NEOVA PROTOCOL

Technical Whitepaper / Vision Document

Inter-Planetary Content Delivery (Inter-Planetary Content Delivery (IPCD))

A Paradigm Shift in Decentralized, Client-Driven Content Distribution

Authors: Neova Protocol

Date: September 28, 2024

Version: Draft 1.0

Abstract: In an era where digital infrastructure is paramount, the chasm between decentralized storage and high-performance content delivery remains a critical bottleneck to mass adoption. This paper introduces IPCD (Inter-Planetary Content Delivery), a proprietary protocol engineered by Neova to bridge this gap. IPCD transforms Neova's robust decentralized storage network into an intelligent, native Content Delivery Network (CDN) by shifting the paradigm of network routing from a centralized server-side model to a dynamic, client-driven one. By empowering clients to algorithmically benchmark and select the optimal data retrieval path in real-time, IPCD fundamentally enhances performance, fortifies network resilience, and actualizes the promise of true decentralization. This document elucidates the strategic context, architectural blueprint, and technical specifications of IPCD—a core innovation designed to position Neova as the definitive backbone of tomorrow's trustless internet.

Why This Matters

The world runs on the cloud. Every photo streamed, every document shared, every video watched depends on infrastructure that has quietly become the backbone of the global economy. By 2032, cloud and storage services will represent a market approaching **$840 billion**.

But today's cloud comes with a hidden cost: it's owned and controlled by a handful of giants. Their systems scale, but they also create single points of failure, expose users to censorship and exploitation, and keep true data ownership out of reach.

The internet of the future cannot be built on such a fragile foundation.

Where Decentralization Stands Today

Decentralized Physical Infrastructure Networks (DePIN) promise a safer, fairer, more resilient alternative. They already excel at storage: data can be split, encrypted, and distributed globally. But there's one critical gap that has held them back from competing with Web2: **fast, reliable delivery.**

In other words, getting data into the network is solved. Getting it *out* at high speed — to millions of people, anywhere in the world — is not.

This is the "last-mile problem."

Neova's Answer

Neova was designed from the ground up to close this gap. It's more than a protocol — it's a decentralized cloud ecosystem that blends three powerful elements:

- **Peer-to-Peer Infrastructure:** From enterprise servers to Raspberry Pi devices, anyone can contribute capacity and earn `$NEOV` rewards. The network scales itself.
- **IPFS at the Core:** Every file is secured by cryptographic hashing and content addressing, ensuring data integrity and efficiency.
- **Enterprise-Grade Security:** Identity, encryption, and key management are integrated from the start, giving users privacy and sovereignty without extra complexity.

On top of this foundation, Neova already powers products like **NeoDrive** (a decentralized storage alternative to Google Drive) and **NeoSign** (a secure signing solution). These tools show how Web3 can feel as simple as Web2 — but without compromise.

The Breakthrough: IPCD

The missing piece was delivery. That's where IPCD comes in.

Traditional CDNs work like traffic cops: a central authority decides which server gives you your data. This model is fast, but it's also a bottleneck — and by definition, centralized.

IPCD flips the script. Instead of a server deciding for you, **your device becomes its own intelligent routing agent.**

Here's the simple version:

1. You request a file. Neova's backend gives you a list of verified providers that host it.
2. Your device pings them all in real time — like checking which warehouse can ship fastest to your door.
3. It chooses the best route and connects directly. No middleman, no lag.

Why This Changes the Game

- **Performance that competes with Web2:** Videos stream instantly. Files open fast. Enterprises can rely on speed.
- **Resilience by design:** If one provider slows down, your client instantly reroutes to another. Outages stop being outages.
- **True decentralization:** Routing decisions happen at the edge, on the client side. No one can censor or intercept.
- **Value that compounds:** Storage alone is passive. With IPCD, Neova becomes a living, breathing delivery network. The utility — and thus the value — of the ecosystem and its token grows exponentially.

The Big Picture

With IPCD, Neova doesn't just store data. It delivers it — securely, privately, and at scale. This elevates Neova from "a decentralized storage solution" to a **complete decentralized cloud platform** ready for enterprise adoption and mass market use.

