The Decentralized Infrastructure Network (DIN)

A permissionless marketplace for high-throughput blockchain APIs and services across N-Networks

-- OPERATIONAL DRAFT --

November 2024

Infura and DIN Team
din@consensys.net

Abstract

The Decentralized Infrastructure Network (DIN) reimagines the accessibility and scalability of APIs and services by establishing a decentralized marketplace for high-throughput, cross-network blockchain services. In traditional blockchain interactions, a Remote Procedure Call (RPC) serves as a bridge between applications and blockchain data, enabling users to retrieve data or send transactions to the network. Most users rely on third-party RPC providers because running personal infrastructure is complex and costly. However, centralized RPC providers come with limitations — they face operational challenges in supporting new networks and risk single points of failure, which could jeopardize network reliability and user access. Building on the principles set by platforms like Ethereum, DIN responds to the growing demand for decentralized, reliable blockchain infrastructure.

DIN introduces a decentralized alternative, enabling multiple infrastructure providers to collectively maintain a robust network that reduces reliance on any single entity and aligns with the ethos of a trustless Web3 ecosystem. Now launching as an Actively Validated Service (AVS) on EigenLayer, DIN integrates AVS functionalities to enhance economic security and service-level agreements (SLAs). By utilizing EigenLayer, many node operators and infrastructure providers can participate in DIN to offer their services using their existing staked assets. This provides a robust economic foundation for SLA adherence, incentivizing performance while managing risks through an established layer of economic protection.

Within DIN, key roles—such as node providers, network watchers, and Web3 Gateways—ensure reliable and accurate API delivery while promoting decentralization and high service standards. The governance structure, managed through a DAO or Foundation, supports long-term sustainability and community-driven evolution. Through this innovative framework, DIN advances a decentralized, scalable infrastructure solution that ensures resilience, economic security, and high efficiency for blockchain services in the Web3 space.

Disclaimer: This document is an operational draft intended for discussion purposes. It outlines the concepts and potential designs for the Decentralized Infrastructure Network (DIN). The contents are subject to change as the protocol and ecosystem evolve, and should not be relied upon as final or complete information. The document is presented to invite feedback and collaboration.

1. Introduction

1.1 An Infura Origin Story

Cryptocurrencies have risen to a market capitalization of over 3 trillion US dollars in over twelve years with Ethereum reaching close to $600bn in November 2021. Over the years, cryptocurrency networks have evolved from being a simple value transfer system to a blossoming eco-system of publicly verifiable and decentralized finance. For example, if we only consider the Ethereum network in 2021, users have collectively paid more than $9bn in network fees, the network has moved over $11tn in assets and over $153bn of assets are locked in decentralized applications [1].

With this backdrop, networks like Ethereum have faced significant scalability challenges as the demand for block space has surpassed the ability to process all transactions at a low-cost. This has led to many dApps deploying on other networks than Ethereum as it is simply no longer economically viable. The community have long foreseen this problem and various scalability solutions to alleviate it are now emerging including a roll-up-centric roadmap, directed acyclic graph based networks, and modifying the parameters of the go-ethereum implementation and battle-testing its capabilities in the wild.

Infura focuses on an orthogonal and equally important problem of scaling services that build on top of a cryptocurrency network. Infura was launched in July 2016 to support developers building dApps on Ethereum by removing the need for them to set up their own node infrastructure to interact with the blockchain. Infura provides an API to developers which enables them to fetch information from the Ethereum blockchain and to use it as a gateway for sending transactions to the network. The API replicates the JSON-RPC API provided by an ethereum node, which allows developers to easily swap between their own infrastructure, Infura, and additional infrastructure providers.

Over the years, Infura has witnessed the scalability challenges for services built on blockchain networks. Infura processed approximately 120 million requests per day in 2016, an average of 6.5 billion requests per day in 2018 and by 2021 it was processing over 2 billion eth_call requests every day.[1]

At the time of publication, Infura is a Web2 company that competes with its rivals in a market that is easily commoditized. The weakness of the Web2 model is the inability to deploy a reliable and robust service with 99.999% uptime and reliability. In November 2021, Infura witnessed this weakness firsthand as it experienced its first severe service interruption in over four years due to a consensus bug affecting specific versions of Geth (v.1.9.9) and (v1.9.13). This impacted several prominent dApps including the MetaMask wallet until the incident was resolved.

The outage became a reflection point for the Infura team to prioritize the development of a more robust design. We began work on a more decentralized design that could overcome the limitations of the Web2 marketplace. It would allow infrastructure providers to collaborate towards building a more robust network that could service a high throughput of blockchain API requests with better reliability, less trust, and greater decentralization.

1.2 The RPC Trilemma

There's a love for trilemmas in the Ethereum community as indicated in early Vitalik blog posts about scaling [2]. Web3 infrastructure demands are rapidly expanding as more developers and users engage with dApps, highlighting the need for scalable, decentralized, and reliable infrastructure solutions [3]. As the backbone of Web3, Infura as a Remote Procedure Call (RPC) provider found itself caught in an "RPC Trilemma," where we must choose between three often-competing priorities: (1) maintaining industry-leading performance, (2) rapidly deploying new services, and (3) keeping costs sustainable.

[1] An eth_call simulates the execution of a transaction and is the most computationally expensive type of request.

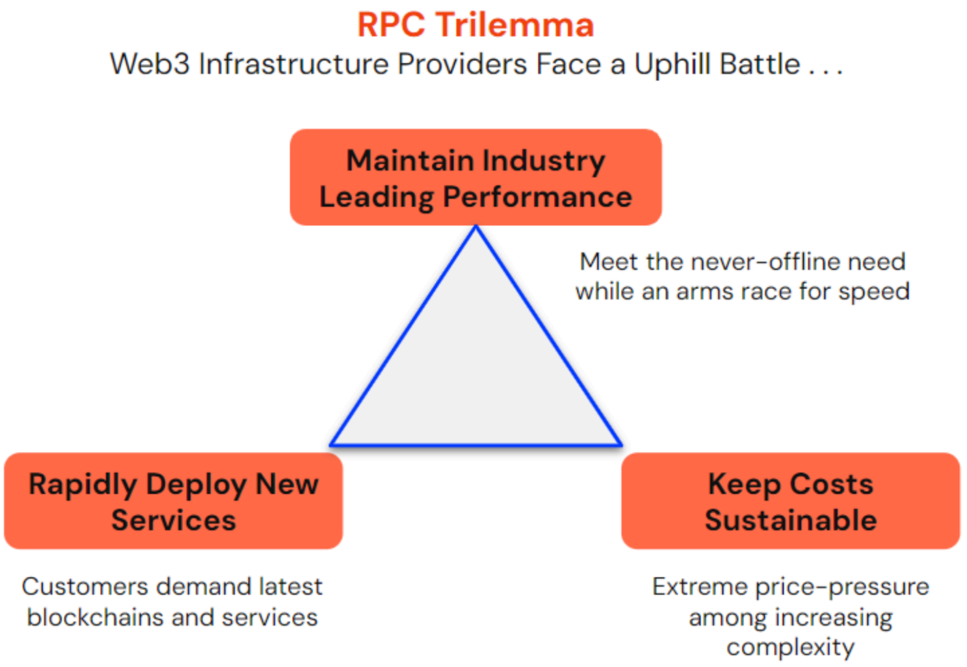

RPC Trilemma
Web3 Infrastructure Providers Face a Uphill Battle . . .
Maintain Industry Leading Performance
Meet the never-offline need while an arms race for speed
Rapidly Deploy New Services
Customers demand latest blockchains and services
Keep Costs Sustainable
Extreme price-pressure among increasing complexity

Figure 1: RPC Trilemma

Achieving industry-leading performance is essential for today's blockchain networks, where the need for "never-offline" reliability is underscored by an arms race for speed and throughput. Users expect seamless, uninterrupted access to data, putting pressure on infrastructure providers to minimize latency and maximize resilience.

The ability to quickly deploy new services is crucial as the Web3 landscape rapidly evolves. Developers and users alike expect instant support for emerging blockchain networks, specialized protocols, and upgraded services, requiring providers to stay agile and responsive to frequent technological changes.

Maintaining sustainable pricing has become increasingly challenging as the infrastructure grows more complex. With the need to balance intensive computational demands, high availability, and rapid scaling, RPC providers face substantial cost pressures in an industry where price competitiveness is often paramount.

1.3 How DIN Addresses Centralized RPC Challenges

DIN provides a decentralized solution by allowing a network of independent infrastructure providers to offer RPC services, removing the reliance on a single, centralized provider. By decentralizing RPC, DIN enhances resilience, as multiple providers collectively handle requests, distributing load and reducing the impact of outages. DIN leverages a decentralized governance model and token-based incentives to ensure that providers meet performance standards, while its integration with EigenLayer enables economic accountability and real-time validation of service quality. This decentralized approach complements the existing RPC ecosystem by creating a more reliable, scalable, and community-driven alternative.

DIN that aims to be a self-sustaining system. Multiple infrastructure providers will work together to provide blockchain API access to anyone, without the need for purchasing from a centralized party.

1.4 Structure of Whitepaper

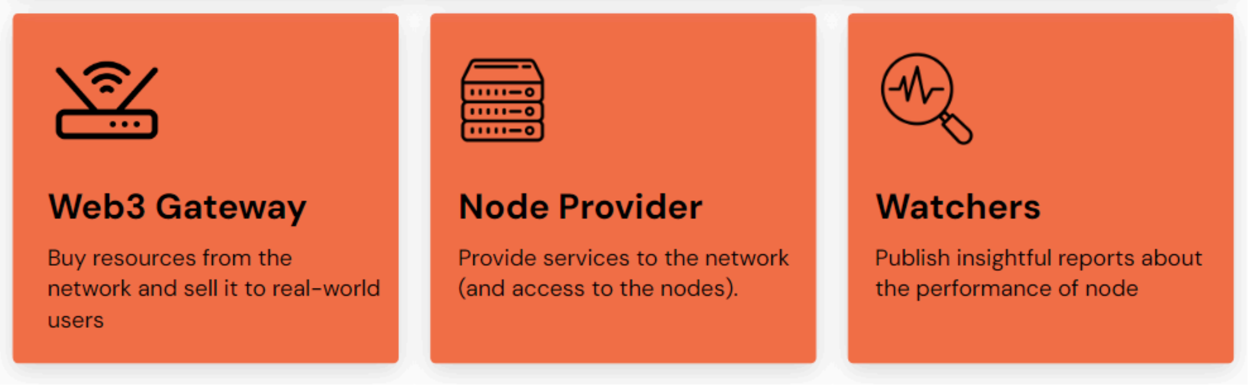
This paper is structured in the following way:

- **Protocol from a long term perspective** - We present the original vision and goals of DIN's actors, incentives, and architecture.
- **Roadmap (Federated to DAO)** - A brief overview of the phases of the roadmap implementation of DIN (since starting in Nov 2022).
- **DIN as an AVS** - Details on the role of EigenLayer implementation with processes in joining the network and authentication.
- **Mechanism Design** - Breakdown of mechanisms and goals from all key actors. A whitepaper dedicated to mechanism design will be published in Q1 2025.
- **Potential Issues, Surface Attacks, and Remedies** - Additional discussion points and edge cases considered by our design.

2. Decentralized Infrastructure Network (DIN)

The Decentralized Infrastructure Network (DIN) is designed to unite infrastructure operators in providing a robust, high-throughput system for handling blockchain API requests. At its core, DIN leverages a decentralized structure to distribute service demands across multiple independent providers, enhancing reliability and reducing the risks associated with single points of failure typical in centralized models.

2.1 Overview



Web3 Gateway

Buy resources from the network and sell it to real-world users

Node Provider

Provide services to the network (and access to the nodes).

Watchers

Publish insightful reports about the performance of node

Figure 2: DIN Key Actors/Agents

The network comprises several key actors/agents, each fulfilling a unique role to ensure operational efficiency and service accuracy:

1. **Node Providers:** These are the core participants who operate blockchain nodes and essential infrastructure to process API requests efficiently. By decentralizing the node operation among multiple providers, DIN enables a dynamic load-balancing system, which distributes traffic based on current demand, reducing latency and improving fault tolerance. If a provider experiences downtime, other providers seamlessly take over to ensure uninterrupted service.

2. **Network Watchers:** Watchers monitor and verify the performance of Infrastructure Providers by sending requests and validating responses against independent data. This decentralized monitoring mechanism supports network transparency and service accuracy, with watchers publishing results to a public ledger. This data informs further crypto-economic incentives, as providers demonstrating high performance are rewarded, while those who fail to meet standards may face penalties.

3. **Web3 Gateways:** These agents accept payments from users and handle the routing of API requests to the appropriate infrastructure providers based on predefined SLAs and user preferences. Web3 Gateways offer value-added services such as customer support and documentation, which enhance the user experience. Although users may interact directly with DIN, most are expected to prefer the ease and added support provided by Web3 Gateways.

4. **DAO or Foundation:** The governance hub, potentially structured as a DAO, oversees DIN's protocol evolution, roadmap, and service standards. This governance model ensures decentralized decision-making, with stakeholders voting on network

policies, protocol upgrades, and reward allocations to maintain the network's stability and continued growth.

DIN is also inspired by The Cosmos Hub, which connects different chains and provides a central governance structure, creating a model for interoperability and decentralized network management [4]. Learning from Cosmos' years of live services, DIN's architecture parallels the ideals of decentralized, interoperable networks.

