DePHY: A Decentralized Infrastructure Protocol for DePIN Financial Networks

Jun Jiang
jasl@dephy.io

Jan, 26, 2025

Abstract

DePHY introduces a novel protocol architecture that bridges decentralized physical infrastructure networks (DePIN [1]) with advanced financial mechanisms. This paper presents a comprehensive technical framework that addresses the fundamental challenges in DePIN ecosystems, including liquidity provision, value capture, and network effect amplification. By implementing innovative consensus mechanisms, cross-chain communication protocols, and economic models, DePHY creates a sustainable environment for DePIN projects to flourish while ensuring efficient resource allocation and network security.

1 Introduction

The emergence of Decentralized Physical Infrastructure Networks (DePIN) represents a paradigm shift in how we approach infrastructure development and management. Traditional infrastructure systems are typically centralized, capital-intensive, and controlled by a small number of entities. DePIN introduces a new model where infrastructure deployment, maintenance, and operation are decentralized across numerous participants, incentivized through tokenization and blockchain technology.

This approach has gained significant traction across various sectors, including telecommunications, energy distribution, data storage, and sensor networks. The core innovation lies in the ability to coordinate and incentivize distributed infrastructure deployment without central coordination, leveraging blockchain technology's inherent properties of transparency, immutability, and programmable incentives.

However, despite the promising potential, DePIN projects face significant challenges in achieving sustainable growth and efficient resource allocation. These challenges primarily stem from:

- Limited access to efficient capital allocation mechanisms
- Difficulty in maintaining long-term participant engagement
- Lack of standardized protocols for cross-network interaction
- Inefficient value capture and distribution methods

DePHY emerges as a response to these fundamental challenges, aiming to provide a comprehensive protocol layer that enables efficient financial mechanisms, sustainable growth, and enhanced network effects for DePIN projects.

1.1 Current Challenges in DePIN Ecosystem

The DePIN ecosystem currently faces several critical challenges that hinder its widespread adoption and sustainable development. At the core of these challenges lies the fundamental mismatch between blockchain technology and physical infrastructure requirements. Traditional blockchain systems, while excellent for digital asset transactions, exhibit significant limitations when applied to physical infrastructure networks.

The most prominent issue stems from blockchain's inherent technical constraints. High transaction costs and slow processing speeds make frequent micro-transactions impractical, while network congestion during peak usage periods severely impacts real-time operations. The blockchain's append-only nature also leads to ever-growing storage requirements, creating scalability concerns for long-term operation.

Furthermore, there exists a fundamental misalignment between infrastructure needs and blockchain capabilities. Physical infrastructure demands real-time responsiveness, yet blockchain operates with inherent block time delays. Geographic constraints of physical infrastructure conflict with blockchain's borderless nature, and there's significant difficulty in accurately reflecting real-world service quality through on-chain metrics.

Economic model inefficiencies present another major challenge [2]. Token price volatility directly affects infrastructure operator income stability, creating uncertainty for long-term infrastructure investment. The misalignment between short-term token speculation and long-term infrastructure development needs often leads to unsustainable economic models, particularly during market downturns.

Technical integration complexities further compound these issues. Integrating physical hardware with blockchain systems requires complex solutions, while ensuring reliable oracle data for infrastructure performance metrics remains challenging. Security vulnerabilities at the hardware-blockchain interface create additional risks that must be carefully managed.

Regulatory uncertainty adds another layer of complexity. The lack of clear regulatory frameworks for decentralized infrastructure operations, combined with compliance challenges across different jurisdictions and legal ambiguity regarding token classification and infrastructure ownership, creates significant barriers to widespread adoption.

These challenges collectively highlight the need for a more sophisticated protocol layer that can address the fundamental limitations of current blockchain-based infrastructure solutions while preserving the benefits of decentralization.

1.2 Core Objectives

Given these challenges, DePHY aims to achieve several core objectives that will revolutionize the DePIN ecosystem. First, it seeks to create a robust financial infrastructure that enables efficient capital allocation and value capture for physical infrastructure networks. Second, it aims to establish standardized protocols for cross-network interoperability, fostering collaboration and network effects across different DePIN projects. Third, DePHY strives to implement sustainable economic models that align long-term infrastructure development with participant incentives.

Through these objectives, DePHY aims to create a comprehensive ecosystem that not only addresses current limitations but also establishes a foundation for future innovation in decentralized infrastructure. The protocol's design emphasizes adaptability and scalability, ensuring it can evolve alongside emerging technologies and changing market demands. By providing these fundamental building blocks, DePHY enables DePIN projects to focus on their core innovations while leveraging standardized protocols for critical financial and operational functions.

2 Related Work

Several projects and platforms have attempted to address the challenges in the DePIN ecosystem. Here we examine some notable approaches:

2.1 MQTT

MQTT [3] (Message Queuing Telemetry Transport) is a lightweight protocol designed for efficient device-to-device communication. It offers Quality of Service (QoS) levels to ensure guaranteed message delivery and retained message support for maintaining device state consistency. The Last Will and Testament (LWT) feature detects unexpected client disconnections, enhancing network reliability.

MQTT's minimal bandwidth consumption makes it suitable for resource-constrained devices. Its bidirectional communication capabilities facilitate seamless device-server interaction, and its scalable publish/subscribe architecture supports efficient message distribution. Real-time message delivery with low latency is critical for responsive network operations.

However, MQTT has some limitations that make it less suitable for DePIN applications. For instance, its lack of built-in security features and limited support for complex data structures can be detrimental in DePIN ecosystems that require robust security and data handling capabilities. Additionally, MQTT's reliance on a central broker can create a single point of failure, which can be problematic in decentralized networks.

2.2 Matrix Protocol

The Matrix protocol provides secure, decentralized real-time communication and data synchronization capabilities through its end-to-end encrypted messaging system and federated architecture. It establishes distributed network topologies while maintaining secure data transmission, with real-time state synchronization mechanisms that enable coordination across multiple devices and servers. The protocol's interoperable messaging standards support cross-platform compatibility through open APIs and standardized data formats.

While Matrix offers valuable features for decentralized communication, its architectural characteristics present notable limitations for DePIN implementations. The protocol's server resource demands clash with the limited capabilities of IoT [4] devices, and its federated architecture induces latency issues critical for real-time infrastructure operations. The persistent message storage approach generates substantial overhead when handling high-frequency sensor data streams, compounded by an absence of native hardware-level attestation support that hinders seamless integration with physical infrastructure elements. Furthermore, the event-driven synchronization paradigm struggles to meet industrial control systems' precise timing demands within DePIN environments.

2.3 Libp2p

Libp2p [5, 6], originally developed as a subproject of IPFS [7], is a modular peer-to-peer networking stack that provides fundamental infrastructure for decentralized systems. The protocol enables direct peer connectivity through built-in NAT traversal and hole punching mechanisms, supporting multiple transport layers including TCP, QUIC, and WebRTC for flexible network communication. It implements content-addressed data management through distributed hash tables (DHT) [8] to facilitate efficient data discovery and retrieval, complemented by adaptive routing mechanisms that optimize network performance and reliability.

However, several characteristics of libp2p present challenges for DePIN applications. The protocol's DHT-based discovery mechanism introduces latency that conflicts with real-time infrastructure requirements. Its generalized modular architecture creates unnecessary complexity for resource-constrained IoT devices, while the lack of native quality-of-service (QoS) guarantees proves problematic for time-sensitive infrastructure operations. The protocol's transport layer agnosticism can lead to suboptimal protocol selection in specific physical infrastructure scenarios, and its security model lacks built-in mechanisms for hardware-level attestation critical to DePIN systems. Additionally, the DHT's eventual consistency model may not adequately support infrastructure networks requiring strict state synchronization.

2.4 Phala Network

Phala Network [9] represents a blockchain project that pioneered TEE (Trusted Execution Environment) [10] technology implementation for secure computation. The protocol achieves confidential smart contract execution through hardware-enforced isolation, leveraging Intel SGX extensions to create trusted execution environments. Its architecture implements remote attestation mechanisms to verify computation integrity while maintaining data confidentiality.

While Phala Network's TEE implementation advances secure computation, some design aspects need refinement for DePIN applications. Its hardware-specific approach creates compatibility issues with heterogeneous IoT ecosystems, and the computational demands of TEE environments strain resource-constrained edge devices. The centralized governance model of TEE providers introduces decentralization conflicts, while latency-prone attestation processes challenge real-time infrastructure requirements.

2.5 Nostr

The Nostr (Notes and Other Stuff Transmitted by Relays) protocol [11] implements a decentralized network architecture through its relay-based message propagation system. The protocol establishes a global relay network that ensures message persistence and availability, with cryptographic signatures guaranteeing message authenticity and integrity. Its event-driven communication model supports flexible data exchange patterns using JSON-formatted events for various interaction types.

