Origins Whitepaper

Simplifying infrastructure for easier user and developer utilization.

Abstract

The purpose of this paper is to describe the primary challenges of adopting advanced infrastructure technologies in the public chain ecosystem and to provide comprehensive solutions to address these challenges through a holistic approach.

Bitcoin, created by Satoshi Nakamoto, pioneered the blockchain economy, introducing decentralization and digital currency to the global financial sector. However, it is Ethereum that truly propels this technological revolution, becoming the world's most open and versatile blockchain network.

Ethereum is not merely a digital currency; it is also a platform for decentralized applications (DApps) that enables trustless transactions and protocols through smart contracts. Its openness and flexibility have positioned Ethereum as a dominant force in the blockchain technology field. The open-source nature of Ethereum is a key factor in its leadership. Open source means that anyone can view, use, and modify its source code. This openness not only laid the foundation for Ethereum's success but also provided robust support for the security of the entire blockchain economy.

As one of the most secure foundational technologies, Ethereum benefits from the openness of its source code. Due to its open-source nature, developers worldwide can collectively review and improve the code, promptly identifying and fixing potential vulnerabilities. This collective wisdom of the review mechanism enhances Ethereum's security, making it a resilient defense against various attacks.

Origins is born against this backdrop. Recognizing the advantages of Ethereum's open source, Origins develops its unique blockchain ecosystem, leveraging the outstanding security of Ethereum's open source as a solid foundation for the robustness of its ecosystem. Choosing to build on the open source foundation of Ethereum is a strategic decision for Origins. By aligning with Ethereum's commitment to security and transparency, Origins inherits a powerful and validated infrastructure. This consistency means that Origins can benefit from continuous improvement and optimization from the global Ethereum community.

By embracing and continuing this spirit, Origins positions itself at the forefront of the blockchain revolution, promising a secure and dynamic ecosystem for the future. Looking ahead, the principles of openness and collaboration will drive Origins to continue guiding the development of the blockchain economy, shaping a decentralized future empowered by technology for individuals and communities worldwide.

Disclosure: The information provided in this document is preliminary and subject to change at any time. Additionally, this document may contain "forward-looking statements."

1.Story Background

The construction of Origins Originates from the three major challenges faced by the blockchain field. Faced with these challenges, current blockchain networks struggle to provide sufficient efficiency and cannot meet the demands brought by large-scale applications. It is important to note that Origins is not a branch version of Diem but an independent project built from scratch. Its focus lies in fundamental scalability to achieve real-time settlement while providing high throughput, low latency, and cost-effective performance, serving as a stable power source for applications of billions of users.

Blockchain Field's Three Major Challenges:

1. Decentralization:

   Decentralization is one of the core features of blockchain. It means that control and decision-making authority are not centralized in the hands of a single entity but distributed among various nodes in the network. This makes it difficult for a single point to be a target for attacks, enhancing the system's resistance to attacks. However, decentralization may also lead to performance bottlenecks and the complexity of achieving consensus.

2. Security:

   The security of a blockchain depends on the cost for an attacker to gain control of the system. Generally, the higher the security, the greater the cost an attacker needs to incur, thereby enhancing the network's security. Consensus algorithms, encryption technologies, and the decentralized nature are crucial factors in ensuring the security of the blockchain.

3. Scalability:

Scalability refers to the system's ability to effectively handle more transactions and data volume. High scalability is crucial for supporting large-scale applications and widespread adoption. However, improving scalability may involve sacrificing some decentralized features because, in a decentralized network, each node must participate in the consensus process, which may lead to limitations in transaction speed.

In the "Trilemma of the Three Major Issues," each of the three characteristics has its own independent technological development path. Sacrificing one characteristic does not necessarily mean gaining an improvement in another. Instead, under existing technological conditions, a blockchain system attempting to maximize these three characteristics typically involves trade-offs. Moreover, if we exclude "decentralization" and "security" from the "trilemma," there can be no talk of a "blockchain" and a "system" at all. Over the years, various blockchain public chain systems, when attempting to overcome the "Trilemma," have often prioritized optimizing system performance by increasing TPS (transactions per second). Origins, too, was born to thoroughly address the challenges of blockchain.

2.Origin Tech Solutions

2.1 Origin Tech Solutions Inc

Origin Tech Solutions Inc. is a company specializing in providing hardware and cloud computing solutions for the fields of deep learning and artificial intelligence. Founded in 2023 and headquartered in the United States, Origin Tech Solutions offers high-performance computing equipment designed specifically for AI and machine learning workloads, such as GPU servers, workstations, and the Origin Cloud computing platform.

The business model of Origin Tech Solutions revolves around its decentralized global computing network, which generates revenue primarily through the leasing of computing resources, on-demand computing services, and blockchain technology services. The company leverages its core network, "Origins," allowing individuals and businesses to tap into idle GPU resources and rent out underutilized computing power to clients requiring high computational resources for tasks like AI training and data analysis, thereby earning leasing fees. Additionally, Origin Tech Solutions offers flexible on-demand GPU computing services to businesses and developers, where clients can pay by the hour or based on usage, making this model particularly suitable for projects with fluctuating computing needs. The company also provides blockchain-based solutions for transparent and secure management of computing resources, including services for data validation, price monitoring, and ad verification, charging relevant consulting or service fees.

Origin Tech Solutions Inc. is actively planning its future listing on the U.S. capital markets, aiming to leverage capital to further solidify the company's leadership in global AI and deep learning hardware solutions. This strategic move is part of the company's long-term growth plan, focused on enhancing its technology research and development capabilities, expanding its global market share, and supporting the intelligent transformation of industries across various sectors. The company has established a GPU cluster in Chicago and plans to set up a second cluster in Los Angeles by the second quarter of 2025. As the company continues to grow through the income generated from its enterprise and individual clients, its listing strategy is steadily progressing and will mark a significant milestone in its development. With the support of the capital markets, the company will be empowered to drive innovation, shape the future tech ecosystem, and lead the widespread and in-depth global adoption of blockchain technology.

Mission and Vision:

The mission of Origin Tech Solutions Inc is to become an international leading provider of blockchain technology services, creating value for clients through digital innovation. In the future, Origin Tech Solutions Inc aims to drive digital transformation globally, becoming a trusted digital partner for enterprises and organizations, collectively shaping the digital future.

2.2 Origins Introduction

Origins is a decentralized infrastructure network based on an Ethereum node collaboration architecture, dedicated to building an efficient node data platform. Users can contribute node data and GPU resources, earning native Origins tokens as rewards. This incentivizes active participation, driving the sustainable development and technological innovation of the ecosystem. Through token rewards, users not only convert idle hardware into real-world earnings but also contribute to the growth of the Origins network. By utilizing user hardware devices, Origins builds a powerful GPU compute cluster, providing strong support for AI training and establishing a solid economic foundation for its own sustainable development. This model optimizes resource usage and fosters the deep integration of blockchain technology with cutting-edge fields like artificial intelligence, paving the way for the future of technological development.

The Origins public blockchain is future-oriented, creating a flexible and scalable market backed by blockchain data services and cryptoeconomic security to realize its vision. Its modular architecture and peer-to-peer node operation network have successfully constructed an infrastructure platform that provides robust support for entering the multi-chain world. On this platform, the value of blockchain data services is maximized, while cryptoeconomic security ensures the safety and stability of the ecosystem. The modular architecture guarantees the platform's flexibility and scalability, and the peer-to-peer network between nodes facilitates efficient and secure information transmission. The Origins public blockchain is poised to become the central hub of the multi-chain world, laying a solid foundation for the diversified development of the future digital economy and demonstrating strong innovative leadership with broad prospects.