Crypto-economic designs can effectively incentivize providers to ensure data accuracy and reliability, promoting adherence to SLAs between users and service providers. These mechanisms encourage positive behavior through rewards for high performance and apply penalties for low-quality or incorrect data, thereby fostering a trustworthy and high-quality infrastructure. By aligning incentives, providers are motivated to maintain excellence and uphold the integrity of the network.

2.2 Agents in detail

2.2.1 Node Provider

Node providers are the agents ultimately responsible for serving API requests. They will fulfill the requirements of at least one capability supported by the network, for example, the Ethereum Mainnet JSON-RPC API.

Providers may additionally, or alternatively, satisfy other capabilities as they are added to the network. A (nonexhaustive) list of potential additions over time:

- Layer 2 protocols like Linea, Arbitrum, or Optimism
- Higher level APIs like NFT metadata and historical transaction indexes
- Additional Layer 1 protocols like Bitcoin, Solana, BNB Smart Chain (BSC), and Avalanche

Node providers may either run their own bespoke configurations as they already have the expertise for, or they may choose to use open-source utilities that Infura will publish to aid in running infrastructure for these blockchain APIs.

In order to be eligible for serving requests on the network, node providers must first register with a smart contract on an EVM-compatible network (e.g. Linea, Ethereum, etc), describing their capabilities and providing a stake to ensure good behavior. This is further described in the Protocol Overview.

2.2.2 Network Watcher

Network watchers are the agents that help ensure that node operators are operating honestly and effectively.

They will operate by running a suite of tests ensuring that node providers are adhering to the published service definition and that they are meeting the quality and performance requirements as dictated by the network. For example, a network watcher may continuously request the latest block information from 11 different node operators and keep track of who is propagating the latest block data accurately and quickly. This addresses a unique challenge in serving JSON-RPC requests within a decentralized system, providing a continuous measurement of how effectively providers maintain synchronization with the blockchain's head, which cannot be easily verified using cryptographic proofs alone.

The results of this monitoring from network watcher agents will be published on a decentralized event stream. Potential consumers of DIN services would directly, or via tooling, use the event stream data to make their Node Provider routing selections.

In order to publish data that may be used for reward and slashing decisions of node providers, network watchers will also need to first register with a smart contract on an EVM-compatible network and provide a stake to ensure good behavior. Network Watchers are subject to crypto-economic incentives to prevent bad behavior or malfunctioning, including slashing conditions for failing to publish updates consistently, excessively publishing, or providing incorrect information.

2.2.3 Web3 Gateways

Web3 Gateways are the agents who serve as DIN’s access point for end users by handling payments and optimally routing requests to the DIN Router based on user-defined preferences and SLA criteria within their own business.

A Web3 Gateway (e.g. Infura) will be responsible to run their own API servicing infrastructure capable of providing an accessible interface for the consumer users of the decentralized infrastructure network to obtain access to the network. They can also provide additional services to users associated with traditional SaaS providers, like technical support and customer service, invoice and receipt generation, and supplementary documentation.

Users of the network are not required to go through a Web3 Gateway, but an assumption of the network is that most users will have a desire to access the services of a Web3 Gateway, making their role in the network valuable. Web3 Gateways are effectively market resellers purchasing service capacity from various Node Providers and offering a unified and simplified user experience.

2.2.4 DIN DAO or DIN Foundation

The DIN DAO or DIN Foundation is the coordinating and governance hub of DIN. It is responsible for creating the roadmap of the network. It is responsible for delegating authority to the participants in the network to take on the roles and tasks required for the sustained operation and required growth of the network. The foundation is responsible for continued development and maintenance of the protocol.

Through community proposals and weighted voting, the DAO oversees protocol decisions such as adjusting reward structures and SLA requirements. The future governance framework will ensure that DIN remains adaptable and responsive to technological progress while preserving community control over strategic directions. In implementation, this phase of governance will require a proof of a sustainable business model. We're wary of decentralizing too early and the overhead of community collaboration.

2.2.5 Blockchain Protocols

Blockchain Protocols are interested in their blockchain having a sufficient number of independent infrastructure operators running nodes for their network. This ensures that users of that chain have ample options to access that chain.

As a blockchain protocol is created, it runs into a problem where node providers require payments from blockchain protocols in order to have the necessary incentive to take on the fixed and variable costs associated with running the infrastructure for that blockchain protocol before there is true demand amongst users for the protocol. Thus, blockchain protocols often find themselves negotiating with multiple node providers to run nodes, and have to give node providers some form of capital. This process tends to be inefficient for both the blockchain protocol and the node provider as the negotiations may include a floating token associated with the blockchain protocol.

Through DIN, Blockchain Protocols gain access to a decentralized marketplace of infrastructure providers where the foundation of the protocol can offer up a protocol bounty to incentivize node providers to run nodes. This node bounty serves as a pool available to a set number of providers who successfully set up and prove a certain service level agreement for that blockchain protocol. The market of operators will converge toward a certain price per network which, if it is more capital efficient, can result in more node providers running nodes at a favorable price for all parties.

This model helps new and growing protocols bootstrap reliable infrastructure without the upfront investment and operational costs typically required to establish node operators.

2.2.6 Users

Users are the ultimate reason for the existence of this network. Many types of users, including dApps, enterprises and other entities that require simple, reliable, and low-cost access to blockchain APIs (as evidenced by the success of existing providers like Infura).

Users can access DIN's services in two ways:

1. **Direct Access:** Users can interact directly with DIN Node Providers, establishing their own configurations and SLA preferences for API requests. This option allows users to engage with DIN in a decentralized manner, while still benefiting from the AVS-validated quality and reliability standards that underpin DIN's operations.

2. **Web3 Gateways:** For users seeking additional support, Web3 Gateways provide a managed interface to DIN. They accept payments, handle request routing, and offer value-added services like technical support and customized billing, making it easier for users to integrate DIN's services into their operations.

Through this dual-access model, DIN adapts to the diverse needs of its user base, offering flexible, decentralized access to blockchain infrastructure while ensuring service reliability.

2.3 Protocol goals

DIN aims to create a resilient network capable of meeting the evolving needs of the Web3 ecosystem. Our goal is to build a reliable and robust network of service providers who can serve high-throughput requests. With this backdrop, we explore the goals of each agent in turn.

2.3.1 User Experience Goals

The user experience should be similar to Web2 when interacting with DIN. To put it another way, a user can pay for usage, send requests to an API, and not be aware of details about DIN.

To summarize:

- **Standard API:** All node operators adhere to a common API which allows a user to send requests to one or more operators using the same software. This standard is governed by the DAO. The standard is implemented via the **DIN Router**, which is a node that handles the routing of requests amongst providers.

- **No staking or on-chain registration:** Users are not required to stake or lock tokens to use the network.

- **Flexible and seamless payments:** The service's payment could be settled in a stablecoin, DIN issued token, or other stable denomination on the network. The system would leverage the DeFI ecosystem to handle immediate conversions without interfering with the user experience. The **DIN Payments** component will use a version of state channel payments on a Layer 3 to net settle these services.

2.3.2 Node Provider Goals

The largest expenditure for a node provider is the operational cost (e.g. Cloud, storage, human capital Devops engineers, etc). It is crucial they can join the DIN as a for-profit venture and sustain their business model in the long-term.

To summarize:

- **Profitable venture:** The user fees and network rewards alongside protocol-incentivized subsidies, enable it to be profitable for an operator to participate in the network.

- **Custom infrastructure:** Operators are not required to run the same software stack as other operators.

- **Optional capabilities:** Operators can choose which networks/protocols they will support. In addition to the common API for these protocols, other APIs and capabilities can be provided if the operator chooses to do so.

- **Common API adherence:** For the protocols they support, the operators must adhere to the common API standard governed by the DAO.

- **Optimize performance:** Operators should compete amongst themselves on the quality of service provided to the users.

- **Economic Security and Accountability:** Operators are required to stake tokens, creating a strong economic incentive to deliver reliable and accurate services. Any deviation from SLA standards may lead to slashing, ensuring operators align with network reliability goals.

2.3.3 Watcher Goals

Network Watchers serve as the decentralized monitoring layer (e.g. status/explorer pages, testing of node providers) for DIN. It is a watcher's core responsibility and commitment to the network to report a good or degraded service alongside evidence of how each individual node provider is performing.

To summarize:

- **Real-Time Monitoring and Validation:** Watchers continuously assess Node Provider performance, tracking SLA adherence, latency, and data integrity. They relay these metrics to a public ledger, supporting transparent, real-time performance monitoring.

- **Indistinguishable requests:** A node provider cannot identify whether a request is sent from a user or a watcher.
- **Standardized testing:** All watchers periodically perform the same set of tests to ensure their results are comparable.
- **Open membership:** A watcher is required to run the infrastructure required to verify that a node provider is returning accurate responses to users within the agreed upon service level agreement. Becoming a watcher will require committing to operate with the necessary infrastructure and integrity. In the immediate term (federated), watchers will be preselected.
- **Invalid responses are publicly verifiable:** A watcher can provide indisputable evidence to other watchers and members of the DAO that a node operator's response is invalid.
- **Economic Incentive Alignment:** Watchers are economically bonded by staking tokens that can be slashed if they fail to perform validation duties with integrity. This ensures their commitment to unbiased, reliable monitoring. Based on the latest implementation, DIN is launching as an AVS to allow for EigenLayer operators to control staking and slashing SLAs, which provides an independent reward structure to network watchers for playing a crucial role to the DIN ecosystem.
- **Reward Structure:** Watchers are rewarded a set fee for testing the network and can also receive a percentage of slashed tokens when they are able to provide indisputable evidence to other watchers and members of the DAO that a node operator has deviated from the protocol specification of DIN.

2.3.4 DAO or Foundation Goals

The DIN DAO or Foundation serves as the governance body, ensuring that DIN evolves in line with community interests, maintains high standards, and responds effectively to changing technology and user needs. Token holders are responsible for governing and maintaining DIN. They vote on a variety of governance issues, including upgrades to the protocol, network integrity, and fee structures. Their incentives are directly aligned with the network's performance and success.

To summarize:

- **Governance and Policy Adaptation:** The DAO oversees network policies, manages SLAs, and makes critical decisions on reward and penalty mechanisms. This includes voting on changes to staking requirements, operator incentives, and network configurations as needed.

- **Transparent Decision-Making:** All proposals and votes are made public, allowing stakeholders to participate directly in DIN's evolution and ensure alignment with the community's vision.

- **Sustainable Economic Model:** The DAO is responsible for managing rewards, penalties, and bounties, ensuring DIN's financial sustainability and maintaining a balanced incentive structure that attracts and retains high-quality Node Operators and Watchers.

- **Crisis Management and Security Audits:** The DAO can implement emergency policies, upgrade protocols, and conduct regular security audits to ensure DIN's resilience against potential vulnerabilities or external threats.

All members can submit and vote on proposals related to:

- **DIN staking threshold:** Parameters for infrastructure providers or specific nodes to be added to the marketplace offering.

- **Mint node provider licenses**: Review the existing services of the node provider on their general trustworthiness and ability to adhere to the staking threshold.

- **Mint node provider licenses:** Review the performance data provided by the watchers and decide to mint a license for a specific set of nodes to be added to the network.

- **Network Integrity:** Temporarily suspend or remove unreliable node operators from the network.

- **Protocol Upgrades:** Upgrade the protocol such as the base API and allow for the evolution of service offerings on the network.

- **Reward structure:** Fee and subsidy parameters for users, watchers and node operators of the network.

2.3.5 Blockchain Protocols Goals

Blockchain Protocols are interested in their blockchain having a sufficient number of independent infrastructure operator entities running nodes for their network. This ensures that users of that chain have ample options to access that chain. Their incentives are directly aligned with the networks' performance and success as it ensures their blockchain is sufficiently resilient in the case any one provider is no longer able to provide services.

To summarize:

- **Robust Network Access:** DIN ensures that users and dApps have consistent, reliable access to blockchain protocols through decentralized infrastructure, even during high-demand periods. This reduces the load on protocols to support dedicated node infrastructure.

- **Bounty Programs for Protocol Support:** DIN allows blockchain protocols to incentivize Node Providers to run network-specific nodes by setting up bounty programs. This helps bootstrap infrastructure support for new or emerging protocols.
- **Decentralization and Economic Security:** Blockchain protocols benefit from DIN's AVS-based staking and slashing framework, which aligns incentives and economic security for Node Operators. This decentralization reduces risks associated with single points of failure typical in centralized API providers.
- **Flexible, Scalable API Service:** DIN is designed to scale as protocols grow and adapt, supporting new chains and enhancing API offerings to meet evolving user needs. Protocols can rely on DIN to integrate emerging technologies and updates, such as light-client capabilities, to enhance network access without compromising decentralization.

3. Roadmap Implementation

DIN is progressing through a carefully structured roadmap that gradually enhances its decentralization, scalability, and governance capabilities. This roadmap is divided into key phases, each designed to build on the last, ensuring a robust and resilient network.

DIN is currently operating in a **Federated Phase**, where alpha customers, including Infura and MetaMask, are driving network traffic and shaping core functionalities. As DIN matures, it will incrementally adopt decentralized components, ultimately evolving into a community-governed, permissionless infrastructure with integrated payment and governance layers.

3.1 Federated Phase (Current Phase)

The **Federated Phase** is the foundational stage of DIN, where the network's initial components are deployed, tested, and refined in a controlled environment with trusted alpha customers. This phase focuses on establishing DIN's basic operational capabilities, ensuring service reliability, and verifying economic viability before fully opening the network.