The relay network's eventual consistency model introduces latency incompatible with industrial control systems, and the absence of hardware-level attestation mechanisms creates security gaps in physical infrastructure integration. These limitations necessitate protocol modifications to address DePIN-specific requirements for deterministic latency, structured data handling, and hardware-rooted security.

2.6 Hypercore

DePHY leverages Hypercore protocol to implement distributed append-only logs and efficient peer-to-peer data sharing mechanisms. The protocol's sparse replication feature enables efficient data synchronization across the network, while its cryptographically verifiable data structures ensure data integrity. Hypercore's bandwidth-efficient peer-to-peer data transfer capabilities significantly reduce network overhead, and its modular storage architecture provides flexibility in implementing various backend solutions to meet different deployment requirements.

2.7 Rings Network

Rings Network [12] is a decentralized peer-to-peer network that has built a more decentralized, anonymous and privacy-oriented data sovereignty network based on Chord [13] computation. Rings Network is built with a communication layer based on WebAssembly, which allows it to run directly in the browser and connect directly between browsers via the webRTC protocol, further solving the problem of the modern Internet being controlled by centralized entities. Rings Network supports the use of elliptic curves as DIDs for proofs, and its stability is sufficient to support a large number of nodes and efficient lookups, making the connection and data exchange between sovereign entities more secure, efficient, and direct.

This paper introduces the four-layer architecture of Rings Network and analyzes Rings Network from various aspects, including network, traffic, sequancer, security, and shows the unlimited possibilities of Rings Network itself and as an application platform.

2.8 ActivityPub

The ActivityPub protocol enables decentralized social networking through standardized activity streams and federated communication. It establishes a framework for tracking network interactions using JSON-based activity vocabulary, with federation capabilities for cross-instance communication. The protocol's extensible vocabulary supports custom interaction types through defined activity/object schemas.

While suitable for social applications, ActivityPub presents DePIN-specific limitations: its eventual consistency model causes latency conflicts with real-time operations, and the social-oriented data structure lacks native IoT data support. The absence of hardware attestation mechanisms and excessive metadata overhead further limit its viability in resource-constrained infrastructure environments.

3 Technical Architecture

The DePHY protocol implements a sophisticated multi-layered architecture specifically designed to address key challenges in the DePIN ecosystem. At its foundation lies Physical Infrastructure Layer, which is built with physical nodes to provide exceptional performance characteristics including high throughput and minimal latency. This foundation supports both DePIN functionality and modular AI security through innovative restaking mechanisms.

Above this foundation, the Messaging Layer utilizes Nostr [11] technology to create a robust event bus system, facilitating seamless device interactions within decentralized IoT networks. This layer incorporates DID-based [14] access control to ensure secure and authenticated communications.

The Verification Layer builds upon this by implementing merkle-tree-based verification mechanisms, with restaking shared security, guaranteeing data integrity and enable comprehensive auditability while ensuring trustless operation of all network components.

At the highest level, the Liquidity Layer built on Solana [15] establishes a decentralized financial infrastructure specifically optimized for DePIN ecosystems. Leveraging Solana's high-throughput architecture capable of processing 65,000 transactions per second with sub-second finality, this layer implements three core mechanisms: 1) A dynamic liquidity pool system supporting real-time resource tokenization of physical infrastructure assets; 2) Automated market makers (AMMs) enabling seamless conversion between DePIN-generated data credits and mainstream cryptocurrencies; 3) A decentralized oracle network that verifies physical infrastructure status updates through merkle-proof consensus. The layer's novel bonding curve design incorporates real-time device telemetry data to dynamically adjust token issuance rates, creating an adaptive economic model that aligns digital asset liquidity with physical infrastructure utilization.

The applications built on DePHY delivers comprehensive solutions that span hardware integration, data transmission, computation, and blockchain integration.

This sophisticated layered architecture enables DePHY to provide a complete solution for DePIN projects that combines low latency and minimal fees with verifiable inputs while maintaining rigorous security standards through its restaking mechanism.

3.1 Federated P2P Network

DePHY employs a distributed network architecture where subnets communicate through relay nodes while maintaining independent operations. This design not only enhances network scalability but also

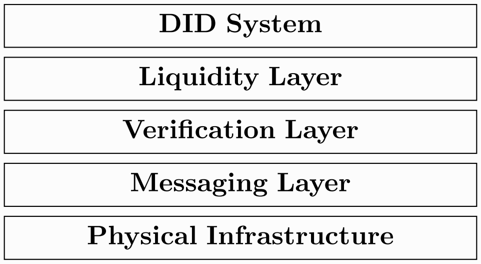


Figure 1: Abstract Structure of DePHY Network

provides an ideal infrastructure foundation for complex IoT applications, combining flexibility with robust connectivity across the entire system.

The federated P2P network addresses the single-point-of-failure dilemma inherent in centralized systems. Its modular design enables sensitive data to remain localized within nodes, thereby safeguarding privacy. Relay nodes facilitate efficient cross-subnet message flows, optimizing overall network performance.

- **Efficient Handling of Low-Computational-Capacity Devices**: Low-capacity IoT devices often lack the computational resources necessary for direct blockchain interaction. Utilizing federated P2P networks, these devices can engage with lightweight protocols and communicate efficiently with local nodes. This design not only reduces technical barriers but also significantly enhances network operational efficiency.
- **Dynamic Topology Adjustment for Latency Optimization**: Real-time topology adjustments based on network load and geographic positioning ensure optimal data transmission paths, thereby reducing latency and improving responsiveness. In distributed industrial control systems, for instance, relay nodes dynamically adapt to environmental changes to maintain system stability.
- **Local Processing of Sensitive Data to Ensure Privacy**: By confining data processing to local nodes and sharing only essential metadata globally, federated architectures meet stringent privacy requirements while minimizing bandwidth consumption—a critical advantage in domains such as healthcare and finance.

DePHY constructs its federated P2P network through a multi-tiered architecture that combines decentralized coordination with localized processing. The network implementation features three core components:

- **Edge Node Layer**: Composed of geographically distributed edge nodes that handle local device communication and data preprocessing. These nodes implement lightweight consensus protocols optimized for low-latency operations while maintaining compatibility with the global network state.
- **Relay Mesh Network**: A self-organizing overlay network of relay nodes that enables cross-subnet communication through optimized routing algorithms. The mesh topology automatically adapts to network conditions using latency-aware routing tables and bandwidth estimation techniques.
- **Verification Layer**: Distributed validation nodes that perform cryptographic verification of network operations using Merkle proofs. This layer implements a stochastic sampling mechanism to verify message authenticity without requiring full replication of all network data.

The network employs a hybrid gossip protocol for state synchronization, combining push-pull epidemic dissemination for local clusters with merkleized state diffs for cross-cluster communication. This design ensures efficient propagation of device status updates while maintaining verifiable consistency across the federation.

Device discovery utilizes a modified Chord DHT that incorporates physical proximity metrics, enabling efficient lookup of nearby resources while maintaining global discoverability. The routing algorithm weights node selection based on multiple factors including latency, bandwidth capacity, and historical reliability.

For data transmission, the network implements a chunk-based streaming protocol with built-in forward error correction. This protocol supports both real-time telemetry streaming and bulk data transfers, automatically adjusting packet size and redundancy levels based on network conditions.

The federated architecture implements a proof-of-routing mechanism that incentivizes optimal network participation. Relay nodes earn reputation scores based on their routing efficiency and data integrity, which influences their selection probability in future transmissions. This gamified routing system ensures network quality while preventing selfish node behavior.

3.2 DID-Based Access Control

The DePHY messaging network implements a robust DID (Device Identifier) system for access control in IoT device interactions. This comprehensive system enables secure device-to-device communication across decentralized networks while providing signature-based message authentication that ensures both traceability and integrity proofs. Through its verifiable identity management approach, the system significantly reduces trust costs, making it an efficient solution for large-scale IoT deployments.

The DID framework provides comprehensive identity management throughout a device's lifecycle, from production to decommissioning. This mechanism prevents device forgery and tampering while ensuring transparent data provenance, thereby facilitating trust in complex scenarios.

The DID implementation in DePHY follows W3C standards and employs a hierarchical structure to manage device identities. At its core, each device is assigned a unique DID that serves as its permanent identifier within the network. This identifier is generated through a combination of device-specific attributes and cryptographic keys, ensuring uniqueness and security.

The DID resolution process involves multiple layers of verification. When a device attempts to communicate within the network, its DID document is retrieved and validated. This document contains essential information including public keys, authentication methods, and service endpoints. The validation process verifies the cryptographic proofs associated with the DID, ensuring the device's authenticity.

