

KeyNet: A Key-Bound Decentralized Internet Protocol

Nadir Mirzaliev

January 07, 2026

This document presents a conceptual whitepaper describing a decentralized Internet based on cryptographic IPv6 addressing, backbone nodes, and blockchain-based economics. The information is based on established concepts of IPv6, decentralized networking, and cryptocurrency protocols.

1. Introduction

The modern Internet critically depends on centralized access providers, backbone operators, and the hierarchical domain name system. Such architecture creates control points, censorship potential, vulnerabilities, and transforms connectivity into a paid service monopolized by a limited number of companies.

This document describes the architecture of a new decentralized Internet (hereinafter referred to as the Network), capable of operating without traditional Internet providers in the literal sense. The Network is built upon:

- Cryptographically key-bound IPv6 addressing.
- Backbone nodes acting as routers, DNS servers, and validators.
- Client nodes based on OpenWrt with a user-friendly interface.
- A blockchain with native currency and smart contracts governing addresses and domains.
- Free data traffic (no charge for packet transmission).

The Network's goal is to create a resilient, openly governed, and cryptographically secured infrastructure that can gradually replace or complement the existing Internet while ensuring decentralization, censorship resistance, and economic independence for its participants.

2. Objectives and Motivation

2.1 Problems of Current Infrastructure

The traditional Internet exhibits several systemic weaknesses:

- Dependence on providers controlling both physical and logical infrastructure.
- A centralized domain name system (DNS) managed by hierarchical organizations.
- The possibility of blocking, filtering, and censorship at the provider or national regulator level.
- Concentration of economic benefit among a narrow group of operators.
- Even decentralized applications (Web3, blockchains) still rely on centralized network layers for accessibility.

2.2 Vision of a Decentralized Internet

The proposed Network aims to:

- Eliminate dependence on traditional providers by distributing routing functions among independent participants.
- Use cryptographically linked addressing so that address ownership is proven via private key possession.
- Make data transmission free; shift the economic model toward blockchain, smart contracts, and ownership of address resources rather than traffic volumes.
- Implement decentralized DNS governed by smart contracts and independent of any hierarchical authorities.
- Enable gradual migration by supporting operation over existing Internet infrastructure (via VPN), Wi-Fi, fiber, or any available physical links.

3. Network Architecture

3.1 Layer Overview

The Network logically consists of two node classes:

Backbone Nodes (Magistral Nodes):

- High-performance servers.
- Perform routing, DNS, blockchain validation, and block storage.
- Participate in consensus when deciding whether to restrict domains or addresses distributing illegal content.

Client Nodes:

- Routers based on OpenWrt.
- Connect to one or more backbone nodes.
- Obtain IPv6 addresses and manage wallets and domains through a web interface.

Connectivity is provided over:

- VPN tunnels through the existing Internet (e.g., using protocols similar to WireGuard).
- Direct Wi-Fi links.
- Optical or any other physical channels.

3.2 IPv6 as the Base Layer

IPv6 provides a 128-bit address space represented as eight groups of 16 bits (hexets) separated by colons, for example:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

The address space is vast enough to:

- Derive addresses from cryptographic identifiers.
- Allocate large subnets to backbone nodes.

- Eliminate the need for centralized address assignment authorities.

4. Cryptographic Addressing

4.1 Wallet and Address Generation

Identification is based on public-key cryptography (e.g., Ed25519 or similar). Each node generates:

- A private key sk
- A public key pk

A fixed-length hash of the public key is then used as the foundation of an IPv6 address, similar in concept to Cryptographically Generated Addresses (CGA).

Example (simplified):

- Wallet hash: 20010db885a3000000008a2e03707334
- IPv6 format: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Thus, each network address is directly bound to a cryptographic key, and possession of the private key grants control over the address.

4.2 Wallet and Address Types

Two fundamental wallet types exist in the Network:

Backbone Wallets:

- Must represent a valid IPv6 address with a specific number of trailing zero hextets.
- Minimum requirement: a fixed count of zero hextets (e.g., 2) at the end.
- A backbone owner may voluntarily generate an address with more trailing zeros to manage a larger network segment.

Client Wallets:

- Not required to follow IPv6 format.
- May use arbitrary or human-readable identifiers that manage assets and interact with smart contracts.

