Avail DA

Build with Avail DA, the validity proven data availability layer unifying Web3

Avail DA is built to meet the needs of next-generation, trust-minimized applications and sovereign rollups. It's strengths lie in its innovative security approach, which allows light clients to easily verify data availability through sampling over a peer-to-peer network. Our modular approach simplifies blockchain integration for developers, as they no longer need to worry about validator sets or tokenomics. With Avail DA's unparalleled data availability interface and powerful security capabilities, developers can create zero-knowledge or fraud-proof-based blockchain applications with greater efficiency and ease.

At its core, Avail DA prioritizes ordering and publishing transactions while enabling users to verify the availability of block data without needing to download entire blocks. Avail DA's data-agnostic nature is one of its defining features. It supports various execution environments, including EVM, WASM, and custom new runtimes, offering a versatile foundation for diverse blockchain applications.

Overview of L2 scailability In traditional blockchain networks, full nodes execute all transactions, ensuring integrity and security. However, while secure, this model limits throughput and scalability due to its comprehensive processing requirements. Layer 2 (L2) solutions emerged to address these constraints, offering enhanced performance by shifting the bulk of transaction execution away from the main chain (Layer 1).

Despite their advantages, L2 solutions face challenges in maintaining data availability and transaction integrity, especially in a manner that is both efficient and cost-effective. Rollups aim to mitigate these challenges by executing transactions off-chain and then posting aggregated results back to the main chain. This approach significantly reduces the strain on Layer 1, leading to lower operational costs and reduced transaction fees, offering a more scalable solution for blockchain networks.

Rollups come in two primary forms:

Optimistic Rollups:

Optimistic Rollups operate on a principle of presumed validity, where transactions are assumed to be valid unless proven otherwise. Their lifecycle involves:

1. Transaction Aggregation
2. : Transactions are gathered by sequencers and formed into a rollup block.
3. Block Submission
4. : This block is submitted to an Ethereum-based smart contract with a bond as a security measure.
5. Assumption of Validity
6. : Transactions are presumed valid upon submission.
7. Challenge Window
8. : A period for submitting fraud proofs, allowing challenges to the block's validity.
9. Outcome
10. :* Challenge Successful
11.
    - : The bond is forfeited, and the block is reversed.
12.
    - No Challenge
13.
    - : The block is finalized if unchallenged.

ZK Rollups:

ZK Rollups require upfront cryptographic proofs of transaction validity, focusing on security and data integrity. Their lifecycle involves:

1. Validity Requirement
2. : A validity proof must be provided before block submission.
3. Block Submission
4. : Blocks are submitted with the required validity proof.
5. Assumption of Validity
6. : Proof of validity is demanded upfront, unlike Optimistic Rollups.
7. Data Availability
8. : While validity proofs are independent of data availability, the chain's security heavily depends on it.
9. Implications of Data Unavailability
10. :* State Recreation
11.
    - : Users can not recreate the state if data is not available.
12.
    - Sequencer Intervention
13.

- : Other sequencers can step in to restore the state and continue operations.

Still, there are constraints with data availability.

Data Availability

What is the data availability problem? The data availability problem is a critical issue in blockchain and distributed ledger technologies, centering on the necessity to make all transaction data publicly accessible and verifiable across the network. This challenge is integral to the blockchain's integrity and security.

In blockchain systems, each block's transaction data requires verification by network nodes. The problem emerges when nodes strive to validate new blocks by downloading and verifying their transaction data. The crux of this issue is not just in publishing data but in ensuring its reliable distribution across the network, guaranteeing equal access to all participants.

The data availability problem is particularly significant in L2 networks in due to several reasons:

- Off-Chain Transactions
- : L2 solutions process transactions off the main chain to improve scalability. However, this can lead to challenges in verifying that all transaction data is complete and accurate, since it's not immediately recorded on the L1 blockchain.
- Security Dependence on Layer 1
- : While L2 networks operate independently for transaction processing, they rely on L1 for security. Ensuring complete and accurate data transfer from L2 to L1 is vital for maintaining the integrity of the overall network.
- Resolution Mechanisms Dependence on Data
- : L2 networks may use mechanisms like fraud proofs for dispute resolution. The effectiveness of these mechanisms hinges on the availability and accessibility of transaction data.
- Transparency and Trust Issues
- : Transparency is a core principle of blockchain technology. In L2 networks, any compromise in data availability can lead to trust issues, as users may not be able to independently verify transactions.
- Increased Complexity in Verification
- : The addition of L2 adds complexity in ensuring that data is accurately reported back to the main chain. This increases the risk of data availability issues, impacting the network's reliability.