3.Token

3.1 Tokenomics

Full Name: Origins - OR Smart Chain
Abbreviation: OR
The initial supply of Origins' token, OR, is 100 million tokens, and Origins operates through the ORC20 channel.

Validator Rewards: 90% of OR tokens are reserved for validators as rewards for staking OR, supporting network security and consensus.

Exchange Allocation: 5% of OR tokens will be strategically allocated to designated partner exchanges.

Allocation to Vitalik Buterin: 5% of OR will be allocated to Vitalik Buterin. As a thought leader in the industry, Vitalik Buterin’ s forward-thinking research and practices have been of great significance to the blockchain sector. This allocation reflects recognition of his contributions to the sustainable development of the industry and aims to inspire more pioneers in the field.

Inflation Model:

Origins operates on an infinite token supply system, without a hard cap on the total supply.
The inflation model is based on the issuance of a certain amount of new coins each year, achieved through the mining and validation processes.
The quantity of Origins (OR) rewarded through mining is not fixed but depends on the state of the network.
Miners and validators have the opportunity to receive newly minted OR as a reward in each block, incentivizing them to provide security and consensus services to the network.
Each node is required to stake OR tokens to unlock computational power for mining.

Origins Staking Model

The native staking model, known as Solo Staking, poses several barriers for users in terms of capital, earnings, operations, and learning. If you wish to become a native staking node, apart from meeting admission and lock-up requirements (at least 1024 OR), you may encounter the following challenges:

1. To run a node independently, you will need a device with at least a 4-core CPU, 8GB of RAM, a 500GB SSD, 1Mbps bandwidth, and the installation of ORDappNode.

2. Ensuring the reliability of the node is crucial, as rewards are directly proportional to the time the node is online and correctly proving. Any downtime or slow network speed may result in penalties.

3.Various security concerns such as hardware maintenance, key storage, and others need to be addressed.

3.2 Token Functions

3.2.1 OR can be staked for a certain period to participate in the Proof-of-Stake (POS) mechanism.

3.2.2 OR can be used to pay Gas fees for on-chain execution, storage of transactions, or other operations (similar to other native blockchain tokens). Additionally, Gas fees are utilized to reward participants in the Proof-of-Stake mechanism and prevent SPAM attacks and denial-of-service attacks.

3.2.3 OR can serve as a liquid asset for various smart contracts and monetary policy applications.

3.2.4 OR can be used for on-chain voting governance in critical transactions such as protocol upgrades.

4.Team Members

CEO - Ilia Nuzhdin

Ilia Nuzhdin serves as the Chief Executive Officer of Origins. A seasoned professional in the Silicon Valley blockchain space, he was previously an investor at Stellar. There, he led a team in successfully developing numerous leading blockchain solutions, showcasing his exceptional capabilities in technical leadership and innovation. Ilia

Nuzhdin entrepreneurial spirit and profound understanding of blockchain technology make him an ideal CEO for Origins, dedicated to driving the company's success in the realms of blockchain technology and innovation.

CMO - Olivia Roberts

Olivia Roberts serves as the Chief Marketing Officer of Origins. She is an outstanding professional in the field of digital marketing and was previously a member of the Adobe team. Known for her creative marketing strategies and exceptional market insights, Olivia successfully drove outstanding performance in the digital market for her previous company. Her innovative thinking and keen insight into market trends make her an outstanding Chief Marketing Officer for Origins, dedicated to advancing the company's market leadership in the blockchain space.

CTO - Benjamin Harris

Benjamin Harris serves as the Chief Technology Officer of Origins. He previously held responsibilities for backend technology at ConsenSys, where he successfully led technical teams in the development and implementation of multiple innovative blockchain solutions. Benjamin is recognized in the industry for his outstanding technical leadership and profound understanding of blockchain innovation. His expertise and sensitivity to emerging technologies make him an ideal Chief Technology Officer for Origins, committed to advancing the company's forefront position in blockchain technology.

COO - Brandon Turner

Brandon Turner serves as the Chief Operating Officer of Origins. Previously, he held the position of Senior Operations Manager at the Silicon Valley technology giant Cisco, where he successfully led a team in optimizing the company's production processes and supply chain management, achieving cost savings and business growth. Brandon Turner is renowned for his excellent operational management and strategic planning abilities. His outstanding operational experience and team leadership make him an exceptional Chief Operating Officer for Origins, committed to driving the company's ongoing development in the blockchain space.

CLO - Jonathan Turner

Jonathan Turner serves as the Chief Legal Officer of Origins. As a partner at the Silicon Valley law firm Cooley LLP, he specializes in technology law and intellectual property. Jonathan is acclaimed in the industry for his outstanding legal expertise and profound understanding of technology industry regulations. He has successfully provided legal counsel to numerous tech companies, achieving significant results in compliance and intellectual property protection. Jonathan's legal acumen and deep understanding of industry regulations make him an exceptional Chief Legal Officer for Origins, dedicated

to ensuring the company's leading position in legal compliance and intellectual property protection.

5.Technical Architecture

5.1 Origins Initial Sharding Scheme - Sharding 1.0

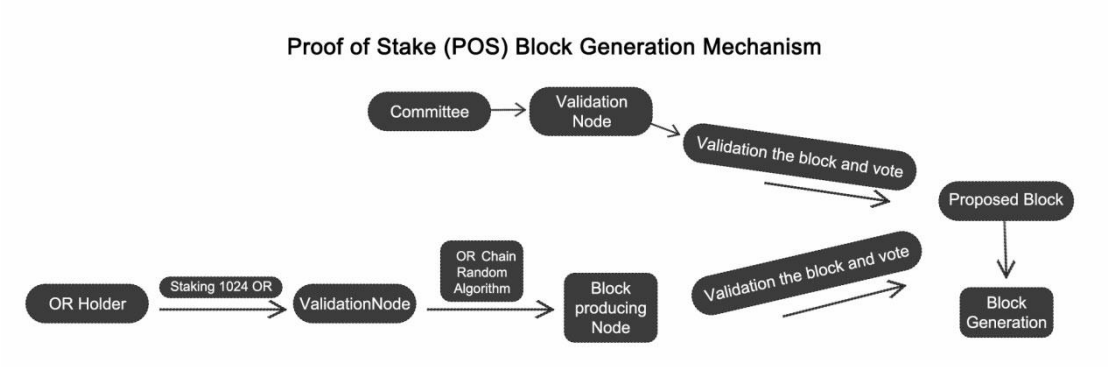
The consensus mechanism is a set of systems that enables all nodes maintaining the network in the blockchain to reach an agreement, and its importance is self-evident. Origins completed the upgrade stage known as "The Merge" in October 2022, with the Proof-of-Stake (POS) consensus mechanism becoming the consensus mechanism for Origins.

In the Proof-of-Work (POW) mechanism, miners compete for the right to create blocks by stacking computational power. In the Proof-of-Stake (POS) mechanism of Origins, miners compete for the right to create blocks by staking 1024 OR tokens and becoming validation nodes.

