Glossary

GLOSSARY AS A REFERENCE FOR CONCEPTS While the Avail documentation is under development, the Glossary is being used to elaborate on key concepts. If you have any questions or concerns, please don't hesitate to contact the Avail team.

App-Chain

Appchains allow developers to optimize their applications by tailoring a chain to the specific needs of their use case, without constraints from a shared blockchain. They provide enhanced performance and scalability by functioning as independent chains, serving specific applications. Appchains also simplify the development process by eliminating the need for developers to manage and maintain a validator set. Avail enables the creation of modular app-chain architectures that can be based on different layer 2 or 3 scaling solutions.

AVL

AVL is the native token of the Avail network. Currently, there is no publicly available "AVL" token with monetary value; it is solely used for testnet purposes.

Avail JS Apps

The Avail JS Apps UI is a forked version of Polkadot JS Apps UI (opens in a new tab) that is used for visualizing and interacting with the Avail network.

BABE

BABE (Blind Assignment for Blockchain Extension), part of the Substrate framework, is the block production mechanism that Avail uses. Please refer to the Polkadot Wiki (opens in a new tab) for more details.

Bonding

Bonding is a process of locking or depositing tokens in order to participate in the operations of the Avail network. This includes participating in the consensus process and securing the network.

Chilling

Chilling refers to the deliberate action of withdrawing from nominating or validating roles. Both validators and nominators can initiate chilling, which becomes effective in the subsequent era. Additionally, chilling can denote the exclusion of a validator from the active set by their peers, rendering them ineligible as candidates for the upcoming consensus cycle.

Commission

Validators earn rewards for block production on the network. They set a commission rate, which is first deducted from their total rewards. The remaining rewards are then distributed to the nominators backing that validator based on this commission rate.

Consensus

Consensus refers to the mechanism by which nodes come to an agreement about what data on the blockchain can be verified as true and accurate. The consensus protocol determines how transactions are ordered and how new blocks are added to the chain, which is NPoS for Avail.

Controller Account

The controller account is tasked with managing staking activities and executing transactions on the network. This includes responsibilities like nominating validators, bonding and unbonding funds, and paying transaction fees. Given its active role, the controller key is used more frequently and is essential for the day-to-day operations of the account.

Data Attestation

Data attestation involves confirming the authenticity and integrity of data. In Avail, this process ensures that data on the chain is both accessible and accurate. An Avail block header incorporates two attestations: KZG polynomial commitments

for the provided data and the Merkle tree root with data blobs as leaves. A supermajority of Avail's validators achieve finality on the header by signing a chain that includes the header, utilizing theGRANDPA protocol.

Data Availability Committee (DAC)

A Data Availability Committee (DAC) consists of a group of nodes responsible for preserving copies of off-chain data and ensuring its accessibility upon demand. DACs can be integral to scaling solutions that enhance a blockchain's throughput by managing transactions on a distinct layer, commonly referred to as off-chain scaling. Unlike DACs, which often cater to specific Layer 2 (L2) solutions, Avail stands out as a universally applicable data availability layer. It operates as an autonomous chain, ensuring a more impartial and versatile approach to data availability.

Data Availability Sampling (DAS)

Data availability sampling allows light clients to confirm the availability of data without downloading complete blocks. Through this method, light clients engage in several rounds of random sampling for small chunks of block data. With each successful round, confidence that the data is available grows. When the light node achieves a set confidence threshold, they recognize the block data as accessible.

DHT (Distributed Hash Table)

A Distributed Hash Table (DHT) is a decentralized system offering a lookup service akin to a traditional hash table. It holds key-value pairs, enabling peers to swiftly find the value corresponding to a specific key. The DHT is pivotal in the process of sharing data cells, especially for random sampling and proof verification. It facilitates nodes in storing and identifying information about providers. Through the DHT, nodes in the network are interconnected, streamlining cell discovery and access.

Decoupling

Decoupling in the context of blockchain refers to the strategic separation of distinct functionalities into independent modules or layers. By doing so, a modular blockchain can specialize and excel in specific tasks, rather than being burdened by the need to handle every function. This modular approach enhances efficiency, flexibility, and scalability, allowing each component to evolve and optimize independently.