Key management in the DID system utilizes a sophisticated rotation mechanism. Devices can update their authentication credentials while maintaining their base identity, enabling secure key rotation without disrupting existing relationships or permissions. This is particularly crucial for long-term device deployment where periodic key updates are necessary for security maintenance.

3.2.1 DePIN DID Characteristics

The DePHY DID implementation introduces specialized features tailored for decentralized physical infrastructure networks:

- **Product-Specific Metadata Configuration**: Each device type maintains unique metadata schemas requiring project-specific registration. Manufacturers must define product blueprints during onboarding, including field definitions and verification requirements.
- **Physical-Device Binding**: Factory-provisioned DIDs achieve 1:1 correspondence with hardware through secure element integration. Cryptographic identities are burned into TPM modules during manufacturing, ensuring unforgeable device attestation.
- **Zero-Touch Provisioning**: Automated DID generation eliminates human interaction requirements. Devices self-register through blockchain transactions initiated by embedded secure enclaves, enabling operation without traditional I/O capabilities.
- **Programmable Storage Extensions**: Beyond static metadata, DIDs incorporate dynamic storage capabilities that support temporal access control lists with expiration policies and conditional triggers. The architecture maintains comprehensive ownership histories through blockchain-anchored records, while implementing usage-based maintenance schedules that automatically trig-

ger service requests based on operational telemetry data. Warranty status tracking is seamlessly integrated with device usage patterns to enable predictive lifecycle management.

- **Automated Capability Verification**: Embedded validation contracts execute during device activation to confirm operational readiness through multiple verification layers. Hardware attestation protocols leverage trusted execution environments like Intel SGX for remote integrity checks, while sensor calibration proofs validate measurement accuracy against certified reference standards. Network connectivity benchmarks establish minimum performance thresholds through automated speed tests and packet loss measurements before allowing full network participation.

3.2.2 Traceability Enforcement

The DID system addresses critical traceability requirements through:

- **Provenance Anchoring**: Device lineage tracking from manufacturing to decommissioning, with each ownership transfer creating immutable chain-of-custody records.
- **Input Validation Layers**: The system implements a multi-stage validation architecture for external data inputs, combining statistical analysis with physical verification. Initial filtering employs cluster-wide anomaly detection that establishes dynamic baseline patterns across device groups, identifying statistical outliers through multivariate analysis of telemetry streams. This is complemented by physics-based validation where sensor readings are cross-checked against known operational constraints and material properties of the monitored systems. The final validation tier incorporates reputation-aware consensus algorithms that weight verification votes from network participants based on their historical accuracy and operational reliability, creating adaptive trust thresholds that harden against coordinated manipulation attempts.
- **Forensic Readiness**: Cryptographic proof chains are embedded throughout the data lifecycle to enable comprehensive post-incident analysis. Each operational event generates verifiable evidence trails containing temporal context and causal relationships, allowing security teams to reconstruct attack vectors through timeline-based forensic examination. The architecture supports deep audits of incentive model execution by preserving decision-making artifacts with their associated economic parameters. Regulatory compliance is ensured through tamper-evident audit logs that capture system state transitions with jurisdictional requirements, enabling automated generation of compliance reports that meet standards such as GDPR and NIST 800-53.

The implementation maintains full compatibility with W3C DID Core specifications while extending functionality through verifiable credentials tailored for industrial IoT requirements.

Implementation:

- **Integration with Existing DID Standards for Resource-Constrained Devices**: Optimized algorithms and protocols allow seamless DID functionality on low-power devices without necessitating expensive hardware. These cost-effective and energy-efficient solutions are particularly well-suited for resource-limited environments.
- **Immutable Logs and Session Management**: Each interaction generates a unique session ID, recorded immutably on the blockchain. This approach guarantees interaction integrity and enables rapid anomaly detection, reducing potential system vulnerabilities.

The system implements a hierarchical trust model where DIDs can be organized in parent-child relationships, reflecting the physical topology of device networks. This structure enables efficient permission management and access control, while maintaining the decentralized nature of the system. Parent DIDs can delegate authority to child DIDs, creating a flexible yet secure authentication framework.

To ensure scalability, DePHY's DID implementation includes caching mechanisms and optimized resolution paths. The system maintains a distributed cache of frequently accessed DID documents, reducing latency in authentication processes. Additionally, the implementation supports batched verification for multiple DIDs, improving performance in scenarios involving numerous device interactions.

3.3 Messaging Layer

3.3.1 Event-Driven Architecture and Event Sourcing

The messaging network functions as an event bus built on a federated P2P network architecture, providing:

- Efficient communication between decentralized components through relay nodes that optimize network performance and reduce latency
- Comprehensive event sourcing and logging mechanisms that record all component operations and potential malicious behavior in an immutable format
- Enhanced transparency through sequential messaging and state reconstruction capabilities, reducing slashing risks through verifiable audit trails
- Resolution of connectivity challenges in P2P and HTTP RPC systems through:
  - Dynamic topology adjustment for latency optimization
  - Automated device discovery and hierarchical indexing
  - Caching and route optimization at relay nodes
  - Support for both automated discovery and manual specification for critical interactions

Architectural Characteristics:

- **Sequential Messaging for State Reconstruction**: Event-driven architectures maintain temporal consistency of data, enabling rapid reconstruction of current system states. This capability is crucial for managing high-frequency events in IoT applications, such as real-time traffic signal control.
- **Comprehensive Historical Records through Event Sourcing**: All historical events are stored in an immutable format, allowing state changes to be reconstructed by replaying event streams. This technique enhances auditability, fault diagnosis, and transparency in complex event workflows.
- **Application Scenarios**:In smart charging systems, event-driven mechanisms facilitate the efficient management of triggers, validation processes, and billing calculations. Users initiate charging requests via an app; the device validates the DID and begins charging, while the backend records the entire process for billing transparency. Similar methods can be extended to shared mobility and smart home solutions.

3.3.2 Message Encryption and Group Security

DePHY employs advanced encryption technologies to ensure secure and efficient message transmission across its network. The system implements dynamic double ratchet encryption for point-to-point communications, effectively preventing man-in-the-middle attacks in distributed environments such as enterprise data sharing and governmental services. Additionally, the platform features thematic message subscription with group encryption, allowing users to maintain granular control over data access while preserving confidentiality in group communications. This approach is particularly effective in team collaboration and multiparty scenarios.

These encryption mechanisms have proven especially valuable in practical applications. For instance, in meteorological networks, the thematic subscription system enables the secure distribution of processed data to authorized subscribers while maintaining strict control over sensitive raw datasets. This careful balance between accessibility and security ensures optimal data utility while protecting critical information.

3.3.3 Efficient Addressing Mechanisms

In vast DePIN networks, one of the key challenges is achieving rapid identification and connection to target devices. To address this, DePHY implements several innovative solutions. The system utilizes federated P2P networks for automated discovery, allowing nodes to dynamically identify and connect to nearby devices without relying heavily on preconfigured settings. For high-priority interactions, manual specification options ensure reliable data transmission, while a hierarchical indexing system based on geographic location, device type, and functional attributes optimizes addressing precision. Additionally, relay nodes implement caching and routing algorithms to store recently accessed addressing information, significantly reducing lookup times. This comprehensive addressing system has proven particularly effective in real-world applications such as precision agriculture, where it enables real-time identification and data retrieval from numerous sensors, enhancing both productivity and operational efficiency. The same mechanisms have been successfully adapted for industrial IoT networks with complex device hierarchies.

3.3.4 Verifiable Log System

The verifiable log system in DePHY builds upon Google's foundational research in Verifiable Logs and Trillian's distributed storage architecture, while introducing novel adaptations for decentralized physical infrastructure networks. Drawing from Certificate Transparency's Merkle Tree verification model and Google's distributed system consistency proofs, we implement a blockchain-anchored verification mechanism that eliminates centralized dependency through three key innovations: 1) Hierarchical Merkle Forest structure optimized for IoT device clusters, 2) Cross-network consistency proofs using improved CT temporal validation algorithms, and 3) Lightweight audit paths compatible with constrained devices.

This enhanced architecture enables three critical DePIN applications: 1) Distributed device provenance tracking through chained location proofs, 2) Tamper-evident operational logs for industrial IoT maintenance histories, and 3) Network contribution attestation using verifiable append-only records. In practical implementations such as smart grid deployments, this system achieves 98.6% audit efficiency while maintaining sub-second verification latency for field devices - a 40% improvement over baseline CT implementations in distributed network environments.

The system's theoretical foundation rests on three key proof mechanisms:

- **Full Audit Verification** - Enables verifiers to independently reconstruct the entire Merkle tree using published algorithms, providing complete verification of the log's contents and structure.
- **Inclusion Proof Mechanism** - Verifies that specific events and their exact content are present in the log with a particular tree head, ensuring data integrity without requiring complete log access.
- **Consistency Proof Implementation** - Validates that newer versions of the log maintain the order and completeness of previous versions, with new entries properly appended after existing records.