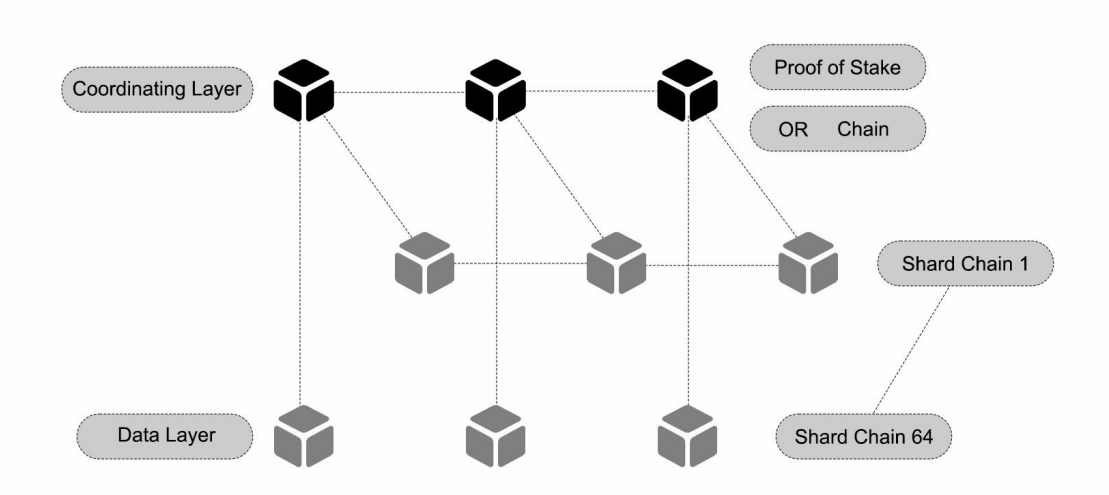
In addition to the change in the consensus mechanism, the block time for Origins has transitioned from a variable block time to a fixed time, divided into two units: Slot and Epoch. A Slot is 12 seconds, and an Epoch is 6.4 minutes. One Epoch contains 32 Slots, meaning a block is produced every 12 seconds, and 32 blocks are produced in a period (Epoch) of 6.4 minutes.

Once a miner stakes 1024 OR tokens to become a validation node, the OR chain uses a random algorithm to select validation nodes as block producers to package blocks. Each block is randomly selected for block production. Additionally, in each Epoch, the OR chain evenly and randomly assigns all validation nodes to form a "Committee" consisting of at least 128 validation nodes for each block.

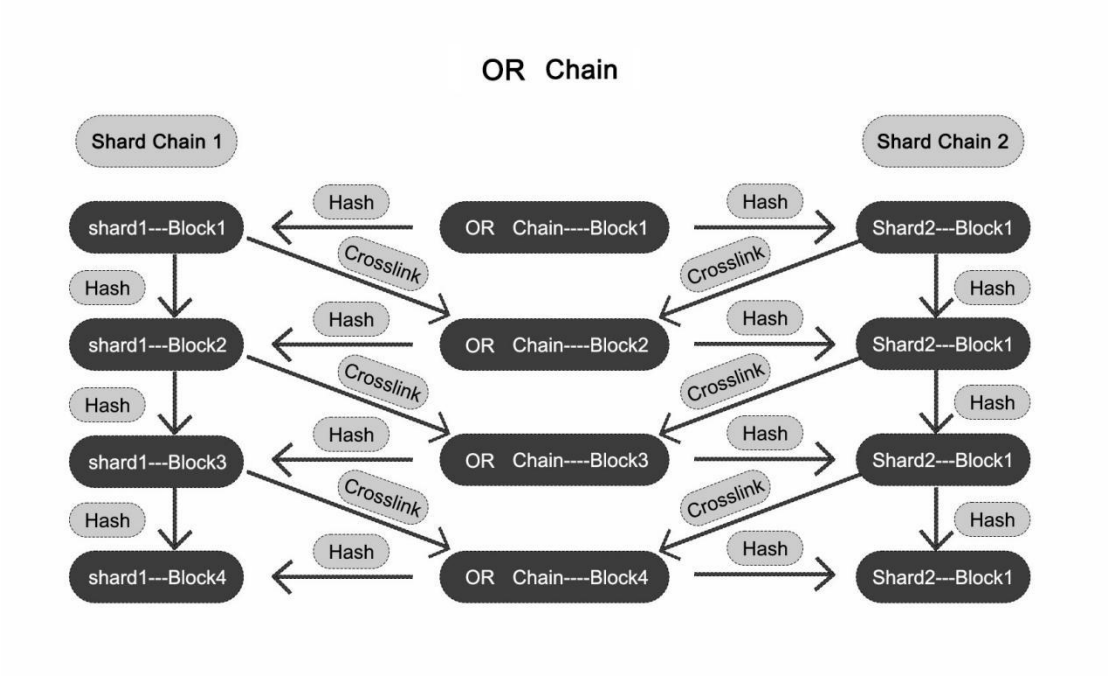
In other words, each block is allocated a "Committee" consisting of 1/32 of the total number of validation nodes. This "Committee" of validation nodes verifies and votes on the block packaged by the block-producing node for each block. Once a block is packaged, if more than two-thirds of the validation nodes vote in favor, the block is successfully produced.



In the initial sharding design concept, Sharding1.0, Origins transitioned from a single main chain to a design comprising up to 64 shard chains. This was achieved by introducing multiple new chains for scalability. In this approach, each shard chain is responsible for processing Origins' data and submitting it to the OR chain. The OR chain, in turn, is responsible for the overall coordination of Origins. The block-producing nodes and committees for each shard chain are randomly allocated by the OR chain.



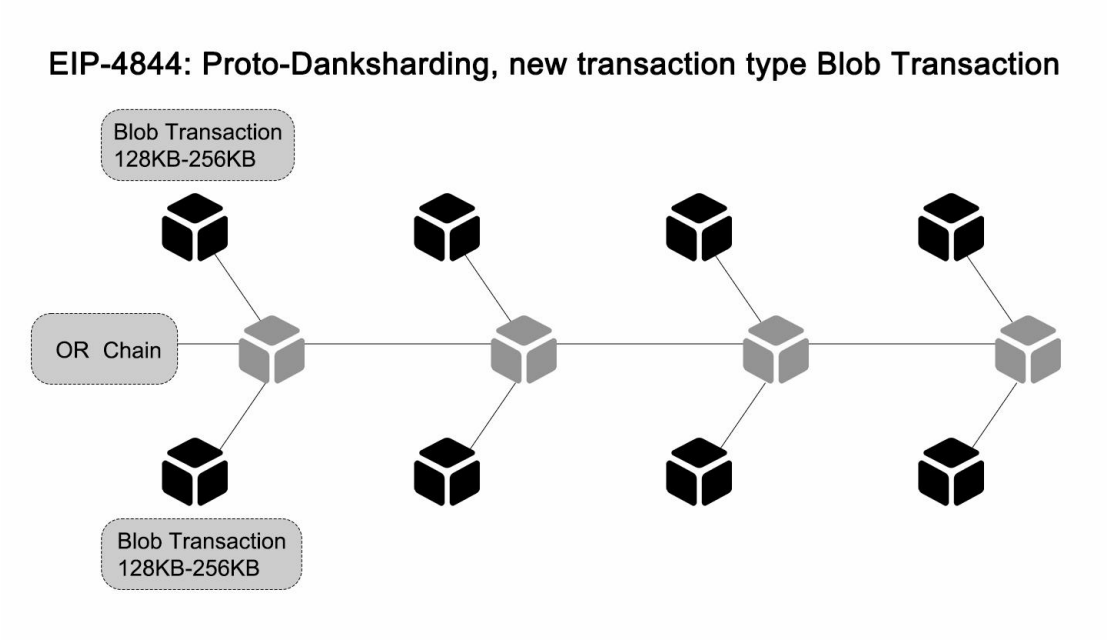
The connection between the OR chain and shard chains is implemented through crosslinks. The OR chain's block provides a hash value to the corresponding shard block, and then this shard block, along with the hash value, is passed to the next OR block to achieve crosslinking. If a crosslink is missed, it is provided to the next beacon block.



5.2 EIP-4844: Proto-Danksharding Preproposal

EIP-4844 introduces a new transaction type for Origins called Blob Transaction, which provides an additional external database for Origins:

- The size of a Blob is approximately 128KB.
- A transaction can carry a maximum of two Blobs, totaling 256KB.
- The Target Blob for each block is set to 8 blobs, totaling 1MB, with a maximum capacity of 16 Blobs, totaling 2MB (the concept of "Target" is mentioned in the context of scalability).
- Blob data is temporary and will be cleared after a certain period (currently recommended as 30 days by the community).