A backbone address that satisfies the zero-hextet requirement defines the size of the address pool under its control. The more trailing zeros, the larger the managed subnet — more computational effort is needed to generate it, but the broader the resulting authority within the Network.

5. Backbone Nodes

5.1 Role and Functions

Backbone nodes perform these key roles:

- Routing traffic between clients and other backbones.
- Announcing and maintaining their IPv6 address pools.
- Maintaining and validating the blockchain (full node operation).

- Processing transactions and smart contracts.
- Hosting and distributing DNS records of domains registered on the blockchain.

Backbone nodes interconnect to form a unified topology. Routing may adopt concepts from BGP or other inter-domain routing protocols adapted to cryptographic addressing.

5.2 Address Pools

A backbone manages an address pool (e.g., a /64 subnet) determined by its IPv6 address and trailing-zero requirement. This pool is used to issue client addresses:

- Clients receive dynamic IPv6 addresses from the backbone's pool.
- Static addresses can be purchased via smart contracts.

Minimum zero-hextet requirements ensure sufficient segment ownership. Voluntarily generating more zeros enlarges available address space, symbolizing higher computational investment and incentive alignment.

5.3 Backbone Connectivity

Backbones may interconnect via:

- Direct physical links (fiber, private lines).
- VPN tunnels over the existing Internet.
- Any reliable transport medium.

Routing between backbones ensures packet delivery across all IPv6 segments managed by various nodes. The design borrows best practices from BGP/IS-IS while adapting them to cryptographic address ownership.

6. Client Nodes

6.1 OpenWrt as a Platform

Client nodes operate as OpenWrt-based routers:

- Inexpensive and widely available devices.
- Flexible systems allowing custom packages and daemons.
- Built-in web UI (LuCI) for configuration.

Installed software includes:

- The Network daemon (routing, tunneling, backbone interaction).
- A lightweight blockchain client.
- A DNS resolver communicating with backbone nodes.
- A web interface for wallet and domain management.

6.2 Client Lifecycle

Typical flow:

- The user installs OpenWrt firmware with Network support or an add-on package.
- A client wallet (arbitrary identifier) is generated via the web UI.
- The user selects a backbone to connect to (by address, list, or reputation).
- A secure tunnel is established (conceptually similar to WireGuard).
- The backbone assigns a dynamic IPv6 address from its pool.
- The client can then interact with the blockchain, register domains, or purchase static addresses.

6.3 Extended Client Capabilities

A client node may also:

- Act as a router for a local LAN, assigning internal addresses.
- Cache DNS records requested from backbones.
- Interact with smart contracts for resource management (addresses, domains).
- Optionally route traffic for others (with proper configuration and incentives).

7. Decentralized DNS

7.1 Domain Name Model

The domain system of the Network is implemented directly on-chain. Domain names:

- Are entries in smart contracts.
- Belong to wallet holders.
- Can be transferred, sold, or delegated.

This model parallels existing blockchain-based DNS systems (e.g., ENS, TON DNS) but is integrated at the network layer.

7.2 Domain Registration

A domain is registered via a smart contract:

- The owner sends a transaction specifying the desired name.
- The contract checks for uniqueness.
- Upon success, ownership is recorded for a fixed or indefinite period.
- Domain-related data (IPv6 mappings and others) are stored on-chain.

7.3 Managing DNS Records

Domain owners can:

- Add or modify record types such as A/AAAA, SRV, TXT, etc.
- Delegate subdomains to other wallets.
- Update records through transactions signed with their private key.

Backbone nodes:

- Synchronize DNS state from the blockchain.
- Respond to client DNS queries using the blockchain as the source of truth.
- Cache frequently used entries to improve response time.

No micropayments are charged for DNS queries; Network economics rely on other mechanisms (see the tokenomics section).

8. Blockchain and Smart Contracts

8.1 Purpose of the Blockchain

The blockchain serves to:

- Account for native currency balances.
- Deploy smart contracts managing addresses and domains.
- Record static IPv6–wallet bindings.
- Confirm backbone node actions (block validation, consensus participation).

It acts as the trust foundation—only critical operations (domain registration, ownership changes, address binding) are permanently recorded.

8.2 Native Currency

The Network includes a native token (Network Coin) that is used for:

- Rewarding infrastructure participants (mainly backbones).
- Paying for smart-contract operations (domain registration, static address acquisition).
- Staking-based incentives and long-term participation.

