📜 SEDA Litepaper

SEDA is a standard for modular data transport and querying. Any data type, for all networks. Learn more in SEDA's Litepaper below!

ℹ️ Introduction

A technical breakdown of the SEDA Network architecture.

SEDA | The Evolution of Data and Blockchains

Blockchain networks are isolated execution environments that lack the ability to directly interface with data sources beyond their native environment. This isolation creates a fragmented landscape between blockchain networks and any data source from the traditional internet. Furthermore, this isolation prevents blockchain networks from unlocking the full potential of their technology, which relies heavily on its capability to query data beyond the confines of the network itself.

Smart contract-based systems, commonly referred to as "oracles", were developed as a technology to bridge this gap. Yet, the prevailing oracle systems exhibit shortcomings, such as unsustainable economic models, centralized bottlenecks, bandwidth restrictions, and limited accessibility, let's call these systems oracles 1.0. When a smart contract depends on oracles 1.0 designs, they inadvertently sacrifice some of the advantages of their base network by introducing a single point of failure.

In this litepaper, we delve into how SEDA has solved these challenges, offering a scalable and secure solution that aligns with the core principles of permissionless technology, enabling the next evolution of oracles, oracles 2.0. SEDA is a layer one network that supports the permissionless data flow from any source to any destination network. SEDA addresses the core centralization and failure risks we see today when accessing off-chain data. SEDA is a necessary building block to achieve a modular, purpose-built future for layer one and layer two networks. SEDA is the foundation for data in web3.

 SEDA: an Intent-Based Modular Data Layer

Introducing SEDA: A Pioneering Shift in Data Transmission

SEDA goes far beyond today's definition of an oracle. SEDA is a data transmission and computation network that enables a permissionless environment for developers to deploy data feeds. SEDA implements a fully modular interface that developers can use to dictate what data feeds to fetch and how to use this data for computation. This approach ensures that developers receive results that can be readily integrated into their networks and/or smart contracts.

The SEDA Network consists of:

- **The SEDA Chain**: which is used for settlement, and data storage for distribution.
- **The Overlay Network**: a Multi-Party Computation (MPC) network that does the data querying and computation.
- **Solvers**: the entities forwarding new data requests to the SEDA Chain and forwarding results to destination chains.
- **Data Providers**: the (private) data providers plugging in to the SEDA Network.

The SEDA Chain and Overlay Network have security guarantees consistent with leading layer one networks. Security guarantees are facilitated through game theory, cryptography, strong backstops, and a high degree of configurability and computability.

SEDA eliminates the need for any trusted authority role within the Network with the use of specially designed economic incentives. Any entity can validate, relay, request, and supply data. As a fully interoperable layer one network, SEDA is universally accessible from any blockchain network with shared security.

Developers on destination networks can request both public and private data depending on their desired use case. The SEDA Network incentivizes data providers to participate by allowing them to earn revenue based on the utilization and the value of the data they provide. Data providers get to set their fee on a per-query basis, and will earn a percentage of the on-chain opportunities their data enables through OEV auctions, more on this later.

When issuing a data request, developers on destination networks can specify a set of instructions that determines how SEDA should perform computation on the fetched dataset. As a result, developers on destination networks utilizing SEDA can perform complex computations off-chain. These complex computations enable developers to perform more extensive computation than what would otherwise be possible within the destination network's rigid smart contract environment.

🔑 SEDA's Key Features

Explore the key features of SEDA Modular Design.

🤹 Multi-Chain Native

The blockchain ecosystem is rapidly expanding with the introduction of purpose-built, modular networks. Now more than ever, it's become increasingly vital to implement a standard for data transmission that enables permissionless data transfers to and between networks. SEDA has guaranteed shared security across all destination networks. Any destination network can verify that data originates from the SEDA chain, resulting in shared security, without native oracle deployments to each destination network.

By default, native deployments of smart contract protocols cannot support multiple chains past their original deployment, as they rely upon the original destination network's data infrastructure stack. This infrastructure may be unavailable on other destination networks that the protocol is looking to support, and implementing this same infrastructure on each destination network increases technical overhead, third-party risk, and cost for the third-party infrastructure provider.

Capital will continue flowing into the crypto ecosystem through well-established networks trickling into design-specific networks with unique configuration trade-offs. SEDA allows any destination network to access its data as long as it can parse the proofs generated on the SEDA Chain. SEDA's design is to be upgradable to ensure a modular approach to updates and stay competitive with future advances in decentralized network technology.

 Fast and Scalable

The efficiency of a network like SEDA hinges on its Time To Finality (TTF), a metric that indicates when a data request's outcome is irreversible. TTF measures the interval between the data request initiation and the definitive network response in the oracle realm.

Quick finality is a desirable and often required feature for many data transport use cases. Without it, transactions might fail or execute incorrectly due to stale, outdated data. Delays or outdated data can jeopardize transactions, threaten network security, and lead to potential financial losses.

Efficient workload distribution drives SEDA's scalability. SEDA minimizes on-chain operations without compromising security by executing data requests off-chain and in parallel. Specific factors, like data source response time, destination network block time, and originating network congestion, will influence TTF for platforms like SEDA.

