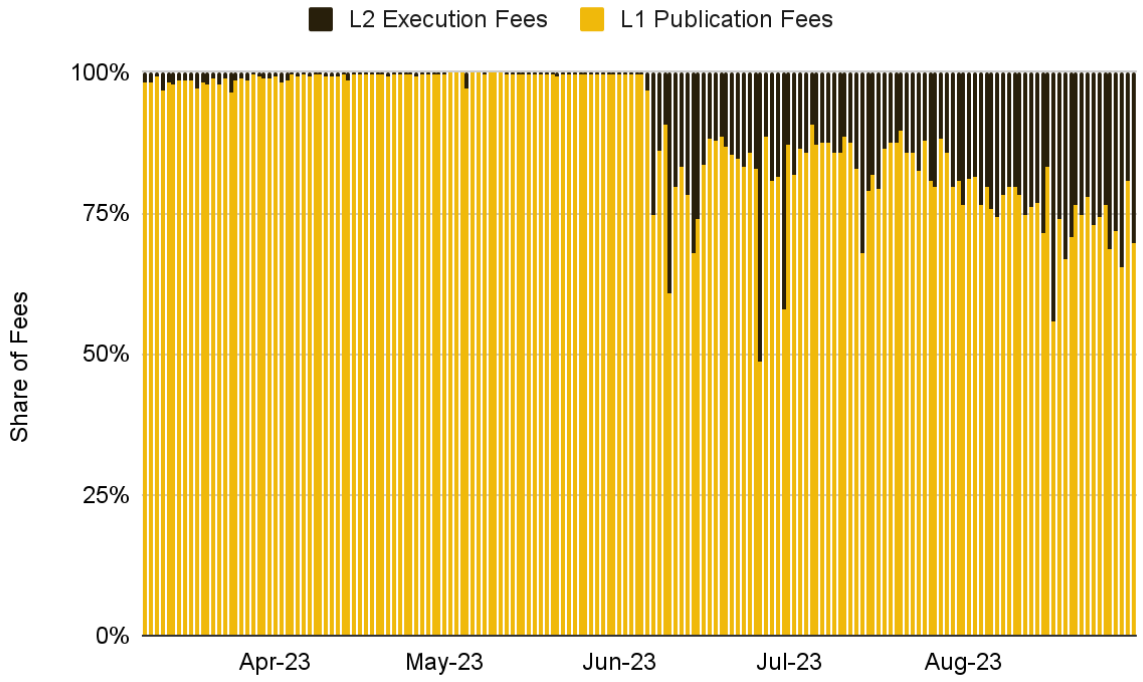
Figure 12: Rollup costs can be categorized into fixed and variable costs



Source: Celestia, Binance Research

Based on market observations, **the dominant cost driver for rollups today is calldata costs.** In fact, taking Optimism as an example, the cost of calldata is at times seen to constitute over 90% of the rollup's transaction fees. This predominance highlights the transformative potential of initiatives aimed at reducing calldata expenses. **Specifically, the implementation of EIP-4844, with its introduction of blob-carrying transactions and a dedicated storage space for DA, could be a game-changer in this regard**. Therefore, it is quite evident that **reducing calldata costs is poised to significantly enhance the economic viability and scalability of rollups**.

Figure 13: L1 publication fees have been a dominant cost driver for rollups



Source: Dune Analytics (@optimismfnd), Binance Research, as of August 31, 2023

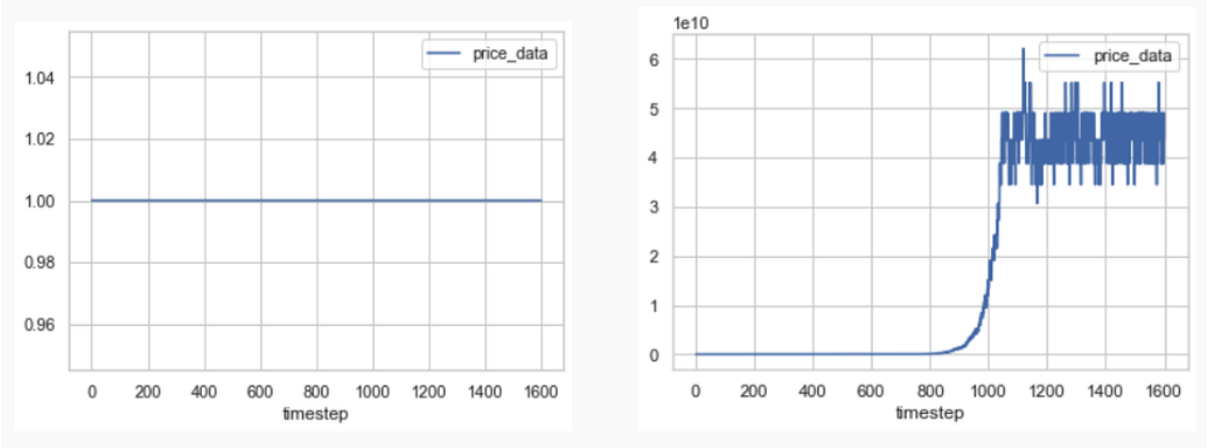
EIP-4844 and its anticipated reduction in DA costs have several implications for L2 rollups and, by extension, the entire Ethereum ecosystem. **Although this reduction in costs will initially be passed on to the end user without affecting the profitability of L2s, this does not tell us the entire story.** The introduction of reduced fees is likely to stimulate increased transaction activity. This increase in activity could, in turn, raise execution costs, potentially leading to greater overall profits for L2s.

