KeyNet: A Key-Bound Decentralized Internet Protocol

Nadir Mirzaliev

07.01.2026

Далее представлен концептуальный whitepaper децентрализованного интернета на основе криптографической IPv6-адресации, магистральных узлов и блокчейн-экономики. Информация основана на общепринятых подходах к IPv6, децентрализованным сетям и криптовалютным протоколам.

1. Введение

Современный Интернет критически зависит от централизованных провайдеров доступа, операторов магистральных сетей и иерархической системы доменных имён. Такая архитектура создаёт точки контроля, цензуры и уязвимости, а также превращает доступ к сети в платную услугу, монополизированную ограниченным числом компаний.

Этот документ описывает архитектуру нового децентрализованного интернета (далее — Сеть), способного работать без классических провайдеров в прямом смысле слова. Основой Сети является:

- Криптографически привязанная к ключам IPv6-адресация.
- Магистральные (backbone) узлы, выступающие маршрутизаторами, DNS и валидаторами.
- Клиентские узлы на базе OpenWrt с удобным пользовательским интерфейсом.
- Блокчейн с нативной валютой и смарт-контрактами для управления адресами и доменными именами.
- Бесплатный трафик данных (отсутствие платы за передачу пакетов).

Цель Сети — создать устойчивую, открыто управляемую и криптографически защищённую инфраструктуру, которая может постепенно заместить или дополнить существующий Интернет, обеспечивая при этом децентрализацию, цензуроустойчивость и экономическую независимость участников.

2. Цели и мотивация

2.1 Проблемы существующей инфраструктуры

Традиционный Интернет обладает рядом системных ограничений:

- Зависимость от провайдеров, контролирующих физическую и логическую инфраструктуру.

- Централизованная система доменных имён (DNS), управляемая иерархией организаций.
- Возможность блокировок, фильтрации и цензуры на уровне провайдеров и национальных регуляторов.
- Концентрация экономической выгоды у ограниченного числа операторов.
- Даже при наличии децентрализованных приложений (Web3, блокчейны) их доступность всё ещё опирается на централизованный сетевой слой.

2.2 Визия децентрализованного интернета

Предлагаемая Сеть ставит перед собой следующие цели:

- Убрать зависимость от классических провайдеров за счёт распределения функций маршрутизации между независимыми участниками.
- Использовать криптографически привязанную адресацию, при которой владение адресом подтверждается приватным ключом.
- Сделать передачу данных бесплатной, а экономику сети строить вокруг блокчейна, смарт-контрактов и владения адресными ресурсами, а не объёмом трафика.
- Реализовать децентрализованный DNS, управляемый смарт-контрактами и не зависящий от иерархических органов.
- Обеспечить плавную миграцию: Сеть должна уметь работать поверх существующего Интернета (через VPN), Wi-Fi, оптику и любые каналы связи.

3. Архитектура сети

3.1 Обзор уровней

Сеть логически делится на два основных класса узлов:

Магистральные узлы (backbone / magistral nodes):

- Высокопроизводительные сервера.
- Выполняют маршрутизацию, функции DNS, валидацию блоков и хранение блокчейна.
- Принимают консенсусное решение о блокировке доменов и/или адресов в случае распространения противозаконной информации

Клиентские узлы:

- Роутеры на базе OpenWrt.
- Подключаются к одной или нескольким магистралям.
- Получают IPv6-адреса, управляют кошельками и доменами через web-интерфейс.

Связность обеспечивается поверх:

- VPN-туннелей через существующий Интернет (например, на базе протоколов, аналогичных WireGuard).
- Прямых Wi-Fi-соединений.
- Оптических линий и других физических каналов.

3.2 IPv6 как базовый слой

IPv6 предоставляет 128-битное адресное пространство, представляемое в виде восьми блоков по 16 бит (хекслеты), разделённых двоеточиями.

Пример:

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

Это пространство достаточно велико, чтобы:

- Назначать адреса на основе криптографических идентификаторов.
- Выделять крупные подсети магистральным узлам.
- Исключить необходимость в централизованной выдаче адресов.

4. Криптографическая адресация

4.1 Генерация кошельков и адресов

В основе идентификации лежат криптографические пары ключей (например, Ed25519 или аналог). Для узла генерируется:

- Приватный ключ sk
- Публичный ключ pk

Из публичного ключа вычисляется хеш фиксированной длины, который затем используется в качестве основы IPv6-адреса. Аналогичные идеи применялись в концепциях криптографически генерируемых IPv6-адресов (CGA).