🥩 Proof-of-Stake for Data Provision

SEDA secures data using heavily battle and time-tested algorithms. SEDA Chain bases its security on Proof-of-Stake (PoS), using the Cosmos SDK as a foundation. The SEDA Network implements another type of PoS, powered by the Overlay Network, which will be explained further.

🏄 Permissionless

In contrast to traditional oracles, where a single entity with majority control poses a risk of data manipulation and introduces a single point of failure, the SEDA protocol is designed to be a fully permissionless and decentralized network. This distinctive approach effectively prevents the existence of centralized gatekeepers and mitigates the potential for individual entities to manipulate data.

SEDA is structured as a fully permissionless network for all stakeholders. Any SEDA token holder can seamlessly join the network by either delegating their tokens or running a validator. Whether opting to function as a SEDA Chain Validator, Overlay Node, or taking on other essential roles within the network, SEDA provides an open and decentralized environment for everyone involved.

💻 Highly Programmable

One-size-fits-all does not apply when it comes to data provision and quality. With SEDA, developer-deployed data requests can fetch and aggregate data from any source in any way, shape, or form their product requires.

Data requests in SEDA provide incredible flexibility – developers can configure them to perform a variety of tasks with the fetched data, such as transforming, weighing, filtering, aggregating, and more. This functionality is made possible through Programs where developers provide instructions on how data should be fetched and computed. No special permissions are needed to deploy a Program, allowing any developer to effortlessly create their custom data feed on SEDA, much like deploying a smart contract on Ethereum. Data requests issued on the destination network include a reference to a certain Program ID. SEDA's Ooverlay Nnetwork then executes this Program as WebAssembly (WASM), a binary instruction format for stack-based virtual machines. WASM VMs allow developers to pick any programming language that compiles to WASM to write these programs. SEDA chain randomly selects Overlay Nodes that will run the deployed program and reach a consensus before being reported to the request issuer on the consumer chain.

🍴 Forkless Upgrades

In many current decentralized systems, system upgrades are challenging and require active participation from all involved parties. SEDA allows for coordinated, forkless consensus upgrades to keep the network updated. Upgrades are proposed and decided upon by the community of SEDA token holders, and are coordinated via a governance upgrade vote.

SEDA achieves this is by having its nodes composed of modular building blocks. In our implementation, most of the SEDA node logic runs on WASM binaries, which are fetched from a source pointed to by the SEDA Governance Module. Nodes watch the SEDA Governance Module for any changes to the binary so that it can upgrade it “in-flight.” This mechanism allows SEDA Token holders to have true verifiable control over the future of the SEDA Network

⚖️ Decentralized Governance

Decentralized Governance is a fundamental aspect of the SEDA protocol, ensuring an inclusive decision-making process. Every SEDA token holder has the opportunity to actively engage in shaping the network's future by creating and voting on proposals. Leveraging the standard Cosmos SDK governance module, users can influence key parameters and functionalities, fostering a democratic and resilient ecosystem. From adjusting consensus parameters to introducing new features, the decentralized governance model empowers the SEDA community to collectively steer the protocol's evolution.

💸 Oracle Extractable Value (OEV)

Putting a value on the data that oracles supply to destination networks has historically been challenging. As a result, oracles have adopted business models from web2. SEDA presents an opportunity to establish an additional revenue stream that can more accurately price the data provided by the system and data providers to various destination networks.

When an oracle pushes data to a network, a state change results: Whether it's a price update, a deposit, or a generated random number, the difference in state between, before, and after the update creates an OEV opportunity. Today, we can observe these opportunities on any blockchain network. Whenever an oracle update results in an opportunity, a "gas war" commences from other network participants, known as "searchers," who monitor the chain to spot current or imminent opportunities for value extraction. This gas war is the result of searchers bidding to be the first transaction to be executed after an oracle state change to extract the newly created value.

New data creates new opportunities. Searchers are, therefore, incentivized to pass a percentage of their potential profits to the validators of the SEDA network, a place with abundant opportunities for further value extractions.

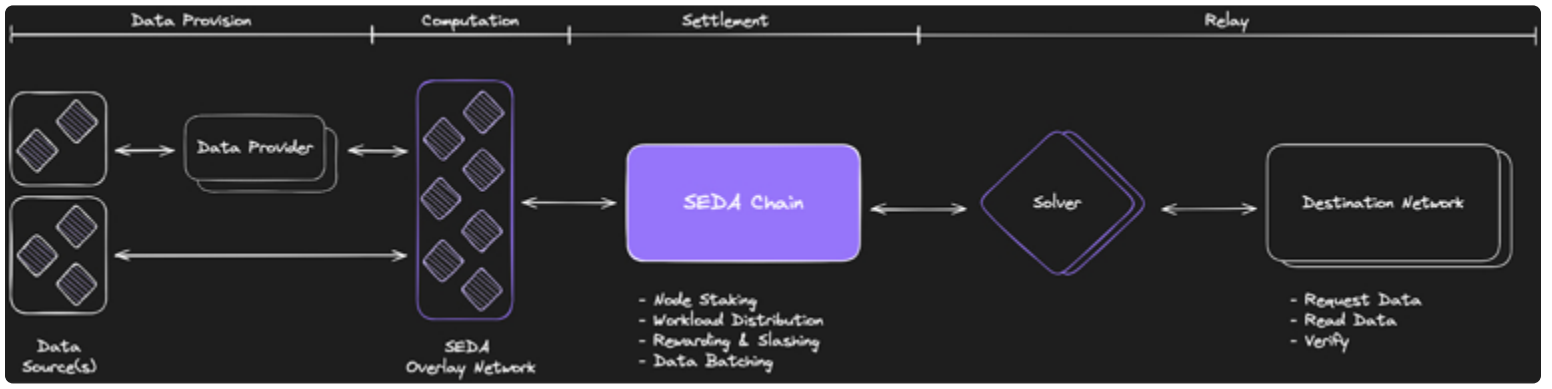
Since searchers don't have guaranteed execution, the gas war results in searchers, who sometimes don't even get to execute their strategies, burning significant amounts of gas on the native destination network. This war means that a ton of value leaks as burned gas for failed transactions, and the destination network experiences unnecessary load.