Importantly, EIP-4844's impact extends beyond mere cost efficiencies. **By reducing the overhead for high-transaction-load use cases such as for gaming- and social-based dapps, it enables more scalability without compromising on decentralization or security, effectively distancing itself from the effects of the blockchain scalability trilemma.** While full DS will be the upgrade that may further invert the scalability trilemma, EIP-4844 sets the stage for these transformative changes by laying out the initial framework with PDS.

Upon considering the current demand for blob space based on batch data from leading rollups like Arbitrum and Optimism[22], we can ascertain the prospective demand for blobs to be several orders of magnitude lower than the target blob amount. **The initial low demand for blob space will likely result in lower blob fees until demand catches up with the targeted blob amount per block**. **This creates an intriguing market dynamic where price discovery for blobs is deferred until demand surpasses the initial block target**. Therefore, in the interim, it is expected that data prices will remain close to their

base level, meaning that transaction fees are likely to be substantially lower. This attractive cost structure may serve as a powerful catalyst for broader adoption and utilization of Ethereum's L2 solutions.

Figure 14: Data prices are expected to remain close to their base level until demand for blobs approaches the target level



Source: ethresear.ch

However, with the introduction of blobs, it is important to keep in mind the inherent complexities and uncertainties that come with bootstrapping a new market. As is always the case with new markets, there is an initial problem of market asymmetry. The uncertainty behind a new fee market may set deviated expectations regarding data costs. Given the initial limitations on the number of blobs per block and the possibility of underutilizing the full data space, it may also be the case that a secondary market for blob pricing emerges. **Hence, in the absence of strong market feedback mechanisms, blob prices might initially experience a period of volatility before reaching a stable price equilibrium**.

Nevertheless, these are likely to be minor considerations, with the overall trajectory for rollups remaining overwhelmingly positive post PDS. **The incentives generated by reduced fees are set to make Ethereum-based rollups among the most cost-effective blockchain solutions in the short to medium term**. The Ethereum community is also not taking this optimistic outlook for granted and is actively reviewing all fronts. Topics related to expediting the blob fee discovery process - such as implementing higher blob fees or lowering the target number of blobs - have already been in discussion.

It is also worth mentioning that the eventual success of EIP-4844 is closely tied to the continued development of L2s, which are themselves in a period of market consolidation and likely to undergo further shifts. While EIP-4844 is certainly **intended to boost the cost-effectiveness of rollups**, the **variables influencing their broader adoption go beyond just PDS and enhancing DA costs**. Despite being more cost-effective than Ethereum even today, **rollups are still in their nascent stages and are yet to offer**

equivalent levels of security, usability, or decentralization. Meaningful enhancements in areas fostering improved user experience and interoperability remain crucial. As such, it remains to be seen whether a significant volume of transaction activity will shift from Ethereum to rollups to capitalize on the cost savings on offer.

Ultimately, EIP-4844 seeks to enhance Ethereum's transactional capacity through PDS, while also laying the foundations for the eventual implementation of full DS. In particular, DS sets the expectation of a future where **Ethereum becomes a unified settlement and DA layer**, thereby unlocking a variety of beneficial use cases for L2s in the long-term. For example, rollups utilizing validity proofs would be able to make synchronous calls with Ethereum's EL. This could potentially lay the groundwork for new L2 primitives, creating opportunities for the development of next-generation dapps. However, it's important to note that **the full realization of DS is likely several years away**, requiring further research, consensus, and likely multiple phases of implementation before it becomes a reality. **PDS is the upgrade to be excited about for now and is the first of many steps toward developing an efficient native DA layer and scalability**.

5 The Scourge

The Scourge comprises a series of upgrades aimed at mitigating the centralizing effect of MEV, while preserving fair and transparent transaction inclusion. **Proposer-builder Separation ("PBS") is the most prominent upgrade, with roadmaps to DS and statelessness both requiring PBS as a prerequisite.**

To understand the context better, it's crucial to first touch upon what MEV is. Simply put, **MEV is a measure of the extra income that miners or validators can earn on top of the block rewards and transaction fees**[23]. This is achieved by strategically including, excluding, or reordering transactions within a block, rather than adhering to a simplistic transaction prioritization based on fees.

Although validators have a unique advantage in identifying and capitalizing on MEV opportunities (they dictate which transactions are included and their sequence), **most of the MEV gains are actually captured by specialized entities known as searchers**, who employ complex trading algorithms. Unfortunately, **the specialization needed to compete for MEV extraction is an inherently centralizing force**, putting it at odds with Ethereum's guiding principle of maximizing network participation. **PBS is the Ethereum development community's answer to this problem.**