Пример (упрощённый):

- Хеш кошелька: 20010db885a3000000008a2e03707334
- IPv6-формат: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Таким образом, каждый сетевой адрес напрямую привязан к криптографическому ключу, а владение приватным ключом означает контроль над данным адресом.

4.2 Типы кошельков и адресов

В Сети существует два базовых типа кошельков:

Магистральные кошельки:

- Должны представлять собой корректный IPv6-адрес с определённым количеством нулевых хекслетов в конце.

- Минимальное требование: фиксированное количество нулевых хекслетов (например, 2) в суффиксе адреса.
- Владелец магистрали может добровольно сгенерировать адрес с большим числом нулевых хекслетов, чтобы управлять более крупным сегментом сети.

Клиентские кошельки:

- Не обязаны иметь формат IPv6.
- Могут быть произвольными строками/форматами (в т.ч. более удобочитаемыми), которые используются для владения активами и взаимодействия со смарт-контрактами.

Магистральный адрес, удовлетворяющий требуемому числу нулевых хекслетов, определяет размер адресного пространства (пула), которым управляет магистраль. При этом:

- Минимальное число нулевых хекслетов определяет минимальный размер сегмента.
- Добровольное увеличение числа нулевых хекслетов создаёт более крупный сегмент, требующий больше усилий на генерацию, но дающий владельцу контроль над большим адресным пространством.

5. Магистральные узлы

5.1 Роль и функции

Магистральные узлы — ключевые участники Сети, выполняющие следующие функции:

- Маршрутизация трафика между клиентами и другими магистралями.
- Объявление и обслуживание своего адресного пула IPv6.
- Поддержание и валидация блокчейна (полный узел).
- Обработка транзакций и смарт-контрактов.
- Хранение и раздача DNS-записей доменов, зарегистрированных в блокчейне.

Магистральные узлы соединяются друг с другом, формируя связанную топологию. Для маршрутизации могут использоваться адаптированные идеи из BGP или иных протоколов, применяемых в межсетевой маршрутизации.

5.2 Адресные пулы

Магистраль отвечает за некоторый пул адресов (например, подсеть /64), который определяется её собственным IPv6-адресом и требуемым числом нулевых хекслетов в суффиксе. Этот пул используется для выдачи адресов клиентам:

- Клиент при подключении получает динамический IPv6-адрес из пула магистрали.
- Статические адреса могут быть «выкуплены» через смарт-контракт.

Минимальное требование по количеству нулевых хекслетов гарантирует, что магистраль владеет достаточно крупным участком адресного пространства. Добровольное увеличение числа нулей усложняет генерацию, но даёт расширенное пространство под клиентские адреса.

5.3 Связность магистралей

Магистрали могут соединяться произвольным образом:

- Через прямые каналы (оптика, приватные каналы).
- Через VPN-туннели поверх существующего Интернета.
- Через любые надёжные транспортные каналы.

Межмагистральная маршрутизация обеспечивает доставку пакетов между любыми сегментами IPv6-адресов, обслуживаемыми различными магистральными узлами. Принципы построения таблиц маршрутизации могут перенимать лучшие практики из BGP/IS-IS, адаптируя их к криптографической модели адресов.

6. Клиентские узлы

6.1 OpenWrt как платформа

Клиентами Сети выступают маршрутизаторы на базе OpenWrt:

- Малозатратные и широкодоступные устройства.
- Гибкая система, позволяющая устанавливать собственные пакеты и демоны.
- Наличие web-интерфейса (LuCI) для управления.

На маршрутизатор устанавливается специализированное ПО, включающее:

- Демон сети (маршрутизация, туннели, взаимодействие с магистралью).
- Клиент блокчейна (облегчённый).
- DNS-резолвер, работающий с магистралью.
- Web-интерфейс для управления кошельками и доменами.

6.2 Жизненный цикл клиента

Типичный сценарий:

- Пользователь устанавливает прошивку OpenWrt с поддержкой Сети или добавляет соответствующий пакет.
- В web-интерфейсе генерируется кошелёк клиента (любой формат идентификатора).

- Пользователь выбирает магистраль, к которой хочет подключиться (по списку, адресу или репутации).
- Устанавливается защищённый туннель (например, на основе идей, аналогичных WireGuard).
- Магистраль выдаёт клиенту динамический IPv6-адрес из своего пула.
- Клиент может взаимодействовать с блокчейном, регистрировать домены, покупать статические адреса.