SEDA's solution removes this inefficiency and moves the opportunity for profit from the destination network to the SEDA Network. The SEDA Network can now split the profit between the network participants and data providers. SEDA achieves this by auctioning off the right to bundle transactions with the oracle updates. Searchers participate in this auction, and the highest bidder gets the guarantee that their transaction is executed as the first transaction after the oracle update is live. The result is searchers do not have to participate in "gas wars" on the destination network. As a result, there's less value leaking through inefficient "gas wars". SEDA's network will now profit from the value of the data it provides, and destination networks will see less congestion around oracle updates.

Architecture Overview

SEDA's design allows it to fetch and deliver any data from any source to any destinationblockchain network. To achieve this, the SEDA Network consists of numerous modular components: settlement, compute, relay, consumer, and data provision.

This section will dive into the individual components and describe how they interact to achieve fast, secure, and accessible data transmission from and to any network.



PAGE
SEDA Chain

PAGE
Destination Network

PAGE
Overlay Network

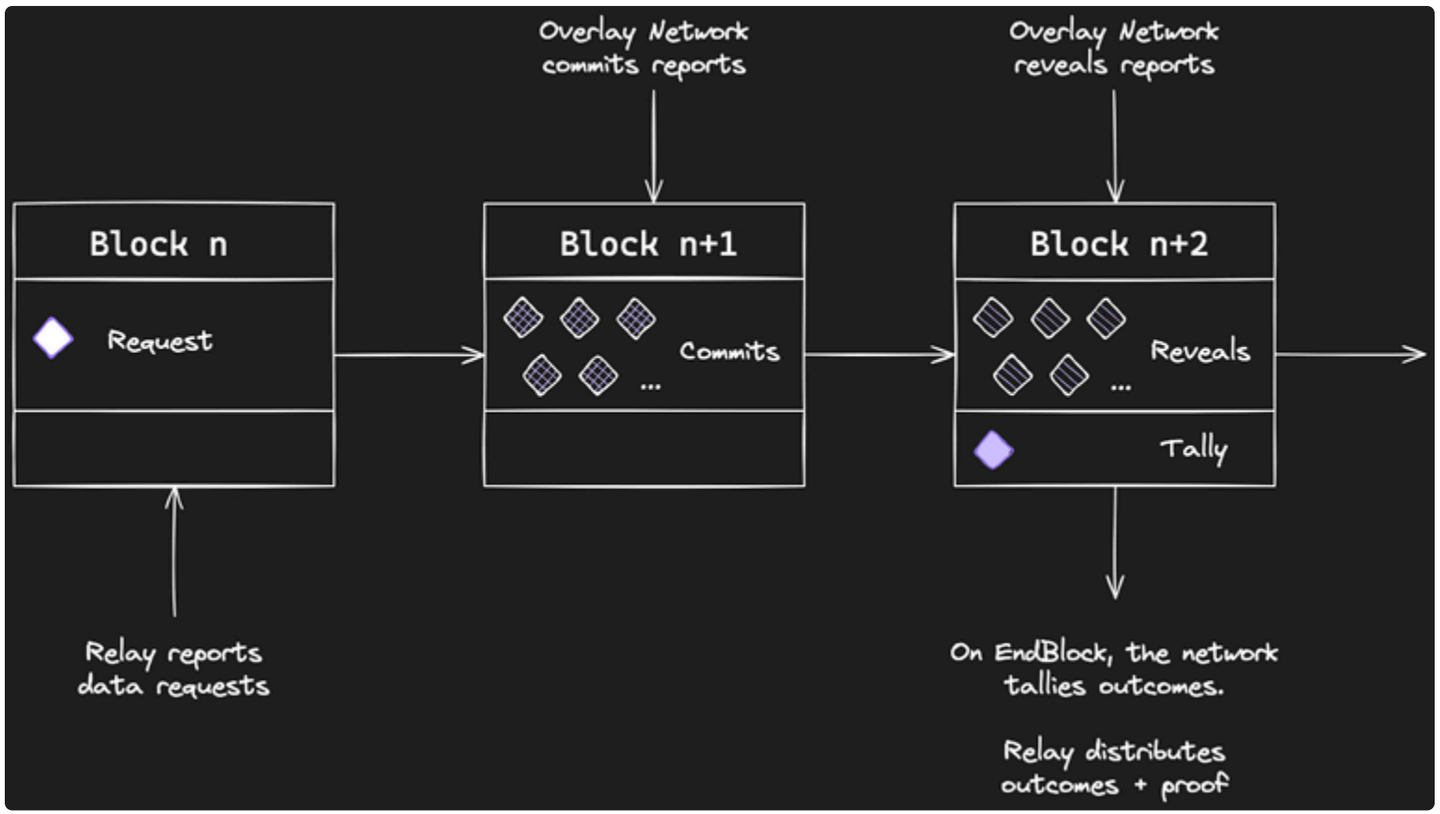
PAGE
Programs

PAGE
Solvers

PAGE
Anchor Network

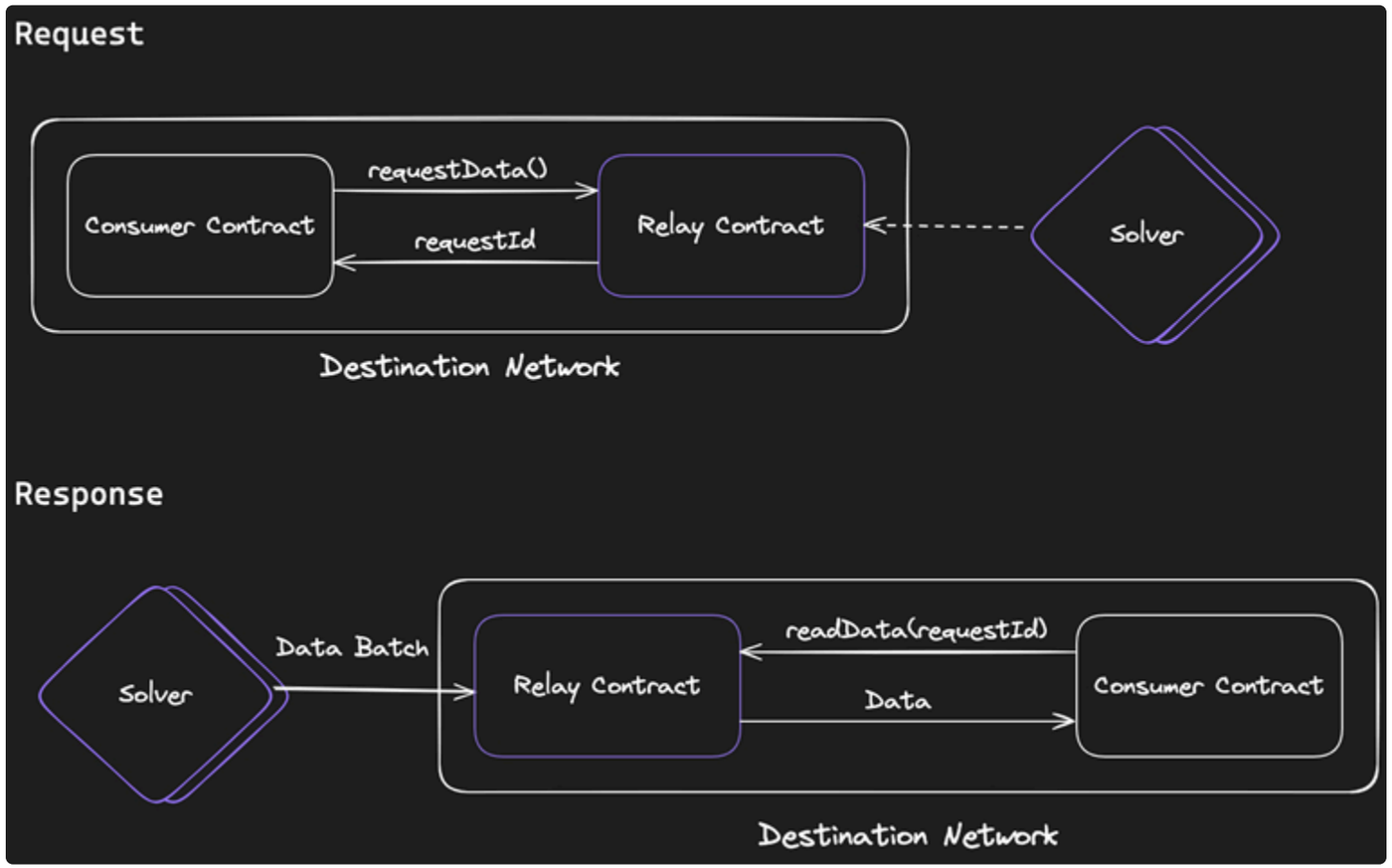
⛓ SEDA Chain

The SEDA Chain is an application-specific blockchain built using the Cosmos SDK as a foundation. The SEDA Chain acts as a settlement and checkpointing layer. The SEDA Chain is responsible for the network's security and consensus, and for generating the proofs that power SEDA's interoperability with destination networks. It acts as a single point of truth for all other components.



🚉 Destination Network

Any network can read and verify SEDA's data, which we call data consumption. All they have to do is deploy a consumer contract that can verify SEDA-generated proofs. Then, a solver, which anyone can set up, can start supplying data to the destination network. Any network or smart contract protocol can seamlessly interact with SEDA and all of its resources without needing to interact directly with the SEDA chain.