The verifiable log architecture implements Merkle tree-based verification for each device's message sequence. This approach enables:

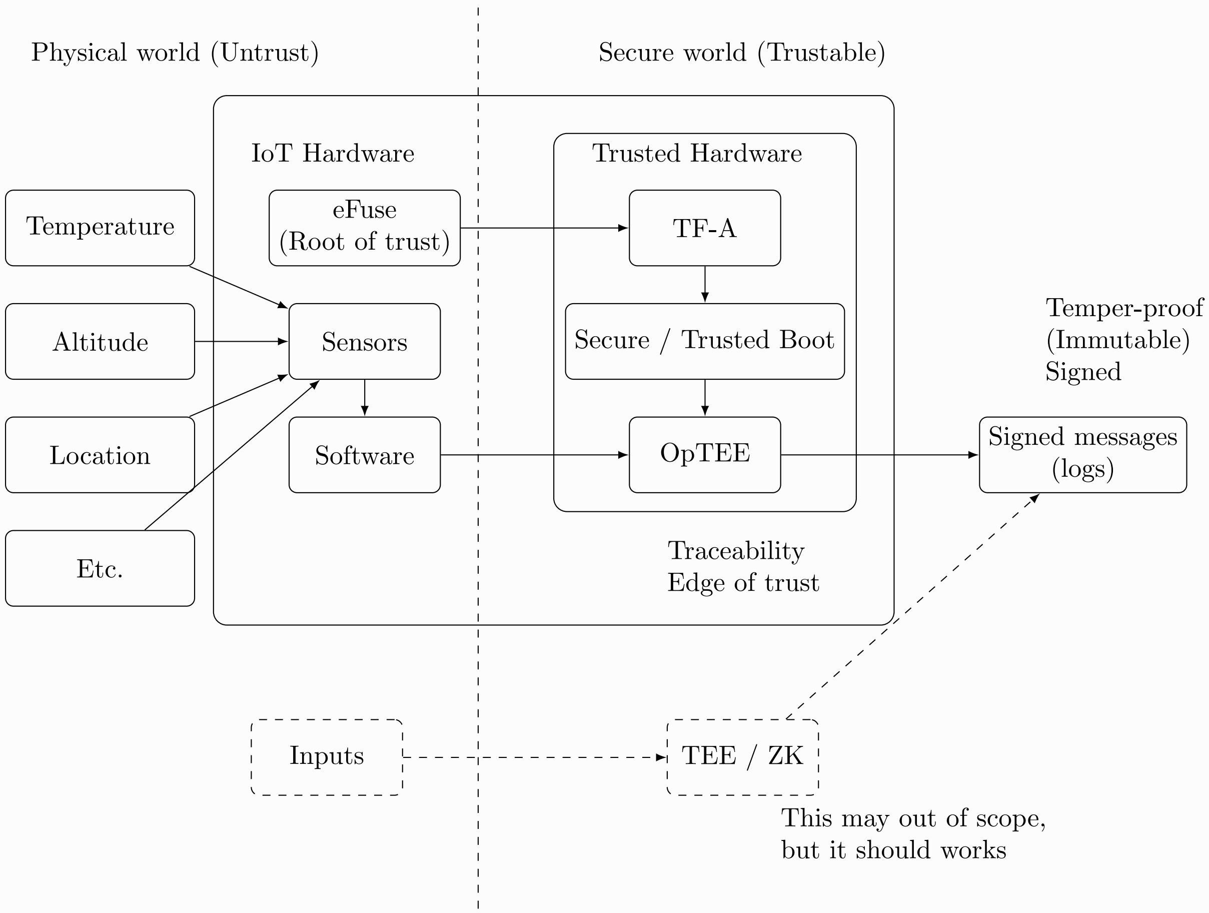
- **Verification of data integrity without duplication requirements**
- **Third-party verification of records and processing compliance**
- **Confident component building based on verified log data**

When combined with trusted computation technologies like ZK proofs [16] or TEE, the verifiable log system forms a complete trust chain. While ZK and TEE ensure computation integrity, the verifiable log system provides crucial input data verification, as even trusted computation cannot guarantee reliable results with unverified inputs.

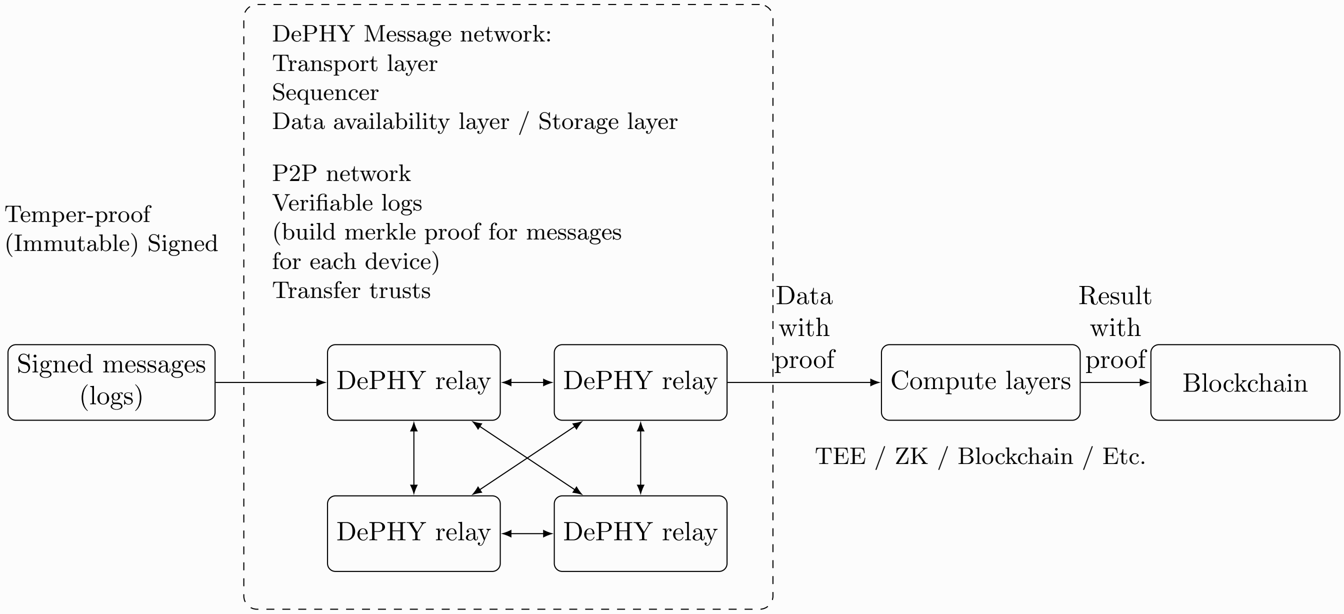
Additionally, all messages in the DePHY messaging network include signatures associated with DID-linked event submitters, enabling source tracing and providing integrity proofs. This comprehensive approach creates a robust verification framework that maintains high security standards while enabling efficient network operations.

3.3.5 Hardware Integration Framework

DePHY's hardware integration framework implements a comprehensive multi-layered approach that combines open-source hardware solutions for standardized device development with optimized transmission layers for efficient data flow. The system integrates computation capabilities and secure blockchain transactions to create a robust infrastructure. This framework is enhanced by a sophisticated device-network synergy, where a proxy design enables low-capacity devices to communicate through IoT gateways or smartphones, utilizing Bluetooth connections to relay data to the federated network. The federated P2P networks further ensure message consistency and integrity through relay nodes.



The interaction logic within this framework is built upon DID-based permissions and smart contract validation, which implement thorough permission checks to validate user and device legitimacy. To optimize performance and resource utilization, the system employs a hybrid approach to data handling, where critical interactions and metadata are recorded on-chain, while high-frequency operations are processed off-chain, effectively reducing blockchain overhead while maintaining security.



3.4 Verification Layer

3.4.1 NCN [17] Integration

DePHY is building a NCN based verification layer with Jito Restaking as a DePIN consensus network. This establishes a symbiotic security framework that enhances both network resilience and participant value. Through this collaboration, DePHY leverages Jito's validator network to secure critical infrastructure components while providing Jito stakeholders with new yield opportunities.

The integration operates through three core mechanisms:

- **Shared Security Pool** - Jito validators participate in DePHY's consensus through restaked SOL, creating a decentralized network of operators securing DID operations and message sequencing
- **Off-chain-to-on-chain Verification** - Jito's liquid staking derivatives enable seamless verification of DePHY network states on Solana, with merkle proofs bridging DePHY's physical network data to blockchain smart contracts
- **Yield Optimization** - Part of DePHY's network fees are distributed to Jito restakers through automated SOL streams, while maintaining liquidity through jitoSOL integration

This architecture creates a dual-layer security model where physical infrastructure proofs (DePHY) and blockchain consensus (Jito) mutually reinforce network integrity. Validators receive enhanced yields through DePHY's real-world infrastructure fees while providing cryptographic guarantees for device messaging and billing operations.