3.1.1 Joining DIN

Acceptance Criteria and Minimum Performance Thresholds: During this phase, DIN implements strict entry requirements for Node Providers and Network Watchers, ensuring that each participant meets predefined performance standards. Providers must demonstrate compliance with service-level agreements (SLAs) covering metrics such as response freshness, data validity, and uptime.

Assigned Identities for DIN Routing: Each participant is assigned a unique identity, enabling seamless routing of developer API requests to the appropriate DIN Providers. This identity management system lays the groundwork for effective transaction processing and tracking, setting clear accountability for each operator within the network.

3.1.2 Processing Transactions for DIN

Transaction Routing from Alpha Customers: Infura and MetaMask generate developer API traffic, which is routed through DIN Provider nodes. This federated setup enables DIN to validate its routing efficiency, latency benchmarks, and load-balancing algorithms under real-world conditions.

Traditional Invoicing and Payment Validation: In this phase, payments from alpha customers to DIN Providers are handled through traditional invoicing, allowing DIN to test and refine its financial tracking and reward distribution processes. This traditional invoicing approach provides DIN with critical insights into payment workflows, helping to prepare the network for decentralized, on-chain payment models in later phases.

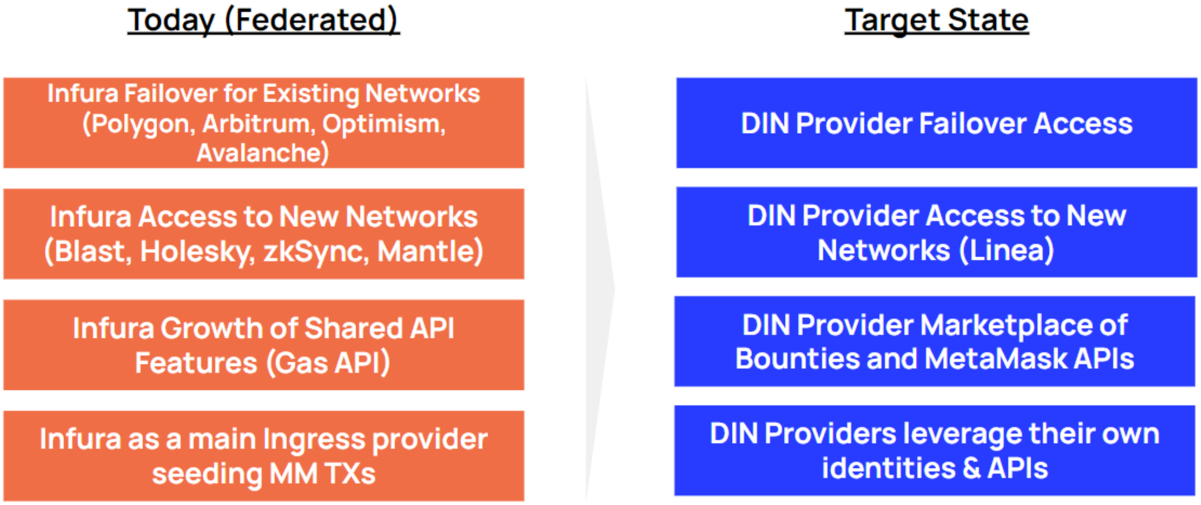

Today (Federated)
Infura Failover for Existing Networks (Polygon, Arbitrum, Optimism, Avalanche)
Infura Access to New Networks (Blast, Holesky, zkSync, Mantle)
Infura Growth of Shared API Features (Gas API)
Infura as a main Ingress provider seeding MM TXs
Target State
DIN Provider Failover Access
DIN Provider Access to New Networks (Linea)
DIN Provider Marketplace of Bounties and MetaMask APIs
DIN Providers leverage their own identities & APIs

Figure 3: Expanding DIN towards Progressive Decentralization

3.2 Progressive Decentralization (2025)

In 2025, DIN will transition from its federated setup to a progressively decentralized network. This phase introduces additional layers of decentralization, with expanded functionality for transaction routing, payments, and governance, marking the beginning of DIN's evolution towards a permissionless infrastructure. With inspiration, the Cosmos Hub introduced a modular approach to interoperability, allowing networks to expand and evolve through phased upgrades [5].

3.2.1 DIN as an AVS

The practical implementation of the network watcher has explored usage of DIN launching as an Actively Validated Service (AVS) on EigenLayer. EigenLayer's AVS model provides a robust framework for economic alignment and real-time performance enforcement [6]. DIN has integrated new functionalities that streamline agent onboarding, improve oversight via a watchtower, and establish a structured accountability model without launching a token that may have floating value.

- **Onboarding Components:** Ability for Providers to stake and add their wallet identities to join the DIN Router Registry contracts

- **Economic Security SLAs:** Watcher and AVS Operator capabilities for staking, slashing, and challenging the onboarded node performance and reputation of entities in DIN.

The DIN AVS system aims to deploy Watchers with a dedicated "Watcher node kit," which operates as both a monitoring tool and a user-friendly interface to the DIN network backend. Through the AVS interface, Watchers access essential modules for onboarding DIN Providers, viewing onboarding notes, tracking network status, and enforcing slashing protocols.

Acting as operators on EigenLayer, DIN Watchers not only monitor service accuracy and reliability but also uphold AVS-based slashing and staking rules for performance infractions. Watchers gather and analyze response data by running simulated requests to ensure adherence to service-level agreements (SLAs). Their results are then published on a public event stream, providing transparency and informing DIN's crypto-economic incentives. By aligning with EigenLayer's AVS structure, DIN strengthens its validation processes, ensuring real-time accountability and economic security for all network participants.

3.2.2 Decentralized Traffic Processing

Provider-Driven Routing Capabilities: Providers in the DIN network will gain the ability to route service traffic through various Web3 Gateways, not limited to Infura. This expanded functionality decentralizes the routing process, creating an open network where multiple Web3 Gateways can interact with DIN Providers.

DIN Payments Layer 3 Network: DIN will implement an on-chain payments layer on Linea as a Layer 3 to facilitate real-time, decentralized payments among DIN Providers and Web3 Gateways. This payments layer will allow for seamless, automated transactions, eliminating the need for traditional invoicing and streamlining economic interactions within DIN. Operators will be compensated based on their service contributions, with payment records transparently available on-chain.

3.2.3 DIN Foundation and Governance

Establishment of the DIN Foundation: The DIN Foundation will be formed to oversee shared services, community initiatives, and technical upgrades, ensuring that DIN remains aligned with the community's evolving needs. The Foundation will manage essential services like security audits, research funding, and cross-protocol collaborations.

Decentralized Governance and DAO: The introduction of a DIN DAO will enable community-led governance, where stakeholders propose and vote on protocol upgrades, SLA adjustments, and economic policies. Token holders who stake within the DAO gain voting rights, empowering them to shape the future of DIN and ensuring that governance decisions reflect the collective interests of the network.

3.3 Incentivized Testnet as a Mechanism Design Laboratory

Incentivized testnets are invaluable for stress-testing decentralized infrastructure and optimizing network mechanics before mainnet deployment [7]. The DIN Incentivized Testnet is a vital component of DIN's mechanism design, allowing the network to test, validate, and optimize its economic structures in a live, controlled environment. The testnet enables DIN to fine-tune its staking, slashing, reward, and governance mechanisms before mainnet deployment.

3.3.1 Economic Testing and Reward Calibration

Staking and Slashing Simulations: The incentivized testnet allows DIN to run simulations of staking and slashing mechanisms, identifying optimal thresholds for penalties and ensuring that the economic deterrents are effective without being overly punitive.

Reward Structure Optimization: By distributing rewards based on testnet performance, DIN collects data on the effectiveness of its incentive structures, including high-performance bonuses and routing efficiency rewards. This feedback helps the DAO calibrate rewards to ensure they align with desired behaviors and network standards.

DAO Policy Feedback: Testnet participants are encouraged to provide feedback on the economic and governance policies in place. This input allows the DAO to make informed adjustments, ensuring that the network's policies are fair, practical, and aligned with community expectations.

3.3.2 Participant Onboarding and Reputation Building

Early Access to Economic Mechanisms: Node Providers, Watchers, and Web3 Gateways gain early access to DIN's staking, slashing, and reward systems through the testnet. This experience allows them to adapt to DIN's operational standards and fine-tune their infrastructure, reducing the learning curve for mainnet.

Reputation Establishment: Participants who perform well on the incentivized testnet build a reputation that can carry over to the mainnet, giving them a competitive edge in request routing and access to higher-tier rewards. This early reputation system encourages operators to establish themselves as reliable contributors to DIN's ecosystem.

3.3.3 Data-Driven Mechanism Refinement

Performance Data Collection: Real-time data on SLA compliance, request throughput, and operator availability from the testnet informs adjustments to the mainnet mechanism design. The DAO reviews this data to refine parameters, ensuring DIN's economic model supports scalability and network resilience.

Iterative Testing for Robust Mechanisms: The testnet enables iterative testing of new policies and mechanisms, allowing the DAO to make adjustments based on test outcomes. This iterative process ensures that only well-tested mechanisms are deployed on mainnet, reducing the likelihood of economic inefficiencies or security vulnerabilities.

3.4 Full Decentralization and Governance-Driven Expansion (2026 and Beyond)

In the final phase, DIN will operate as a fully decentralized, community-governed infrastructure, with robust economic mechanisms, autonomous routing, a sustainable business model, and a mature governance framework.

3.4.1 Open Network Access and Permissionless Onboarding

Permissionless Onboarding of Operators: The DIN onboarding process will become permissionless, enabling anyone who meets the staking and SLA requirements to join as a Node Operator or Network Watcher. This open access expands DIN's capacity to accommodate growing demand and diversifies the operator base, enhancing network resilience.

Automated SLA Compliance and Enforcement: Through further integration with EigenLayer's Actively Validated Service (AVS) model, DIN will implement automated SLA compliance checks and penalty enforcement. This ensures that performance standards are consistently maintained without manual intervention, supporting a fully autonomous infrastructure.

3.4.2 Advanced Payment and Reward Structures

Dynamic Pricing and Custom SLAs: As DIN matures, the DAO may introduce dynamic pricing for API requests and allows operators to offer customized SLAs. This flexibility enables providers to compete based on specialized services, fostering a competitive and adaptable market for blockchain API services.

Cross-Protocol Staking and Partnerships: DIN will explore partnerships with other Web3 projects, such as staking collaborations, liquidity pooling, and cross-chain integrations, enhancing DIN's economic resilience and extending its ecosystem reach.

3.4.3 DAO-Managed Innovation Fund and Ecosystem Growth

Funding for Ecosystem Development: The DIN DAO will establish an innovation fund, supporting projects that build on DIN, integrate with other blockchain networks, or advance Web3 infrastructure. This fund will fuel ecosystem growth and attract developers, researchers, and contributors to enhance DIN's utility and reach.

Community-Driven Upgrades and Enhancements: As a fully decentralized network, DIN's growth will be guided by community-driven proposals and DAO-backed initiatives. The DAO will support upgrades to DIN's core protocol, expand governance mechanisms, and enable ongoing innovation, ensuring that DIN remains adaptable and responsive to technological advancements and user needs.

3.5 Summary of Roadmap Milestones

Phase	**Milestones**	**Description**
Federated Phase (2024)	Joining DIN, Processing Transactions	Alpha customers (Infura, MetaMask) route API traffic and seed developer calls; Providers meet performance thresholds and handle transactions, with payments managed through traditional invoicing.
Progressive Decentralization (2024-2025)	DIN as an AVS, Decentralized Transaction Processing, DIN Payments Layer 3, DIN Foundation and DAO, Incentivized Testnet	Early stage integration of economic security and staking/slashing through DIN as an AVS; Providers gain routing flexibility beyond Infura; payments move to Layer 3 on-chain protocol; DIN Foundation oversees shared services and governance transitions to DAO-driven decision-making.
Full Decentralization (2025-2026)	Permissionless Onboarding, Advanced Payments, and DAO-Managed Innovation Fund	DIN becomes fully permissionless, enabling automated SLA enforcement, dynamic pricing, cross-protocol staking, and DAO-led growth initiatives, establishing DIN as a decentralized, community-driven infrastructure for Web3.

4 DIN Protocol Overview

This section describes the details of the key components and specifications within the DIN Protocol. It covers how a Node Operator or Watcher can join the network, how a user pays and makes requests to the node operators, and how the watchers can monitor the node operator's behavior. This section also covers the reward mechanism to pay the agents for running the protocol.