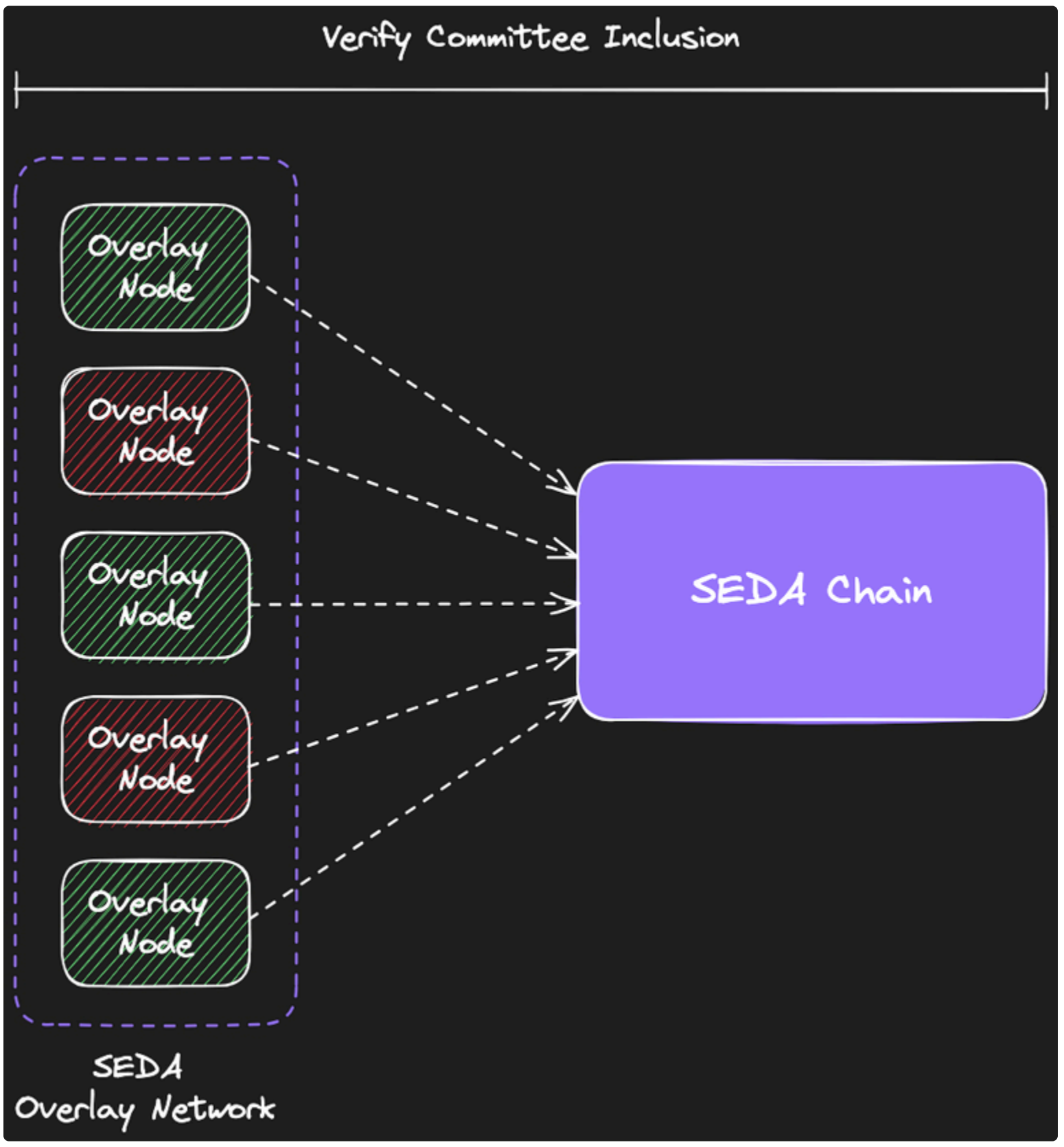


In the example above, we go over the most basic flow possible: a consumer fetches some data and then consumes it. In practice, there will likely be middleware services that will make it easier to consume data for popular feeds. That way, the cost of a feed can be split amongst multiple participants, and the frequency of updates can be higher.