Equivocation

Equivocation is when a validator signs two or more conflicting blocks or messages. This can be done intentionally or unintentionally.

Era

An Era in Avail represents a predefined number ofsessions during which the validator set is determined and rewards are distributed. At the onset of each era, validators are chosen to be part of the active set based on their staked amount. The selection also considers other factors, such as a validator's performance in the previous era—specifically, if they were inactive due to being chilled or slashed. Should a new validator stake a higher amount than current validators, or if an active validator underperforms, they can be replaced in the active set for the upcoming era.

Epoch

An Epoch is a designated time frame during which a specific group of validation nodes undertakes the task of verifying transactions and appending them to the blockchain. The duration of an epoch can vary across different blockchain networks.

Execution

In traditional blockchains, execution refers to how nodes process transactions to transition the blockchain between states. However, Avail operates differently. As a modular base chain, Avail does not possess a general-purpose execution layer. Instead, execution occurs in other layers, such as rollups, and the resulting data is posted to Avail in its raw form, without undergoing execution on Avail itself.

In Avail's context, "Consensus" carries a more specific meaning than in typical blockchains with integrated execution layers. For Avail, consensus signifies the network's agreement that data has been appropriately published. Explicitly, validator nodes in Avail do not execute transactions as a prerequisite for attesting to the validity of blocks. With a few exceptions, such as balance transfers, validators primarily attest to the correct packaging of published data within blocks. This streamlined approach is a primary reason Avail can accommodate larger block sizes. Since validators undertake less work per block, increasing block size has a reduced impact compared to other blockchains.

Finality Gadget

A finality gadget is a mechanism that ensures blockchain state finality by requiring validators' commitment through signed messages. Once sufficiently validated, the state is finalized and secure from malicious modifications.

Fraud Proofs

Fraud proofs are cryptographic proofs employed to validate the legitimacy of a transaction or state transition on Avail. Any node can generate and share a fraud proof across the P2P network. App clients can then assess these proofs and respond accordingly.

GRANDPA

GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement), part of the Substrate framework, is the finality gadget Avail uses. Please refer tothe GRANDPA paper(opens in a new tab) for a full description of the protocol.

KZG Commitments

KZG commitments, pioneered by Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg in 2010, offer a concise method for committing to polynomials. These commitments have recently gained prominence, especially in PLONK-like zero-knowledge frameworks.

In Avail's design, KZG commitments are employed for several key reasons:

- They enable succinct commitments, ideal for inclusion in block headers.
- They support brief openings, facilitating light client availability verification.
- Their strong cryptographic binding ensures the prevention of fraud proofs by rendering the creation of false commitments
- computationally challenging.

Kademlia DHT (Kad-DHT)

Kad-DHT is a specific Distributed Hash Table (DHT) variant that organizes nodes and data based on a chord ring—a logical arrangement of nodes ordered by their IDs. Avail employs Kad-DHT to establish a decentralized network for data storage and retrieval. In this structure, each node is tasked with holding a portion of the data. Nodes can directly communicate to access data. Avail utilizes Kad-DHT to store data cells and pinpoint which peer possesses a particular data segment, with matrix data cells uniquely mapped to Peer IDs.

libp2p

libp2p (opens in a new tab) is an open-source modular network stack designed for constructing peer-to-peer (P2P) applications. It offers a flexible framework for data transfer across diverse transport protocols. Avail integrates libp2p to establish a decentralized network dedicated to data availability, ensuring that transaction data is efficiently stored and disseminated to validators and full nodes.

Light Client

Light clients enable users to engage with a blockchain network without synchronizing the entire blockchain, preserving both decentralization and security. Typically, they retrieve only the blockchain headers, omitting the full block contents. Avail's light clients enhance this by employing Data Availability Sampling. This method ensures block content availability by downloading and verifying random segments of a block.

Mainnet

A mainnet is a blockchain network that is fully operational and open to the public. It is the "production" version of a blockchain network, and it is where real-world transactions and applications are deployed. View theRoadmap to Mainnet blog post(opens in a new tab) for more information on Avail's mainnet.