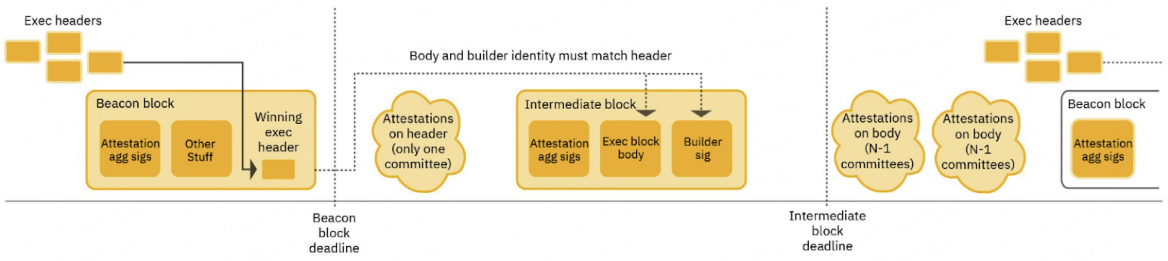
Proposer-Builder Separation

PBS seeks to create a division of labor between two crucial functions performed by Ethereum validators today: proposing a block, and building it[24]. In this model, the chosen validator for proposing the next block, known as the block proposer, offloads the task of block construction (transaction selection and ordering) to a specialized market of block builders. **This creates a distinct, in-protocol role for builders, who assemble blocks and make bids to have their blocks selected by the proposers**. In a well-functioning market, competitive builders would bid up to the full value of the MEV they can extract from blocks, enabling the decentralized validator set to reap the majority of MEV rewards. **Therefore, PBS is able to effectively combat the centralizing force of MEV.**

The implementation of PBS also means that **validators lose their ability to single out specific transactions for inclusion or exclusion**, as the **block's content is now determined by a separate entity**. Such an arrangement **offloads the computationally challenging task of block assembly** to more specialized parties, thereby **allowing validators to operate with reduced hardware requirements**. This design is particularly **advantageous for DS**, given its implementation inherently imposes an increased computational load on block builders. **To alleviate the burden placed on regular validators, PBS serves an important role in the DS roadmap**[25]**.** While this setup does **centralize the task of block building**, it **preserves the decentralized and trustless nature of block validation**. This adheres to Vitalik Buterin's post on Endgame: All paths lead to the endgame of centralized block production with decentralized trustless block validation.

Details regarding the technical implementation of PBS are still under consideration, but a two-slot framework using a commit-reveal scheme is one option that has gained traction. Notably, the commit-reveal scheme is important for safeguarding against MEV theft. In this approach, block builders submit their bids along with a preliminary block header to the proposer. The proposer then picks a winning bid and header, after which a committee of attestors validates it. Once approved, the block builder unveils the complete block body.

Figure 15: Visual representation of two-slot PBS

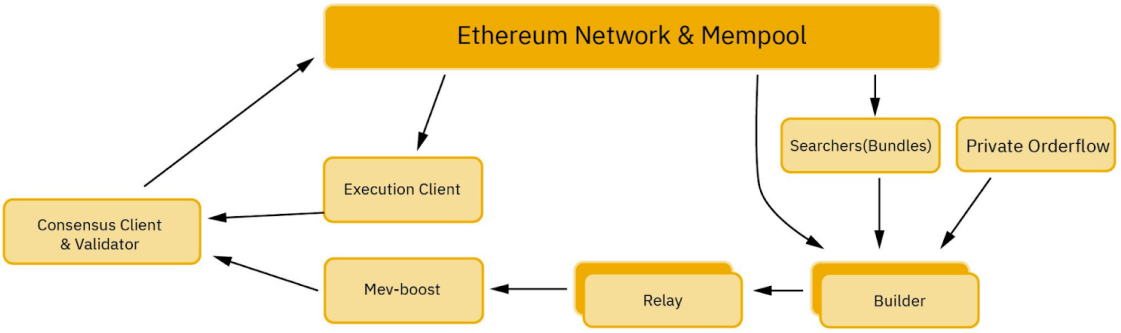


Source: ethresear.ch, Binance Research

A notable feature in this system is that trusted relays, which have acted as intermediaries between proposers and builders, will no longer be necessary. Builders will submit their bids directly to the block proposers, and these bids will be irrevocable, even if the builder fails to deliver a valid block. **The unconditional payment structure negates the need for the proposer to place trust in the builder.**

In the interim, while PBS is being formally integrated into Ethereum, **third-party solutions like Flashbots' MEV-Boost are filling the gap**[26]. **MEV-Boost establishes a free market for block building, effectively separating the roles of proposer and builder.** In this system, proposers can maximize their MEV returns by delegating the task of block construction to specialized builders. However, **a key difference is that MEV-Boost employs a mutually-trusted relay** to facilitate the transfer of block data between both parties. This ensures that the proposer cannot siphon off MEV from the builder. Therefore, although the relay system does require a level of trust, it functions primarily to confirm the validity and existence of the block body, thereby eliminating the need for validators to trust builders directly.

Figure 16: PBS is only possible today by running third-party middleware from Flashbots known as MEV-Boost



Source: Flashbots Documentations, Binance Research

While MEV-Boost serves as a useful interim fix, its utility may diminish as future upgrades like DS, designed for builder specialization, come into play. Non-specialized validators may find it challenging to locally construct blocks under such conditions. Therefore, it is expected that in-protocol PBS will eventually encapsulate the benefits provided by MEV-Boost. **Not only does PBS maintain the same division of roles, but it also facilitates easier decentralization of builders and eliminates the need for proposers to place trust in any other party**.