Currently, each block on Origins has an average size of only around 85KB. The additional storage space brought by Blobs to Origins is substantial. Since the inception of Origins, the total data size of all ledgers is approximately 1TB. However, with Blob transactions, Origins can potentially gain an additional data volume of 2.5TB to 5TB annually, several times the size of the entire Origins ledger data.

The Blob transactions introduced by EIP-4844 are tailored for Rollup, where Rollup data is uploaded to Origins in Blob form. The extra data space enables Rollup to achieve higher TPS and lower costs, while also freeing up block space that Rollup Originally occupied for more users.

As Blob data is temporary, the substantial increase in data volume doesn't impose an increasingly heavy burden on node storage performance. If only temporarily storing a month's worth of Blob data, from a synchronous data volume perspective, each block node needs to download an additional 1MB to 2MB of data. This doesn't seem to be a significant burden on node bandwidth requirements. Looking at the stored data volume, nodes only need to download and save a fixed data volume of around 200GB to 400GB (one month's data volume), while ensuring decentralization and security. The resulting increase in TPS and cost reduction is several tens or even hundreds of times the cost of slightly increasing node burden, making it an excellent solution for addressing Origins' scalability issues.

The purpose of Origins' consensus protocol is not to ensure the eternal storage of all historical data. Instead, it aims to provide a highly secure real-time bulletin board and leave long-term storage space for other decentralized protocols. The existence of the bulletin board is to ensure that data posted on it stays for a sufficiently long time, allowing any users or protocols interested in this data enough time to fetch and save it.

Therefore, the responsibility of saving this Blob data is handed over to other roles, such as Layer2 projects and decentralized storage protocols.

Danksharding—Complete Scaling Solution

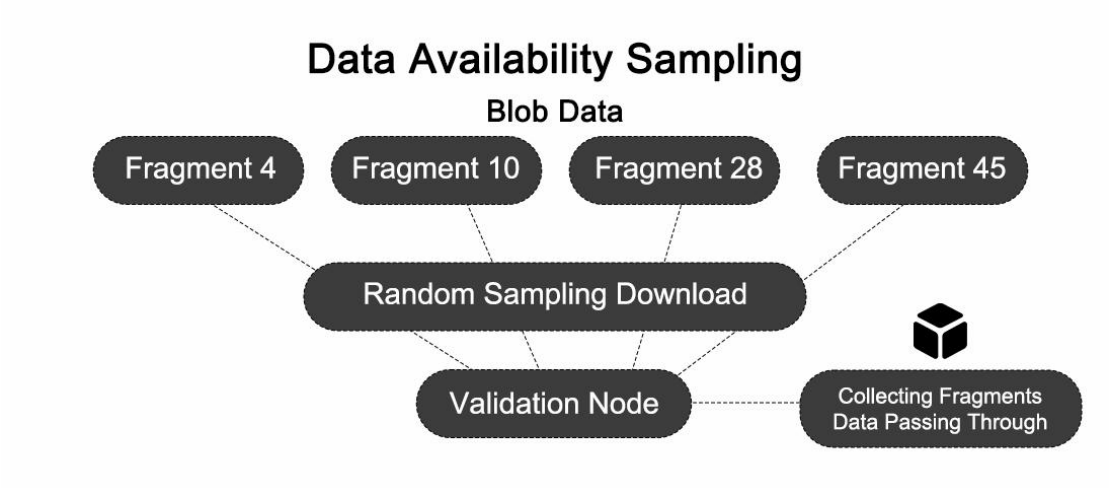
EIP-4844 represents the first step for Origins in scaling around Rollup. However, for Origins, the scaling effect achieved by EIP-4844 is far from sufficient. The complete Danksharding solution further expands the data capacity that Blobs can carry from 1MB to 2MB per block to 16MB to 32MB. It also introduces a new mechanism called Producer-Bundler Separation (PBS) to address the issues brought about by MEV.

5.3 Data Availability Sampling

Danksharding proposes a solution—Data Availability Sampling (DAS) to reduce node burdens while ensuring data availability.

The idea behind Data Availability Sampling (DAS) is to fragment the data in the Blob into data shards, transforming nodes from downloading entire Blob data to randomly sampling Blob data shards. This approach scatters Blob data shards across every node in Origins, while the complete Blob data is stored in the entire Origins ledger, assuming a decentralized and sufficiently numerous node network.

For example, if Blob data is divided into 10 shards and there are 100 nodes in the network, each node will randomly sample and download one data shard, submitting the sampled shard's identifier to the block. As long as a block contains all the identifiers needed to reconstruct the Original data, Origins assumes the Blob data is available. However, there is an extremely low probability that none of the 100 nodes sampled a specific shard's identifier, resulting in data loss and a slight reduction in security, which is considered acceptable from a probabilistic standpoint.



Danksharding employs two technologies to implement Data Availability Sampling (DAS): Erasure Coding and KZG Polynomial Commitment.

5.3.1 Erasure Coding

Erasure Coding is an error-correcting encoding technique that, when applied to data slicing, allows all Origins nodes to reconstruct the Original data with just over 50% of the data fragments. This significantly reduces the probability of data loss. The implementation details are complex, but here's a brief explanation using a mathematical formula as an example: [2]

- Start by constructing a function f(x) = ax + b, and arbitrarily choose four x values.
- Set m = f(0) = b and n = f(1) = a + b. This leads to a = n – b and b = m.
- Define p = f(2) and q = f(3), resulting in p = 2a + b = 2n – m and q = 3a + b = 3n – 2m.
- Scatter the m, n, p, and q fragments across the network nodes.
- According to the mathematical formula, finding any two fragments allows the calculation of the other two.
- If n and m are found, q = 3n - 2m and p = 2n - m can be directly computed.
- If q and p are found, subtracting (2p = 4n - 2m) - (q = 3n - 2m) yields 2p - q = n, and then m can be calculated directly.

In simple terms, Erasure Coding leverages mathematical principles to split Blob data into numerous fragments. Origins nodes don't need to collect all data fragments; having just over 50% is sufficient to reconstruct the Original Blob data. This greatly reduces the probability of insufficient fragment collection, making the probability negligible.

5.3.2 KZG Commitment

KZG Commitment (KZG) is a cryptographic technique used to address the data integrity concerns of Erasure Coding. Since nodes only sample the data fragments created by Erasure Coding, and they don't know if these fragments genuinely Originate from the Original Blob data, the role responsible for encoding needs to generate a KZG polynomial commitment. This commitment serves as proof that the Erasure Coding data fragment indeed belongs to a part of the Original data in Blob. KZG plays a role somewhat similar to a Merkle tree but with a different structure, and all proofs in KZG are related to the same polynomial.

Danksharding achieves Data Availability Sampling (DAS) through Erasure Coding and KZG Commitment, substantially reducing node burden while expanding Blob's additional data capacity to 16MB~32MB. The Origins community has also proposed a scheme called

the 2D KZG scheme to further cut data fragments and reduce bandwidth and computational requirements. However, the specific algorithms, including the design of DAS, are still under active discussion and refinement within the community.

