Создание децентрализованной сети на основе IPv6 и концепциях Web3

Актуальность и проблема

Современные сетевые сервисы зависят от:

- Централизованных серверов
- NAT и прокси
- Нестабильной адресации
- Доверия к посредникам

=>

- Центральные точки отказа
- Множество уязвимостей
- Утечки конф.данных
- Блокировки

Почему это критично?

Проблемы данных:

- Данные концентрируются у компаний
- Пользователи *не контралируют*, где/как их информация используется
- *Утечки* персональных данных и мошеннечество - *массовое* явления
- Централизированные узлы - *удобная цель* для атаки

Ограничения сетевой инфраструктуры:

- Требует доверия к посредникам, которые могут быть скомпроментированы
- Плохо масштабируется

Что такое Web3?

Web3 - не “криптовалюта”, а **концепция *будущего* интернета**

- Аккаунт
- Доверие компании **Web2** => **Web3**
- Сервера

- Ключ
- Криптография
- P2P

Ключевые принцицы:

- Пользователь *сам* владеет своей идентичностью
- *Проверка* вместо доверия
- Данные *не завися*т от одного узла
- Любые действия можно *доказать*

Web3 позволяет строить **устойчивые**, **безопасные** и **независимые** распределённые системы`

Цели и задачи

Создать **архитектуру** и **прототип** децентрализованной p2p-сети, узлы:

- Имеют *криптографическую* индентичность
- Находят друг друга *без сервера*
- Устанавливают *прямые защищённые* каналы
- Строят *меш-граф*

Основные задачи:

- Разработать модель *идентификации* на *блокчейне*
- Реализовать распределённое обнаружение (*DHT)*
- Реализовать алгоритм установления защищённого *p2p*-соединения
- Обеспечить *отказоустойчивость* и *безопасность*

Новизна и значимость

Прямых конкурентов проекту нет - *Yggdrasil, Matrix, libp2p* - другие идеи и задачи. Проект предлагает **оригинальную архитектуру** сети:

- *IPv6* - основной транспорт
- *Блокчейн* - реестр идентичностей, а не платёжная система
- *DHT* для маршрутизации
- Минимум *централизованной* инфраструктуры