Censorship Resistance List

An important externality from PBS is that it creates the potential for increased centralization, particularly with respect to transaction censorship[27]. By specializing the role of block builders, **the upgrade may enable builders to strategically outbid competitors and exclude specific transactions**. To counter this, various designs aimed at ensuring censorship resistance are under consideration, such as full block auctions featuring inclusion lists or partial block auctions. One proposal suggests that **block proposers could publish a censorship resistance list ("crList") to highlight transactions in the mempool that they consider should not be censored.** Builders would be obligated to include these transactions from the crList unless they deliver a complete block. **The nuances of these designs are still in the process of being ironed out**, making it an important area to monitor closely in the future.

Other Focus Areas

Beyond PBS, there are additional areas of interest that warrant attention. **Identifying ways for the more equitable distribution of MEV** to counter its centralizing effects is one such example. An idea under consideration is committee-driven MEV smoothing[28], designed to make the distribution MEV as uniform as possible. **Another focus area aims to burn MEV, redirecting its value to all ETH holders rather than exclusively benefiting ETH stakers**[29]. The final significant item on the long-term roadmap is **the exploration of distributed block building**. While many forthcoming Ethereum upgrades concede the necessity of specialized builders to reduce the computational burden on validators, it may still be beneficial to decentralize the task of block building in the long term.

In summary, **PBS is at a relatively mature stage of research** and represents a crucial step in addressing challenges that arise from MEV and DS. While PBS has mostly confined centralization risks to block builders, additional mechanisms are still needed to ensure equitable and transparent transaction inclusion.

6 The Verge

The Verge focuses on a set of upgrades with the primary goal of instituting statelessness within Ethereum. **By eliminating the need for validator nodes to keep a full copy of Ethereum's state, The Verge aims to simplify the process of block validation, using enhanced proof techniques to do so**. This change is expected to significantly **reduce the storage and bandwidth prerequisites for validators**, thereby **bolstering decentralization**. The ultimate vision for The Verge is to equip lightweight clients with security assurances on par with current full nodes.

However, **storing this data becomes expensive,** particularly for high throughput blockchains, as the **growing nature of Ethereum's state data greatly bloats disk space usage**. This growing storage requirement consequently **elevates the hardware prerequisites for running a full node**, **risking a potential centralizing effect** on validators. To address this, Ethereum's development community has come up with statelessness and Verkle Trees.

Statelessness

Statelessness essentially refers to not needing the state on hand to perform a particular role or function. **Specifically, Ethereum aims for weak statelessness, where validators can verify blocks without holding a copy of Ethereum's entire state, although block builders still require access to the state for constructing blocks**. Given the separation of block building from proposing through PBS, this limitation is less concerning. Specialized block builders are already anticipated to handle state growth effectively due to their centralized nature.

Witnesses play a crucial role in enabling stateless execution. These are essentially cryptographic proofs verifying proper state access, which builders will include in every block. Validation does not require access to the entire state but rather just the segments impacted by the transactions within the block. **Block builders will include these specific pieces of state in each block and verify their accuracy via witnesses**.

The adoption of weak statelessness allows Ethereum to scale its execution throughput by mitigating the constraints posed by state growth[30]. **While most of the transaction execution is projected to shift to L2s, enhancing L1 throughput remains advantageous**. Rollups, for instance, depend on Ethereum for DA and settlement, requiring L1 execution. As Ethereum scales its DA layer, the amortized cost of submitting proofs might become a significant part of rollup expenses. However, **to achieve weak statelessness, more bandwidth will be required** given the inclusion of witness data and proof. **Fortunately, the transition to Verkle trees will no longer render this to be a bottleneck**.

Verkle Trees

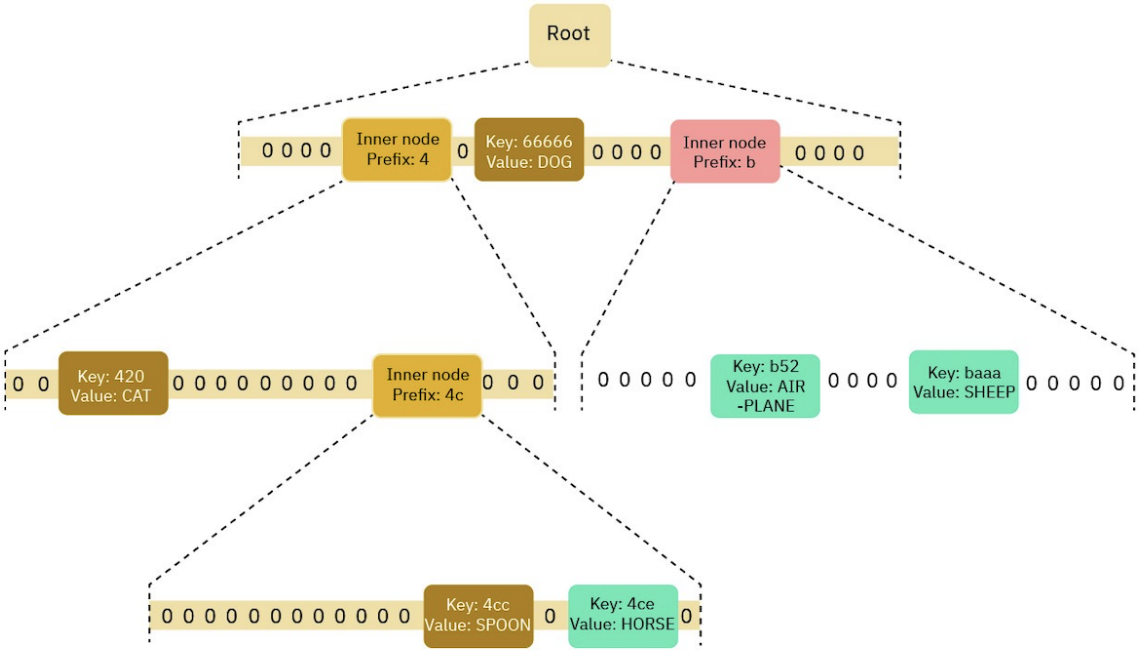
Presently, Ethereum relies on a Merkle-Patricia Tree to hash and compress its state data. However, **the size of Merkle proofs in this tree structure can become far too large**, **making them less suitable for the witnesses** needed in a stateless model. To address this issue, **Ethereum plans to transition to Verkle Trees**, a more efficient data structure. Both Merkle-Patricia and Verkle Trees share the important ability to generate witnesses - cryptographic proofs that allow anyone to easily confirm the existence of a particular piece of information against the publicly available state root.