6.3 Расширенный функционал клиента

Помимо базовых функций, клиентский узел может:

- Выступать маршрутизатором для локальной сети (LAN), раздавая адреса внутренним устройствам.
- Кэшировать DNS-записи, запрашиваемые у магистралей.
- Взаимодействовать со смарт-контрактами для управления собственными ресурсами (адресами, доменами).
- При желании участвовать в маршрутизации трафика других клиентов (при соответствующих настройках и стимуляции).

7. Децентрализованный DNS

7.1 Модель доменных имён

Роль доменной системы в Сети выполняет блокчейн. Доменные имена:

- Являются записями в смарт-контрактах.
- Принадлежат кошелькам владельцев.
- Могут быть переданы, проданы или делегированы другим кошелькам.

Это концептуально схоже с существующими системами доменов на блокчейне (ENS, TON DNS и другие), но интегрировано непосредственно на уровне сетевой инфраструктуры.

7.2 Регистрация домена

Регистрация домена осуществляется смарт-контрактом:

- Владелец кошелька отправляет транзакцию с желаемым доменным именем.
- Контракт проверяет уникальность имени.
- При успешной проверке домен закрепляется за кошельком владельца до выбранного срока (или бессрочно, в зависимости от протокола).
- Информация о домене (включая указание на IPv6-адреса и другие записи) хранится в блокчейне.

7.3 Управление DNS-записями

Владелец домена может:

- Добавлять и изменять записи типа A/AAAA (для IPv6 — AAAA), SRV, TXT и другие.
- Делегировать поддомены другим кошелькам.
- Изменять записи через транзакции, подписанные приватным ключом владельца домена.

Магистрали:

- Синхронизируют DNS-состояние через блокчейн.
- Отвечают на DNS-запросы клиентов, используя данные блокчейна как источник истины.
- Кэшируют наиболее востребованные записи для ускорения ответа.

При этом микроплатежи за отдельные DNS-запросы отсутствуют: запросы DNS в рамках Сети бесплатны. Экономическая модель опирается на другие виды активности (см. раздел о токеномике), а не на тарификацию резолвинга.

8. Блокчейн и смарт-контракты

8.1 Назначение блокчейна

Блокчейн в Сети служит для:

- Учёта владения нативной валютой.
- Реализации смарт-контрактов для управления адресами и доменами.
- Фиксации статических привязок IPv6-адресов к кошелькам.
- Подтверждения действий магистральных узлов (валидация блоков, участие в консенсусе).

Блокчейн является ядром доверия: все критические операции (регистрация доменов, покупка статических адресов, изменение владельцев ресурсов) фиксируются в неизменяемой распределённой книге.

8.2 Нативная валюта

В Сети существует нативный токен (условно — Network Coin), который используется для:

- Вознаграждения участников, поддерживающих инфраструктуру (прежде всего магистралей).
- Оплаты операций смарт-контрактов (регистрация доменов, покупка статического адреса и т.п.).
- Стимулирования долгосрочного участия через механизмы стейкинга или аналогичные.

При этом перенос данных (сетевой трафик) остаётся бесплатным; никакие комиссии за передачу пакетов не взимаются.

8.3 Смарт-контракты

Смарт-контракты реализуют:

- Регистрацию доменных имён.
- Покупку и закрепление статических IPv6-адресов.
- Управление делегированием ресурсов.
- Возможные DAO-механизмы управления протоколом в будущем.

Контракты могут быть совместимы с существующими экосистемами (например, EVM-подобными), что упрощает разработку и аудит.

9. Токеномика и стимулирование

9.1 Принципы экономической модели

Экономика Сети строится вокруг следующих принципов:

Основная ценность создаётся за счёт:

- Поддержания инфраструктуры (магистрали, хранение блокчейна).
- Владения дефицитными ресурсами (читаемые домены, статические «красивые» адреса).
- Трафик данных бесплатен, не является источником платежей.
- Вознаграждения распределяются через блокчейн-механизмы (консенсус, стейкинг, вознаграждения за обслуживание).

Чёткая и детализированная модель распределения комиссий на данном этапе умышленно не фиксируется в спецификации: это оставляет пространство для дальнейшего развития и обсуждения в сообществе и DAO.

9.2 Стимулы для магистралей

Магистральный узел получает:

- Вознаграждения за участие в консенсусе и генерацию/валидацию блоков.
- Возможность экономической монетизации инфраструктуры за счёт владения крупным адресным сегментом и связанных с ним сервисов (продажа статических адресов, доменов и т.п. через смарт-контракты).
- Репутацию надёжного участника сети, что привлекает клиентов.

Факт добровольной генерации адреса с большим числом нулевых хекслетов повышает значимость магистрали, поскольку она берёт на себя управление более крупным сегментом сети.