Modular Blockchain

A modular blockchain specializes in managing specific tasks while delegating other responsibilities to distinct layers or components.

Monolithic Blockchain

A monolithic blockchain encompasses all core functionalities (Execution, Settlement, Ordering, Data Availability) within a singular blockchain structure.

Nominated Proof of Stake

Nominated Proof of Stake (NPoS) is a consensus algorithm where users nominate validators to process blocks for them. These validators verify and append transactions to the blockchain. For their services, validators receive rewards in the form of the native tokens. They then commission a portion of these rewards to nominators based on a set commission rate. Avail uses NPoS as implemented within Substrate.

Oversubscribed

Oversubscribed refers to a situation where the number of nominators wishing to participate in the consensus process exceeds the available slots.

Scalability

Scalability within Avail pertains to the capacity to augment the volume of data disseminated by the chain, ensuring that the experience of its participants and users remains unaffected. Avail achieves this by adopting a modular approach, taking DA off-chain, which allows the main network to primarily focus on execution. This modular design facilitates the individual optimization of key constructs, enabling each component to be scaled according to its unique requirements.

Session

A session refers to a specific duration during which a fixed set of validators operate. Validators can enter or exit the set only at the transition between sessions.

Settlement

In the context of Avail and modular blockchains, settlement refers to the process by which modular layers agree on the correct execution outcome of transaction data. This includes any necessary dispute resolution processes. Since Avail operates as a modular base chain, it merely receives and stores raw transaction data without executing it. This data can encompass a wide range, from valid transactions to potential spam.

The actual execution of these transactions and the subsequent validation of their outcomes occur in other layers or systems. Once these layers reach an agreement on the outcome, the results are "settled." For instance, in the case of a validium, transaction data is published to Avail, sequencers then execute these transactions, and finally, proofs of these executions are posted to Ethereum for settlement. Different modular constructions might employ varying mechanisms or platforms for settlement, but the core principle remains the same: determining and agreeing upon the correct outcome of transactions.

Slashing

Slashing is a penalty that is imposed on validators who misbehave. For example, a validator may be slashed if they equivocate, meaning that they sign two or more conflicting blocks. Slashing can be a severe penalty, as it can result in the loss of a portion of the validator's stake.

Sovereign Rollup

A sovereign rollup is a type of blockchain that publishes its transactions to another blockchain, typically for ordering and data availability, but handles its own settlement. This means that sovereign rollups have their own canonical chain and validity rules, and they do not need to rely on a settlement layer to determine which transactions are valid.

Stash Account

The stash account holds the tokens you wish to stake/bond. This account is like a cold storage account and is used for bonding and unbonding tokens, as well as for designating the controller account.

Testnet

A testnet is a simulated blockchain network that is used to test and debug blockchain applications before they are deployed on the mainnet. Testnets are typically open to the public, and anyone can participate in them.

Validium

Validiums are designed to store transaction data off the primary layer (L1), such as Ethereum. They can seamlessly leverage the benefits of Avail's scalable and specialized module. Rather than directing transaction data to aDAC or other alternatives, Validiums can commit this data to Avail.

A layer 2 solution, like a rollup, can evolve into a Validium by choosing off-chain data storage over the main chain. This distinction is subtle, as a Validium isn't strictly a "layer 2" in the traditional sense; it doesn't post data to L1, introducing different trust considerations. However, in many contexts, it's still categorized as a layer 2 solution. Fundamentally, a Validium can be described as a rollup combined with off-chain data availability, akin to Avail's approach.

Validator

An Avail validator is a full node that is responsible for verifying transactions and adding them to the blockchain.

Volition

Volitions represent an advanced form of zero-knowledge rollups, offering developers the flexibility to decide the storage location for transaction data, be it on-chain or off-chain. This adaptability ensures that developers can optimize for both cost and DA based on the specific requirements of their application. In the context of Avail, volitions can leverage the platform's robust DA layer, ensuring that off-chain data remains easily accessible and verifiable, thereby enhancing the security and efficiency of decentralized applications.