The advantage of Verkle Trees lies in their efficiency in generating smaller proof sizes[31]. Unlike Merkle-Patricia Trees, which demand an increasing number of hashes as the tree broadens, **Verkle Trees utilize vector commitments to allow expansion without proportionally increasing the size of the witness**. **This optimization reduces the amount of data that needs to be transmitted**, making stateless validation more feasible.

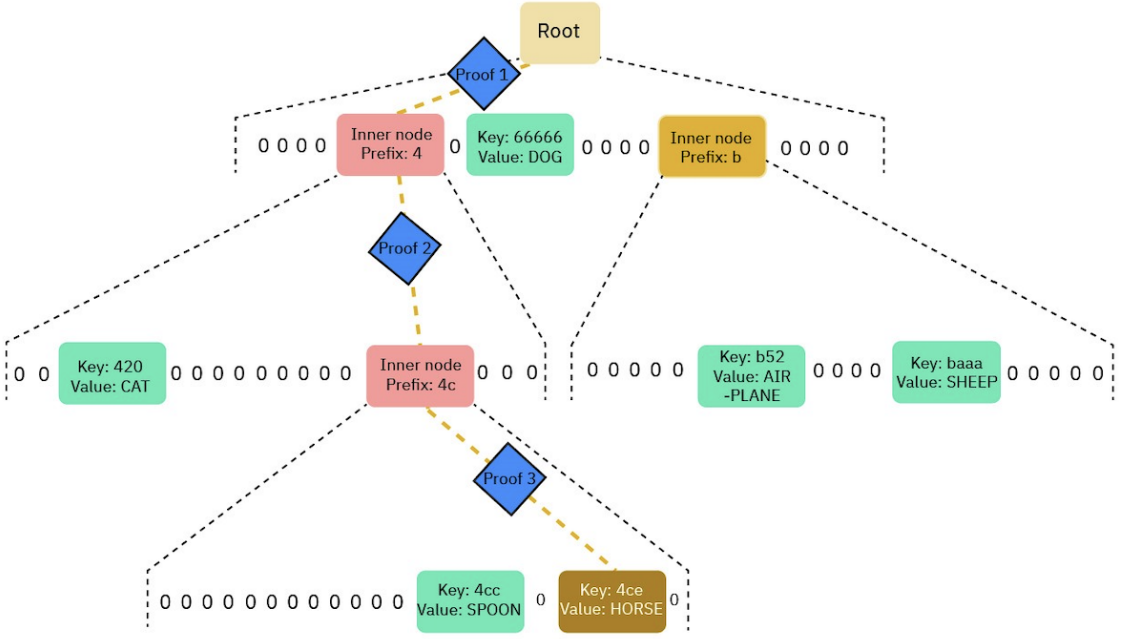
The shift to Verkle Trees will substantially facilitate the proliferation of stateless clients[32]**.** Validators will no longer need to maintain a local copy of the entire Ethereum state. Instead, block builders will supply a Verkle proof encapsulating the portions of the state that are relevant to a particular block. **Validators can then use these proofs to verify blocks without needing to access the full state**. This approach also enables new nodes to begin validating blocks immediately, as they would not be required to synchronize the complete state history.

Figure 17: Verkle proofs are far more efficient, so they can serve as viable witnesses to enable weak statelessness

With Merkle Trees, all of the witnesses marked in brown are required to demonstrate that Key: 4ce, at the very bottom, is included in the tree. Specifically, ***the proof of value must consist of the entire set of sibling nodes****. This is clearly inefficient.*



In Verkle Trees, however, it is unnecessary to provide all of the brown-colored witnesses described above to prove that Key: 4ce is included in the tree. Instead, ***only the path itself plus a few short proofs are sufficient****. Verkle trees use* ***efficient vector commitment*** *rather than a simple hash.*



Source: vitalik.ca, Binance Research

As of today, **testnets for Verkle trees are already operational, yet considerable updates to clients are still needed** before the migration to Verkle Trees takes place. Looking ahead, **Ethereum aims to integrate even more advanced proof technologies**, such as zk-SNARKs, **to further improve proof efficiency and ease block verification**. As specialized hardware for generating SNARK proofs becomes more advanced, zk-SNARKs will increasingly enable the verification of more complex statements. **Ultimately, quantum-resistant zk-STARKs are expected to be the endgame, though current proof generation times are seen as a constraint.**

7 The Purge

The Purge is a planned sequence of **upgrades designed to simplify the Ethereum protocol by minimizing the burden of historical data storage and eliminating technical debt**. This is especially important for Ethereum, given that the **ever-increasing historical data and state complexity** may **raise node storage requirements** and thereby **affect decentralization**. The stakes are even higher once DS is implemented, as it is anticipated to substantially increase average block size. Among these upgrades, EIP-4444 is particularly notable.