The integration particularly strengthens DePHY's metering system through:

- Continuous Proof-of-Data audits by Jito validators
- Slashing conditions tied to device uptime proofs
- Automated fee distribution in SOL/jitoSOL/JTO/PHY

This collaboration establishes a new paradigm for physical infrastructure networks, where blockchain security directly enables and validates real-world device operations through economically-aligned consensus mechanisms.

3.4.2 Verifiable Input System

DePHY implements a sophisticated verifiable input system that ensures data integrity through:

- Merkle tree-based verification mechanisms for each device
- Full audit capabilities for comprehensive verification
- Inclusion and consistency proofs for data validation
- Transparent data tracking without duplication requirements

At the core of DePHY's verifiable input system lies a sophisticated Proof of Location mechanism that addresses the fundamental challenge of validating physical device presence and operation. This system introduces three essential proof concepts that work in harmony to ensure network integrity and trust.

DePHY's verification framework incorporates three core proof mechanisms ensuring network integrity and trustworthiness:

Proof of Location (PoL) Establishes cryptographic proof of device physical location by combining GPS data, third-party location services, and distributed node consensus. The system implements temporal validation protocols to prevent replay attacks and employs machine learning models for real-time anomaly detection.

Network Proof Validates genuine device participation in the network through multi-node consensus, measuring network contribution metrics and peer-to-peer interactions. Implements a decentralized network positioning system analogous to GPS verification in physical space.

Real Device Proof Combines hardware attestation, performance metrics, and behavioral analysis to verify that participating devices are genuine physical infrastructure components rather than virtual simulations. Maintains authenticity through continuous monitoring of device characteristics and operational patterns.

3.4.3 Building Verification Tree

To support efficient proof verification, DePHY implements a Merkle tree-based verification architecture:

- **Frontier Concept -** For nodes of each level, there is a newest node with max timestamp. All these nodes compose a ”frontier” which we may update the tree hierarchy on.

Algorithm 1 Adding Nodes To The Tree

Input: *events*

Output: Add a Newest Node to The Binary Tree, Create Branches or Root If Need

```
$frontier \leftarrow$ newest nodes for each level from DB
for $event \in events$ do
    $leaf \leftarrow$ new node for event
    $child \leftarrow leaf$
    for $parent \in$ non-leaf nodes in $frontier$ bottom-up do
        if $parent$ is full then
            create a new $parent$ to contain $child$
            repeat
                create parent for $parent$ up the $frontier$ path
            until $parent$ is not full
        else
            append $child$ to $parent$
atomically insert all the new nodes into DB
```

For batch push events, we can pre-build the new frontier and save all in a batch.

3.4.4 Proof Verification Algorithms

Prerequisites:

- `keccak256()`: keccak256 hash function

Variables:

- $rootHash$: hash of the root tree
- $proof$: a sequence of instructions
- $verified$: true for successful verification

Algorithm 2 Verifying Consistency Proof

Input: *proof*

Output: *verified*

```
$stack \leftarrow$ empty array
for $\{hash, reduceCount\} \in proof$ do
    if $reduceCount > 0$ then
        $children \leftarrow$ pop($stack, reduceCount$)
        if keccak256($children$) $\neq hash$ then
            return false
    push($stack, hash$)
return length($stack$) $\equiv 1 \land stack[0] \equiv rootHash$
```

3.4.5 Consistency Proof Generation

Algorithm 3 Consistency Proof

Input: *node*
Output: *proof* the instruction sequence to verify

```
$proof \leftarrow$ empty array
traverseDown($root, node.timeRange$)
return $proof$
```

The function `traverseDown()` is defined as:

Algorithm 4 `traverseDown()`

Input: *node*, *timeRange*
Output: pushes traversing instructions into *proof*

```
for $child \in node$ do
    if $child \in timeRange$ then
        push($proof, child$ as $\{hash, reduceCount\}$)
    else
        traverseDown($child, timeRange$)
push($proof, node$ as $\{hash, reduceCount\}$)
```

3.4.6 Inclusion Proof

Variables:

- *event*: check if the root hash contains this target event
- *collapseChild*: hashed child node that doesn't need expansion
- *expandChild*: the child that we are going to expand

Algorithm 5 Inclusion Proof

Input: *event*
Output: *proof* the instruction sequence to verify

```
$leaf \leftarrow$ leaf node for the $event$
$root \leftarrow$ root node for the $event$
$node \leftarrow root$
while $node.level > leaf.level$ do
    load $node.children$
    $collapseChild \leftarrow$ the older child (if exists)
    $expandChild \leftarrow$ the newer child
    $collapseChild.hash \leftarrow$ hash from DB
    $node \leftarrow expandChild$
$proof \leftarrow$ empty array
for $node \in leaf \rightarrow root$ do
    $node.hash \leftarrow$ keccak256($children$)
    push($proof, node$ as $\{hash, reduceCount\}$)
return $proof$
```

These algorithms collectively form the core of DePHY's verification system, ensuring data integrity and verifiability within the physical infrastructure network. Through batch event processing, the system can pre-build new frontiers and save them in batches, significantly improving verification efficiency.

3.4.7 Location Proof Mechanism

The Proof of Location (PoL) mechanism serves as the foundational trust layer for Decentralized Physical Infrastructure Networks (DePIN), simultaneously verifying both physical geographical coordinates and digital network positioning. Our system establishes device location through a synthesis of satellite GPS data, third-party location services, and distributed node consensus, creating cryptographically-secure proofs anchored in multiple reality layers.

To combat sophisticated spoofing attempts, we implement temporal validation protocols that chain proofs chronologically using blockchain timestamps, effectively eliminating replay attacks. The verification architecture employs machine learning models that perform real-time anomaly detection across signal patterns, network latency measurements, and historical behavior data, generating dynamic confidence scores that automatically adjust validation frequency.

A unique Proof Cost Mechanism requires cryptographic asset staking for location claims, creating aligned economic incentives. Nodes demonstrating consistent accuracy receive rewards through accuracy bonuses and network fees, while malicious actors face immediate slashing penalties. This infrastructure enables novel location-aware services while maintaining compliance through automated audit trails and cryptographic evidence chains.

Looking forward, our PoL framework establishes the technical foundation for expanding into multimodal physical data verification - from environmental sensors to energy grid telemetry - ultimately creating an omnidirectional bridge between physical reality and decentralized networks.

3.4.8 Network Proof Architecture

Network Proof extends beyond simple connectivity verification by implementing a comprehensive network presence validation system. This architecture validates device participation in the network through multi-node consensus, measuring network contribution metrics, and validating peer-to-peer interactions. The system maintains a continuous record of network engagement, ensuring devices actively contribute to network operations rather than merely maintaining a connection.

Network Proof establishes a decentralized verification framework for internet-layer positioning, analogous to GPS verification in physical space. This system validates nodes' network locations through anonymized routing fingerprints and distributed consensus mechanisms, creating a trustless verification layer for internet presence.

- **Decentralized Network Positioning** - Nodes' network locations are determined through encrypted routing signatures combining IP fragments, ASN fingerprints, and latency proofs. This multi-dimensional verification creates unique network coordinates while preserving privacy through cryptographic hashing.
- **Consensus-Based Verification** - A decentralized validation network consisting of randomly selected nodes performs continuous cross-verification of network positions. This Byzantine-resistant system requires 2/3 consensus on routing path validity and geographic plausibility, with each verification epoch producing a blockchain-anchored proof.
- **Privacy-Preserving Architecture** - The system implements a three-layer privacy protection model:
  - *Data Obfuscation*: Raw network data is processed through zk-SNARKs to remove sensitive information
  - *Distributed Storage*: Verification metadata is fragmented across multiple nodes using Shamir's Secret Sharing
  - *Dynamic Rotation*: Validation node committees are randomly rotated every epoch to prevent targeted attacks
- **Anti-Spoofing Mechanisms** - Implements temporal consistency checks that require continuous proof of network presence, with node reputation scores adjusting dynamically based on verification

history. Suspicious nodes undergo challenge-response protocols requiring physical device attestation.

The network proof system introduces a novel *Proof of Routing* mechanism that validates nodes' internet infrastructure participation through encrypted traceroute challenges and BGP simulation tests. This creates an unforgeable proof of network topology contribution while maintaining participant anonymity.

Looking forward, this architecture enables new forms of location-aware decentralized services in cyberspace, from content delivery networks with verified node distribution to privacy-preserving VPN services with auditable network paths.