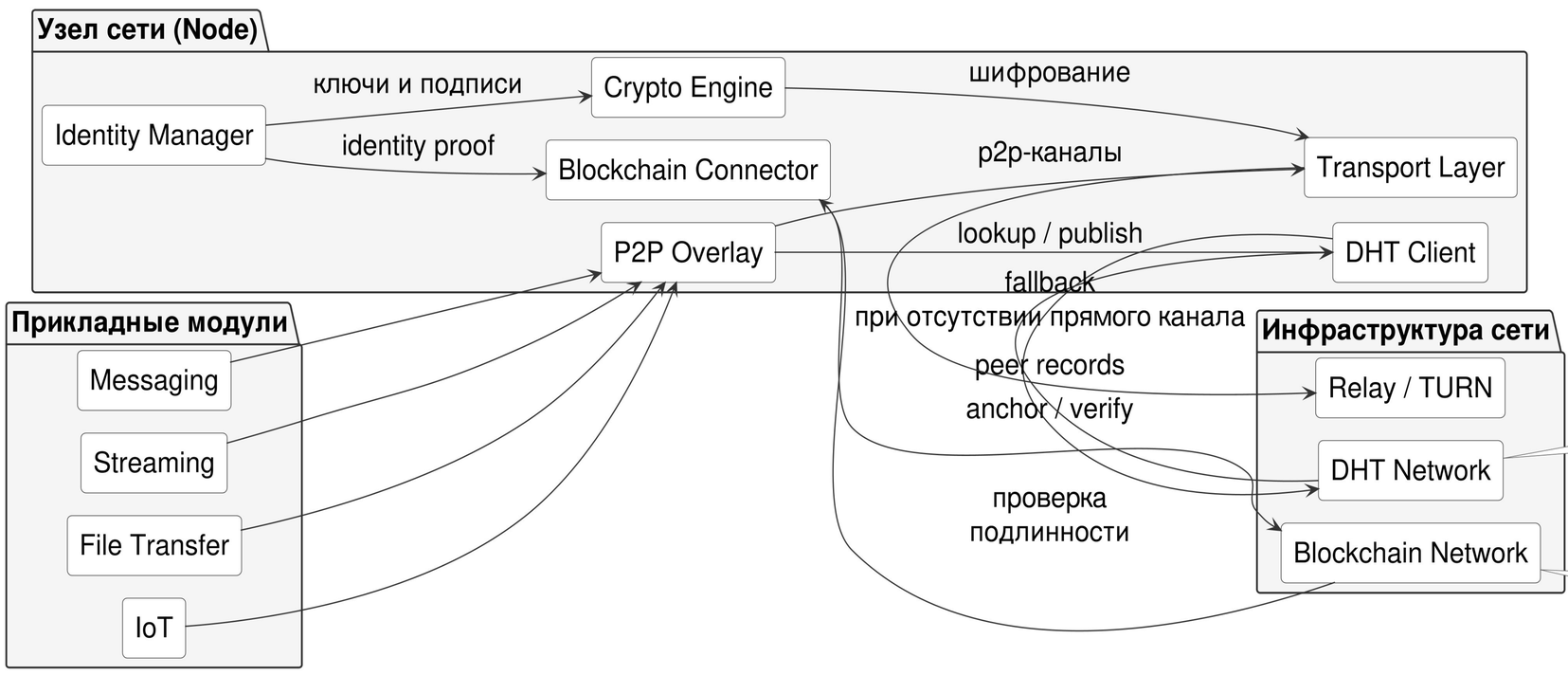
В отличие от существующих решений:

- Не требует постоянной *серверной* инфраструктуры
- Не привязан к *конкретному* протоколу или платформе
- Ориентирован на *сетевой уровень*