History Expiry (EIP-4444)

EIP-4444 aims to implement history expiration, an upgrade that mandates nodes to cease hosting historical blocks on the peer-to-peer network that are older than one year[33]. This deletion of historical data **significantly eases disk space requirements for node operators**. At the same time, it also **streamlines client software by removing the need for code that accommodates varying versions of historical blocks**. Additionally, the combination of EIP-4444 with PDS ensures regular data pruning; EIP-4444 prunes annually, whereas PDS prunes blobs on a monthly basis. Although this is advantageous in reducing data storage requirements for nodes, it does raise concerns about the preservation and recovery of historical data.

The deletion of historical data poses challenges primarily for applications built on Ethereum that rely on analyzing past transaction information. While storing history is increasingly viewed as a responsibility best managed outside the core Ethereum protocol, clients will still have the capability to import such data from external sources. Various approaches are likely to emerge for accessing historical data beyond the Ethereum network, whether through **block explorers like Etherscan**, **indexing services like The Graph**, or potentially via more **decentralized solutions backed by the Ethereum Foundation**. Once EIP-4444 is implemented, the preservation of historical data is certainly going to be a point of interest.

State Expiry

As previously discussed in The Verge, weak statelessness eliminates the necessity for validators to maintain the entire state for block validation. However, **the state doesn't simply vanish; its continued growth remains a long-term challenge for the network**. To address this underlying issue, The Purge incorporates something called state expiry. **State expiry automatically prunes parts of the state that have remained static for a defined period**, such as one year, moving them into a separate tree structure and excising them from the primary Ethereum protocol[34].

State expiry is one of the more distant upgrades on Ethereum's developmental roadmap and only becomes viable after the migration to Verkle Trees. **Though its urgency may seem diminished after the implementation of stateless clients, state expiry still serves to alleviate the burden of dormant accounts and other idle addresses on Ethereum's state**. Looking ahead, both L1 and L2 throughputs are expected to increase over time. In particular, L2 state growth may occur at a much higher rate, potentially affecting even high-performance block builders at some point in the future. As such, a proactive strategy for managing state growth is certainly beneficial.

All things considered, **both history expiry and state expiry remain under active research**, and their specifics may change as the roadmap progresses. Before these proposals can come to fruition, some of the other roadmap items, such as PBS and Verkle Trees, would need to be completed first.

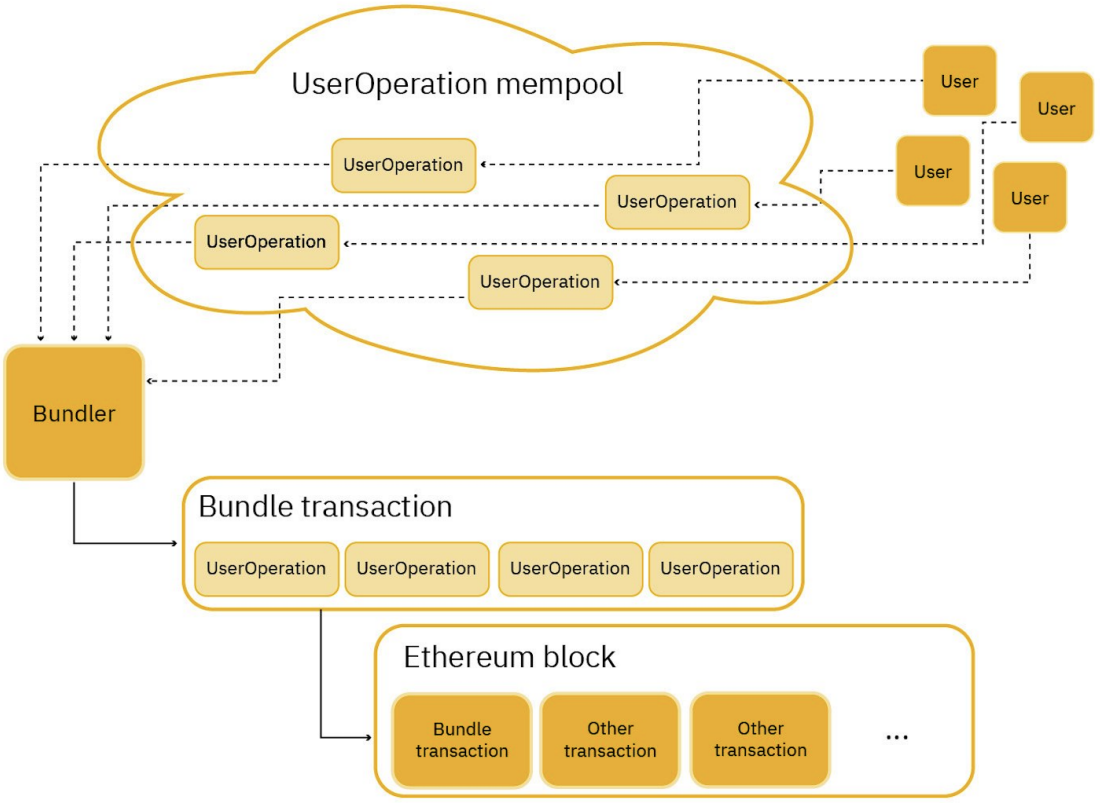
8 The Splurge

The Splurge serves as a miscellaneous category for upgrades that don't readily align with the themes of the preceding sections. This section encompasses a range of developments, with some of the more notable upgrades including **Account Abstraction**, and **Multidimensional EIP-1559**, and **Verifiable Delay Functions.**