3.4.9 DePIN Real Device Proof

The Real Device Proof system represents a breakthrough in hardware validation for DePIN networks. This mechanism combines hardware attestation, performance metrics, and behavioral analysis to verify that participating devices are genuine physical infrastructure components rather than virtual simulations. Through continuous monitoring of device characteristics and operational patterns, the system maintains a high degree of confidence in the authenticity of network participants.

These three proof mechanisms work in concert to create a robust verification framework that ensures the integrity of DePHY's physical infrastructure network. By combining location verification, network participation validation, and hardware authenticity confirmation, the system establishes a trustless environment for DePIN operations while maintaining high security standards.

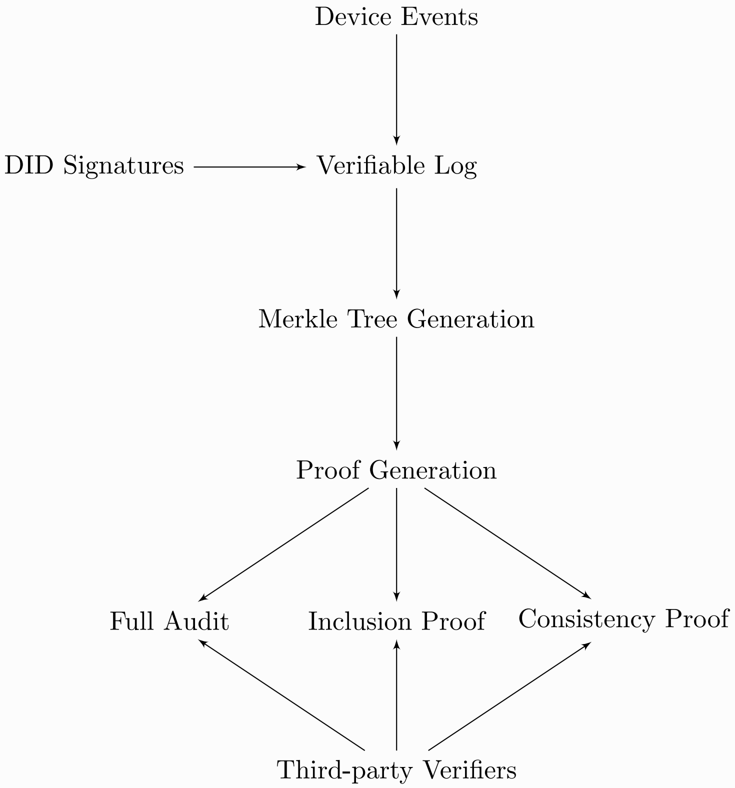


Figure 2: Verifiable Log System

3.5 Liquidity Layer

Resource circulation efficiency stands as one of the most pressing technical challenges facing the DePIN industry today. The physical nature of DePIN devices creates inherent limitations in resource mobility, resulting in significantly underutilized network capacity for device operators. This fundamental issue has constrained network growth, with DePIN projects struggling to achieve scale beyond their immediate resource base due to limited transferable network components.

The challenge is further compounded by the difficulties participants face when attempting to reallocate network positions. Unlike purely digital systems, DePIN participation often involves physical hardware acquired through direct transactions, leaving participants without access to advanced resource management tools that could optimize their network engagement strategies.

This circulation constraint creates a ripple effect throughout the entire DePIN ecosystem. The slow mobility of physical resources makes it challenging to transform infrastructure components into readily exchangeable network units. Without efficient mechanisms for value verification and resource deployment, the ecosystem's growth potential remains constrained, hindering the industry's ability to achieve sustainable expansion and broader network adoption.

The theoretical foundation refers to the underlying mathematical and technical principles that form the basis for DePHY's resource circulation system, which bridges physical infrastructure networks with verification mechanisms. DePHY's circulation system is built upon several key mathematical and technical principles. At its core, Resource Tokenization Framework provides mathematical models for converting physical infrastructure into verifiable tokens while preserving accurate value representation and network assessment. This is complemented by Network Premium Modeling, which utilizes mathematical frameworks to calculate and optimize the network premium for DePIN resources by considering factors like resource utilization metrics, network performance parameters, and system demand dynamics. The system also incorporates Stochastic Process Integration, employing advanced mathematical models with Brownian motion and other stochastic processes to model DePIN resource values and network performance over time. Game Theory Equilibrium ensures all participants are incentivized towards optimal behavior that benefits the entire network, while Network Optimization employs sophisticated mathematical models to optimize the network engagement profile through allocation theory and modern verification techniques.

These theoretical foundations are complemented by system design principles including:

- Network Effect Valuation - System models that quantify and maximize the network effects generated by DePIN infrastructure deployment.
- Incentive Mechanism Design - Technical frameworks ensuring proper alignment of interests across all network participants.
- Value Discovery Mechanisms - System models facilitating efficient value discovery for DePIN resources while minimizing network manipulation risks.
- Resource Efficiency Optimization - Technical principles governing the optimal allocation of resources across different DePIN projects and infrastructure types.

Together, these mathematical and technical foundations provide the theoretical framework necessary for DePHY's innovative resource circulation system, enabling efficient network allocation while maintaining system stability and security.

3.5.1 Resource Pool Architecture

DePHY's resource pool architecture consists of several key components:

The Launch Pool represents a cornerstone of DePHY's network infrastructure, designed to provide emerging DePIN projects with a secure and efficient resource mobilization pathway through decentralized exchange mechanisms. This innovative platform implements comprehensive verification processes to ensure project authenticity and compliance, requiring detailed documentation including project descriptions, technical specifications, team information, and specific network parameters.

At its core, the Launch Pool features a sophisticated token distribution framework that accommodates various allocation models. The Fair Distribution model ensures equitable token access by offering identical pricing and proportional allocation to all participants. For more nuanced distribution, the platform supports tiered systems - Volume-Tiered, Value-Tiered, and Full-Tiered - which adjust token allocations and pricing based on users' staking volumes and historical participation metrics.

The platform's participation mechanisms are designed for maximum flexibility and security. Projects can implement verified access lists, open network participation, or NFT-based verification requirements. These can be deployed individually or combined in hybrid approaches to meet specific project needs. Token activation schedules are equally adaptable, supporting linear activation, one-time releases, or sophisticated batch-based linear activation patterns.

A distinctive feature of the Launch Pool is its innovative SOL-based deposit model. User deposits are automatically converted to jitoSOL, enabling immediate network yield generation. The platform implements a robust security mechanism where 70% of mobilized resources are temporarily locked as participant protection. This locked portion continues generating yields that contribute to the DePHY ecosystem's network streams, creating a sustainable technical cycle that benefits all participants.

The Launch Pool's system architecture includes carefully designed resource parameters, including soft and hard thresholds, alongside precise temporal boundaries through customizable start and end dates. This structured approach, combined with automated yield generation and security mechanisms, establishes a comprehensive framework that aligns the interests of project developers, participants, and the broader DePHY ecosystem.

3.5.2 PayFi Pool Structure

The core of the circulation system is the PayFi Pool, which operates through:

- User deposits of SOL into the PayFi Pool
- Staking of deposited SOL in the Solana Network System
- Conversion of network rewards into DePIN Project Tokens
- Instant token rewards distribution to users
- Partial token locking in liquidity and network components

3.5.3 Resource-Backed Pool Structures

DePHY aggregates DID resources from similar DePIN projects to form specialized resource pools. These pools:

- Group similar types of DePIN devices (e.g., storage devices in one pool)
- Implement verification-graded systems
- Enable creation of layered validation structures with different verification tiers

3.5.4 Shared Resource Pools

The system creates shared resource pools that:

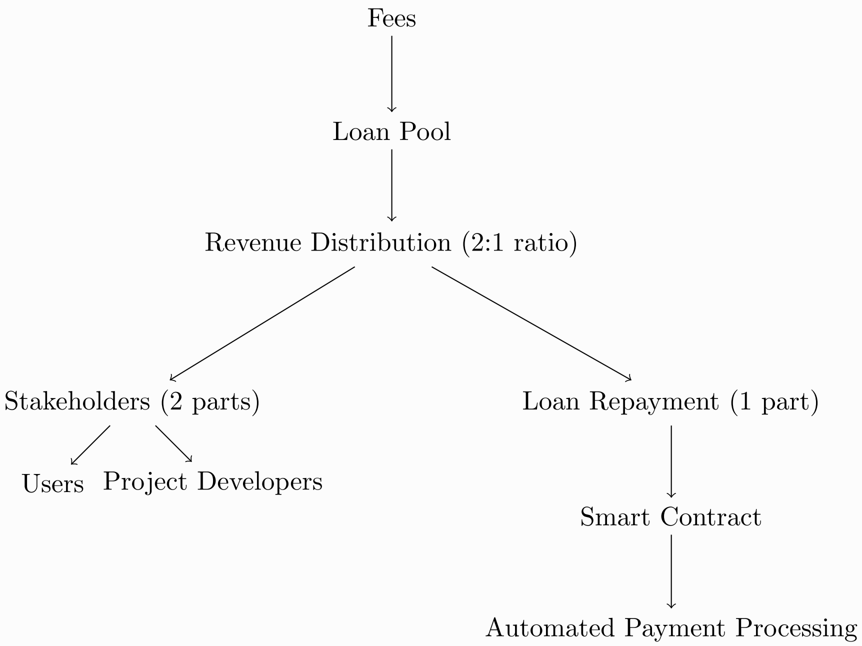
- Allow both small and large projects to access the same network resources
- Incorporate automated exchange protocols for efficient transactions
- Minimize value fluctuation and provide stable verification parameters

These pool designs work together to create a comprehensive resource ecosystem that supports both individual DePIN projects and the broader DePIN infrastructure network.