4.1 Technical Components

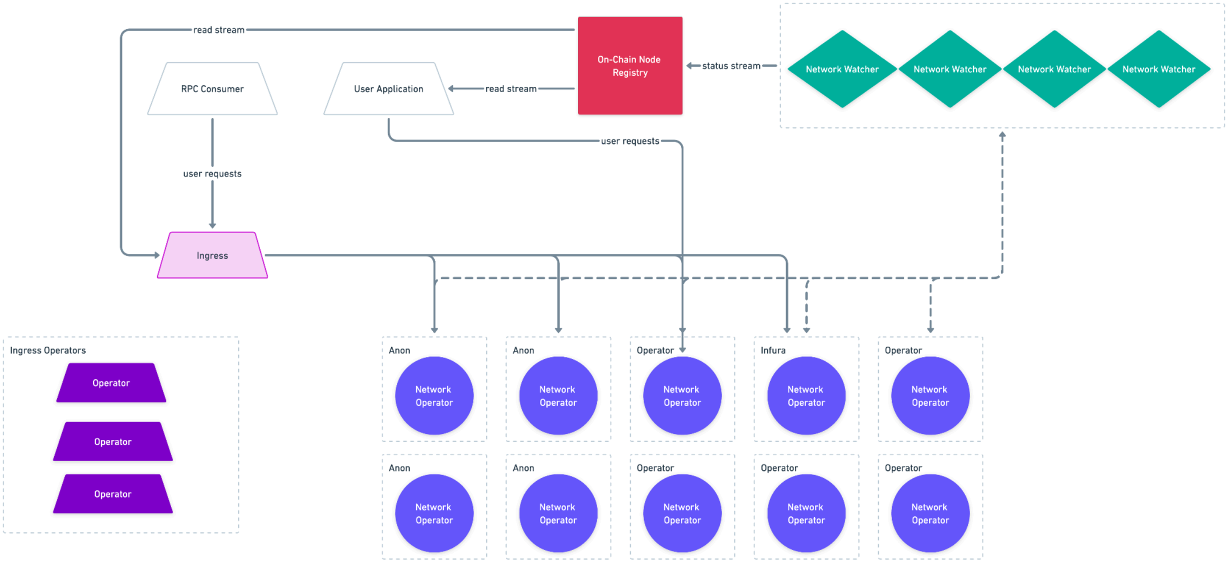


Figure 4: DIN Technical Architecture (without EigenLayer)

The Decentralized Infrastructure Network (DIN) is a high-performance, decentralized infrastructure framework designed to support blockchain data requests and API services at scale.

At the heart of DIN's architecture is a robust routing protocol in the **DIN Proxy/Router** that dynamically allocates requests across Node Operators based on capacity and performance. The DIN Router handles all traffic mapping between ingress operators and the node providers. Ingress Operators / Web3 Gateways handle payments and facilitate access to users with their own set of SLAs. Note that the **DIN Payment** component was created to focus on the Provider-to-Provider netting of balances between DIN actors. The Network Watchers monitor data validity, freshness, and availability, publishing results to a public ledger for transparency. The **DIN Watcher** component is implemented with DIN as an AVS.

This layered, modular design allows DIN to operate with high reliability and transparency, ensuring a resilient infrastructure capable of meeting the evolving demands of the Web3 ecosystem.

4.2 DIN Smart Contracts

DIN's decentralized infrastructure is supported by a suite of smart contracts on an EVM-based network (e.g. Ethereum, Linea, or a combination of networks), each designed to facilitate key functions, enforce economic security, and ensure seamless governance. These five proposed contracts manage everything from token issuance to staking requirements, registry services, and reward distribution.

Note that this model of smart contracts can be complementary to the DIN as an AVS integration. Additional mechanisms such as reward tokens or subscription-capacity NFTs may be implemented in later phases.

4.2.1 DIN DAO or Foundation Contract

The DAO contract is responsible for coordinating its members to submit proposals and collectively vote upon them.

There are two options for deploying a DAO contract: Snapshot and Gnosis Safe**.** The Snapshot platform provides a tool to authenticate users (and the tokens held) to coordinate voting. Gnosis Safe is a multi-sig wallet where appointed key holders are ultimately responsible for acting upon the actions of an approved proposal.

The contracts are written to allow for direct on-chain voting. An on-chain governance contract that can collect proposals, count votes and ultimately act upon the final decision without an intermediary. The final implementation details of the DAO contract will be decided prior to launch, but the long-term goal is to support direct on-chain voting by all token holders.

4.2.2 Staking Contract

The staking contract enforces DIN's economic security model by requiring Node Operators and Watchers to lock tokens as collateral. This stake serves as a guarantee of service quality and availability, with mechanisms in place to penalize underperforming or malicious actors. Managed via EigenLayer's Actively Validated Service (AVS), the staking contract aligns operator incentives with network performance and SLA compliance, deterring harmful behavior.

Slashing functionality will be available to allow the DAO (if malicious behavior is detected) to remove the agent alongside their deposit from DIN.

4.2.3 Node Registry Contract

The Node Registry Contract functions as DIN's public directory, where Node Operators register their supported protocols, services, and capabilities. By staking tokens and listing their services, Node Operators make themselves available for API requests from DIN users and Web3 Gateways. This registry provides transparency into each operator's credentials, performance history, and service reliability, ensuring users can make informed choices.

Node operators must submit their capabilities to an on-chain registry contract which includes:

- **Supported Networks:** A list of cryptocurrency networks supported by the operator.
- **JSON RPC Commands:** The API supported by the operator for each blockchain network. It can include custom commands.
- **Additional Metadata:** The protocol has taken into account some metadata that might be sensitive to be shared on public ledger. Information such as the IP addresses of customers or specific location of nodes for each network may be useful in the routing algorithm, but leak too much information about the Infrastructure Provider's strategies.

4.2.4 Gateway Contract

The Gateway Contract collects and manages payments from users and allocates resources across the network based on user preferences and SLAs. By holding a treasury of DIN tokens, the contract distributes rewards to Node Operators and Watchers proportionally to their service contributions. It also handles user entitlements, such as balances and request prioritization, which are monitored and enforced according to real-time SLA data from Network Watchers.

This gateway contract has two responsibilities:

- **Split reward:** It should issue a portion of the treasury as a subsidy and split the fees amongst agents who run the network.
- **Resource control:** It specifies the quantity of computational units alongside an expiry time such that a node operator can verify a user's entitlement on the network.

4.3 Joining the Network

DIN's decentralized infrastructure is designed to grow and adapt as the Web3 ecosystem evolves. Node providers and Watchers join the network through a structured onboarding process that aligns their operations with DIN's economic and performance standards.

4.3.1 Watcher Staking and Onboarding

Watchers join DIN as AVS Operators by staking via EigenLayer restaking (or DIN token registration through the staking contract). Their stake serves as collateral, with penalties enforced through EigenLayer's slashing protocols for any lapses in performance or accuracy. The watcher set is open-membership such that anyone can join given their economic staking and report on the DIN network's reliability. The quantity of required stake is adjusted by the DAO.

4.3.2 Node Operator Registration and Licenses

Node Operators must acquire a license to participate in DIN, which is obtained by joining the DIN AVS through EigenLayer restaking (or staking tokens in the staking contract). Upon registration, operators declare the blockchain protocols they support, such as Ethereum, Layer 2 networks, or additional Layer 1s, and detail their API capabilities in the Node Registry. Node Operators are then available to service requests from users, governed by SLA requirements and monitored by Watchers.

Note that the identity registration of the Infrastructure Providers (entity) and Node operators (nodes) for specific blockchain protocol services are separate. The completed registration of an Infrastructure Provider adds its identity for the application and set of tools via EigenLayer, while the individual set of nodes fulfilling the blockchain protocol requirements are separately tested and audited by the Node Watchers. In other words, an Infrastructure Provider may have an overall reputation that is impacted by their combination of nodes operating across networks. This allows specific nodes to be removed without necessarily removing the infrastructure provider entity..

The network license itself may be implemented as a non-fungible token (NFT) or identity issued within EigenLayer's protocol. This implementation is more relevant when moving from the federated to permissionless phase.

4.3.3 Protocol-specific Bounties

Blockchain protocols may offer bounties within DIN to incentivize Node Operators to support specific networks. By funding these bounties, protocols can encourage a reliable and distributed infrastructure for their ecosystem without establishing a dedicated node network. These bounties are allocated through the Gateway Contract, providing rewards to operators who meet protocol-specific SLAs.

Within this DIN Marketplace, the bounties created by protocols provide technical requirements (e.g. eth_* methods, requests per second, daily volume, etc), regional diversity (e.g. APAC nodes for higher number of customer demands from APAC), and client diversity (e.g. Reth vs Geth implementations). DIN allows protocols to shop their prices across the number of providers to effectively share our Business Development leads and pipeline into a transparent and competitive bid.

4.3.4 Web3 Gateway Enrollment / DIN Router Initial Registration

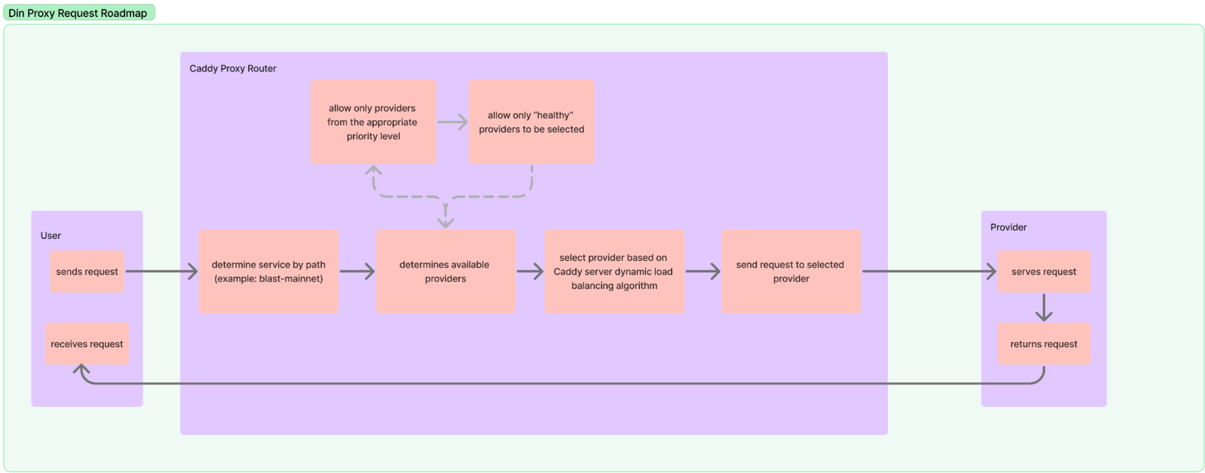

Din Proxy Request Roadmap
Caddy Proxy Router
allow only providers from the appropriate priority level
allow only "healthy" providers to be selected
User
sends request
receives request
determine service by path (example: blast-mainnet)
determines available providers
select provider based on Caddy server dynamic load balancing algorithm
send request to selected provider
Provider
serves request
returns request

Figure 5: DIN Proxy Request Flowchart

Web3 Gateways (e.g. Infura) act as intermediaries (usually SaaS companies), accepting payments from users and routing requests according to SLAs and developer preferences. To enroll, Web3 Gateways stake tokens and register through the Gateway Contract. They gain access to real-time performance data from the AVS monitoring system, allowing them to optimize routing and ensure SLA compliance. Web3 Gateways also provide support services, such as invoicing, request prioritization, and technical assistance, enhancing the user experience.

In the current state, proxy registration is completed via Sign in With Ethereum, and the DIN team would allowlist the Ethereum address that the new Gateway is using to access the DIN Router. The Ethereum address is required in order to authenticate.

4.4 Using the Network

4.4.1 Authentication

To ensure secure and efficient access to DIN Provider endpoints, the Decentralized Infrastructure Network (DIN) employs an authentication protocol that enables a handshake between DIN Routers and DIN Providers. This protocol ensures that only authorized DIN Routers can access provider endpoints, even though these endpoints are not designed to be kept secret and are publicly accessible. The authentication mechanism is based on Ethereum’s EIP-4361 standard ("Sign-In with Ethereum") and is designed to be compatible with future upgrades, including potential payment integrations. EIP-4361 establishes a secure, decentralized standard for Web3 authentication using Ethereum signatures [8].

Authentication Challenges and Goals

Given that DIN provider endpoints are intended to be publicly accessible, the network requires a method to control access and prevent unauthorized users from making large volumes of requests. The primary goals of the DIN authentication system are:

- To ensure only authorized DIN Routers can access provider endpoints, even when these endpoints are public.
- To support a smooth transition to a payments-enabled protocol in the future.
- To minimize complexity for DIN Providers, making upgrades straightforward when integrating payment protocols.

In order to transition from a Web2 to Web3 security model, DIN's authentication approach is modeled after the OAuth 2.0 framework. The OAuth 2.0 framework enables secure access delegation, establishing a foundation for decentralized Web3 authentication [9].

Future Considerations

As DIN evolves, several configuration enhancements and protocol adjustments are anticipated.

Smart Contract Configuration for Dynamic Mappings: The DIN Router's current configuration relies on a hard-coded mapping of services to provider endpoints, but this is expected to transition to a smart contract-based setup. This dynamic approach will enable real-time updates, decentralizing endpoint management and allowing DIN Providers to update service listings seamlessly.

Dynamic Whitelisting and Payments Integration: The DIN Provider's current whitelist configuration, currently static, will also transition to a smart contract model, allowing for real-time adjustments. As payment protocols are integrated into DIN, the authentication protocol will incorporate session-specific payment parameters and permissions, adapting the session duration or usage limits based on payment tiers or allowances.

Seamless Payments Integration: DIN aims to transition toward payments between DIN Routers and Providers managed directly through the protocol. This change will be structured to require minimal upgrades for existing DIN Providers, who will be able to adapt smoothly using the foundational configuration implemented in this initial authentication setup.

4.4.2 Sharing The Load

To achieve decentralized scalability, **DIN distributes the computational load across multiple Node Operators**, enhancing reliability, reducing latency, and maintaining high service levels even during peak demand periods. This load-sharing mechanism allows DIN to balance requests dynamically, preventing any single operator from becoming a bottleneck or point of failure.

Load-Balancing Mechanism

Distributed Routing: Requests are routed through Web3 Gateways to available Node Operators based on network conditions, SLA requirements, and real-time performance metrics. This distribution ensures that requests are handled by the most capable and responsive operators, reducing latency and improving overall network performance.