Account Abstraction (ERC-4337)

Account Abstraction ("AA") represents a pivotal upgrade, with ERC-4337 emerging as one of the most significant proposals. AA refers to the decoupling of the relationship between the account and the signer for EOAs. **This enables users to use smart contract wallets as their primary Ethereum accounts, effectively supplanting traditional EOAs and thereby elevating the overall user experience**[35]. Remarkably, it accomplishes this by replicating the functionality of a transaction mempool in a higher-layer system, thereby eliminating the need for changes to the Ethereum protocol itself.

Figure 18: Instead of modifying the logic of the consensus layer itself, ERC-4337 replicates the functionality of the transaction mempool in a higher-level system



Source: erc4337.io, Binance Research

The widespread enthusiasm for AA is wholly justified, given its array of benefits, some of which are outlined below.

- **Enhanced Security:** AA introduces **multiple options for authentication and recovery**, moving beyond the current reliance on seed phrases for account recovery and management.
- **Improved User Experiences:** **The complexity of handling EOAs and private keys is simplified**. AA **enables developers to innovate on user experiences,** such as introducing user-friendly security features and transaction processes, making Web3 wallets as intuitive as Web2 apps.
- **Batch Transactions:** Instead of individually authorizing each transaction, AA allows users to **bundle multiple actions into a single operation**, making it more convenient for dapps like gaming that require frequent transactions.
- **Automated Transactions:** This **enables users to set up recurring payments and other automated transactions**, which are not possible with the current EOA system.

- **Flexible Gas Payments:** AA **allows transaction fees to be paid in ERC-20 tokens**, not just ETH. It also **enables third-party payment of gas fees**, which can be particularly beneficial for onboarding new users to interact with the network.

Token Bound Accounts (ERC-6551)

While this upgrade is somewhat divergent from this phase, token bound accounts ("TBAs"), a feature of ERC-6551, is a notable AA-related development worth mentioning. **ERC-6551 is a new standard that empowers NFTs to function as their own smart contract accounts and wallets, utilizing a permissionless registry.** This enables an integrated mechanism for owners to custody NFTs within the TBA. Originating from the **increasing need for NFTs to hold assets in scenarios like gaming**, TBAs are **designed to overcome barriers that prevent NFTs from engaging with other on-chain assets**. This innovation provides a flexible framework that enriches the NFT landscape without necessitating alterations to the existing ecosystem, paving the way for innovative applications and additional possible enhancements.

Looking ahead, **additional EIPs may be introduced to enable the conversion of EOAs into smart contract wallets**, with a potential mandatory conversion proposal aimed at simplifying the protocol by standardizing all accounts as smart contract wallets. For more information on AA and TBA, including their growth and adoption, please check out our recent report: A Primer on Account Abstraction.

Multidimensional EIP-1559

Multidimensional EIP-1559 expands on the concepts initially discussed with the introduction of blob-carrying transactions. In particular, PDS introduces a multi-dimensional EIP-1559 fee market, where two resources, gas and blobs, have separate floating prices and associated limits. **Multidimensional EIP-1559 emphasizes the potential for enhancing gas market efficiency through the partitioning of costs associated with the specific resources consumed by Ethereum transactions**. As it stands, **gas in Ethereum is a composite of several distinct resources**, including EVM execution, transaction calldata, witness data, among others.

A multidimensional fee market seeks to address the challenges that arise from the differences between the average and worst-case load for each of these resources. **By independently pricing each resource according to its own supply and demand dynamics, multidimensional EIP-1559 effectively curtails the extent of divergence between average and peak loads**. This marks a **noteworthy advancement in the subject of resource pricing** within the Ethereum ecosystem, helping to resolve occurrences of sub-optimal gas fees.

Verifiable Delay Functions

Finally, to fully appreciate Verifiable Delay Functions ("VDFs"), one must first understand the critical role that randomness plays in a PoS blockchain like Ethereum. In the current system, **randomness is chiefly sourced from a RANDAO value stored in the beacon state**, and it is **important for fairly allocating tasks such as block proposals and committee assignments among validators**.

VDFs bring an **enhanced layer of randomness by using specialized hardware to carry out a sequence of non-parallelizable computations**, each requiring a predetermined amount of time, known as the delay[36]. This makes the output more secure and removes the potential for bias. Importantly, the results of these calculations can be rapidly verified without the need for specialized equipment. **In short, VDFs offer Ethereum a more robust source of randomness, which could be crucial for the development of certain applications in the future.**

9 Closing Thoughts

Although Ethereum's **transition from a PoW to a PoS consensus mechanism marked a major milestone,** the platform's development journey is far from complete. With a clear roadmap at hand, the development team is actively pursuing various upgrades to realize their full range of benefits.