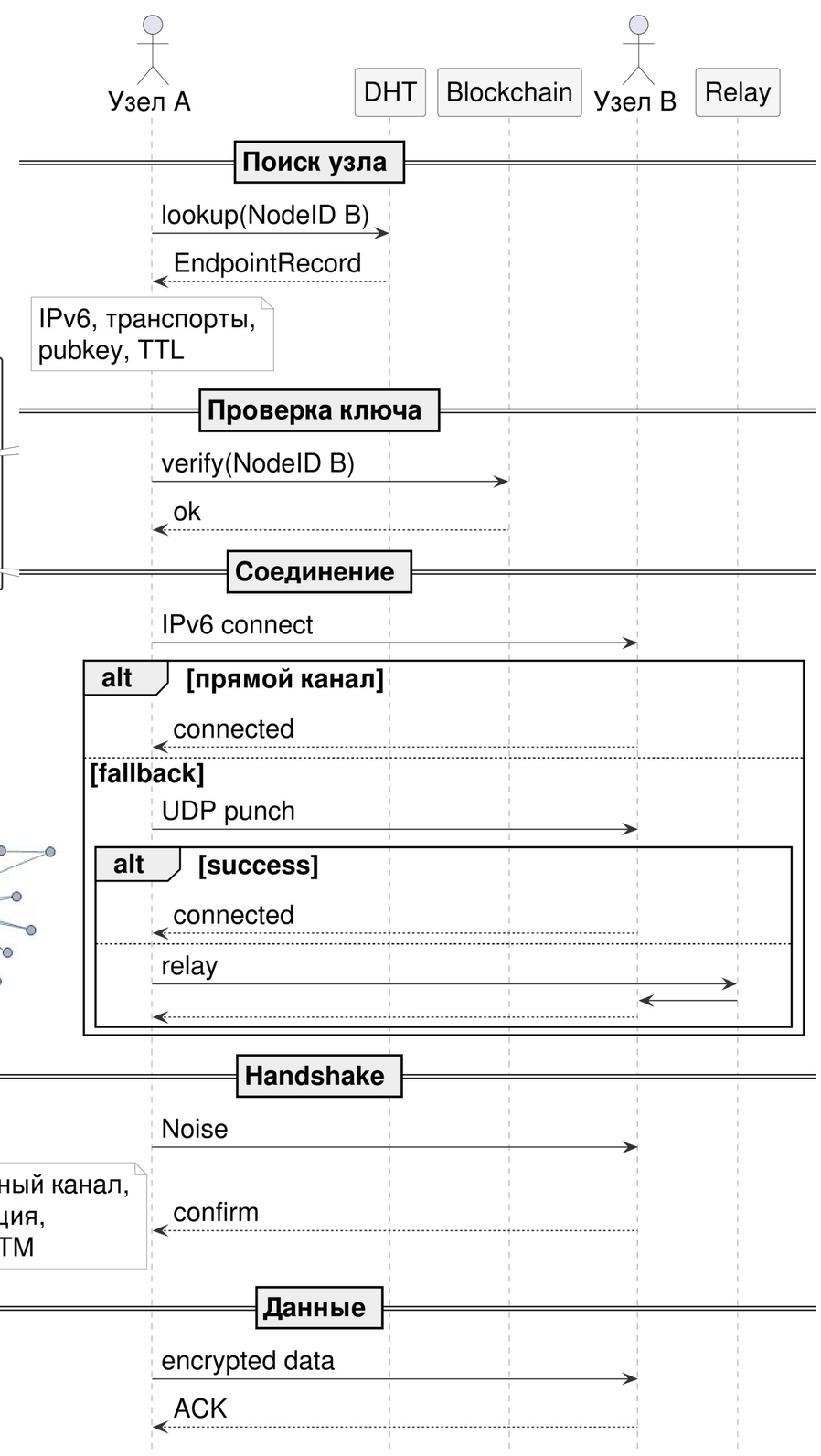
Безопасноть (MITRE ATT&CK)

- **T1557 (MITM)** - проверка ключей через блокчейн
- **T1040 (Sniffing)** - end-to-end шифрование
- **T1498/T1499 (Dos)** - отсутствие сервера
- **T1016 (Recon)** - минимум раскрываемых метаданных

Архитектура децентрализованной P2P Web3 IPv6 сети



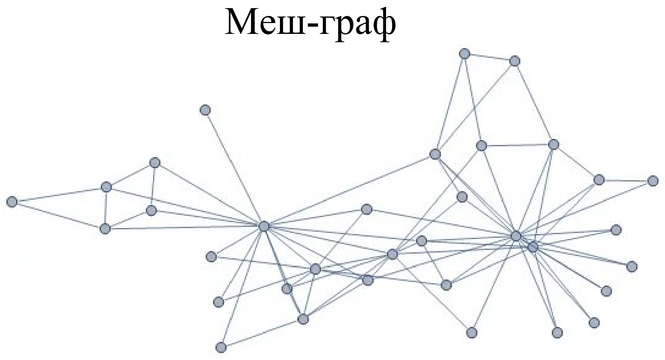
Установление P2P-соединения



Целевая аудитория

- *Разработчики* распределённх и Web3 приложений
- *Инженеры* сетевой и информационной безопасности
- *IoT* и автономные системы
- *Организации*, создающие закрытые распределённые сети
- *Государственные* и *корпаративные* заказчики

Меш-граф



Итоги и перспективы

- Обеспечена *криптографическая идентификация* узлов
- Разработана защищённая *p2p*-архитектура
- Устранены *центральные* точки отказа
- *Начата* программная разработка

- dMessengers
- IoT-сети
- Web3-приложения без серверов
- Корпоративные и ггосударственные mesh-сети