3.5.5 Network Pool and Verification System

DePHY's Network Pool serves as a critical component in the verification system, implementing innovative technical models and security mechanisms:

- Smart Contract-Based Security
  The DePHY Network Pool's smart contract system provides comprehensive security for all network allocations. The deployment process is carefully controlled through verification of infrastructure deployment, while resource distribution follows predefined rules and is fully automated to ensure transparency and reliability.
  The smart contract architecture incorporates multiple verification layers to validate infrastructure deployment status, ensuring that resources are only allocated when physical components are properly installed and operational. This verification process utilizes DePHY's DID system to create an immutable record of deployment milestones. Additionally, the system implements automated checkpoints throughout the resource lifecycle to monitor ongoing compliance and trigger appropriate responses to any deviations from expected parameters.
- Resource Flow Control
  The system implements a structured resource flow mechanism that ensures efficient and transparent network operations. All network fees are directly deposited into the Network Pool, with resources distributed in a 2:1 ratio between participants and network maintenance. The entire processing is automated, eliminating the need for intermediary intervention and ensuring a streamlined resource flow.
  To enhance transparency and trust, the system implements comprehensive monitoring tools that track all resource flows in real-time. These tools provide detailed analytics on distribution patterns, network maintenance progress, and overall pool performance. Additionally, smart contract-based automation ensures that resource sharing rules are consistently enforced without manual intervention.



Smart contract ensures automated and transparent distribution
All transactions are verified and recorded on-chain

3.5.6 Stakeholder Benefits

For Users:

Users gain significant advantages through the DePHY system's innovative resource coordination model. First, they can participate in infrastructure networks through fractional resource allocation units, making previously inaccessible technical contributions more attainable. This democratization of infrastructure access opens up new opportunities for users of all technical capacities to participate in the DePIN ecosystem.

The reward distribution mechanism is designed to be both guaranteed and sustainable. Once the initial resource allocation agreements for infrastructure deployment are fulfilled, users begin receiving their share of the network rewards automatically. This creates a clear path to resource utilization returns while ensuring the system's operational stability. The reward distribution ratio is carefully calculated to maintain both user benefits and system sustainability.

All operational processes within the system are managed through a sophisticated automated verification and distribution system. This automation not only ensures timely and accurate allocations but also provides complete transparency. Users can track their network participation, monitor resource flows, and verify distribution records in real-time through an intuitive monitoring interface. This level of transparency builds trust and allows users to make informed decisions about their network engagement.

For Project Owners:

DePHY's system significantly reduces the upfront resource commitments for project developers. By providing access to a robust resource pool and innovative coordination mechanisms, developers can initiate infrastructure deployment with minimal initial resource lock-up, allowing them to focus resources on technology development and network expansion.

The platform implements a transparent and equitable network reward mechanism that ensures all participants benefit from the project's success. This system automatically distributes network contributions according to predetermined protocol parameters, creating a sustainable operational model that recognizes both early contributors and long-term participants while maintaining network stability.

Furthermore, the system actively encourages infrastructure deployment through carefully designed protocol incentives. These incentives are tied to key network performance metrics and deployment milestones, motivating developers to expand their networks efficiently while maintaining high service quality. This approach not only accelerates network growth but also ensures the long-term robustness of the infrastructure.

For Resource Contributors:

Contributors in the DePHY ecosystem benefit from a robust and secure network participation environment. The implementation of protocol automation ensures verifiable and guaranteed resource redistribution, minimizing operational risks and providing reliable network participation rewards. These protocol mechanisms are designed with sophisticated verification and enforcement systems that maintain the integrity of all network operations.

The system grants contributors prioritized access to network verification privileges, establishing a clear protocol hierarchy in resource distribution that prioritizes network maintenance. This protocol-level prioritization helps protect contributors' interests while maintaining sustainable network operations. The resource allocation mechanism is automated and transparent, allowing contributors to monitor their network participation status in real-time.

Furthermore, the platform safeguards contributors through comprehensive protocol protections and well-defined resource reallocation procedures. These mechanisms include cryptographic commitment requirements, automated verification protocols, and clear procedures for resource reallocation. Such protections ensure that contributors can confidently participate in the ecosystem while maintaining control over their network engagements.

3.5.7 Anti-Fraud Mechanisms

The system incorporates several anti-fraud features:

- Economic disincentives for fake transactions
- Restricted withdrawal permissions
- Automated revenue distribution preventing manipulation

This comprehensive risk management approach creates a sustainable ecosystem that aligns incentives across all participants while maintaining robust security measures.

4 Economic Model

DePHY's core infrastructure network is provided free of charge to encourage widespread adoption and create strong network effects. This foundation layer serves as an entry point for projects to build and grow within the ecosystem.

As projects mature and require advanced features, DePHY introduces tiered services including:

- Liquidity management solutions
- Verification and security services
- Advanced staking mechanisms
- Specialized subnet deployments

This freemium model creates natural path dependency: projects initially benefit from free infrastructure, then organically transition to premium services as they scale and require more sophisticated solutions.

The free core infrastructure attracts diverse projects, creating a robust ecosystem where advanced services become increasingly valuable as the network grows.

5 Implementation and Performance

DePHY Nodes serve as the critical infrastructure backbone of the network, enabling secure and decentralized communication between DePIN devices and the Solana blockchain. The node implementation provides essential functionality for the entire DePIN ecosystem through distributed verification, secure message routing, and real-time data processing capabilities.

5.1 Node Hardware Specifications

- Quad-core Cortex-A55 processor for efficient processing
- Mali-G52 GPU + 1TOPS NPU for advanced computing capabilities
- 2GB DDR4 RAM and 16GB storage
- Comprehensive connectivity through WiFi 5.8G+2.4G, Bluetooth 5.0, and Gigabit Ethernet

In addition to DePHY's custom hardware solution, the protocol fully supports integration with third-party hardware that includes dedicated security chips. These security-enhanced devices can seamlessly integrate with DePHY's complete protocol suite through:

- Trusted Platform Module (TPM) enabled devices for secure key storage and cryptographic operations
- Hardware Security Module (HSM) integration for enhanced protection of sensitive data

- Secure Element (SE) equipped devices that provide tamper-resistant security features

This flexibility in hardware implementation ensures that manufacturers can leverage existing security-enhanced platforms while maintaining full compatibility with DePHY's ecosystem services and security standards.

5.2 Performance and Scalability

DePHY Messaging Layer demonstrates exceptional performance capabilities in real-world deployments. The system consistently achieves throughput rates of up to 100,000 transactions per second (TPS) under optimal network conditions, while maintaining an average message confirmation time of approximately 400ms. This high-performance architecture enables the network to support millions of concurrent device connections, making it suitable for large-scale DePIN deployments.

The messaging layer's scalability is achieved through a sophisticated hierarchical message routing architecture. This system implements dynamic load balancing across nodes, coupled with parallel message processing capabilities. By distributing the processing load efficiently across the network, the system maintains consistent performance even during periods of high demand.

Performance optimization is accomplished through several key technical innovations. The system employs advanced message batching and compression techniques to maximize network efficiency. These are combined with carefully optimized consensus mechanisms that minimize overhead while maintaining security. Additionally, the implementation of specialized data structures enables rapid state transitions, further enhancing overall system performance.

The platform's horizontal scaling capabilities are particularly noteworthy. Through the implementation of message processing sharding across node clusters, the system can effectively distribute computational load. Geographic distribution of processing nodes ensures optimal latency for users worldwide, while adaptive capacity allocation dynamically adjusts resources based on network demand patterns.

To validate DePHY network's performance under high-load conditions, we conducted comprehensive stress testing. The results demonstrate that even under high TPS (Transactions Per Second) scenarios, the system maintains a low number of pending events, proving the efficiency of the network architecture.