Dynamic Reallocation: As demand fluctuates or if certain Node Operators experience downtime, requests can be rerouted in real time to maintain uninterrupted service. Watchers continuously monitor operator performance, and the system automatically reallocates requests to ensure consistency.

Preventing Resource Overload

Session Token Expiration and Usage Limits: To prevent unauthorized or excessive request loads, session tokens are configured with usage limits or expiration timestamps, managed by each DIN Provider. These tokens control the number of requests each authorized DIN Router can make, preventing overloading of any single provider.

SLA-Based Throttling: Requests that exceed a user’s CU allocation or violate SLA terms may be deprioritized or rejected, ensuring equitable distribution of network resources. Throttling ensures that network load remains balanced, supporting stable performance across all users.

Role of Network Watchers

Real-Time Monitoring: Network Watchers play a vital role in the load-sharing process by continuously tracking and validating operator response times, accuracy, and SLA compliance. This monitoring data is published to the public bulletin board, allowing the DAO and users to assess operator reliability and request routing.

Load Redistribution: If a Node Operator underperforms or faces connectivity issues, Watchers flag the issue, and requests are automatically rerouted to maintain service continuity. EigenLayer’s AVS integration supports slashing penalties for operators that fail to meet performance benchmarks, encouraging operators to maintain consistent and reliable service.

Transparency and Governance

DAO Oversight: The DIN DAO regularly reviews performance data and can make adjustments to the load-sharing algorithm, enabling the network to adapt to new challenges or increased demand as Web3 grows.

User and Provider Feedback: Both users and Node Operators can provide feedback on load-sharing policies, which the DAO may consider when updating the protocol to optimize efficiency, fairness, and resilience.

4.4 Monitoring behavior of operators

Network Watchers act as Actively Validated Service (AVS) Operators, responsible for assessing the operational behavior of Node Operators and ensuring their compliance with DIN's performance standards. Each Network Watcher stakes DIN tokens through EigenLayer's AVS, aligning their economic incentives with the network's integrity.

Real-Time Data Validation: Watchers validate operator responses to API requests, checking for data accuracy, response times, and adherence to SLA terms. This data verification process prevents unauthorized data alterations and provides users with reliable blockchain information.

Independent Oversight: Watchers operate independently of Node Operators, verifying data against independently sourced information to detect any discrepancies. This independence is crucial for maintaining unbiased oversight across the network.

Verifying Work by Watchers

A key aspect of DIN's reliability is the verification process conducted by Network Watchers, who monitor Node Operators for SLA compliance. However, as Watchers monitor operator behavior, there is an inherent risk of "auditing the auditors," where dishonest Watchers might falsify reports.

To mitigate this risk, DIN operates on an assumption of an honest-majority Watcher set, incentivized through staking and slashing mechanisms to maintain integrity. By requiring Watchers to stake funds, DIN aligns their financial interests with truthful reporting, providing economic assurance that Watchers will act in the network's best interest. In cases where questions arise over Watcher accuracy, the DAO may review or audit Watcher data, ensuring transparency and accountability.

4.4.1 Monitoring Metrics and SLA Compliance

DIN's monitoring framework focuses on three essential metrics to ensure service quality: **Freshness**, **Validity**, and **Availability**. Network Watchers assess each metric in real time, flagging any deviations from SLA standards.

Freshness of Responses

- **Definition**: Freshness measures how up-to-date the data provided by a Node Operator is relative to the blockchain's current state.
- **Monitoring Mechanism**: Network Watchers continuously check response freshness by verifying that Node Operators provide data from the latest blockchain state, avoiding outdated or cached responses. Freshness is assessed through metrics such as block height or timestamp in response headers.
- **SLA Requirements**: Operators are expected to maintain a close alignment with the latest block data, with SLAs specifying acceptable latency thresholds. Operators providing stale data are flagged, and repeated offenses may lead to slashing penalties.
- **Automated Detection**: For future upgrades, DIN may implement automated freshness thresholds, dynamically adjusting SLAs based on network load or traffic, to further improve freshness standards.

Validity of Responses

- **Definition**: Validity ensures that the data returned by Node Operators accurately reflects the correct blockchain state and has not been tampered with.
- **Validation Process**: Network Watchers verify the correctness of responses by comparing them to independently sourced blockchain data. This process involves cross-referencing key data points, such as transaction details or account balances, against verified nodes or trusted third-party sources.
- **Cryptographic Verification**: Each response is cryptographically signed by the Node Operator, allowing Watchers and users to verify the data's integrity. This signature also serves as an accountability mechanism, binding operators to the accuracy of their responses.
- **SLA Enforcement**: If a response is found to be invalid or inconsistent with verified sources, the Node Operator is flagged, and appropriate penalties are applied. Persistent validity issues may lead to temporary suspension or removal from the network.

Availability of Service

- **Definition**: Availability refers to the operator's ability to respond to requests consistently, without excessive downtime or interruptions.

- **Uptime Monitoring**: Network Watchers monitor each Node Operator's uptime and request handling to ensure they meet SLA requirements for availability. Operators experiencing extended downtime are flagged, with Watchers capturing and reporting the exact duration and frequency of outages.

- **Load Management**: Watchers also monitor request throughput to confirm that operators can handle demand without compromising on response times. Overloaded operators may be deprioritized, and requests can be rerouted to maintain a stable service level.

- **Penalty Structure**: Operators failing to meet availability standards are subject to AVS-based slashing, where their staked tokens are partially reduced as a deterrent against poor performance. Chronic unavailability may lead to suspension from the network to ensure user requests are consistently served by reliable operators.

4.4.2 Public Reporting and Transparency

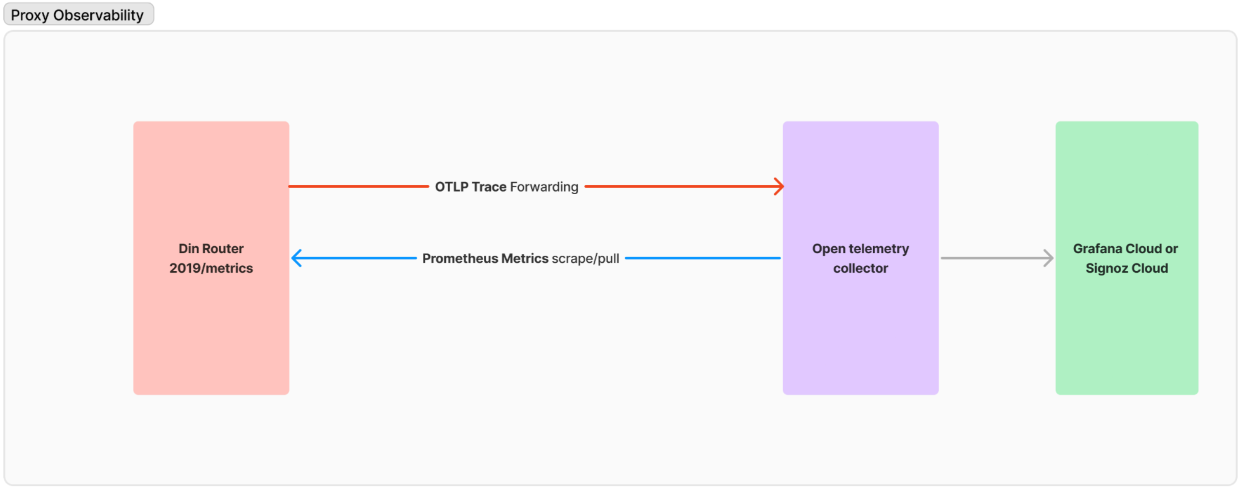


Figure 6: DIN Proxy Observability

DIN is committed to transparency, with real-time monitoring data published to a decentralized public bulletin board. This transparency allows users, the DAO, and other stakeholders to review performance metrics and make informed decisions regarding operator reliability.

Bulletin Board Access: Metrics related to freshness, validity, and availability are available on a public ledger, allowing stakeholders to view each operator's performance history. This data-driven approach fosters a transparent and accountable ecosystem.

DAO Oversight: The DIN DAO has access to detailed monitoring reports and can enforce policy adjustments or initiate investigations based on performance trends. This oversight ensures that operators adhere to SLA standards and align with DIN's operational goals.

4.4.3 Enforcement Mechanisms

DIN employs both incentives and penalties to maintain high standards among Node Operators, using EigenLayer's AVS model to enforce economic alignment.

Rewards for High Performance: Operators who consistently meet or exceed SLA expectations for freshness, validity, and availability are rewarded with additional tokens, promoting reliable service across the network.

Slashing Penalties: Non-compliant operators who fail to maintain SLA standards face AVS-based slashing, where a portion of their staked tokens is forfeited. This mechanism enforces accountability and discourages repeated violations.

Suspension for Severe Violations: For severe or repeated breaches of SLA terms, such as chronic downtime or consistent invalid responses, the DIN DAO may temporarily suspend or remove the operator to maintain network integrity.

4.4.4 Continuous Improvement and Feedback

DIN's monitoring framework is designed to evolve with the network, allowing for adjustments based on data insights and stakeholder feedback. This iterative approach ensures that DIN remains adaptable to changes in network demands and blockchain technologies.

DAO-Driven Updates: The DIN DAO reviews monitoring data and can implement updates to SLAs, adjust performance thresholds, or refine monitoring processes based on network conditions.

Operator and User Input: Both operators and users are encouraged to provide feedback on the monitoring and enforcement process. This input is used to optimize DIN's monitoring framework, striking a balance between strict compliance and operational flexibility.

4.4.5 Future Enhancements in Monitoring

DIN's monitoring approach is future-proofed with plans for additional enhancements that will further improve reliability and accuracy:

Automated Freshness and Validity Detection: To improve response times, DIN may implement automated freshness and validity checks, allowing for quicker intervention if operators fail to deliver up-to-date or accurate data.

Adaptive Availability Thresholds: DIN aims to develop adaptive availability thresholds, dynamically adjusting SLA requirements based on real-time network traffic, demand, and seasonal load variations to optimize performance standards.

Light Client Support: DIN's long-term goal is to expand accessibility to users who prefer lightweight blockchain data solutions through potential support for light clients. Light clients, which require minimal storage and processing power, could make DIN more accessible to a broader range of users, including those on mobile or low-bandwidth devices. The DAO will analyze JSON RPC requests to evaluate the technical feasibility and resource requirements for light client support, ensuring that it aligns with DIN's performance and security standards. This future enhancement would enable DIN to reach more users and create a more inclusive network, supporting varied user needs.

4.5 Leaving the network

DIN provides a structured process for Node Operators and Network Watchers who wish to leave the network, either voluntarily or due to enforced penalties. This process ensures a smooth exit, upholds network stability, and allows for the fair settlement of obligations and rewards. The procedure balances flexibility for exiting participants with rigorous protocols to maintain DIN's performance standards, transparency, and security.

4.5.1 Voluntary Exit Process

Node Operators and Watchers may choose to leave DIN at any time, provided they follow the protocol's exit requirements and complete a formal "challenge period" designed to prevent service disruptions.

1. **Exit Request and Challenge Period**
    - **Initiating an Exit**: Operators and Watchers submit an exit request via the **Staking Contract**, formally declaring their intent to leave. This initiates the challenge period, which gives the DIN DAO and Watchers an opportunity to review the operator's recent performance history for any SLA violations, discrepancies, or outstanding penalties.

- **Challenge Period Duration**: The challenge period typically lasts several days, depending on DAO-established policies. During this time, exiting participants must continue fulfilling service commitments and maintain SLA compliance until their final request has been processed.

- **Challenge Verification**: If any SLA breaches or penalties are identified during the challenge period, operators may be subject to additional slashing. This protocol ensures that operators cannot exit the network with unresolved issues that could harm network integrity.

2. **Unstaking and Final Settlement**

    - **Unstaking Tokens**: Once the challenge period concludes without incident, the exiting operator's staked tokens are released by the Staking Contract. The staked amount, minus any applicable penalties, is returned to the operator's designated wallet.

    - **Final Rewards and Settlement**: Any earned rewards accumulated prior to the exit are distributed to the exiting operator or Watcher. Final rewards are calculated based on service contributions during the exit period, ensuring participants are compensated fairly for their final days on the network.

3. **Rejoining the Network**: Operators or Watchers who previously exited may reapply to join DIN, but they must undergo the full onboarding process, including new staking requirements, to demonstrate ongoing commitment to DIN's standards.

4.5.2 Forced Exit and Removal for SLA Violations

In cases where a Node Operator or Watcher repeatedly fails to meet SLA standards or engages in behavior detrimental to DIN, the network may enforce a forced exit, effectively removing the participant to maintain service quality and network integrity.

1. **Conditions for Forced Exit**

    - **Chronic SLA Violations**: Operators who consistently breach SLA terms on freshness, validity, or availability may be flagged for forced exit by Network Watchers. These violations are escalated to the DAO for review, and if deemed critical, the operator may be removed from the network.

    - **Repeated Slashing Events**: Operators subjected to multiple slashing penalties within a set timeframe may be automatically enrolled in the forced exit process. This approach minimizes the impact of underperforming operators on DIN's overall performance.

    - **DAO and Watcher Consensus**: The DIN DAO, in consultation with Watchers, votes on forced exits for severe cases. This decision-making process ensures that removals are both justified and backed by transparent, community-led governance.

2. **Forced Exit Process**
    - **Immediate Suspension**: Once a forced exit is approved, the operator or Watcher is immediately suspended from handling further requests, preventing any additional service disruptions or SLA breaches.
    - **Final Settlement and Slashing**: The operator's staked tokens are subject to final review, with penalties applied as necessary. The remaining balance is returned to the operator, and they are permanently barred from rejoining DIN under the same address unless explicitly approved by the DAO.