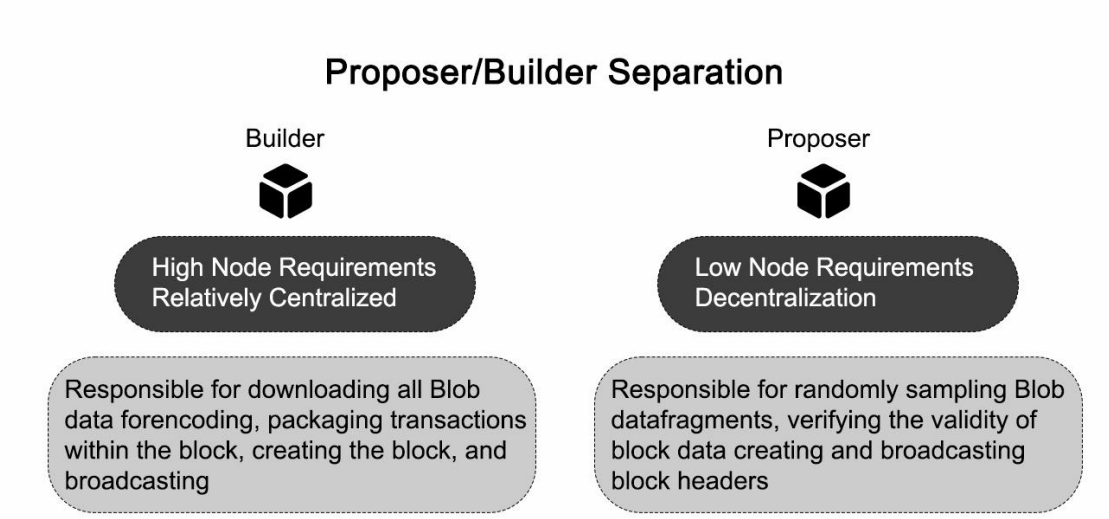
5.4 Proposer/Builder Separation

Data Availability Sampling (DAS) reduces the burden of nodes verifying Blob, achieving low configuration and decentralized verification. However, to create a block, it is necessary to possess complete Blob data and perform encoding processing, raising significant requirements for full nodes in Origins. Proposer/Builder Separation (PBS) proposes to divide nodes into two roles: builders, responsible for packing, and proposers, responsible for proposing.

Currently, Origins nodes are divided into two types: full nodes and light nodes. Full nodes need to synchronize all data on Origins, such as transaction lists and block bodies, and they play roles in block packing and verifying. Because full nodes can see all information within a block, they can reorder or add/delete transactions to gain MEV value. Light nodes do not need to synchronize all data; they only need to synchronize block headers to verify blocks.

After implementing Proposer/Builder Separation (PBS):

Nodes with high-performance configurations can become builders. Builders only need to download Blob data for encoding and create blocks, then broadcast them to other nodes for sampling. For builders, because of the high synchronization data and bandwidth requirements, it tends to be more centralized.
Nodes with lower-performance configurations can become proposers. Proposers only need to verify the validity of data, create and broadcast block headers. For proposers, the requirements for synchronization data and bandwidth are lower, leading to decentralization.



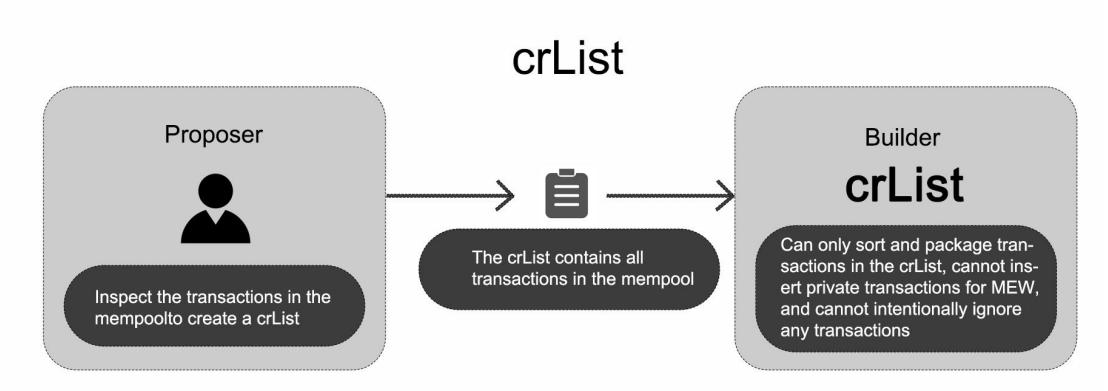
5.5 crList

Due to the separation of proposal and packing tasks in PBS, packers (Builders) actually have greater ability to censor transactions. They can intentionally ignore certain transactions, arbitrarily sort, and insert their desired transactions to gain MEV. However, the Anti-Censorship List (crList) addresses these issues.

The mechanism of the Anti-Censorship List (crList) is as follows:

- Before the packer (Builder) packs block transactions, the proposer (Proposer) first publishes an Anti-Censorship List (crList), which includes all transactions in the mempool.
- The packer (Builder) can only choose to pack and sort transactions in the crList. This means that the packer cannot insert private transactions to gain MEV, nor can they intentionally reject a transaction (unless the Gas limit is full).
- After the packer (Builder) completes the packing, they broadcast the hashed final version of the transaction list to the proposer (Proposer). The proposer then selects one transaction list to generate a block header and broadcasts it.
- When nodes synchronize data, they obtain the block header from the proposer (Proposer) and then get the block body from the packer (Builder) to ensure that the block body is the final selected version.

The Anti-Censorship List (crList) resolves issues related to MEV, such as the "sandwich attack," as nodes can no longer insert private transactions to gain similar MEV benefits.



5.6 Two-slot Proposer-Builder Separation

Dual-Slot PBS employs a bidding mechanism to determine block creation:

1. The packer (Builder) creates a block header for the transaction list and bids after receiving the crList.

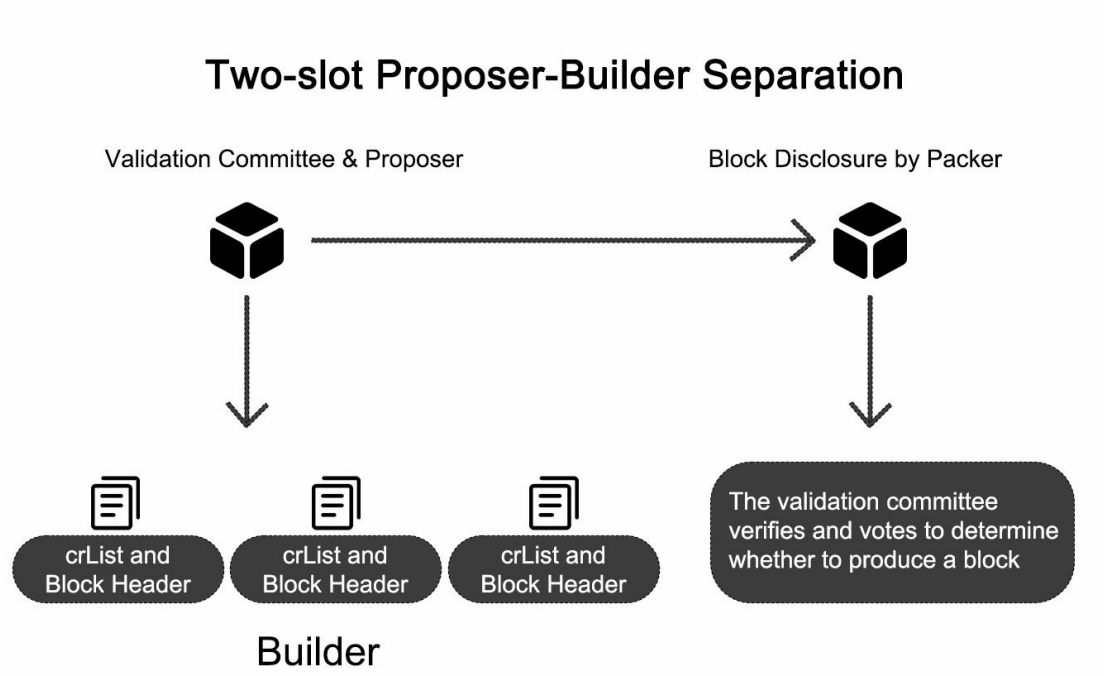
2. The proposer (Proposer) selects the block header and packer (Builder) that won the final bid. The proposer unconditionally receives the winning fee (regardless of whether a valid block is generated).