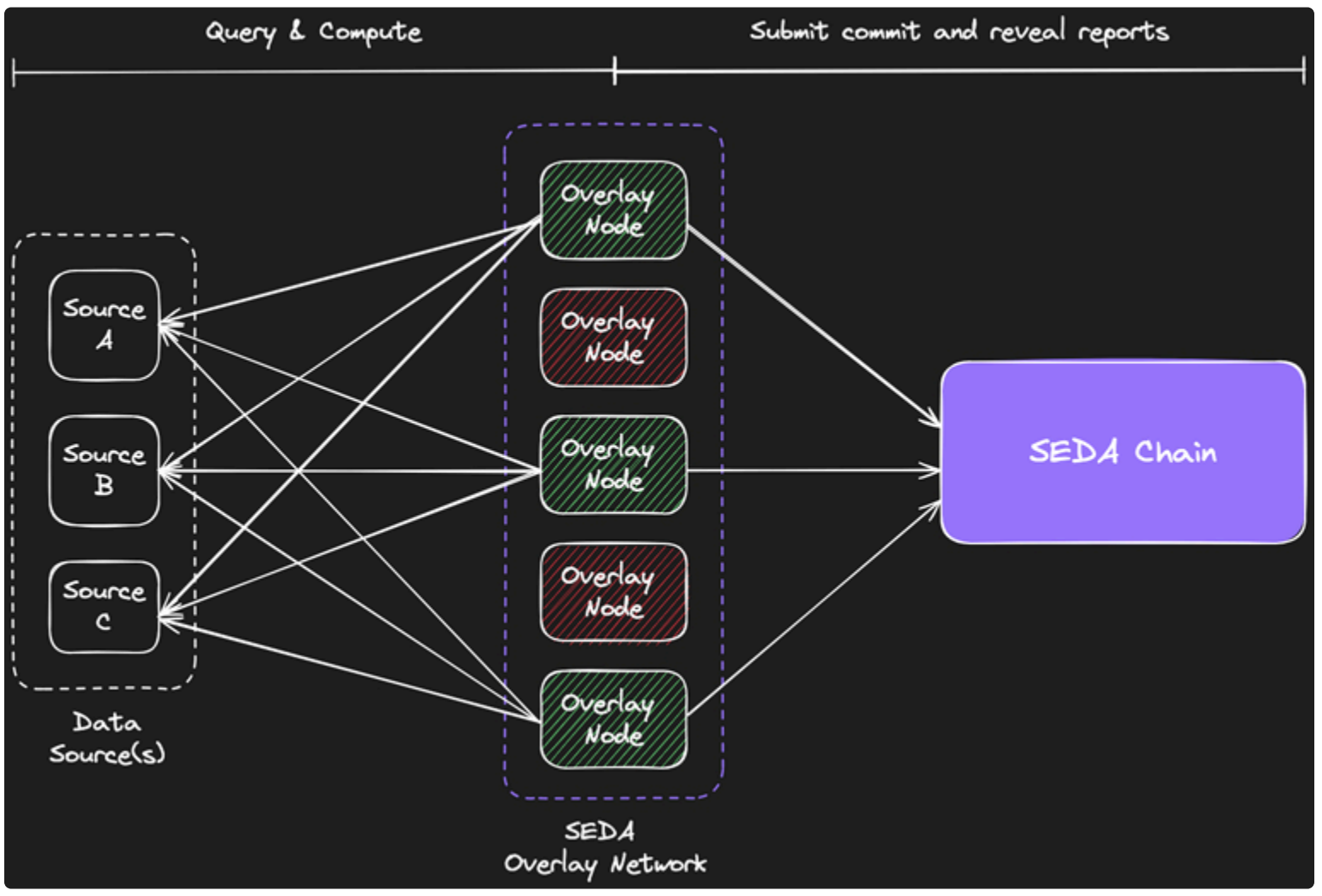
Overlay Network

The Overlay Network is a Multiparty Computation (MPC) network of nodes, independent of the SEDA Chain Nodes. Where the SEDA Chain inherits the staking mechanism from the Cosmos SDK, the Overlay Network's staking scheme is more similar to Ethereum 2.0's staking. There is both a minimum and a maximum stake weight. This minimum stake weight incentivizes validators to run multiple instances of the Overlay Nodes in case they want to stake more tokens than the maximum staking weight.

The Overlay Network is tasked with the execution of Data Request Programs. The SEDA Chain generates a new Verifiable Random Function (VRF) seed for each incoming Data Request. We seed the VRF with the VRF seed of the previous block and the Data Request ID. Overlay Nodes then use this seed and input it into their own VRF, which generates a verifiably random number that decides whether the Overlay Node is eligible for resolving this request.



After the SEDA Chain randomly selects Overlay Nodes to form a secret committee, they execute the Program's binary, referenced by the Data Request, and report the computed outcome in the form of a commit-reveal scheme. After which the outcomes are tallied and distributed.



💾 Programs

Programs are WASM binaries that Overlay Nodes directly execute. They are unique for a blockchain network because the nodes can execute HTTP requests. This type of execution means the nodes can query any data that's either public or made available by the network. Besides the ability to query, developers can write complex algorithms to generate unique, secure data feeds.

🔧 Solvers

Solvers forward messages between the SEDA Chain and external chains. External-to-SEDA chain messages contain newly created data requests. The solver pays the gas cost of the request computation upfront to prevent solvers from being able to spam or DDoS attack the SEDA Chain with non-existent data requests. As a result, the solver receives rewards for bridging the result back to the destination network. SEDA-to-external chain messages relay the SEDA Chain state and data request results. Due to the cryptographic proof supplied with this message, there's no way for the solver to corrupt or alter the data provided to the external chain.

⚓ Anchor Network

Some PoS security assumptions don’t hold up for interoperable networks such as SEDA. The design of SEDA ensures that we secure and trigger certain smart contract protocols across a diverse range of networks based on the data SEDA provides.

Consequently, if a malicious actor gains control over the SEDA Network—even momentarily—they could jeopardize the assets on the affected chains. In the case of an attack, Proof of Stake networks can fork off or roll back the chain to a pre-attack state, resulting in the attacker's profit of attack being lower than their cost of attack. Given the negligible likelihood of a destination network implementing SEDA rolling back its state due to an attack stemming from an exploit on SEDA, this solution should not be a consideration in the design of SEDA's network security.