4.5.3 Balance Settlement and Unfulfilled Requests

During the exit process, DIN ensures that user services are not impacted by an operator's or Watcher's departure. This is achieved through controlled reallocation of tasks and thorough settlement of outstanding obligations.

1. **Reallocation of Requests**: Requests pending with an exiting Node Operator are immediately rerouted to active operators in good standing. This minimizes any risk of service disruptions for users and maintains consistent network performance.
2. **Balance Settlement**: If the exiting participant has a remaining balance of requests allocated to their service, those costs are refunded to users or reallocated to cover any outstanding service needs, ensuring a fair distribution of resources.

4.5.4 Challenge Process and DAO Review

To uphold transparency and fairness in the exit process, DIN includes a final challenge process for all exiting participants, allowing the DAO to review performance data and address unresolved issues.

- **Challenge Review Protocol**: The challenge process is initiated automatically upon an exit request. The DAO and Network Watchers review recent monitoring data to ensure that the exiting participant's service history aligns with network standards.
- **DAO Authority**: The DAO holds authority to impose additional penalties if performance discrepancies are discovered, and may choose to delay the release of staked funds until all issues are resolved. This challenge protocol reinforces

accountability and safeguards the network against operators attempting to evade penalties.

4.5.5 Future Considerations for Streamlining Exits

As DIN continues to evolve, enhancements to the exit process are anticipated, including:

1. **Automated Exit Verification**: A future upgrade may introduce automated checks during the challenge period, enabling faster exit processing for participants in good standing and streamlining the exit review.

2. **Dynamic Stake Release**: For operators with consistently high performance, DIN may implement a tiered stake release system, allowing a portion of the stake to be released before the full challenge period concludes, based on real-time data and SLA compliance history.

5 DIN as an Actively Validated Service (AVS)

DIN leverages EigenLayer's AVS model to establish a robust framework of economic security, performance accountability, and dynamic governance. By implementing DIN as an AVS, the network aligns incentives among Node Operators, Network Watchers, and other participants, ensuring high standards of service quality, resilience, and transparency across all operations.

Through AVS, DIN enforces rigorous standards for Service Level Agreements (SLAs), incentivizes consistent performance, and incorporates real-time slashing and staking mechanisms, providing a reliable and economically secure infrastructure for Web3 applications.

5.1 Role of AVS in DIN

The integration of EigenLayer's AVS enables DIN to enhance its operational framework by incorporating continuous validation, economic deterrents against underperformance, and a streamlined process for enforcing SLA compliance [6]. AVS brings a layer of financial accountability that ensures Node Operators and Network Watchers adhere to DIN's performance benchmarks, protecting the network's reliability and user experience.

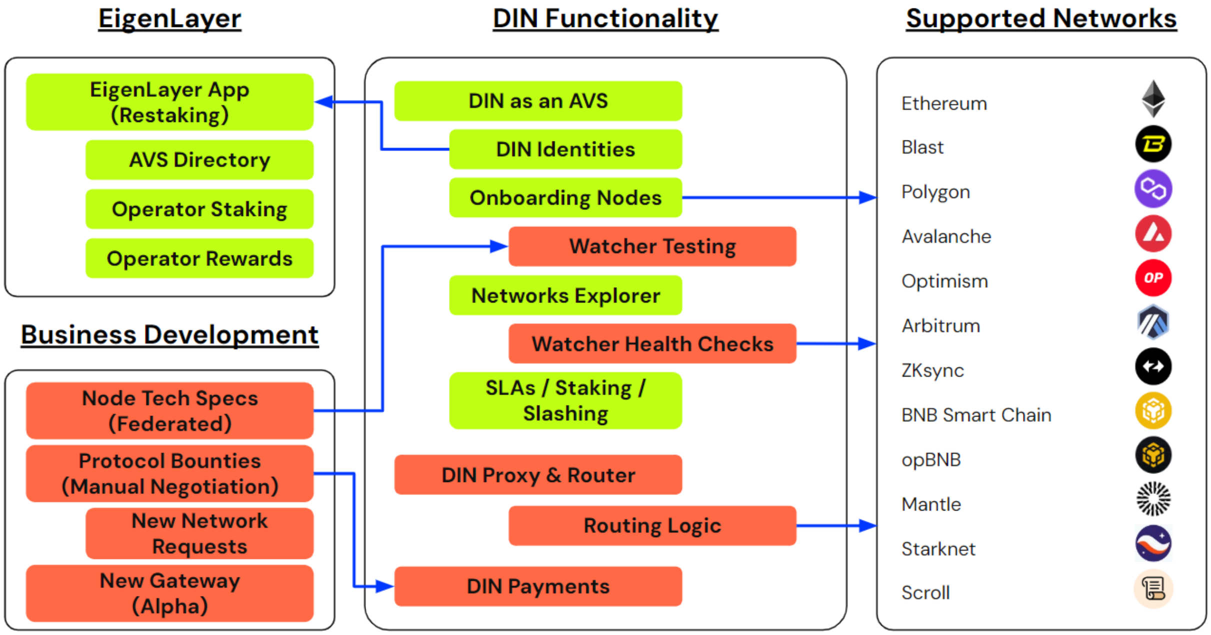


Figure 7: DIN Components including EigenLayer

5.1.1 Economic Alignment through Staking and Slashing

Staking Requirements: Each Node Operator and Watcher within DIN must stake tokens through the EigenLayer AVS model, creating an economic commitment to their roles. This stake acts as collateral, guaranteeing that operators and Watchers are financially invested in maintaining network standards.

Slashing Mechanisms: To enforce compliance, AVS enables slashing protocols, where staked tokens are deducted if operators or Watchers fail to meet SLA standards for freshness, validity, or availability. By financially penalizing non-compliance, AVS reduces the likelihood of low-quality service and incentivizes participants to uphold their obligations.

5.1.2 Real-Time SLA Enforcement

Continuous Validation: Network Watchers serve as AVS Operators, continuously monitoring the performance of Node Operators to validate adherence to SLAs. They track key metrics—such as response freshness, data validity, and service availability—and report any deviations. This real-time validation ensures that any breaches in service quality are quickly detected and addressed.

Automated Penalties for SLA Violations: AVS automates the enforcement of penalties for SLA breaches, enabling immediate slashing for operators who fail to meet performance standards. This process ensures swift accountability without requiring manual intervention, protecting network integrity and user trust.

5.1.3 Transparent Monitoring and Reporting

Decentralized Public Ledger: DIN's AVS integration ensures that performance data, including SLA compliance and slashing events, is published on a public ledger. This decentralized transparency allows users, DAO members, and other stakeholders to review the historical performance of Node Operators and Watchers, fostering trust and accountability.

Performance Reputation System: AVS supports the development of a reputation system within DIN, where Node Operators and Watchers build credibility based on their adherence to SLA standards. Consistent high performers may gain a higher reputation, making them preferred options for request routing, while poor performers face economic consequences and potential removal.

5.2 Enhanced Security and Reliability

DIN's implementation as an AVS strengthens the network's security and reliability by embedding economic deterrents and incentivizing reliable performance. This integration addresses several core challenges faced by decentralized infrastructure networks described in the next sections.

5.2.1 Mitigation of Malicious Behavior

Deterrence through Collateral: The AVS model deters malicious actors by requiring a significant token stake from each participant. The potential loss of collateral discourages bad actors from attempting to game the system, as economic penalties for misconduct are severe.

Automated Slashing for Tampering: In cases of data tampering or intentional SLA breaches, AVS's automated slashing mechanisms swiftly penalize offending operators, minimizing the impact on DIN's overall performance and ensuring that malicious behavior is not profitable.

5.2.2 Consistent Performance across High Demand

Dynamic Load Balancing: By continuously validating Node Operator performance, AVS supports dynamic load-balancing within DIN. If a Node Operator begins to underperform, requests are automatically redirected to operators in good standing, maintaining a stable user experience.

Reliability during Peak Usage: The AVS framework enables DIN to operate effectively even during periods of high demand. The system identifies and prioritizes operators who meet SLA requirements, ensuring that critical services remain available when needed most.

5.2.3 Transparency and Decentralized Oversight

DAO Access to Performance Data: The DIN DAO has full visibility into AVS-generated performance metrics and slashing events. This data enables the DAO to make informed decisions about reward allocations, performance benchmarks, and potential policy updates, creating a feedback loop for continuous improvement.

Public Confidence through Transparent Operations: Publishing AVS data on a decentralized ledger builds confidence in DIN's reliability and integrity, attracting users who seek trustworthy infrastructure solutions for their Web3 applications.

5.3 Incentive Structures and Reward Mechanisms

The AVS model within DIN provides structured incentives that reward high-performing Node Operators and Watchers while penalizing those who fail to meet expectations. This incentive structure ensures the network's sustainability and aligns participant behavior with DIN's quality standards.

5.3.1 Performance-Based Rewards

Additional Rewards for SLA Compliance: Operators and Watchers who consistently meet or exceed SLA standards receive additional token rewards. These rewards, distributed through the Gateway Contract, encourage participants to prioritize performance and reliability.

Reputation-Linked Incentives: As AVS supports a reputation system, operators with high SLA compliance scores can attract more request routing, maximizing their earning potential while reinforcing a culture of quality service.

5.3.2 Deterrents for Underperformance

Incremental Slashing for Repeated Violations: AVS implements a tiered slashing system, where penalties increase in severity for operators with repeated SLA violations. This graduated approach encourages operators to rectify issues promptly, reducing long-term service disruptions.

Suspension and Removal for Persistent Non-Compliance: Operators with chronic performance issues face suspension or removal from the network, ensuring that DIN maintains only reliable and committed participants.

5.4 Future Directions with AVS Integration

The AVS model within DIN is structured to support future enhancements as the network scales and adapts to new technologies. Key areas for potential growth include:

Smart Contract-Enabled Dynamic SLAs: As DIN evolves, the AVS model can support dynamic SLA requirements managed directly through smart contracts. This flexibility allows for adaptive SLA terms based on real-time network conditions, providing a more responsive and tailored service experience for users.

A**dvanced Penalty and Reward Structuring:** DIN's AVS integration may incorporate advanced reward structures, such as performance multipliers for operators who maintain a top-tier performance record over extended periods. This framework also enables customized slashing rules for different types of SLA violations, allowing DIN to align incentives more precisely with network needs.

Real-Time Notifications and Alerts: Future AVS enhancements may include real-time notifications and alerts for Node Operators and Watchers when they approach SLA thresholds. This proactive approach enables operators to address potential issues before penalties are triggered, fostering a more resilient network.

6 Mechanism Design

DIN is built on a carefully structured economic model that aligns incentives across Node Operators, Network Watchers, Web3 Gateways, and other stakeholders to ensure a high-performing, reliable, and secure infrastructure. Mechanism design in blockchain systems is about aligning incentives so that participants act in ways that benefit the network as a whole [11]. The mechanism design of DIN combines economic rewards, slashing penalties, and governance controls to promote network stability and incentivize compliance with service-level agreements (SLAs). The incentivized testnet serves as a proving ground, allowing DIN to test and refine these mechanisms in a controlled environment before mainnet deployment.

DIN's mechanism design aims to create a self-sustaining ecosystem where each participant's actions are economically aligned with network goals. This approach ensures that service quality, security, and scalability are maintained, benefiting both users and operators within the network.

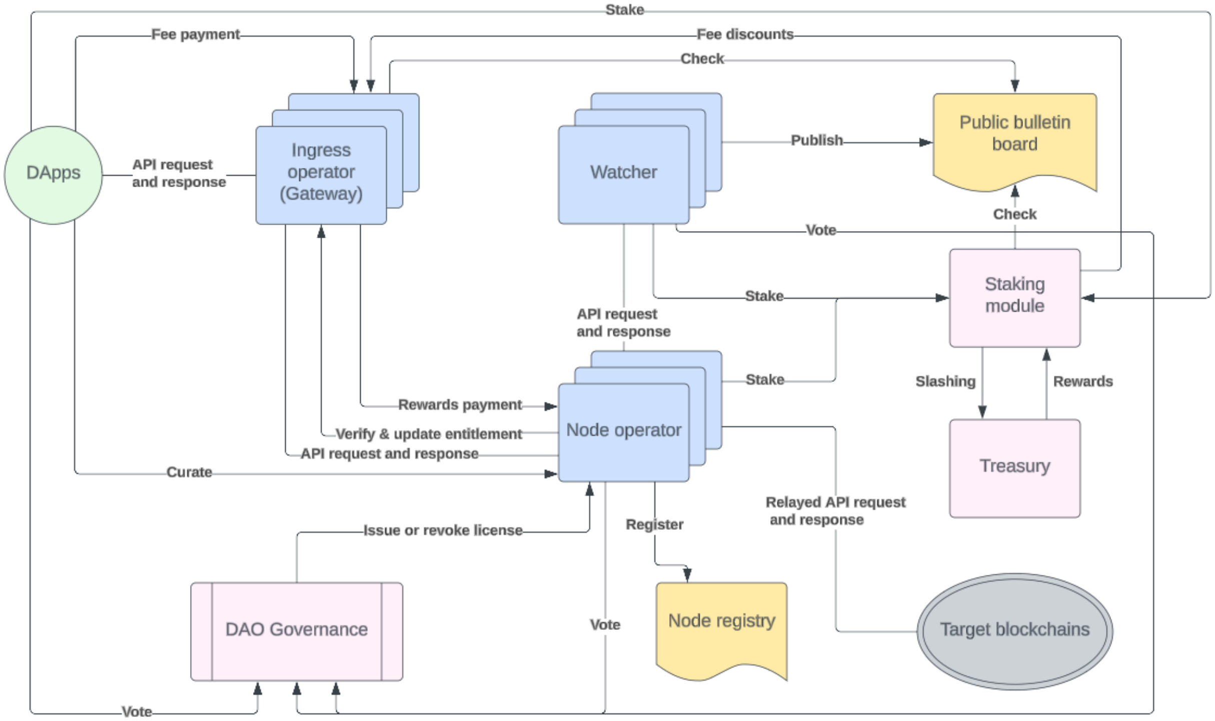


Figure 8: DIN Ecosystem Actor Interactions

6.1 Core Principles of Mechanism Design

DIN's mechanism design is based on the following principles, which underpin all interactions and incentive structures within the network:

6.1.1 Economic Alignment through Staking and Slashing

Each Node Operator and Watcher is required to stake tokens, creating a direct economic link between their performance and their financial stake. The staking requirement ensures that all participants have "skin in the game," while slashing mechanisms deter non-compliance by penalizing SLA breaches.