9.3 Стимулы для клиентов

Клиентские узлы получают:

- Доступ к децентрализованному интернету без зависимости от классических провайдеров (на уровне логики доступа).

- Возможность владеть доменами и статическими адресами как цифровыми активами.
- Возможность строить сверхустойчивые сервисы, доступные через децентрализованную инфраструктуру.

10. Безопасность

10.1 Криптографическая защита

Поскольку IPv6-адрес и кошелёк привязаны к криптографическому ключу, узел доказывает владение:

- Подписывая сообщения своим приватным ключом.
- Обеспечивая невозможность подмены адреса без знания ключа.

10.2 Sybil и злоупотребления

Проблема Sybil-атак (создание множества поддельных идентичностей) частично решается через:

- Стоимость генерации магистрального адреса с требуемым количеством нулевых хекслетов.
- Необходимость инвестировать ресурсы (в вычисления и инфраструктуру), чтобы поддерживать крупный сегмент сети.
- Механизмы консенсуса и возможного стейкинга, требующие экономических ставок, которые сложно масштабировать злоумышленнику.

Для клиентских узлов Sybil менее критичен, но экономическая значимость привязана к владению реальными ценностями (адреса, домены, токены).

10.3 DDoS и отказоустойчивость

Децентрализованная топология магистралей и отсутствие единой точки входа повышают устойчивость к DDoS.

- Перегрузка конкретного магистрального узла не приводит к остановке сети: клиенты могут переподключиться к другим.
- Распределённая маршрутизация позволяет обойти перегруженные участки.
- Возможны дополнительные механизмы фильтрации и rate limiting на уровне магистралей.

11. Масштабируемость

11.1 Адресное пространство

IPv6 предоставляет практически неограниченное адресное пространство, что позволяет:

- Назначать крупные пулы магистральным узлам.

- Делать криптографическую привязку адресов без риска исчерпания.

Минимальные требования к нулевым хекслетам задают базовую гранулярность сегмента. Магистрали с большим числом нулей управляют более крупными сегментами, добровольно принимая на себя повышенную ответственность и потенциально получая более значимую роль.

11.2 Блокчейн-уровень

Для обеспечения масштабируемости блокчейна:

- Могут применяться решения второго уровня (L2), шардинг, оптимизация консенсуса.
- Основной принцип: блокчейн фиксирует только критически важные операции (регистрация и блокировка доменов, статические адреса, экономические транзакции), не дублируя объёмы пользовательского трафика.

12. Приватность

Криптографическая адресация сама по себе не гарантирует анонимности, но:

- Позволяет отказаться от привязки адресов к реальным идентичностям.
- Уменьшает необходимость в централизованных реестрах.
- Дополнительно могут применяться:
- VPN-туннели с современными протоколами шифрования.
- Методы маршрутизации, вдохновлённые существующими анонимными или приватными сетями.

13. Практическое развёртывание

13.1 Пилотная стадия

На первоначальном этапе:

- Разворачиваются несколько магистральных узлов, поддерживаемых независимыми участниками.
- Разрабатывается и распространяется OpenWrt-пакет, включающий демон Сети, web-интерфейс и лёгкий блокчейн-клиент.
- Ранние участники (энтузиасты, разработчики) подключаются через VPN и тестируют основные функции.

13.2 Расширение

По мере стабильности протокола:

- Количество магистралей растёт органично.
- Пользовательские устройства получают готовые прошивки.

- В Сети начинают появляться сервисы (сайты, приложения), доступные только через децентрализованный уровень.

14. Заключение

Представленная Сеть — это попытка пересобрать фундамент интернета на основе трёх ключевых идей:

- Криптографическая адресация: каждый адрес привязан к ключу и не требует централизованной выдачи.
- Децентрализованная маршрутизация и DNS: магистрали независимы, а домены управляются смарт-контрактами, а не иерархическими органами.
- Экономика, не основанная на плате за трафик: трафик свободен, ценность создаётся владением адресами, доменами и участием в инфраструктуре.

Минимальное требование к нулевым хекслетам обеспечивает базовую структуру магистрального уровня, а добровольное увеличение числа нулей позволяет участникам брать на себя управление крупными сегментами сети, усиливая свою роль и ответственность.

Этот whitepaper определяет общую архитектуру и принципы работы Сети, но оставляет пространство для эволюции протоколов консенсуса, деталей токеномики и механизмов управления, которые могут быть сформированы сообществом в рамках децентрализованного управления (DAO) и последующих версий спецификации.