To counteract these limitations, SEDA employs an “Anchor Network.” When issuing a data request, the issuer can optionally select an array of anchors to perform the data request in parallel to the SEDA Network. The outcome provided by the anchors acts as a backstop to SEDA Network's outcome. The destination network should not consume this outcome. Instead, the network can set a deviation threshold based on the type of data queried, which, if crossed, should result in a sensible action for the issuer's use case e.g., this outcome gets ignored, and it reissues data request. Running an anchor is permissionless; projects with large amounts of value at stake should query multiple anchors and potentially run their own.

Anchors add a layer of security to data requests by acting as a backstop mechanism. You could argue that anchor nodes can censor certain data requests by passing incorrect data, which will stall the data request. Data consumers can circumvent this by checking for anchor liveness and rotating between a set of anchors in a case where they suspect an anchor is actively censoring their requests.

SEDA Validators

Validators have two distinct purposes in the SEDA Network: Chain Validators and Overlay Network Validators. In this page we break down the roles and responsibilities of each stakeholder.

PAGE
Chain Validators

PAGE
Overlay Nodes

🔷 Chain Validators

Validators secure the SEDA Chain by staking SEDA Tokens, participating in block production, and generating cryptographic proofs that can be parsed by consumer chains, enabling full network interoperability.

The validator committee with the highest amount of stake weight signs data request batches using multi-signature public key aggregation. We create batches deterministically so that validators don't have to perform any ordering service, only attestation. Next to signing batches, the SEDA Chain Validators randomly generate a random number for secretly selecting Overlay Nodes to process certain data requests randomly.

🔵 Overlay Nodes

Overlay Nodes are verifiably randomly selected by the SEDA Chain to execute the binaries referenced by Data Request. Random secret selection relies on cryptographic primitives such as Verifiable Random Functions (VRFs). Additionally, data reporting follows a commit/reveal scheme to deter malicious behaviors that may affect data request quality (e.g., coordinated attacks, free-riding. etc.).

SEDA Token

In this section we breakdown the different utility profiles of the SEDA Token.

The SEDA Token (SEDA), previously known as Flux Token (FLX), serves three distinct purposes: governance, participation, and network utilization.

PAGE
Secure (Stake)

PAGE
Utilize (Build)

PAGE
Govern (Vote)

🔓 Secure (Stake)

Token holders can stake their SEDA tokens by running their own validator node or delegating them to a professional node operator. Within the network, economic incentives encourage token holders contributing to the network to behave honestly. Honest actors earn rewards, while malicious actors may lose part of their stake in the network. Network participants include Validators, Solvers, and Data Request Executors (DRES). Incentives can be fee payments, token staking, or token distribution through token creation.

🏗️ Utilize (Build)

To query the SEDA Network and utilize the data it supplies, data consumers that issue data requests lock value that solvers can claim by bridging the data request outcome back to the destination network. The solver burns a designated amount of SEDA Tokens to issue the data request on the SEDA Network. The number of tokens burned scales with the complexity of the issued data request.

📯 Govern (Vote)

Token holders have control over the SEDA Network. They can post and vote on proposals for network changes, such as consensus updates or network parameter changes (token creation, fees, etc.).

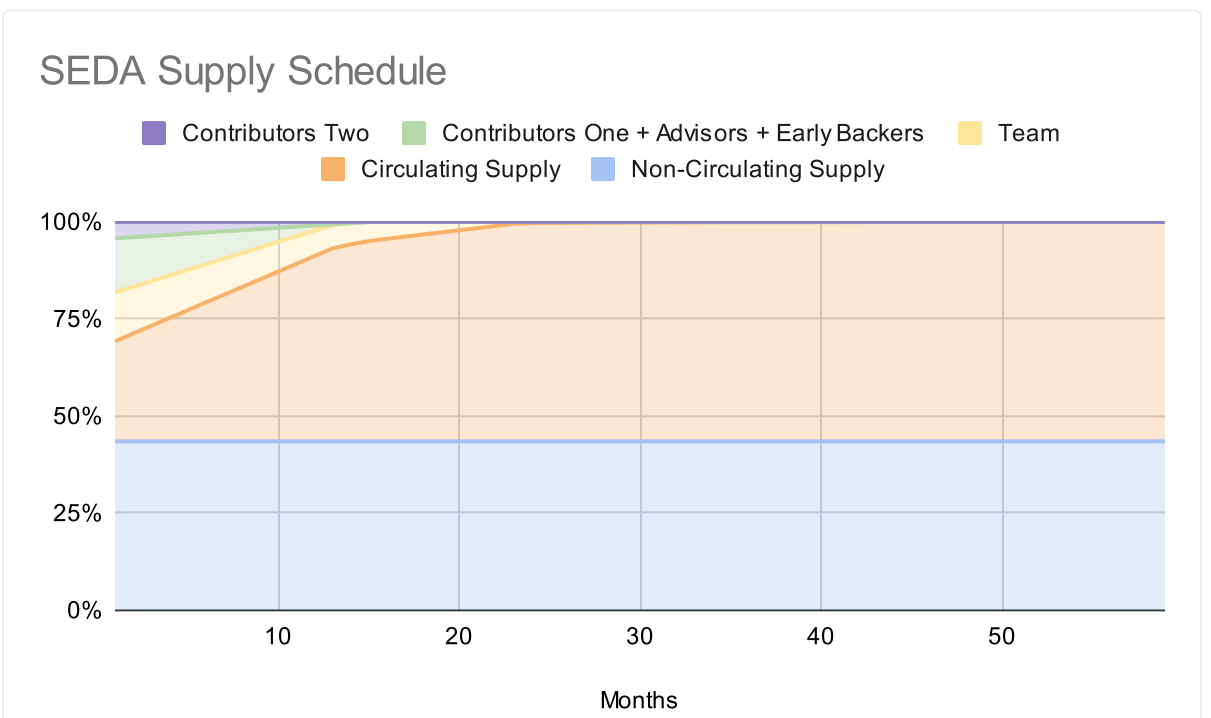
SEDA Distribution Schedule

Please find information about the SEDA Token Distribution Below.