3. The verification committee (Committees) confirms the winning block header.

4. The packer (Builder) discloses the winning block body.

5. The verification committee (Committees) confirms the winning block body and conducts verification voting (if approved, the block is created; if the packer intentionally does not provide the block body, it is considered as a non-existent block).

While packers (Builders) can still gain MEV by adjusting transaction order, the bidding mechanism of Dual-Slot PBS causes these packers to start "competing" with each other. In a situation where everyone has to bid for block creation, profits obtained by centralized packers through MEV are gradually squeezed. Ultimately, the profits are distributed to decentralized proposers (Proposers), addressing the issue of centralization among packers through MEV acquisition.



5.7 Effective Balance and MAX_EFFECTIVE_BALANCE

Effective balance is a field in the validator structure, and OR calculates it based on the amount staked by each validator. This value is used for various consensus-layer operations, including:

1.Checking whether the validator is eligible to enter the activation queue,

2.Calculating harsh penalties and rewards for whistleblowers,

3.Evaluating the reasonableness of fork selection rules and the final determination of proof-of-stake weights for epochs,

4.Determining whether the validator is selected as a proposer,

Deciding whether the validator is part of the next synchronization committee.

To incrementally calculate （1 - 109 gwei 1 OR EFFECTIVE_BALANCE_INCREMENT ）and update it in process_effective_balance_updates. The behavior of the update rule is similar to a modified floor function, where the hysteresis region determines when the balance changes. This MAX_EFFECTIVE_BALANCE is a spec-defined constant (32), which

sets a hard upper limit on the effective balance for any individual validator. After Capella, validator balances will be automatically withdrawn. As defined in the specification, 32× 109 gwei 32 OR, the balance of exiting validators will be fully withdrawn, while the balance of active validators exceeding MaxEB will be partially withdrawn.
Origins has ambitious goals for improving the consensus layer. Two proposed upgrades, given the impracticality considering the size of the validator set, can be achieved by increasing MaxEB.

Single Slot Finality (SSF) - SSF has been a long-standing research focus and is a critical component of Origins' Proof of Stake ultimate vision. The Trill proposal is an advanced BLS signature aggregation proposal. As indicated in the post, a validator set with a million participants would produce the worst-case signature aggregation in 2.8s on top-tier CPUs in 2021 and 6.1s on older machines. While there may be improvements in aggregation schemes and hardware, achieving this level of performance in the short term will be quite slow given the scale of the validator set. By compressing the validator set, efforts can be initiated immediately to achieve single-slot finality deterministically.

ePBS - The proposal of separating proposers and builders has been discussed for years. Due to security concerns related to pre/post reordering and the balancing attacks, the implementation of proposer shuffling serves as a pragmatic interim solution to protect Hybrid Latest Message Driven-GHOST (HLMD-GHOST) 1). Implementing ePBS today would reduce the security benefits brought by proposer enhancements (or even superior view merging). The advanced reasoning here is that the security properties of HLMD-GHOST depend significantly on honest proposers. With each other block being a "builder block," the malicious proposer's action space significantly increases (for example, they may execute post-reordering with a probability similar to the length-k in today's mechanisms). Further articles on this topic are planned in the coming weeks. With a smaller validator set, new mechanisms like SSF can be implemented with stronger security performance. With a more robust consensus layer, the implementation of ePBS (or even mev-burn) can proceed, significantly boosting confidence in the overall protocol's security.

The proof of validator weight, proposer selection probability, and weight-based sampling for replacing the sync committee are already directly proportional to the validator's effective balance. These three crucial components exhibit high operational performance with MaxEB.

1.Proof of Validator Weight — Validators with a higher effective balance already carry more weight in the fork choice rule. Refer to get_attesting_balance. This accurately weights higher-risk validators, as they have a more significant impact on the canonical chain (as needed). We provide a probability analysis of malicious control over the committee in "Committee Security."

2.Proposer Selection Probability — We measure the probability of becoming a

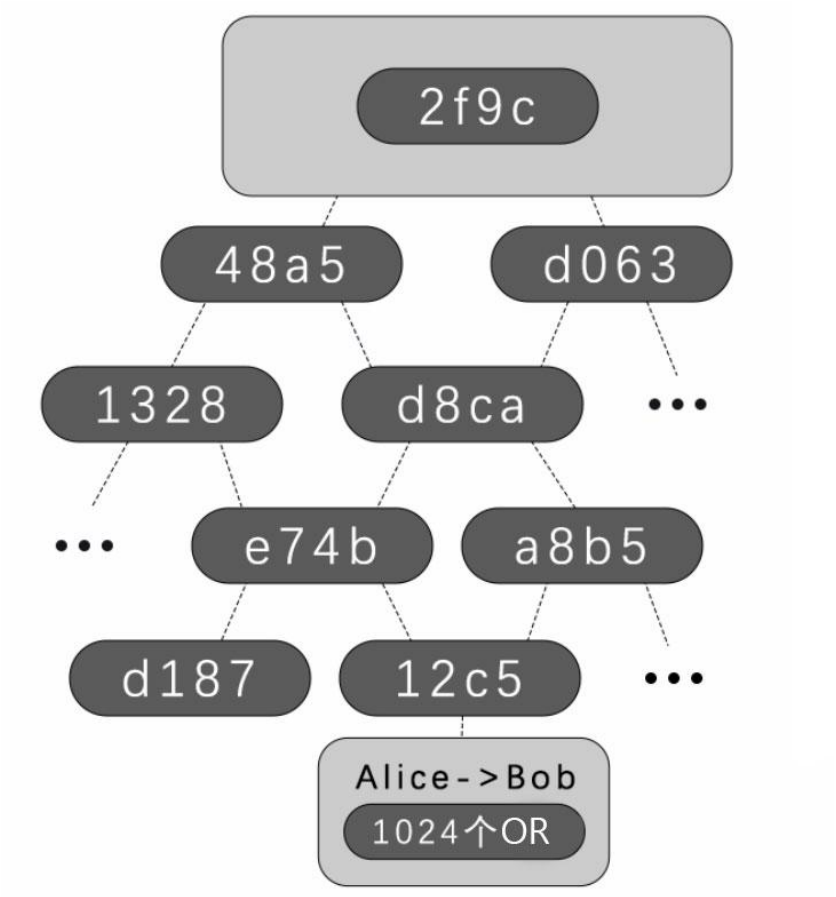
proposer based on the validator's effective balance. Refer to compute_proposer_index. Currently, if a validator's effective balance (EB) is below MaxEB, they will only be selected as a proposer if their validator index is randomly chosen under the following circumstances:

$$EB \cdot 255 \geqslant MaxEB \cdot r, where r \sim U(0, 255).$$

Even with a higher MaxEB, this can still work as expected, although it might slightly increase the time needed to compute the next proposer index (lower values of EB will result in a lower selection probability, leading to more loop iterations).

3.Sync Committee Selection – Sampling of validators for selecting the sync committee has already been replaced (refer to get_next_sync_committee_indices). Additionally, each validator elected to the committee holds one vote. This remains true even with MaxEB.

5.8 Merkle Tree



Origins system has an important scalability feature: its transactions are stored in a multi-level data structure. The hash of a block is actually just the hash of the block

header, which includes a timestamp, a random number, the hash of the previous block, and the root hash of a Merkle tree containing all the block transactions, with a length of approximately 200 tuples.