Part 2: RFC-Style Technical Specification

2.1. Abstract

This document provides the technical specification for IPCD (Inter-Planetary Content Delivery), a client-driven performance optimization protocol for the Neova network. IPCD leverages Neova's P2P provider network as a decentralized CDN fabric. It defines a protocol wherein a client, upon receiving a candidate set of provider nodes from a central metadata service, executes performance benchmarks (e.g., latency, throughput) to algorithmically determine the optimal data delivery path. This specification details the architecture, protocol flow, cryptographic models, data schemas, and integration with existing Neova components, notably the Go-based `Superviseur` service resident on each provider node. The protocol is designed to be incrementally implementable within the existing Neova ecosystem.

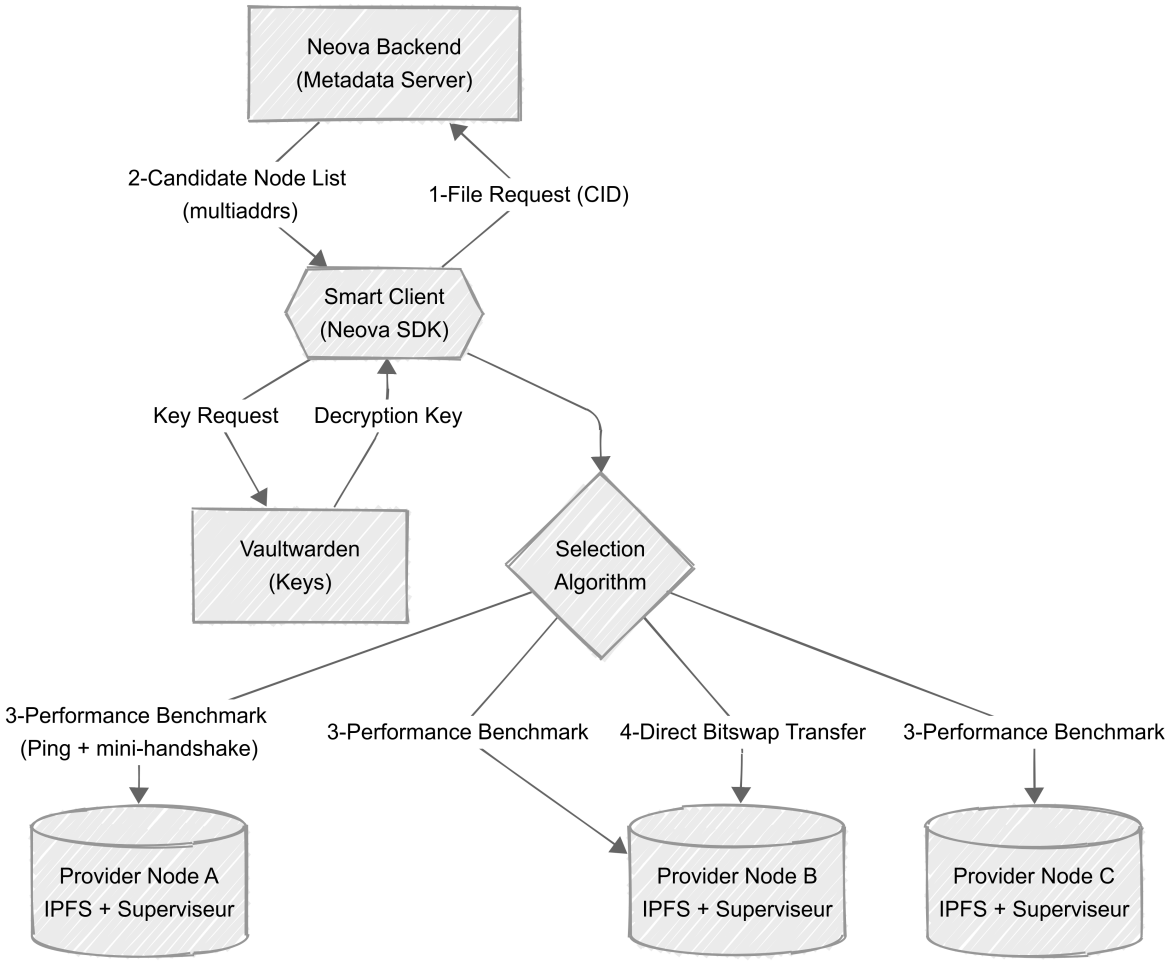
2.2. Architectural Framework & Components

IPCD integrates seamlessly into Neova's existing microservices architecture, orchestrating three primary actors:

- **Metadata Server (Neova Backend):** A core Neova service that maintains a real-time registry of provider nodes, their cryptographic identities, operational status, reputation scores, and a mapping of the Content Identifiers (CIDs) they host. In the IPCD protocol, its function is to serve a filtered, pre-optimized list of candidate nodes to the client.
- **Provider Node (Storage & Distribution Layer):** A P2P network participant running the Neova provider stack, which includes **IPFS Kubo**, **IPFS Cluster**, and the **`Superviseur`** Go service. Its role within IPCD is to store encrypted data blocks, respond to client-initiated performance probes, and serve content requests via IPFS's Bitswap protocol.
- **Smart Client (Intelligence Layer):** A software module (SDK) embedded within Neova's native applications (e.g., **NeoDrive**) and offered through its IaaS/STaaS API solutions. It is responsible for orchestrating the entire IPCD selection process: requesting the candidate list, executing the benchmark, applying the selection algorithm, and managing the resilient data transfer.

<Schema 1: IPCD High-Level Actor Architecture>

<A textual diagram illustrating the three main actors. A central "Neova Backend (Metadata Server)" is at the top. An arrow labeled "1. Content Request (CID)" points from the "Smart Client (Neova SDK)" on the left to the Backend. An arrow labeled "2. Returns Candidate Node List" points back from the Backend to the Smart Client. From the Smart Client, multiple arrows labeled "3. Performance Probes (e.g., Ping)" point to a set of three "Provider Nodes (IPFS + Superviseur)" at the bottom. A final arrow labeled "4. Direct Data Download from Optimal Node" points from the Smart Client to one of the Provider Nodes.>



2.3. Detailed Protocol & Data Flow

The end-to-end data retrieval sequence under the IPCD protocol is a multi-stage, orchestrated process designed for security and performance.

1. **Authentication & Key Retrieval:** The user authenticates via **Keycloak**. Concurrently, the Smart Client securely fetches the file's decryption key from a **Vaultwarden** instance, ensuring a zero-knowledge architecture from the perspective of the infrastructure.

2. **Candidate Set Acquisition:** The Smart Client issues a secure API call to the Neova Metadata Server (e.g., `GET /api/v1/content/{cid}/nodes`). The server returns a JSON object containing a list of `multiaddrs` for provider nodes known to host the requested content. This list is pre-filtered by the backend based on node reputation, historical uptime, and other metrics reported by each node's `Superviseur` service.
3. **Client-Side Benchmarking:** The Smart Client initiates parallel performance probes to the candidate nodes.
    - **Primary Mechanism:** The client leverages libp2p's standard ping protocol (`/ipfs/ping/1.0.0`) to measure round-trip time (RTT). The Neova ecosystem utilizes an optimized tool, `peeng`, for this purpose, designed for efficient, concurrent probing of IPFS peers.
    - **Advanced Mechanism:** For more sophisticated scoring, the client may initiate a "mini-handshake" by requesting a single, small data block to derive a combined metric of latency and initial throughput.
4. **Optimal Node Selection & Load Balancing Strategy:** The client applies a configurable scoring algorithm to rank the nodes.
    - **Latency-First:** Prioritizes the lowest RTT, optimal for small files and interactive applications. Score = 1/RTT.
    - **Hybrid Scoring:** A weighted function balancing latency and throughput for general-purpose use.
    - The node with the highest score is selected as the primary source.
5. **Resilient Data Transfer:** The Smart Client initiates a direct P2P connection to the chosen provider node(s) to fetch the encrypted data blocks via the IPFS **Bitswap** protocol. The process incorporates several resilience mechanisms:
    - **Automatic Fallback:** If the primary node becomes unresponsive, the client seamlessly retries with the next-best node from the ranked list.
    - **Adaptive Switching:** The SDK continuously monitors transfer performance. If conditions degrade, it can migrate the session to a better-performing node mid-transfer.
    - **Multi-Source Fetching:** For large files, the client can segment the download across the top 2-3 performing nodes simultaneously, maximizing bandwidth utilization.
6. **Client-Side Decryption & Verification:** Upon successful download, the Smart Client performs two final actions:

- **Integrity Verification:** The client cryptographically verifies the integrity of the received (encrypted) data by hashing it and comparing the result to the requested CID. This is an intrinsic security guarantee of IPFS.
- **Decryption:** The client uses the key retrieved from Vault to decrypt the data locally in memory, making the plaintext file available to the user.

