Glossary

A

Autonomy Autonomy is the control you gain from owning your blockchain execution layer with the exception of having to adhere to the underlying base layers protocol rules. Some of the advantages of having autonomy entails choice of native network fee token and a full control over the blockchain logic.

B

Batching Execution layer sequencers gather executed transaction related data and store it on the base layers for security. The frequency of data batching is decided by the Sequencer but may be enforced by the underlying protocol. BLOB Binary large Objects (BLOBs) encapsulate block information posted to a data availability providers. Bond Optimistic rollups require a bond to be placed with the protocol as a form of insurance for any fraudlent activity. If a Sequencer, that has bonded tokens, is proven to committed fraud within the dispute period the tokens they've bonded are partially allocated to the prover and the rest are burned.

C

Cosmos SDK The Cosmos SDK is an open-source framework for building public Proof-of-Stake (PoS) blockchains. Blockchains built with the Cosmos SDK are generally referred to as application-specific blockchains.

D

Data Availability Problem The data availability problem states: If the block proposer does not publish all of the data no one would be able to detect hidden transactions.

If a block producer just publishes the block header but not the transaction data, then full nodes won't be able to check if the transactions are valid and generate fraud proofs if they're not valid. It is a requirement that block producers must publish all the data for their blocks, but we need a way to enforce this.

The most obvious way, as discussed, to solve the data availability problem is to simply require everyone (including light clients) to download all the data. Clearly, this doesn't scale well. This is what most blockchains, such as Bitcoin and Ethereum, currently do.

Data availability proofs are a new technology that allows clients to check with very high probability that all the data for a block has been published, by only downloading a very small piece of that block. Data availability proofs utilize a core technology called erasure coding to increase the size of the data and use light clients to sample.

Reference: https://coinmarketcap.com/alexandria/article/what-is-data-availability Dispute Period Anytime the sequencer publishes a batch of state transitions there is a "dispute period" during which any party can publish a "fraud proof" which indicates that one of the state transitions was invalid. This is proven by replaying the transaction which caused the state transition onchain and comparing the resulting state root with the one that was published by the sequencer. If the state roots do not match, then the fraud proof is successful and the state transition is cancelled. If there were more state transitions after the invalid one, they also get cancelled. Transactions which are older than the dispute period cannot be disputed anymore and are considered final.

Reference: https://www.paradigm.xyz/2021/01/almost-everything-you-need-to-know-about-optimistic-rollup

E

Execution Layer The top layer of the modular stack. This layer is in charge of transactions processing and gossiping, state transition function and communication with other layers of the modular stack. Embedded AMM Dymension embeds a native automated market maker (AMM) into the settlement hub enabling the creation of a core financial center. The embedded AMM is designated as an infrastructure tool that is designed to help developers and users interact within the dymension ecosystem. The settlement layer is dedicated to facilitate easy RollApp deployment, providing a stable infrastructure for developers to innovate in and aggregating liquidity to create efficiently priced assets. The settlement hub is designed to solely embed a dedicated AMM and provide the tools for developers to build products within dymension's RollApp ecosystem. Enshrined RollApps RollApp servicing logic is embedded in the settlement layer, an attribute known as 'enshrined rollups', increasing seamless cooperation and safety between RollApps and the dymension hub. Smart contract bridges on Ethereum, as an example, are not embedded into the protocol and thus the protocol is not concerned with smart contract bugs. For example, if a smart contract bridge contract for Arbitrum were to be hacked the Ethereum protocol would need to make a governance decision as to what to do with the user funds (e.g. DAO hack). However, with RollApp servicing embedded in the protocol a hack on the IBC bridging module would halt the chain and a patch would be created.

F

Fraud Proof Fraud proofs indicate that a state transitions was invalid. This is proven by replaying the transaction which caused the state transition onchain and comparing the resulting state root with the one that was published by the sequencer. If the state roots do not match, then the fraud proof is successful and the state transition is cancelled.

Reference: https://research.paradigm.xyz/rollups

H

Honest Majority Assumption The assumption that a majority of blockchain participants (such as the validator set) are honest and follow the rules of the protocol. If a majority of participants are dishonest, attacks can be made that are within the rules of the protocol but cause negative effects.

In Tendermint Core when +1/3 of the voting power drops offline for whatever reason, the chain will stop making progress. In order to start making progress again, the network will need to wait for the +1/3 of voting power to come back online. If validators don't come back online for whatever reason, they may need to be forked out via manual intervention from the community. Honest Minority Assumption The assumption that only a minority of blockchain participants are honest and follow the rules of the protocol. Honest minority assumptions can come in multiple forms, such as a 1-of-N assumption where only a single honest participant is required to be honest for the blockchain to hold a guarantee. For example, optimistic rollup users and nodes require a 1-of-N assumption for safety as at least one honest full node is required to monitor the rollup and submit fraud proofs in the event of fraud.

Reference: https://celestia.org/glossary/

I

Inter-Blockchain Communication (IBC) The Inter-Blockchain Communication Protocol (IBC) is an open-source protocol for relaying messages between independent blockchains. The messages pass across trust-minimized channels that rely on the honest-majority of the corresponding chain. ISRs Blobs include block transactions and Intermediate State Roots (ISRs) used for transaction validation and fraud proofs. Intermediate state roots are the resulting state root after the processing of a single transaction.