The staking model is structured to scale with operator capacity and anticipated request load, ensuring that larger and higher-stakes operators are proportionally accountable to DIN's performance standards.

6.1.2 Performance-Based Rewards

DIN incentivizes high-quality service by distributing rewards based on compliance with SLAs, request throughput, and overall performance metrics. Operators and Watchers earn token rewards for meeting SLA requirements, while those who exceed benchmarks may earn additional performance-based incentives.

This reward system promotes reliable service, encourages efficient load management, and reinforces the importance of maintaining consistent uptime and data accuracy.

6.1.3 Transparency and Accountability through AVS and DAO Governance

EigenLayer's Actively Validated Service (AVS) model is integrated into DIN's economic model, automating the enforcement of SLAs and ensuring real-time monitoring of operator performance. The AVS system enables automated penalties and rewards, ensuring transparency in the enforcement of network standards.

The DIN DAO oversees all critical economic policies, including staking thresholds, reward structures, and performance metrics, ensuring these mechanisms evolve based on community input and operational data.

6.2 Key Mechanisms and Incentives

Slashing penalties and staking requirements form the backbone of Ethereum 2.0's proof-of-stake security model [12]. DIN employs a variety of mechanisms to ensure that incentives align with network stability and performance, including slashing penalties for non-compliance, performance-based rewards, and a tiered reputation system.

6.2.1 Staking and Slashing Mechanism

Staking Requirements: Node Operators and Watchers are required to stake tokens based on their anticipated service level and workload. This stake serves as collateral, aligning their financial interests with the performance standards set by DIN's SLAs.

Slashing Penalties: The AVS system enforces slashing penalties for operators who fail to meet SLA requirements. Slashing events can be triggered by prolonged downtime, invalid responses, or repeated breaches in data freshness or availability. By imposing financial penalties for non-compliance, DIN incentivizes operators to maintain high standards.

Partial and Full Slashing: The slashing mechanism includes both partial and full penalties, depending on the severity of the SLA violation. Minor infractions may result in partial slashing, while chronic or severe breaches can trigger full slashing, leading to significant financial loss and potential removal from the network.

6.2.2 Performance-Based Rewards and Bonus Incentives

SLA Compliance Rewards: Operators who consistently meet SLA standards receive token rewards that are proportional to their level of activity and compliance history. These rewards encourage reliable performance and incentivize operators to uphold DIN's quality standards.

High-Performance Bonuses: In addition to base rewards, DIN offers bonuses to operators who exceed SLA benchmarks, such as maintaining near-perfect uptime or exceptionally low response times. These high-performance bonuses attract experienced operators who aim to maximize their earnings by delivering premium service quality.

Reputation-Linked Incentives: A reputation system tracks each operator's performance history, with higher reputation scores translating to increased request routing and priority. This reputation-based approach helps users select operators based on demonstrated reliability, further incentivizing operators to build and maintain high-performance records.

6.2.3 Web3 Gateway Incentives

Routing Efficiency Rewards: Web3 Gateways earn rewards for efficient request routing and load management, with incentives linked to their ability to distribute traffic evenly and prevent overload on specific Node Operators.

User Satisfaction Bonuses: Operators that achieve high user satisfaction scores, based on metrics like response time and support quality, earn bonuses. This incentivizes Web3 Gateways to provide an excellent user experience, enhancing DIN's reputation as a reliable infrastructure provider.

6.2.4 Governance Participation and DAO Voting Power

Token-Based Voting Rights: Token holders who stake within the DIN DAO gain voting rights proportional to their stake. This voting power allows them to participate in governance decisions, including updates to SLA standards, adjustments to staking requirements, and changes to reward allocations.

Proposal Incentives: The DAO encourages stakeholders to submit governance proposals that align with network goals. Contributors whose proposals are accepted may receive governance rewards, fostering a collaborative environment where the community actively contributes to DIN's evolution.

6.2.5 Watcher Mechanism Design

Incentivizing Timely and Honest Onboarding Duties: Encourage Watchers to perform onboarding tasks promptly and honestly.

Ensuring Good Coverage Across Networks, Providers, and Locations: Achieve comprehensive monitoring coverage across all networks, providers, and geographic zones.

Encouraging Data Sharing Among Watchers: Promote collaboration and data sharing among Watchers while ensuring that only those who contribute can consume shared data, thus preventing free-riding.

Ensuring Watchers Send Real Requests to Providers: Prevent Watchers from faking monitoring data and ensure authenticity.

Promoting Accurate Analytics via API: Ensure that Watchers provide high-quality, accurate analytics data accessible via API.

Ensuring Watchers' Business Sustainability: Make the Watcher role financially viable to encourage long-term participation.

Encouraging Long-Term Historical Data Storage: Incentivize Watchers to store and maintain access to historical monitoring data.

Timely Detection of Providers Missing SLAs: Encourage Watchers to promptly detect and report providers failing to meet SLAs.

Implementing Slashing Mechanism for Insufficient Data Contribution: Encourage Watchers to contribute data proportionally to their consumption by penalizing (slashing) those who do not meet contribution thresholds.

6.4 Dynamic Adjustments and Future Mechanism Enhancements

DIN’s mechanism design is intended to be adaptive, enabling the network to respond to changing conditions, growth in demand, and advances in Web3 technology. The DAO regularly reviews economic data and participant feedback, making dynamic adjustments to maintain network sustainability and incentivize high performance.

6.4.1 Dynamic SLA and Reward Adjustments

Adaptive SLA Requirements: As the network grows, the DAO may implement adaptive SLAs that adjust requirements based on network load, demand fluctuations, and seasonal usage patterns. This approach ensures that SLAs remain both challenging and attainable, optimizing DIN's quality standards without overburdening operators.

Flexible Reward Tiers: The DAO may introduce reward tiers based on performance, enabling high-reputation operators to earn increased rewards while encouraging newer operators to improve their services.

6.4.2 Automated Monitoring and Real-Time Penalties

Automated Performance Alerts: DIN plans to implement automated alerts that notify operators and Watchers when they approach SLA violation thresholds, allowing them to take corrective actions before penalties are enforced.

Real-Time Slashing Adjustments: Based on insights from the testnet, DIN may refine its slashing mechanisms to apply penalties in real time for critical SLA breaches, such as extended downtime or invalid responses, ensuring immediate accountability and preventing service degradation.

6.4.3 Cross-DAO Collaborations and Shared Economic Models

Collaborative Governance Initiatives: As DIN matures, the DAO may explore partnerships with other Web3 projects and DAOs to coordinate governance and economic strategies. Shared economic models, such as cross-protocol staking or pooled slashing reserves, could enhance network resilience and establish DIN as part of a broader decentralized infrastructure ecosystem.

Tokenomic and Liquidity Partnerships: The DAO may collaborate with DeFi protocols to enhance DIN's token utility and liquidity, offering staking rewards or liquidity mining opportunities that incentivize long-term token holding and network participation.

6.4.4 Node Operator License and Capacity

To maintain a balanced and efficient network, DIN implements a node operator licensing system, where each license defines the maximum requests per second that an operator can handle. This system allows the DIN DAO to issue licenses with specific capacity constraints, represented by NFTs that operators can acquire through auctions. The final price for a license is based on the expected revenue that an operator can generate given their compute capacity, ensuring a fair distribution of network load and rewards. By controlling the total capacity across all issued licenses, the DAO can distribute traffic effectively, prevent over-concentration of resources, and adjust the network's operational scope as demand grows.

6.5.3 Staking

Staking is a foundational mechanism in DIN's economic model, aligning incentives and ensuring commitment to network standards. Node Operators, Network Watchers, and Web3 Gateways must stake as an EigenLayer AVS operator to participate, establishing a bond that ties their economic success to their performance.

Node Operator Staking Requirements: Each Node Operator must stake a predefined amount of tokens as collateral, which scales based on their anticipated request volume and SLA requirements. This stake ensures they are economically committed to meeting DIN's performance standards.

Watcher Staking Requirements: Network Watchers, who validate operator performance, also stake tokens to establish economic accountability. This stake serves as collateral for their monitoring activities, ensuring they report accurate, unbiased data on operator compliance.

Dynamic Staking Adjustments: The DAO may adjust staking requirements over time based on network conditions, demand, and operational requirements. This flexibility allows the network to scale while maintaining security and performance integrity.

6.5.4 Network Rewards

DIN incentivizes participation through a reward model that distributes tokens based on SLA compliance, request volume, and other performance metrics. Rewards are allocated to participants who uphold DIN's standards and contribute to a reliable, high-quality user experience. In inspiration of Ethereum 2.0 design, Ethereum's phased rollout enables each stage to refine core elements like staking, slashing, and validator rewards, creating a robust economic and security model for the network [12].

SLA Compliance Rewards: Node Operators and Watchers receive rewards proportional to their adherence to SLAs. Operators who maintain high availability, accurate data responses, and quick processing times earn additional rewards, promoting consistent quality.

High-Performance Bonuses: DIN may offer bonuses for top-performing participants who exceed SLA benchmarks, such as near-perfect uptime or exceptionally low response times. These bonuses attract experienced participants who strive to maximize their efficiency and reliability.

Incentivized Testnet Rewards: Participants who contribute to the incentivized testnet are rewarded with tokens, incentivizing them to help refine DIN's mechanisms and prepare for a seamless mainnet launch. Testnet rewards allow participants to build a reputation and establish their standing within DIN's ecosystem.

While Network Operators can earn revenue directly from providing services to consumers, they also earn Network Rewards from the protocol for providing services that meet the needs of the network.

Examples of Network Reward conditions:

- 2% of total network tokens issued annually and distributed proportionally across all Stakers.
- 3% of total network tokens issued annually based on DAO proposals based on Network needs. This will appropriately incentivize new service additions.

DIN Payments component facilitates flexible payment options between Node Providers within the marketplace. Flexible payment options in Web3 improve accessibility, allowing users to interact with decentralized networks using both fiat and crypto [15]. Given the emphasis on user experience, we will allow for stablecoin and provider-selected token payments.

6.5.5 Token Slashing

To enforce accountability and SLA compliance, DIN employs a token slashing mechanism through EigenLayer's Actively Validated Service (AVS) model. Slashing provides a financial deterrent against poor performance and malicious behavior, ensuring participants adhere to network standards.

SLA Violation Penalties: If a Node Operator or Watcher fails to meet SLA requirements (such as downtime, data inaccuracies, or delayed responses), they are subject to slashing. This penalty deducts a portion of their staked tokens, incentivizing them to prioritize reliability and high-quality service.

Severity-Based Slashing: Slashing penalties are tiered based on the severity of SLA violations. Minor infractions may incur partial slashing, while severe or repeated breaches can result in full slashing and potential removal from the network.

Automated Enforcement: The AVS integration allows slashing to be applied automatically when SLA breaches are detected, ensuring real-time enforcement without manual intervention. This immediate accountability helps maintain network integrity and user trust.

6.5.6 Network Fees

To support ongoing development and treasury funding, DIN collects network fees based on request volume and resource usage. These fees are designed to be fair and sustainable, ensuring affordability for users while contributing to the network's financial health.

Usage-Based Fees: Network fees are calculated based on their request complexity and service demand. These fees allow DIN to manage resource allocation while covering operational costs and rewarding participants for their services.

Fee Allocation to Treasury: A portion of network fees is allocated to the DIN treasury, managed by the DAO. These funds support research, security audits, and ecosystem development, ensuring that DIN can scale sustainably and continue evolving as Web3 infrastructure demands grow.

Adjustable Fee Structures: The DAO holds authority to adjust network fees in response to market conditions, user demand, and resource availability. This flexibility allows DIN to remain economically sustainable while accommodating growth and technological advancements.

To make DIN accessible to a broader user base, the network's payment structure supports multiple currencies, allowing users to pay in either fiat or various tokens. Web3 Gateways, who can be businesses or individual operators, are equipped to manage these transactions by converting other tokens or fiat to DIN's native token via integrated DeFi protocols. This flexibility allows users who may not hold the necessary token to interact with DIN while still aligning payment with the network's native economy. Through token conversion and payment facilitation, DIN ensures that the payment experience remains simple and accessible.

6.5.7 Governance and Token Utility

Beyond staking and rewards, the DIN token enables token holders to participate in DAO governance, influencing critical network policies and decisions.

DAO Voting Rights: Token holders who stake within the DIN DAO gain voting rights proportional to their stake, allowing them to participate in governance decisions. These decisions include protocol upgrades, policy adjustments, and treasury allocations.