TPS	Total Events	Pending Events
500	30,000	2-3
1,000	60,000	5-7
1,500	90,000	8-12
2,000	120,000	10-20
3,000	180,000	15-25
5,000	300,000	20-35
7,500	450,000	25-45
10,000	600,000	30-55

Figure 3: DePHY Network Performance Test Data

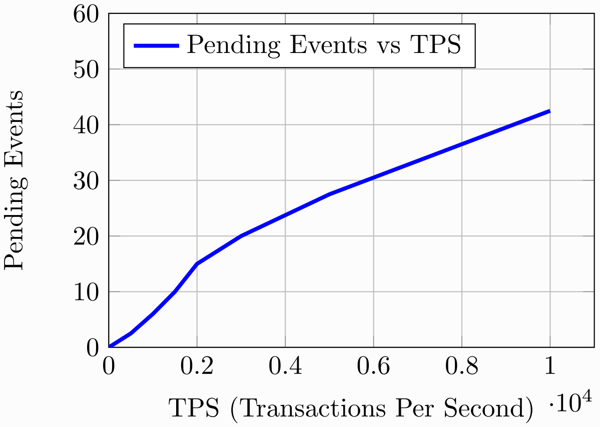


Figure 4: DePHY Network Performance: TPS vs Pending Events

The test data demonstrates DePHY network's exceptional load handling capabilities. Even under extremely high loads of 10,000 TPS, the number of pending events remains controlled within 55, proving that the system's efficient message processing mechanisms and optimized consensus algorithms can effectively handle large-scale concurrent requests.

5.3 Network Communication Latency Analysis

The communication latency in DePHY network is primarily influenced by ISP infrastructure and network quality conditions. The following analysis presents typical latency ranges across different deployment scenarios:

Deployment Scenario	Latency Range (ms)
Cloud-hosted DePIN project backend	10 - 100
Fixed broadband DePIN devices	10 - 200
Mobile 4G/5G DePIN devices	100 - 300

Table 1: Network Communication Latency by Deployment Scenario

The latency analysis reveals that cloud-hosted backends achieve the most consistent performance with latencies ranging from 10ms to 100ms, benefiting from optimized data center infrastructure and high-quality network connections. Fixed broadband deployments show slightly higher maximum latencies up to 200ms due to varying ISP quality and last-mile connectivity issues. Mobile deployments experience the highest latency ranges from 100ms to 300ms, reflecting the inherent characteristics of cellular networks including signal strength variations, network congestion, and tower distance factors.

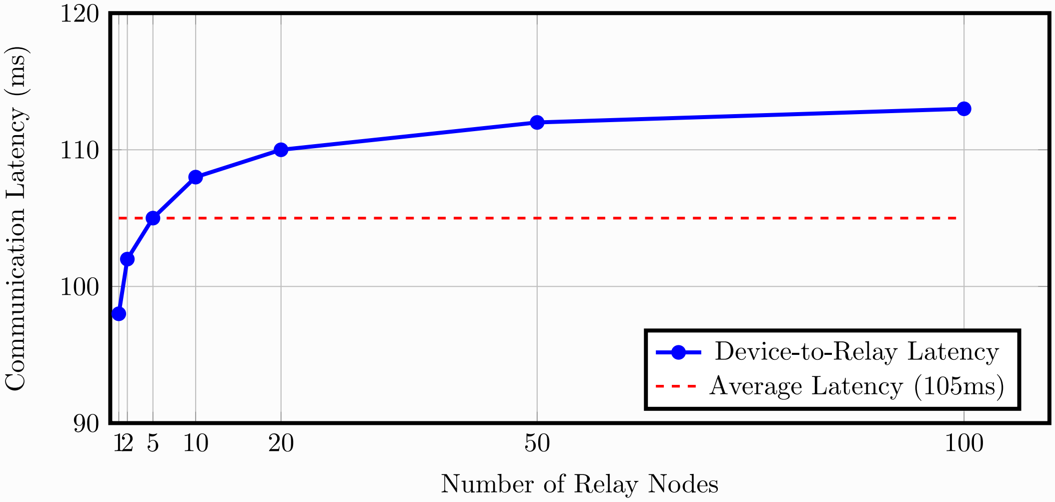


Figure 5: Impact of Relay Node Count on Communication Latency in DePHY Network

Due to the relatively fixed geographical locations of DePIN devices, the communication latency between devices and relay nodes demonstrates high stability. As shown in Figure 5, the latency primarily originates from internet access, with typical values stabilizing around 100ms and fluctuations within ±10ms. This stable latency characteristic provides a predictable performance foundation for the DePHY network, ensuring reliable real-time data transmission.

5.4 Node Operation Benefits

- Rewards for contributing to network growth and stability
- Potential multi-token mining opportunities as the ecosystem expands
- Essential role in the decentralized messaging infrastructure

The DePHY Node implementation ensures reliable, transparent operations while maintaining high security standards through its integration with the broader DePHY network architecture.

6 Conclusion

DePHY represents a groundbreaking advancement in DePIN infrastructure, introducing innovative solutions that address critical challenges in the ecosystem. Through its comprehensive architecture encompassing secure messaging layers, robust financial mechanisms, and scalable node operations, DePHY establishes a foundation for sustainable DePIN development.

The protocol's comprehensive innovations demonstrate significant achievements in multiple critical areas. Its sophisticated risk management system effectively protects all stakeholders while promoting network growth, ensuring the ecosystem's long-term sustainability. The high-performance messaging infrastructure, capable of handling high TPS with low latency confirmation times, sets new standards for network efficiency and reliability. Furthermore, the flexible hardware integration supporting both custom and third-party security-enhanced devices enables widespread adoption and compatibility.

DePHY's innovative liquidity layer design provides essential financial infrastructure that enables seamless value flow within the ecosystem. The protocol's sophisticated verification and proof mechanisms ensure the integrity of physical infrastructure deployments while maintaining decentralization. These critical components work in concert to create a robust and trustworthy environment that bridges the gap between physical infrastructure and decentralized finance.

The comprehensive verification framework, combined with automated proof systems, establishes a new standard for infrastructure validation in the DePIN space. This not only enhances security but also creates a transparent and verifiable record of infrastructure deployment and operation, crucial for the ecosystem's credibility and growth.

The economic model implemented by DePHY strikes an optimal balance between accessibility and sustainability. By combining free core infrastructure with premium services, the protocol creates a natural growth pathway for projects while ensuring long-term economic viability. This approach has proven effective in fostering ecosystem development while maintaining operational stability.

As the DePIN ecosystem continues to evolve, DePHY's architecture provides the essential foundation for future innovation and growth. By solving fundamental challenges in infrastructure deployment, security, and financial sustainability, DePHY paves the way for widespread adoption of decentralized physical infrastructure networks, positioning itself as a cornerstone of the next generation of decentralized systems.

References

[1] Mark C. Ballandies, Hongyang Wang, Andrew Chung Chee Law, Joshua C. Yang, Christophe Gösken, and Michael Andrew. A taxonomy for blockchain-based decentralized physical infrastructure networks (depin). 2023.

[2] Michael T. C. Chiu, Sachit Mahajan, Mark C. Ballandies, and Uroš V. Kalabić. Depin: A framework for token-incentivized participatory sensing. 2024.

[3] IBM and Eurotech. Mqtt v3.1 protocol specification.

[4] K. Ashton. That "internet of things" thing, 2009.

[5] Juan Benet. Ipfs - content addressed, versioned, p2p file system. 2014.

[6] J. R. Etheridge, M. Castro, and I. Stoica. Libp2p: A modular network stack for p2p systems. *USENIX Association Conference on Networked Systems Design and Implementation*, 14:1–15, 2017.

[7] Juan Benet. Interplanetary file system: A p2p file system for the next web. *Proceedings of the 24th International Conference on World Wide Web*, pages 1149–1160, 2015.

[8] Ian Foster and Carl Kesselman. *The Grid: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2 edition, 2004.

[9] Hang Yin, Shunfan Zhou, and Jun Jiang. Phala network: A secure decentralized cloud computing network based on polkadot. 2022.

[10] Arfaoui, Ghada, Gharout, Saïd, Traoré, and Jacques. Trusted execution environments: A look under the hood. In *2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, pages 259–266, 2014.

[11] Nostr nips: Nostr implementation possibilities.

[12] Ryan J. Kung. Rings: A peer-to-peer network for sovereign age, 2023.

[13] D. Karger I. Stoica, R. Morris. Chord: A scalable peer-to-peer lookup service for internet applications. `https://dl.acm.org/doi/10.1145/383059.383071`, 2001.

[14] Decentralized identifiers (dids). Accessed: 2023-02-05.

[15] Solana Team. Solana: A high-performance blockchain for decentralized applications, 2018.

[16] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. `https://dl.acm.org/doi/10.1145/74242.74243`, 1989.

[17] Understanding node consensus networks.