L

Light Client Light clients are a process that only verifies a particular state machine's consensus, without executing the transactions. This allows it to be used in mobile wallets or other low-powered devices.

The light client connects to a set of full nodes and verifies the new headers can be trusted. Most of the communication is happening with just one node, called a primary, other nodes are called witnesses.

Reference: https://medium.com/tendermint/different-types-of-evidence-in-tendermint-5de4440fdd54

M

Modular Blockchain Modular blockchain architecture design decouples different functions of a 'Monolithic' blockchain for greater performance and scalability. Modular blockchains handle one or more of the functions of a monolithic blockchain but not all. Monolithic blockchains handle transaction execution, state settlement, data processing and provide a consensus on the canonical history of the chain.

O

Optimistic Rollups Optimistic rollups assume an optimistic view towards the honesty of the sequencers, hence the term optimistic rollup. Meaning that it's initially assumed the sequencer who is processing transactions is acting honestly. However, in order to produce an environment where users of a network do not have to simply trust sequencers, a dispute period is installed. This period enables others to verify that the sequencer is reporting correct state updates. If anyone discovers a batch that is not correct, they can publish a "fraud proof" demonstrating the correct state transition. If indeed the sequencer provided incorrect information the state of the blockchain is reverted and the sequencer is "slashed" (they lose tokens they've bonded to participate in the network).

R

Relayer A relayer acts as a bridge between two blockchains in the IBC network. Its main job is to listen to events on one blockchain, and then relay (or communicate) that information to another blockchain. These are trust-less entities that pass information from one network to another. RollApp RollApp is an application specific rollup. Unlike dApps built on a generic-purpose rollups, apps built as a RollApp have their ownautonomy . RollApp Development Kit (RDK) Dymension's rollapp factory takes its inspiration from the Cosmos ecosystem which introduced the successful Cosmos SDK. A RollApp instance on dymension is an application-specific rollup (which we refer to as RollApp), built by using the dymension RollApp Development Kit, termed RDK. The development kit is a pre-packaged set of generic modules which enable compatible Cosmos SDK functionality, such as creating accounts and token management. The RDK simplifies the process of deploying rollups on top of dymension's settlement layer. RollApp Virtual Machine (RVM) The RollApp Virtual Machine is a novel

dispute mechanism which generates a RollApp specific virtual machine for resolving transaction disputes within the settlement layer. RVM simulates the exact context and logic in which a transaction is executed resulting in a deterministic output. As such, RVM is capable of resolving disputes in various execution environments.

S

Settlement Layer The dymension hub is a Cosmos SDK Proof-of-Stake chain, that utilizes the Tendermint Core state replication model for networking and consensus. The dymension hub acts as a settlement layer that is specifically designed to provide a specialized service optimized for RollApps. In dymension's case the settlement layer acts as a hub for bridging, security, and liquidity for the dymension ecosystem. Sequencers Sequencers are the nodes operating the RollApp. sequencers are responsible for storing and executing transactions off-chain. Sharding One way of increasing the throughput of a blockchain is to split the blockchain into multiple chains called shards. The point of sharding is to split up the block producers in the network so that instead of every block producer processing every transaction, they split up their processing power into different shards that only process some transactions. RollApps are execution environment shards, Sequencers and participating full nodes network transactions and maintain a light client of the settlement layer for updating state and connecting to other execution shards. Shared Security Shared security means that all RollApps that are connected to the dymension settlement hub and benefit from the economic security provided by the dymension validators. The notion of shared security is different from interchain protocols that build on an architecture of bridges. For bridge protocols, each chain is considered sovereign and must maintain its own validator set and economic security.

Reference: https://wiki.polkadot.network/docs/learn-security Slashing A mechanism employed in PoS blockchains that is used to deter and punish malicious behavior. Slashing was originally conceived as a method to solve the nothing at stake problem, which presented the problem that validators weren’t restricted by the number of forks they could vote on – unlike in PoW where miners only have a limited amount of hash power to dedicate to forks.

To become a validator, a node is typically required to stake a minimum amount of the network’s native token. If the validator is caught double-voting or voting for any competing fork other than the canonical chain, the validator's stake is reduced (slashed). The degree by which validators are slashed varies by network and the severity of the malicious behavior.

Slashing can also occur for behavior that is deemed dishonest despite any lack of malicious intent. Dishonest behavior can include going offline or missing network duties. Slashing as a deterrent for dishonest behavior is important for blockchains that employ BFT-like consensus mechanisms, where ≥1/3 of voting power can halt the network if they are offline or refuse to vote.

Reference: https://celestia.org/glossary/slashing

V

Verifiers Verifiers are entities responsible for watching RollApp Sequencers in case of fraud. RollApp Verifiers run full nodes of the RollApp state transitions. Verifiers submit fraud proofs to the settlement layer. Upon a successful fraud proof the Verifier is rewarded a portion of the Sequencer's bonded token and the rest are burned. Edit this page

Previous Dymension Litepaper