Proposal Incentives: The DAO incentivizes token holders to propose improvements, from protocol changes to economic adjustments. Accepted proposals may be rewarded with governance tokens, encouraging active participation and community engagement.

Future Use Cases: The DIN DAO may introduce additional token utilities over time, such as staking rewards in other protocols, token-based access to premium services, or liquidity mining programs. These initiatives enhance token utility and encourage long-term holding.

8 Potential Issues, Surface Attacks, Remedies

Given DIN's decentralized structure and integration as an AVS, the network incorporates multiple layers of defense to mitigate risks that could impact data integrity, service reliability, or economic security.

8.1 Agents and protocol assumptions

For DIN to function securely and efficiently, the protocol is built on several key assumptions about the network and its environment. In this section, we considered the agents involved in the Infura network, assumptions about the protocol's environment and software capability, and the threat model.

8.1.1 Agent Assumptions

We assume there is a user who wants to send requests to a node on the Infura network and there are five agents who support the Infura network:

- **Node operator:** One or more agents who provide the infrastructure for handling high-throughput requests and providing a gateway to blockchain networks.
- **Watcher:** One or more agents who periodically probe the set of node operators and publish a status report about their performance and capabilities.
- **Web3 Gateway:** One or more agents who accept payment from a data consumer and take responsibility for optimally routing requests to the network.
- **DAO:** A collection of members who propose and vote on proposals, where voting weight is proportionally based on their token holdings.
- **Blockchain Protocols:** One or more agents who represent a blockchain, either due to being a company or foundation associated with that blockchain. Examples include The Ethereum Foundation, the Arbitrum Foundation, and Protocol Labs.

8.1.2 Protocol assumptions

We consider the node software used by the operators, the cryptographic primitives available, and the external environments which are necessary for the Infura network to operate.

Authenticated Responses: Node Operators use public-key cryptography to sign all responses, ensuring that users and Watchers can authenticate data accuracy. Digital signatures are exposed in the response header, enabling verification and alignment with AVS performance standards.

Light-Client Enabled Nodes: Each Node Operator must be capable of generating proofs for data accuracy, particularly for light-client verification. This supports efficient data validation without requiring a full node setup from each user, further decentralizing DIN's accessibility.

Public Bulletin Board: Performance data from Network Watchers is published on a decentralized, long-lived public repository. This bulletin board serves as a source of record for service quality, allowing the DAO, users, and Web3 Gateways to review Node Operators' reliability over time and make informed decisions about routing and governance. These sets of explorers are viewable via the DIN AVS.

Assumptions of Honest Majority: The protocol assumes that a majority of Network Watchers and Node Operators will act in good faith, adhering to protocol rules. This aligns incentives across agents and ensures system integrity. In cases of service lapses, EigenLayer's AVS slashing protocols provide a deterrent to discourage poor performance and penalize malicious behavior effectively.

8.2 Threat Model Assumptions

We assume node operators are financially rational, but could periodically offer a degraded service or incorrect data throughout their course of operating API services. They may return a response that is out-of-date, invalid, provide no response at all, or block a response. We assume a majority of the watchers honestly follow the protocol. Finally, we assume DAO members have a vested interest in the health of the Infura network and their incentives are aligned with the network's.

8.2.1 Malicious Node Operators

Malicious Node Operators may attempt to provide incorrect, delayed, or outdated responses, compromising the integrity of the API data delivered to users.

To mitigate this, Network Watchers, acting as AVS Operators, continuously monitor and validate responses from Node Operators. Any discrepancies detected in real-time, such as invalid or out-of-date data, trigger slashing penalties enforced through EigenLayer's AVS, disincentivizing malicious behavior. Additionally, all responses are authenticated with cryptographic signatures, allowing users and Watchers to verify data authenticity independently.

8.2.2 Collusion Between Node Operators and Web3 Gateways

Node Operators and Web3 Gateways could collude to prioritize specific requests, interfere with the fair distribution of network resources, or manipulate data to benefit specific users.

EigenLayer's AVS validation and DIN's decentralized monitoring limit the impact of such collusion. Network Watchers independently monitor all network interactions, including request routing and response handling, and report any deviations from SLAs to the public bulletin board. This data is accessible to DIN's governance body (DAO), allowing for prompt community intervention and policy adjustments if suspicious activity is detected.

8.2.3 Sybil Attacks

Adversaries may create multiple Sybil nodes to gain disproportionate control over network resources, potentially disrupting DIN's decentralized consensus or service quality.

EigenLayer's staking requirements help deter Sybil attacks by requiring Node Operators and Watchers to stake tokens, raising the economic barrier for creating multiple identities. Furthermore, the protocol includes slashing mechanisms for Node Operators and Watchers that fail to meet SLA standards, making it economically unfeasible for Sybil nodes to remain active without performing at a high level.

8.2.4 Latency and DDoS Attacks

Adversaries could launch Distributed Denial of Service (DDoS) attacks to degrade the performance of Node Operators or Web3 Gateways, potentially causing delays in request handling.

DIN's decentralized structure reduces the impact of such attacks by distributing requests across multiple Node Operators, making it difficult for attackers to target the network as a whole. EigenLayer's AVS further supports this by enforcing penalties for prolonged downtime, incentivizing Node Operators to adopt DDoS mitigation measures. Additionally, DIN Watchers verify response times, ensuring any operators experiencing performance degradation are flagged for potential penalties or slashing.

8.2.5 Double-Spending and Forking Attacks

Bad actors could attempt double-spending or forking attacks by providing conflicting responses to different users or tampering with transaction data in transit.

DIN's reliance on cryptographic proofs, digital signatures, and EigenLayer's AVS monitoring allows Watchers to detect any conflicting or out-of-sync data. The public bulletin board records any detected discrepancies, enabling rapid verification of data integrity.

Slashing mechanisms in AVS ensure that any Node Operators caught engaging in double-spending or forking activities are promptly penalized.

8.2.6 Majority Collusion by Watchers

A majority of Network Watchers may collude to manipulate monitoring data, concealing faults or malicious behavior by Node Operators or Web3 Gateways.

DIN assumes an honest majority among Watchers and implements AVS mechanisms to enforce compliance. Additionally, DIN's governance body (DAO) actively reviews performance data on the public bulletin board. If any manipulation or collusion is suspected, the DAO can adjust network policies, including adding new Watchers or adjusting incentives, to restore transparency and accountability.

8.2.7 Service Disruption by Smart Contract Vulnerabilities

Vulnerabilities within DIN's smart contracts, including staking and slashing protocols on EigenLayer, could lead to unintentional fund loss or disruption of network operations.

All smart contracts within DIN undergo rigorous security audits before deployment. Additionally, DIN's governance can implement emergency protocols, such as pausing or upgrading smart contracts, to respond to any detected vulnerabilities quickly. By maintaining a decentralized yet controlled upgrade path, DIN ensures that smart contracts are both secure and flexible.

8.2.8 Data Censorship and Tampering by Web3 Gateways

Web3 Gateways, as intermediaries between users and Node Operators, could censor specific data requests or manipulate data responses to benefit certain users or themselves.

DIN's decentralized routing model allows users to interact directly with Node Operators if desired, bypassing Web3 Gateways entirely. Furthermore, Watchers monitor Web3 Gateway activity and flag any deviations from established SLAs. EigenLayer's AVS penalties reinforce adherence to routing fairness and SLA compliance, discouraging censorship and data tampering by Web3 Gateways.

8.2.9 Governance Risks

Poorly aligned governance decisions by the DAO or DIN Foundation, such as altering staking requirements or reallocating rewards, could compromise network stability or disincentivize participation.

DIN's governance is community-driven, with proposals subject to review and weighted voting by stakeholders. By incorporating transparent decision-making and community feedback, the DAO aims to protect network stability and participant incentives. Emergency voting mechanisms also allow for swift action if governance decisions are found to harm the network's integrity.

9. Conclusion

The Decentralized Infrastructure Network (DIN) is designed to address the growing demand for a reliable, scalable, and decentralized infrastructure for blockchain applications. As the blockchain ecosystem grows, so too does the demand for scalable, decentralized infrastructure that can meet the needs of developers, users, and institutions seeking reliable and efficient access to blockchain data [17]. Through a carefully crafted roadmap, DIN transitions from a federated model with alpha customers like Infura and MetaMask to a fully decentralized, community-governed network.

By leveraging the Actively Validated Service (AVS) model for economic security, automated SLA enforcement, and a dynamic token-driven incentive system, DIN aligns incentives across Node Providers/Operators, Network Watchers, and Web3 Gateways. This alignment ensures high-quality service, economic accountability, and real-time compliance with performance standards, creating a resilient infrastructure suited to the evolving needs of Web3.

As DIN progresses, the network will incorporate decentralized transaction processing, an on-chain payments layer, and DAO-led governance, establishing a self-sustaining ecosystem that is both adaptive and community-driven. DIN's phased approach to decentralization allows for robust testing, iterative improvements, and broad community participation, resulting in an infrastructure that scales effectively and remains responsive to technological advancements. By empowering a diverse community of operators, developers, and stakeholders, DIN is well-positioned to become a foundational element in the Web3 ecosystem, providing a reliable, transparent, and economically sustainable infrastructure for the decentralized future.

References

[1] The Year in Ethereum 2021 Stark, J., Van Ness, E. (2022) The Year in Ethereum 2021. Mirror. Retrieved from https://stark.mirror.xyz/q3OnsK7mvfGtTQ72nfoxLyEV5lfYOqUfJIoKBx7BG1I

[2] The Limits of Blockchain Scalability Buterin, V. (2021). *Vitalik Buterin's website.* Retrieved from https://vitalik.eth.limo/general/2021/05/23/scaling.html

[3] Web3 Infrastructure Report Electric Capital. (2023). *State of Web3 Infrastructure: Trends, Growth, and Demand Analysis*. Electric Capital. Retrieved from https://electriccapital.com/reports

[4] Cosmos Incentivized Testnet Kwon, J., & Buchman, E. (2018). *Cosmos: A Network of Distributed Ledgers*. Cosmos Network. Retrieved from https://cosmos.network/resources/whitepaper

[5] Cosmos Network Roadmap Cosmos Network. (2022). *Cosmos Roadmap: Expanding the Internet of Blockchains*. Cosmos Hub Documentation. Retrieved from https://docs.cosmos.network/roadmap

[6] EigenLayer Documentation EigenLayer. (2023). *EigenLayer Documentation: Actively Validated Service (AVS)*. EigenLayer. Retrieved from https://eigenlayer.io/docs/

[7] Polkadot Testnet Documentation Wood, G. (2016). *Polkadot: Vision for a Heterogeneous Multi-Chain Framework*. Web3 Foundation. Retrieved from https://polkadot.network/PolkaDotPaper.pdf

[8] EIP-4361: Sign-In with Ethereum Siu, A., & Johnson, T. (2021). *EIP-4361: Sign-In with Ethereum*. Ethereum Improvement Proposals. Retrieved from https://eips.ethereum.org/EIPS/eip-4361

[9] OAuth 2.0 Authorization Framework Hardt, D. (2012). *The OAuth 2.0 Authorization Framework*. Internet Engineering Task Force (IETF). RFC 6749. Retrieved from https://datatracker.ietf.org/doc/html/rfc6749

[10] Credit Costs Infura (2024). *Infura docs.* Retrieved from https://docs.infura.io/api/learn/pricing/credit-cost

[11] Mechanism Design for Blockchain Systems Carstens, A., Eichengreen, B., & Others. (2020). *Mechanism Design for Blockchain Systems*. Bank for International Settlements. Retrieved from https://www.bis.org/publ/othp37.pdf

[12] Ethereum 2.0 Economics Buterin, V. (2020). *Ethereum 2.0 Economics: Staking, Slashing, and Network Security*. Ethereum Foundation Blog. Retrieved from https://blog.ethereum.org

[13] Ethereum 2.0 Phased Rollout Plan Ethereum Foundation. (2019). *Ethereum 2.0 Roadmap: Phases and Future Implementation*. Ethereum Foundation Blog. Retrieved from https://blog.ethereum.org

[14] Uniswap Tokenomics Adams, H. (2021). *Uniswap v3 Whitepaper: Tokenomics and Governance*. Uniswap Labs. Retrieved from https://uniswap.org/whitepaper-v3.pdf

[15] State of Web3 Infrastructure Consensys. (2023). *State of Web3 Infrastructure: Trends, Challenges, and Opportunities*. ConsenSys Research. Retrieved from https://consensys.net/reports/web3-infrastructure/

[16] Compound Governance Protocol Leshner, R., & Hayes, G. (2019). *Compound Governance: A Decentralized Governance Framework for the Compound Protocol*. Compound Labs. Retrieved from https://compound.finance/governance

[17] Messari Annual Crypto Theses Report Selkis, R. (2023). *Crypto Theses for 2023*. Messari Research. Retrieved from https://messari.io/reports/crypto-theses-for-2023

Disclaimer

This whitepaper is for informational purposes only and does not represent an offer or solicitation to buy or sell any tokens or assets related to the Decentralized Infrastructure Network (DIN). As an evolving project under active development, all specifications, features, and timelines discussed here are subject to change without notice. This document should not be relied upon for financial, legal, or investment decisions.

Readers are encouraged to conduct their own due diligence and consult trusted sources for the most up-to-date project information. The authors, contributors, and associated entities make no warranties or representations about the accuracy or completeness of this document and disclaim all liability for any direct or indirect losses arising from its use.