Data Availability in Layer 2s

Data availability in L2 solutions can be classified into two methods:

- On-Chain Data Availability
- : All transaction data is stored on the L1 chain, offering higher security but at a greater cost.
- Off-Chain Data Availability
- : Data is stored off-chain, with only cryptographic summaries (hashes) on-chain. This method is cost-effective but depends on external entities for data retrieval.

These methods emphasize the role of L2s in enhancing state management and interaction with L1.

Taking Layer 2 Data Off-Chain

Adaptations of rollups represent a class of scalability solutions that offer off-chain data availability while maintaining the integrity of transaction processing. These solutions are the following:

- Validiums: ZK Rollups + Off-Chain DA
- Optimiums: Optimistic Rollups + Off-Chain DA
- Volitions: ZK Rollups + Validiums
- Sovereign Rollups: Independent Rollups with Custom DA and Security Models

Moving data availability off-chain inherently incorporates additional trust dependencies due to their reliance on external data managers.

What are Validiums? Validiums are a direct adaptation of ZK rollups, shifting data availability off-chain while continuing to use validity proofs.

They represent a class of scaling solutions characterized by off-chain computation and robust validity proofs. Unlike traditional approaches, Validiums do not store data on the Ethereum main chain, resulting in significantly enhanced transaction throughput. The cornerstone of these systems is using zero-knowledge proofs, such as ZK-SNARKs or ZK-STARKs. These cryptographic tools enable one party to confirm the truth of a statement to another without revealing any additional information beyond the statement's validity.

In Validiums, the integrity of all transactions is secured through these validity proofs, while data availability is maintained off-chain. This architecture allows users to execute withdrawals by providing a Merkle proof. Such proofs can attest to including a user's withdrawal transaction, enabling the on-chain contract to facilitate the withdrawal process.

Interactions between Validiums and Ethereum are orchestrated through a suite of smart contracts. The primary component in this setup is the main attestation contract. This contract stores state commitments, represented as Merkle data roots, which block producers submit. Additionally, a verification contract is critical in verifying the validity proofs during state transitions, ensuring the seamless integration and operation of Validiums within the Ethereum ecosystem.

What are Optimiums? Optimium are a direct adaptation of Optimistic rollups and also take data availability off-chain. They retain fraud-proof mechanisms for verification while boosting scalability.

At the heart of Optimiums lies the principle of assumed transaction validity. Transactions within this system are initially presumed to be valid. This assumption holds until proven otherwise, a process facilitated by fraud-proof mechanisms. These mechanisms are crucial in maintaining the integrity and reliability of the network. If a transaction is challenged and found to be fraudulent, it is reverted, ensuring the network's security and fidelity.

The key distinction of Optimiums from their traditional counterparts is the off-chain storage of transaction data. This strategic shift markedly increases network efficiency and scalability by reducing the data load on the main Ethereum chain. However, this also introduces new data retrieval and verification considerations, which are adeptly handled through the fraud-proof system.

In Optimiums, users can execute transactions and interact with the system seamlessly. Withdrawals are processed by submitting fraud proofs that validate the transaction's authenticity. These proofs serve as the cornerstone for ensuring that all operations within the network are legitimate and under the established rules.

The integration of Optimiums with the Ethereum main chain is managed via a set of specialized smart contracts. These contracts collectively oversee the transaction lifecycle, from submission to finalization, while ensuring that all data, though stored off-chain, remains accessible and verifiable as needed.

What are Volitions? Volitions represent a versatile approach in the realm of scaling solutions. They blend the features of ZK-Rollups and Validiums. This hybrid model offers flexibility in data storage, allowing users to choose between on-chain and off-chain data availability based on their specific requirements and preferences.

At their core, Volitions leverage zero-knowledge proofs, such as ZK-SNARKs or ZK-STARKs, to ensure the integrity and validity of transactions. This mechanism enables transaction verification without compromising privacy or revealing underlying data.