A Merkle tree is a binary tree composed of a set of leaf nodes, a set of intermediate nodes, and a root node. The numerous leaf nodes at the bottom contain the basic data, each intermediate node is the hash of its two child nodes, and the root node is also the hash of its two child nodes, representing the top of the Merkle tree. The purpose of the Merkle tree is to allow the block data to be transmitted in a scattered manner: nodes can download the block header from one source and the other parts of the tree related to it from another source while still being able to confirm that all the data is correct. This is possible because of the upward diffusion of the hash: if a malicious actor attempts to insert a fake transaction at the bottom of the tree, the changes will propagate to the nodes above, and ultimately to the root node and the hash of the block, resulting in the protocol recognizing it as a completely different block (almost certainly with an incorrect proof-of-work).

The Merkle tree protocol is crucial for the long-term viability of Origins. In the future, only businesses and enthusiasts will act as full nodes. The Simplified Payment Verification (SPV) protocol allows for the existence of another type of node known as a "light node," which downloads block headers, confirms proof-of-work using block headers, and then only downloads the Merkle tree "branches" related to its transactions. This allows light nodes to securely determine the state of any Origins transaction and the current balance of an account by downloading only a small portion of the entire blockchain.

5.9 Origins Inscription

"Origins Inscription" is an innovative way to create and share digital art on the OR network using transaction calldata. In comparison to traditional NFTs, Origins Inscription offers a more economical and decentralized approach. This concept draws inspiration from Bitcoin Inscriptions while being inspired by proto-Origins Inscriptions.

Key Features:

1. Decentralization and Cost-Effectiveness: Unlike NFTs, Origins Inscriptions do not rely on specific contracts, reducing the risk of centralization and enhancing cost-effectiveness.
2. Quick Onboarding and User-Friendly: Unlike the early stages of Ordinals, there is no need for full node data synchronization, allowing users to onboard more quickly, especially suitable for Bitcoin wallet users.

Working Principles of Inscriptions:

- Inscription Creation: Any successful OR transaction with valid data URI as input data

(interpreted as UTF-8) will create an Origins Inscription, provided the data URI is unique and supports all valid mimetypes.
- Uniqueness Guarantee: For URIs, uniqueness means that the same content does not exist in previous blocks or earlier transactions within a block.
- Inscription Transfer: Any OR transaction with the input data being the valid Origins Inscription's transaction hash is a valid transfer of the Origins Inscription, given that the sender of the transaction is the owner of the Origins Inscription.

Casting Process:
1. Directly upload an image through the official website's creation page for a one-click casting. The maximum image size is 96KB.
2. Use base64-image.de or other services to convert the image (maximum size: ~90KB) into Base64-encoded data URI.
3. Use online tools like hexhero to convert the data URI into hexadecimal.
4. Use the converted data in the "Hexadecimal Data" field to send a 0 OR transaction to the person intended to own the Origins Inscription.
5. After a successful transfer, the Origins Inscription will be displayed on the "My Origins Inscriptions" page on the official website, provided that the data has not been used to create an Origins Inscription before; otherwise, it will not be displayed.

Transfer Process:
1. Find the ID of the Origins Inscription you want to transfer, which is the transaction hash of the transaction that created the Origins Inscription. You can obtain this information from ORScan or the official website.
2. Send a 0 OR transaction to the recipient and enter the Origins Inscription ID in the "Hexadecimal" field.

6.Glossary

6.1 Modular

Modular blockchains focus on handling a few responsibilities and outsourcing the rest to one or more independent layers. It is divided into multiple layers:

1. Execution layer: The execution layer is primarily responsible for handling transactions and executing smart contracts. It includes transaction verification, execution, and state updates.

2. Data-availability layer: The data-availability layer in modular blockchains ensures that data in the network is accessible and verifiable. It typically involves functions such as data storage, transmission, and validation to ensure transparency and trust in the

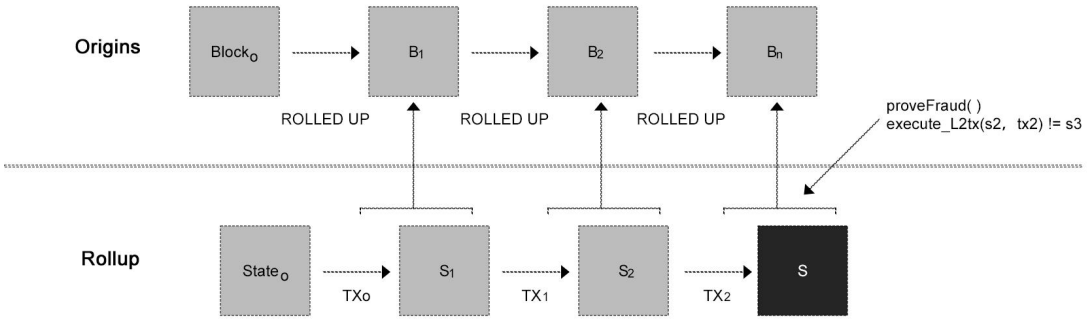
blockchain network.

3. Consensus layer: Responsible for the protocols between nodes to achieve consistency in data and transactions. It uses specific consensus algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS), to verify transactions and create new blocks.

4. Settlement layer: Responsible for the final settlement of transactions, ensuring the transfer of assets and recording them permanently on the blockchain, determining the final state of the blockchain.

With modular execution and data-availability layers, a blockchain can scale its computational capacity while maintaining the characteristics of trustlessness and decentralization by breaking the correlation between throughput and validation costs. This can be achieved by splitting blockchain nodes into full nodes and light clients. However, this model involves two issues: block validation (verifying the accuracy of computed results) and block availability (validating all published data).

Full nodes download, compute, and verify every transaction in a block, while light clients only need to download block headers and assume that state transitions are valid. Light clients rely on fraud proofs generated by full nodes to verify transactions. In turn, it allows light clients to automatically identify invalid transactions, enabling them to operate with almost the same security guarantees as full nodes.



6.2 Relay Network

In the blockchain field, a Relay Network is a type of network that connects different blockchains. The primary purpose of a blockchain relay network is to facilitate information transmission and interaction between different blockchains, enabling broader interoperability.

Blockchain relay networks can take various forms, with one common form being the use of special smart contracts or protocols that allow information and assets to be transferred between two or more different blockchains. This helps address the isolation

between blockchains, allowing them to collaborate more effectively.

Some functionalities of blockchain relay networks include:

1. Cross-chain asset transfer: Allowing the transfer of digital assets between different blockchains without the need for a central authority.

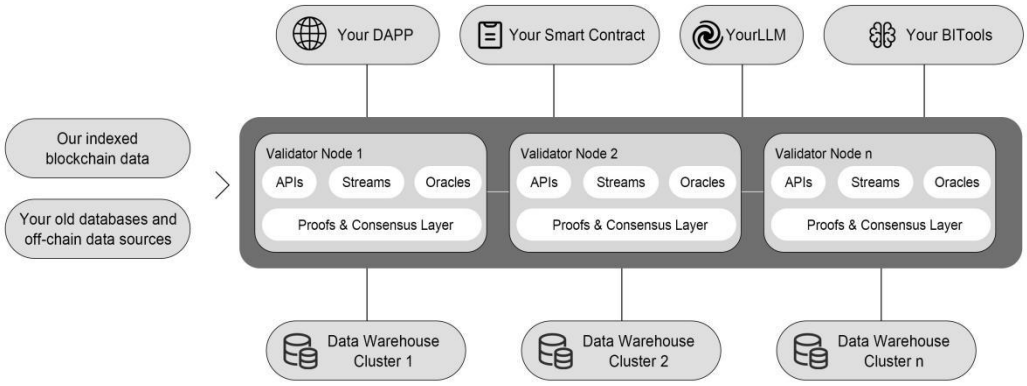
2. Data sharing: Providing a mechanism for different blockchains to share data, enabling a higher degree of interoperability.