<Schema 2: IPCD Detailed Sequence Diagram>

```
<A sequence diagram showing interactions between the "Client," "Neova Backend,"
"Vault," and two "Provider Nodes (A, B)."
1. Client sends a Login request to Neova Backend, receives a JWT.
2. Client requests a File from Backend, receives its CID.
3. Client requests the File Key from Vault (authorized via Backend), receives the
decryption Key.
4. Client requests Nodes for the CID from Backend, receives a list containing Node A
and Node B.
5. Client sends parallel Ping requests to both Node A and Node B.
6. Node A and Node B respond with Pong messages containing their respective RTTs.
7. Client internally processes the RTTs and selects Node A as optimal.
8. Client sends a "Get Encrypted Blocks" request directly to Node A.
9. Node A returns the encrypted blocks.
10. Client performs "Local Decryption" and presents the file to the user.>
```

2.4. Cryptographic & Security Architecture

IPCD's security model is multi-layered, leveraging the cryptographic primitives of the underlying Neova and IPFS architecture.

- **Data Integrity:** Content-addressing via IPFS CIDs provides absolute data integrity. Any alteration of the data in transit would result in a different CID, causing the client-side verification to fail.
- **Data Confidentiality:** End-to-end encryption ensures that all data stored on and traversing the provider network is opaque. Decryption keys are managed by an enterprise-grade secrets management system (**Vaultwarden**) and are accessible only to the authenticated user, enforcing a zero-knowledge policy for the infrastructure.
- **Provider Authentication & Sybil Resistance:** Each provider node possesses a cryptographic identity tied to its IPFS Cluster private key. This identity is used to sign a registration payload containing its EVM address, proving ownership to the Neova backend. This, combined with Neova's economic model of rewards and **slashing**,

creates a strong disincentive for malicious behavior (e.g., Sybil attacks) by enforcing financial penalties for non-compliance.

- **Secure Transport:** All P2P communication is conducted over secure channels established using protocols like Noise or TLS 1.3, as provided by the libp2p stack, protecting against eavesdropping and tampering.

2.5. Conclusion: A New Paradigm for Content Delivery

IPCD is more than an optimization; it is a foundational technology that completes Neova's vision for a fully decentralized cloud. By architecting an intelligent, client-driven CDN layer, Neova solves the critical "last-mile" performance problem that has hindered the widespread adoption of decentralized infrastructure. This innovation not only delivers a superior user experience but also enhances the economic value and technical defensibility of the entire Neova ecosystem. IPCD represents a generalizable paradigm for decentralized content delivery, positioning Neova at the forefront of the next generation of internet infrastructure.

Glossary

Concepts

CDN – **Content Delivery Network**: Distributed network of servers that deliver content with low latency; typically centralized in Web2.

DePIN – **Decentralized Physical Infrastructure Network**: Networks that incentivize deployment of real-world infrastructure (storage, compute, bandwidth).

Metrics

RTT – **Round-Trip Time**: Latency metric measuring time for a ping to go and back.

Neova

IPCD – **Inter-Planetary Content Delivery**: Client-driven content delivery protocol in Neova that benchmarks provider nodes and selects optimal paths. 1, 2, 2, 2, 2, 4, 4, 4, 4, 5, 5, 5, 5, 5, 5, 6, 6, 8, 8, 9

Neova – **Neova Protocol**: Decentralized cloud ecosystem combining P2P providers, IPFS, and security primitives.

Superviseur – **Neova Superviseur service**: Go service running on provider nodes for monitoring, reporting, and control.

Protocols

Bitswap – **IPFS Bitswap protocol**: Block exchange protocol used by IPFS for content transfer.

CID – **Content Identifier**: Cryptographic hash identifying content in IPFS; used for integrity checks.

IPFS – **InterPlanetary File System**: Content-addressed, peer-to-peer storage network using CIDs and Bitswap.

libp2p – **libp2p networking stack**: Modular P2P networking library providing transports, security (Noise/TLS), and ping.

Security

EVM – **Ethereum Virtual Machine**: Runtime environment for smart contracts; provider identities may link to EVM addresses.

Keycloak – **Keycloak**: Open-source identity and access management used for authentication.

Vaultwarden – **Vaultwarden**: Self-hosted secrets manager providing key storage; used to retrieve decryption keys.

Tools

peeng – **peeng (libp2p ping tool)**: Optimized tool to measure RTT to IPFS/libp2p peers concurrently.