Traffic transmission itself remains free; no per-packet fees exist.

8.3 Smart Contracts

Smart contracts implement:

- Domain registration.
- Purchase and assignment of static IPv6 addresses.
- Delegation of resources.
- Potential DAO-based governance mechanisms.

Contract environments may be EVM-compatible to simplify development and auditing.

9. Tokenomics and Incentives

9.1 Economic Principles

The Network’s economy is based on these concepts:

- Primary value arises from infrastructure support (backbones, blockchain storage).

- Ownership of scarce assets (readable domains, “beautiful” static addresses).
- Data traffic is free and not monetized.
- Rewards are distributed via blockchain mechanisms (consensus, staking, operational rewards).

A detailed revenue distribution model is intentionally left open for future refinement via community and DAO governance.

9.2 Incentives for Backbones

Backbone nodes earn:

- Rewards for consensus participation and block validation.
- Economic returns from owning large address segments and offering related services (selling static addresses, domains, etc.).
- Reputation for reliability, attracting more clients.

Generating addresses with a higher count of trailing zero hexets increases a backbone’s significance, representing both computational effort and expanded responsibility.

9.3 Incentives for Clients

Clients benefit by:

- Accessing a decentralized network independent of traditional providers.
- Owning domains and static addresses as digital assets.
- Hosting resilient services reachable exclusively via the decentralized layer.

10. Security

10.1 Cryptographic Integrity

Because each IPv6 address and wallet is bound to a cryptographic key, a node proves ownership by:

- Signing messages with its private key.
- Preventing address spoofing without key possession.

10.2 Sybil and Abuse Protection

Sybil attacks (mass identity creation) are mitigated through:

- The computational cost of generating valid backbone addresses with required zero hexets.
- The need to invest in hardware and connectivity to maintain large segments.
- Consensus and staking mechanisms that demand economic stakes, limiting scalability for an attacker.

For clients, Sybil risk is less critical since economic value ties to actual resources (addresses, domains, tokens).

10.3 DDoS and Fault Tolerance

Decentralized topology and lack of single entry points improve DDoS resilience:

- Overloading one backbone does not disrupt the Network; clients can migrate.
- Distributed routing bypasses congested paths.
- Additional filtering and rate limiting can operate at backbone level.

11. Scalability

11.1 Address Space

IPv6's vast address space allows:

- Large pool allocation to backbones.
- Cryptographic address binding without exhaustion risk.
- Tiered segmentation via zero-hextet requirements.

Backbones managing larger segments (more zeros) voluntarily assume higher responsibility and influence.

11.2 Blockchain Layer

To ensure blockchain scalability:

- Layer-2, sharding, and consensus optimizations may be introduced.
- The blockchain records only critical actions (domain/address registrations and economic transactions), excluding user traffic data.

12. Privacy

Cryptographic addressing does not inherently guarantee anonymity but:

- Removes linkage between addresses and real-world identities.
- Reduces dependence on centralized registries.
- Additional privacy can be achieved via:
 - Encrypted VPN tunnels.
 - Routing approaches inspired by existing anonymous or privacy-focused networks.

13. Practical Deployment

13.1 Pilot Stage

Initial phase steps:

- Launch several independent backbone nodes.
- Develop and distribute an OpenWrt package containing the Network daemon, web UI, and light blockchain client.

- Early adopters join via VPN, testing essential functions.

13.2 Expansion

As stability improves:

- The number of backbones grows organically.
- Public firmware releases enable consumer devices.
- Services (websites, apps) emerge, accessible only through the decentralized layer.

14. Conclusion

This Network seeks to rebuild the Internet's foundations on three core principles:

- Cryptographic addressing: each address is key-bound, eliminating centralized allocation.
- Decentralized routing and DNS: backbones operate independently, domains are smart-contract-governed.
- Traffic-free economy: value centers on address/domain ownership and infrastructure participation, not bandwidth billing.

A minimum zero-hextet requirement defines foundational backbone structure, while voluntarily generating additional zeros grants participants stewardship over larger segments—enhancing responsibility and influence.

This whitepaper outlines the Network's architecture and principles while leaving consensus mechanics, tokenomics, and governance open for community-driven evolution through DAO-like frameworks and future protocol iterations.