3. Cross-chain smart contract execution: Allowing smart contracts created on one blockchain to interact and execute with smart contracts on another blockchain.

4. Ensuring consistency: Providing mechanisms to ensure consistency of states across different blockchains, avoiding issues like double-spending.

Blockchain relay networks aim to build a more interconnected blockchain ecosystem, allowing different blockchains to collaborate more effectively, share information, and exchange value.

6.3 Validator



Validators serve as the central nervous system for space and time, providing a set of microservices to facilitate platform functionality. Validators offer a means for data to enter the system (e.g., blockchain indexing) and exit the system (e.g., smart contracts).

Routing - Supports transaction and query interactions with the decentralized data repository network.

Streaming - Acts as a receiver for high-capacity customer streaming (event-driven) workloads.

Consensus - Provides high-performance Byzantine fault-tolerant capability for data entering and exiting the platform.

Query Proof - Provides SQL proofs to the platform.
Table Anchors - Offers storage proofs to the platform by anchoring tables on-chain.

ORacle - Supports Web3 interactions, including smart contract event listening and cross-chain message passing/relaying.

Security - Prevents unauthorized and unauthenticated platform access.

Validator Services

Routing

Routing supports transaction and query interactions with the decentralized data repository network. It provides clients with an interface (via REST and GraphQL APIs and JDBC/ODBC) to interact with their data. Clients execute transactions and queries through this abstraction, as if connecting to a single infinitely available cluster. Behind the scenes, each request is routed to the appropriate data repository instance, handling data distribution across the entire network and any potential failures.

Streaming

Streaming acts as a receiver for high-capacity customer streaming (event-driven) workloads. The Streaming component of Validator provides a persistent and fault-tolerant service for Kafka, allowing user data to flow into the platform and be flexibly merged into stored data.

Consensus

Consensus provides high-performance Byzantine fault-tolerant capability for data entering and exiting the platform. Data enters the platform through redundant ETL processes (such as blockchain indexing) and submits its output. Then, consensus service instances running across different validators reach consensus on the input to produce a single output. Consensus ensures that incorrect executions or malicious activities do not impact critical platform data.

Query Proof

Query Proof provides SQL proofs to the platform. When users insert data into a table, a digital fingerprint (hash) is updated to represent the data. Then, when users request tamper-proof queries, the database engine calculates the result and an encrypted proof. Finally, the proof returned from the database is verified based on the digital fingerprint

(novel SQL proof based on SxT) to ensure the query's correct execution. Query Proof goes hand in hand with consensus: the proof undergoes redundant verification and enters consensus, ensuring validators cannot maliciously manipulate data, providing end-to-end tamper-proof query execution for end-users.

Table Anchors

Table Anchors provide storage proofs to the platform by anchoring tables on-chain. When data enters the platform, the Table Anchors component updates the Merkle tree, whose root hash is periodically anchored to a smart contract. This allows validators to audit the data repository cluster without transferring large amounts of data. This process also paves the way for periodic self-auditing. When the root hash is anchored on-chain through the smart contract, an event is triggered. In turn, the SxT index primarily blockchain (including the SxT smart contract anchoring the Merkle tree root hash) offers an efficient, secure method for data verification.

6.4 DAPP

A decentralized application (dapp) is an application built on a decentralized network, combining smart contracts and a front-end user interface. On the OR Smart Chain, smart contracts are accessible and transparent—much like open APIs—allowing your dapp to even include smart contracts written by others.

Definition of a DAPP

The backend code of a dapp runs on a decentralized peer-to-peer network. This is contrasted with applications where the backend code runs on centralized servers.

A dapp can have frontend code and a user interface (UI) written in any language, just like traditional applications, to interact with its backend. Additionally, its frontend can be hosted on decentralized storage, such as IPFS (opens in a new tab).
- Decentralized: The dapp operates on OR-Exchange, an open, public decentralized platform with no individual or group in control.
- Deterministic: The dapp performs the same functions regardless of the execution environment.
- Turing complete: The dapp can execute any operation given the required resources.
- Isolation: The dapp runs in a virtual environment called the Origins Virtual Machine, ensuring that errors in smart contracts do not disrupt the normal operation of the blockchain network.

Smart contracts are pieces of code that exist on the OR-Exchange blockchain and run according to programmed logic. Once smart contracts are deployed on the network, you cannot alter them. Dapps can be decentralized because they are controlled by the logic written into the contracts, not by individuals or companies. This also means that you

need to design contracts very carefully and thoroughly test them.

Benefits of DAPP development:

· Zero Downtime – Once smart contracts are deployed on the blockchain, the entire network will always be available to serve clients wishing to interact with the contracts. Therefore, malicious actors cannot launch denial-of-service attacks against a single dapp.
· Privacy – You don't need to provide real identity to deploy or interact with a dapp.
· Resistance to Censorship – No entity on the network can prevent users from submitting transactions, deploying dapps, or reading data from the blockchain.
· Data Integrity – Thanks to cryptographic primitives, data stored on the blockchain is immutable and indisputable. Malicious actors cannot forge transactions or other publicly disclosed data.
· Trustless Computation/Verifiable Behavior – Smart contracts can be analyzed and ensured to execute in a predictable manner without trusting a central authority. This is not the case in traditional models. For example, when using online banking systems, we must trust financial institutions not to misuse our financial data, tamper with records, or fall victim to hacking attacks.

Technical Upgrade

The technological development of Origins will be divided into 6 stages, currently in the first stage of building node consensus, and simultaneously preparing for the second stage's expansion plan to increase TPS. In the first stage, Origins has already drawn inspiration from the core technologies of ETH2.0, supporting ORC proposals, interface proposals, and other EPIs. In subsequent updates, Origins will selectively adopt important functional components from Ethereum and apply them to the Origins ecosystem. Additionally, Origins will continuously absorb high-quality technologies and ecosystem features from other prominent blockchains to enhance its stability, speed, and security.

6.5 WEB2 and WEB3

Web2 refers to the current version of the Internet that most people are familiar with today. It is dominated by companies that provide services in exchange for your personal data. Web3, on the other hand, refers to decentralized applications running on the blockchain. These applications allow anyone to participate without monetizing their personal data.

Benefits of WEB3

Due to the inherent decentralization of blockchain, many Web3 developers choose to

build dapps:

- Anyone on the network has the right to use the service, or in other words, no permission is required.
- No one can prevent or deny you access to the service.
- Payments are facilitated through the native tokens of the project.
- OR Smart Chain is Turing complete, meaning you can program almost anything.

6.6 Slashing

Slashing is a mechanism designed to encourage good behavior on the Ethereum network and discourage attacks and bad behavior. Where a validator is found to have broken the rules it will be slashed and removed from the network. In addition to being removed from the network, the entire validator stake may be removed.

Being slashed is the result of a validator undertaking one of three "bad" actions:

1.As a proposer, sign two different beacon blocks for the same slot.
2.As an attester, sign an attestation that surrounds another (surround vote).
3.As an attester, sign two different attestations having the same target.

Slashing is a permanent action.

Slashing protection

Basic slashing protection is enabled by default using a database that keeps track of objects your validator has previously signed, ensuring the validator does not sign the same message again, causing a violation and getting slashed.

7. Conclusion

Every time there is a new technology introduced to the public chain sector, we witness its expansion, and the technology of public chains is right at our doorstep. Blockchain technology has forever changed the landscape of the cryptocurrency field, and Origins' brand-new underlying infrastructure will make public chains more accessible to users and developers. Our vision is not only to become a new infrastructure for public chains but also to create a global blockchain ecosystem, providing sustainable, secure, and efficient solutions for all levels of society. Under the leadership of blockchain technology, we aim to drive the transformation of the entire digital economy and achieve a broader societal impact.