The unique feature of Volitions lies in their dual-mode operation. Users can opt for the ZK-Rollup mode, where transaction data is stored on-chain, thus benefiting from the security and decentralization of the Ethereum main chain. Alternatively, users can choose the Validium mode, which stores transaction data off-chain, enhancing scalability and throughput while maintaining robust validity proofs.

In both modes, the transaction integrity is maintained through zero-knowledge proofs, but the choice of data availability mode allows for a customizable balance between scalability, security, and cost-efficiency.

The interaction of Volitions with the Ethereum ecosystem is also facilitated through a comprehensive set of smart contracts. These contracts manage state commitments and validity proof verifications, ensuring the system remains secure, efficient, and seamlessly integrated with Ethereum, regardless of the chosen data availability mode.

What are Sovereign Rollups? Sovereign Rollups represent a distinct class of blockchain scaling solutions, where each rollup operates as a self-governing entity with its own validator set and consensus rules. Unlike traditional rollups tied to a specific main chain's security and data availability model, Sovereign Rollups maintain autonomy over these aspects.

These rollups provide a unique combination of scalability and sovereignty, allowing them to tailor their infrastructure to specific use cases or community needs. By managing their own data availability, either on-chain or off-chain, Sovereign Rollups can optimize for performance, cost, and security as per their requirements.

The key feature of Sovereign Rollups is their independence in decision-making regarding upgrades, tokenomics, and governance models. This autonomy enables a more flexible and adaptive approach to blockchain scalability, catering to diverse and evolving ecosystem needs.

In Sovereign Rollups, the transaction integrity is usually maintained through customized consensus mechanisms or cryptographic proofs, and their interactions with main chains (if any) are defined by their unique governance protocols. This structure empowers them to operate as independent blockchains while still benefiting from the scalability features of rollup technology. Avail DA addresses these trust assumptions by providing a robust and reliable off-chain data availability mechanism. This integration significantly strengthens transaction data integrity and accessibility while minimizing reliance on trust-based data management, thus enhancing the overall security and efficiency of various scaling solutions.

System Design Overview

By decoupling the data hosting, execution, and verification, Avail DA optimizes each component's efficiency and effectiveness as a direct result of modularity.

Data Hosting and Ordering Layer (DA Layer)

At the foundational level, the DA Layer is tasked with ingesting and ordering transactional data. This layer does not engage in executing transactions but is dedicated to storing the data and guaranteeing its availability. The DA Layer is pivotal for ensuring that the system does not rely on every full node to execute transactions, thus mitigating the bottleneck issues in traditional blockchains.

Execution Layer (Exec Layer)

The Exec Layer interfaces with the DA Layer to access the ordered transactions. It then processes these transactions and generates the necessary checkpoints, assertions, or proofs. These are subsequently committed to the Verification/Dispute Resolution Layer (DR Layer), which can be regarded as the security anchor of the Avail ecosystem.

Verification/Dispute Resolution Layer (DR Layer)

The DR Layer serves as the adjudicating component where checkpoints or proofs submitted by the Execution Layer are verified. This ensures that only valid state transitions are accepted within the network.

Network Participants

Avail DA comprises three types of nodes:

- Full Nodes
- : These nodes download and verify the correctness of blocks but do not partake in the consensus process. Their role is essential for maintaining the network's integrity.
- Validator Nodes
- : These nodes are central to Avail DA's consensus mechanism. They are responsible for generating blocks, deciding on transaction inclusion, and maintaining the order. Validator nodes are incentivized through consensus participation and are fundamental to the DA Layer's operations.
- Light Clients
- : Operating with constrained resources, light clients rely on block headers to participate in the network. They can query full nodes for specific transactional data as required and are crucial for upholding a decentralized and accessible network.

Consensus

Avail DA opts for a Nominated Proof-of-Stake (NPoS) consensus model for its scalability and energy efficiency benefits. Specifically, it employs Substrate's BABE/GRANDPA consensus, offering a blend of fast block production and provable finality.

How Does Avail DA Work?

Avail DA redefines blockchain scalability by combining erasure coding, KZG polynomial commitments, and data availability sampling to deliver world-class data availability guarantees. It functions as a foundational (base) layer, offering scalable data hosting without transaction execution, specifically for rollups.