General Token Information

- **Total Supply at Genesis:** 1,000,000,000 SEDA
- **Circulating Supply:** https://explorer-api.mainnet.seda.xyz/main/trpc/supply.circulating

SEDA Vesting Schedule



SEDA Vesting Schedule Overview

Vesting Schedule Breakdown

Qualified Network Launch of SEDA (prev. known as FLX) **December 4th, 2021. Lock-ups start for Founders, Contributors, Advisors, and early Team at the Qualified Network Launch.**

Team + Advisors

- **cliff/lock-up:** variable between 6-14 months
- **vesting:** variable between 36-60 months

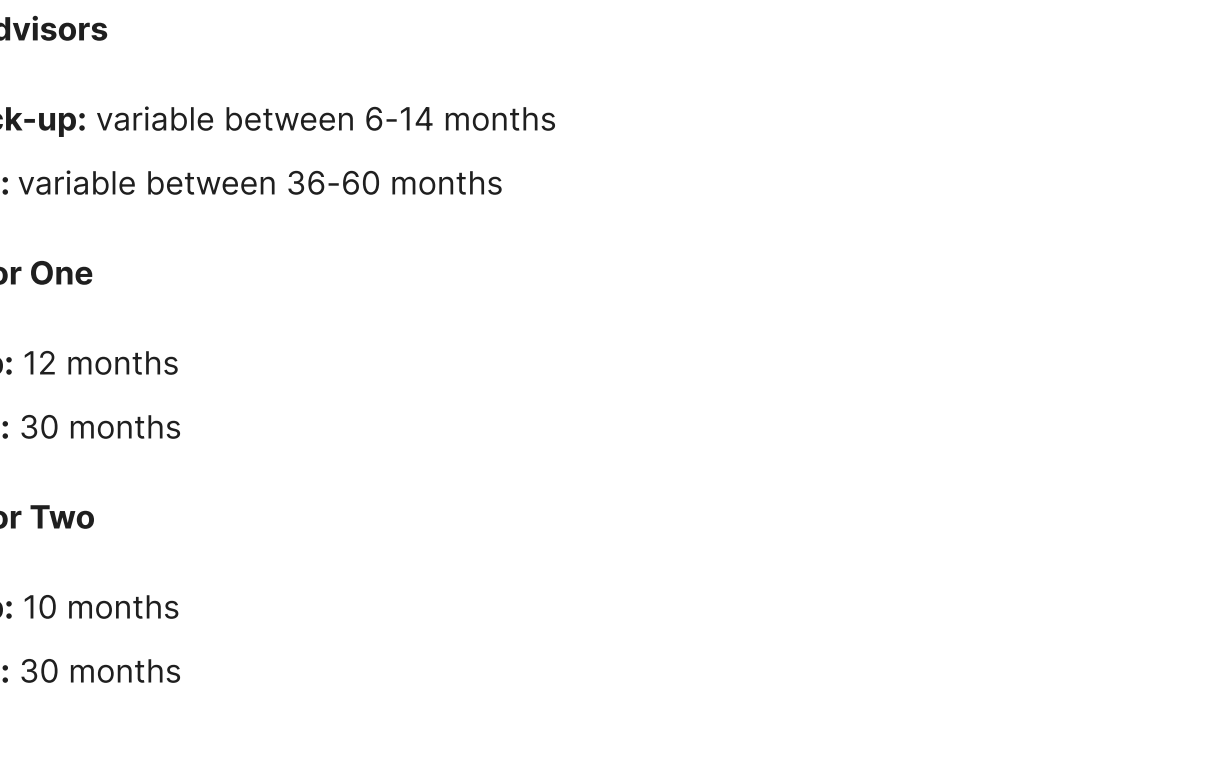
Contributor One

- **lock-up:** 12 months
- **vesting:** 30 months

Contributor Two

- **lock-up:** 10 months
- **vesting:** 30 months

SEDA Remaining Allocation Breakdown



SEDA Allocation Breakdown

- **SEDA Treasury:** 43.5%
- **Circulating Supply:** 25.8%
- **Contributors One + Advisors + Early Backers:** 13.9%
- **Contributors Two:** 4.2%
- **Team**: 12.6%

Fundraising Information:

SEDA has raised $22m in total funding from Coinbase Ventures, Reciprocal Ventures, Distributed Global, Hack VC, Uncorrelated, Coinfund, among others in addition to a token sale via a Liquidity Bootstrap Pool.

Token Upgrade - FLX -> SEDA

Upgrade from the FLX token standard to SEDA

Existing holders of the FLX utility token will be able to upgrade, one-to-one, to the new token standard that will power the SEDA Network. The SEDA Token will act as the main utility token and will be launched with the mainnet deployment of the SEDA Network.

Stay tuned