To summarize, **SSF will significantly refine Ethereum's PoS architecture**, offering reduced finality and better user experience. **Starting with PDS, The Surge aims to lower DA costs and distribute the workload of checking DA amongst nodes**, enhancing scalability, particularly for L2s. **The Scourge incorporates PBS to counteract the centralizing effects of MEV** and redistributes MEV income in a credibly neutral manner. **The Verge focuses on achieving statelessness by migrating to Verkle Trees**, enabling stateless clients to verify blocks without requiring a local copy of the Ethereum state. **The Purge reduces historical data storage and technical debt** to further simplify the protocol. Finally, **The Splurge adds several additional features**; one notable recent addition is Account Abstraction, which allows for expanded wallet choices, improved gas market efficiencies and enhanced functionalities.

Though many of these **upgrades are still in their formative stages** and are yet to be fully executed or defined, the information presented in this report offers a snapshot of an ever-changing landscape. **When fully realized, Ethereum is expected to significantly scale computational throughput while maintaining its already leading security and decentralization.** This will clear the path for **widespread adoption**, **free from any scalability or cost constraints**, and thus help Ethereum fulfill its goal of creating a

universal, trustless, permissionless DA and settlement layer. We look forward to witnessing how the next phase of Ethereum's roadmap unfolds.

References

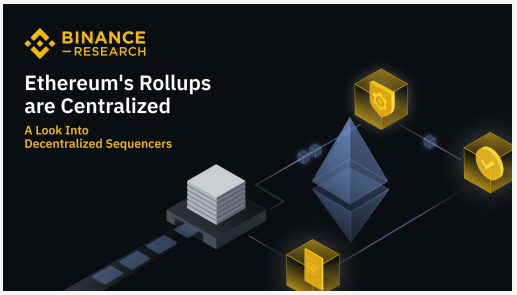
1. https://defillama.com/chain/Ethereum
2. https://coinmarketcap.com/currencies/ethereum/
3. https://ethereum.org/en/roadmap/
4. https://www.bankless.com/-99-endgame-vitalik-buterin
5. https://twitter.com/VitalikButerin/status/1570306185391378434
6. https://www.coindesk.com/tech/2022/08/01/ethereum-after-the-merge-what-comes-next/
7. https://ethereum.org/en/developers/docs/nodes-and-clients/
8. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
9. https://www.coindesk.com/business/2022/09/15/vitalik-buterin-says-ethereum-merge-cut-global-energy-usage-by-02-one-of-biggest-decarbonization-events-ever/
10. https://ethereum.org/en/roadmap/merge/issuance/
11. https://github.com/ethereum/distributed-validator-specs
12. https://ethereum.org/en/roadmap/secret-leader-election/
13. https://notes.ethereum.org/@vbuterin/single_slot_finality
14. https://ethereum.org/pt/roadmap/scaling/
15. https://ethereum.org/en/roadmap/danksharding/
16. https://www.eip4844.com/
17. https://ethresear.ch/t/eip-4844-fee-market-analysis/15078
18. https://hackmd.io/@vbuterin/sharding_proposal
19. https://notes.ethereum.org/@vbuterin/proto_danksharding_faq
20. https://scroll.io/blog/kzg
21. https://dankradfeist.de/ethereum/2020/06/16/kate-polynomial-commitments.html
22. https://github.com/dcrapis/blockchain-dynamic-pricing/blob/685b837dda64d149bd330e5619cf9682f4e58dc8/eip-4844-sim.ipynb
23. https://ethereum.org/en/developers/docs/mev/
24. https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance
25. https://ethereum.org/nl/roadmap/pbs/
26. https://docs.flashbots.net/flashbots-mev-boost/introduction
27. https://notes.ethereum.org/@fradamt/H1TsYRfJc#PBS-censorship-resistance-alternatives
28. https://ethresear.ch/t/committee-driven-mev-smoothing/10408
29. https://ethresear.ch/t/burning-mev-through-block-proposer-auctions/14029
30. https://dankradfeist.de/ethereum/2021/02/14/why-stateless.html
31. https://vitalik.ca/general/2021/06/18/verkle.html
32. https://www.youtube.com/watch?v=Q7rStTKwuYs
33. https://ethereum.org/en/roadmap/statelessness/
34. https://hackmd.io/@vbuterin/state_size_management#A-more-moderate-solution-state-expiry

35. https://www.erc4337.io/
36. https://ethresear.ch/t/verifiable-delay-functions-and-attacks/2365

Latest Binance Research Reports

Emerging Stablecoins: Latest Developments

A review of the evolving stablecoin landscape



Ethereum's Rollups are Centralized. A Look Into Decentralized Sequencers

A deep dive into the world of decentralized, shared sequencing solutions

A Primer on Account Abstraction

An introduction to account abstraction

Monthly Market Insights: August 2023

A summary of the most important market developments, interesting charts and upcoming events

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to the crypto ecosystem, blockchain technologies, and the latest market themes.

Moulik Nagesh

Macro Researcher

Moulik is a Macro Researcher at Binance, having been involved in the cryptocurrency space since 2017. Prior to joining Binance, he had experience spanning cross-functional roles in Web3 and Silicon Valley-based tech companies. With a background in co-founding start-ups and a BSc in Economics from the London School of Economics & Political Science ("LSE"), Moulik brings a comprehensive perspective to the industry.

Resources

Read more here

Share your feedback here