Transaction Lifecycle

1. Transaction Submission
2. Data Extension and Erasure Coding
3. Commitment Creation
4. Block Propagation
5. Light Client Network
6. Proof Verification

Starting with Transaction Submission

As Avail DA's primary consumers, rollups begin the process by submitting transactions to Avail DA. Each transaction carries a uniqueapplication ID (or appID for short), signifying its origin and purpose within the broader ecosystem.

Enhancing Data Reliability Through Erasure Coding

Once transactions reach Avail DA, they are processed through erasure coding. This procedure adds redundancy, enhancing the data's reliability and integrity. Blocks are divided inton original chunks and extended to2n , allowing for reconstruction from anyn out of2n chunks. While Avail DA incorporates mechanisms for fraud proofs, the primary reliance for data integrity is on the consensus of validators. Over 2/3 of the validators are required to be honest to reach a consensus, ensuring robust security for the erasure-coded data.

To combat the misconstruction of erasure-coded chunks, full nodes can create and propagatefraud proofs , ensuring that light clients can verify the authenticity of block headers.

Solidifying Data Integrity with Commitment Creation

Avail DA takes the redundant data and applies KZG polynomial commitments to each block. These commitments serve as cryptographic proofs of the data's integrity, ensuring that what is stored is accurate and tamper-proof. The commitments are used byvalidators to confirm the data's integrity before it is attested and transmitted to main chain via Avail DA's data attestation bridge .

Ensuring Consensus & Block Propagation

Validators play a pivotal role in Avail DA. They receive the commitment-laden blocks, regenerate the commitments to verify their accuracy and reach a consensus on the block, which requires agreement from at least two-thirds (super majority). Validators ensure that only verified and agreed-upon data is propagated through the network. They reach consensus This stage is vital for ensuring that the data, once validated, can be relayed via Avail DA's data attestation bridge.

Light Clients: The Guardians of Data Availability Using DAS

Light clients within Avail DA's ecosystem useData Availability Sampling (DAS) to verify block data integrity. They check KZG polynomial openings against the commitments in the block header for each sampled cell, enabling them to independently and instantly verify data availability. This method bypasses the need for reconstructing full KZG commitments or relying on fraud proofs, underpinning Avail DA's high security and data integrity standards maintained by decentralized verification. However, for more comprehensive data integrity checks, especially for row integrity within the data matrix, app clients perform KZG reconstruction. This approach is more optimal for verifying the integrity of entire rows than validating individual cells.

On the other side, full nodes use Kate commitments for two primary purposes: reconstructing the full data for network-wide verification or creating fraud proofs to challenge any discrepancies in the data. This dual mechanism of light clients and full nodes working in tandem also strengthens the overall security and reliability of the network.

Proof Verification: The Final Checkpoint

The journey culminates with light clients performing proof verification. This process involves generating cell-level proofs from the data matrix, enabling light clients to efficiently and independently verify the state of the blockchain. This decentralized approach to verification underpins the security and integrity of Avail DA.

The settlement in Avail DA is primarily about ensuring data availability for rollups. The actual transaction execution and finality occur at the rollup layer, while Avail provides the necessary data infrastructure.

What's Next?

With your foundational understanding of Avail DA, if you're new to the ecosystem, be sure to visit theEnd user guide section.

Additionally, consider experimenting with a light client. For this, theQuickstart guide is great resource. To run an Avail DA light client, all you need to do is install and use the Avail CLI.

To install the CLI fromnpm , run the following command:

npm

i

-g

@availproject/cli Then run:

avail

lc

up That's it!

Join the Clash of Nodes Campaign

As you delve deeper into Avail's ecosystem, an exciting opportunity awaits. Avail is advancing the frontiers of modular blockchains, and we invite node operators to participate in the dynamic Clash of Nodes campaign. This campaign is a cornerstone in testing the capabilities of the Avail DA, offering a real-time, incentivized testnet environment. It's a chance to be part of a community shaping the future of blockchain infrastructure. If you're ready to further your journey with Avail and

engage in this innovative campaign, visit theClash of Nodes section in the documentation.

The Avail Trinity Avail Nexus