

IoTeX 2.0 – DePIN для всех!

Версия 1.1

Команда IoTeX

23 июля 2024 г.

Аннотация

Децентрализованная сеть физической инфраструктуры (DePIN) в настоящее время является одной из самых горячих тем в Web3 и представляет собой серьезный сдвиг парадигмы, который может фундаментально изменить то, как строятся, эксплуатируются и управляются сети физической инфраструктуры в ближайшем будущем. Из-за нехватки средств и технической компетентности новые стартапы DePIN сталкиваются с серьезными трудностями при своевременном выводе своих идей на рынок. В этом техническом документе мы представляем IoTeX 2.0, преобразующий шаг в эволюции сети IoTeX, направленный на решение вышеупомянутых проблем и помочь сообществу DePIN в реализации окончательного видения «DePIN для всех!».

IoTeX 2.0 содержит следующие основные инновации:

- Новый дизайн токеномики, который подробно исследует полезность токенов IOTX в модульной инфраструктуре DePIN;
- Модульная инфраструктура DePIN, которая позволяет стартапам DePIN создавать свои приложения поверх децентрализованной инфраструктуры, принадлежащей сообществу;
- Модульный пул безопасности (MSP), который обеспечивает единый доверенный уровень для модулей инфраструктуры DePIN посредством повторной ставки;
- Децентрализованная сеть с несколькими проверочными устройствами под названием W3bstream, которая позволяет разработчикам DePIN использовать различные подходы к проверке достоверности для реализации проверки DePIN;
- Унифицированная система идентификации под названием ioID, которая управляет и защищает взаимоотношения между машинами и машина и машинами и людьми внутри и вне цепочки в приложениях DePIN;
- Универсальный встроенный SDK под названием ioConnect, который расширяет возможности абстрагирования устройств и облегчает взаимодействие интеллектуальных устройств в приложениях DePIN;
- Цепной SDK под названием ioDDK, который позволяет проектам DePIN создавать самостоятельные цепочки приложений и одновременно наследовать безопасность IoTeX L1.

Содержание

1.	DePIN сегодня	5
1.1.	Почему важен DePIN	6
1.2.	DePIN Ландшафт	7
1.3.	Технический стек DePIN и его проблемы	9
1.4.	Наша философия DePIN	11
2.	IoTeX 2.0	13
2.1.	Введение	
2.2.	Что мы (не) строим	15
2.3.	Токеномика	18
2.3.1.	Полезность IOTX в IoTeX 2.0	18
2.3.2.	Вознаграждения за инфляционные ставки	22
2.3.3.	Дефляционное сжигание	22
2.3.4.	Стимулы роста	23
2.4.	Общественные блага	24
2.5.	Поддержка разработчиков на протяжении всего жизненного цикла проекта	26
2.6.	Будущее	27
3.	Модульный пул безопасности (MSP) — единый доверенный уровень для модулей инфраструктуры DePIN	29
3.1.	Проблема	29
3.2.	Открытый рынок безопасности и доверия	29
3.3.	Архитектура	30
4.	W3bstream — децентрализованная сеть мультипруверов для проверки DePIN	33
4.1.	Архитектура W3bstream	33
4.1.1.	Четыре типа пруверов	34
4.1.2.	Наши собственные инновации в области ZKP	37
4.2.	Рабочий процесс W3bstream	38
4.2.1.	Регистрация и управление пруверами	38
4.2.2.	Рабочий процесс	38
4.3.	Проверка DePIN и искусственный интеллект вне сети	39
4.3.1.	Проверка DePIN	39
4.3.2.	ИИ вне блокчейна	39
5.	ioID — унифицированная система идентификации для DePIN	41
5.1.	Идентификация внутри и вне цепочки	41
5.1.1.	Ончейн идентификация	41
5.1.2.	Идентификация вне сети	41
5.2.	Генерация ioID на устройстве	42
5.2.1.	Генерация ioID на устройстве	42
5.2.2.	Регистрация и привязка ioID — путь владельца устройства к подключению устройств DePIN	43
5.2.3.	Безопасное взаимодействие между машинами	45
5.3.	Интеграция ioID в проект DePIN	45
5.3.1.	Смарт-контракты в ioID	45
5.3.2.	Развертывание контракта NFT устройства	45

5.3.3.	Регистрация проекта DePIN	46
5.3.4.	Настройка контракта NFT устройства	46
5.3.5.	Запрос iOLD	46
5.3.6.	Регистрация устройства	46
6.	ioConnect — универсальный встроенный SDK, абстрагирующий аппаратную сложность устройств	
		47
6.1.	Варианты подключения	47
6.1.1.	Подключение к уровню централизованного подключения	47
6.1.2.	Подключение к децентрализованному уровню подключения	48
6.2.	Особенности проектирования для создания универсального встроенного SDK для устройств DePIN	49
6.2.1.	Крипто API, сертифицированный PSA Arm	49
6.2.2.	Самосуверенная идентичность (SSI)	50
6.3.	Спецификация реализации	51
6.3.1.	Ядро ioConnect SDK	51
6.3.2.	Совместимость устройств DePIN	52
7.	ioDDK — включение самостоятельных цепочек приложений DePIN	54
7.1.	Обоснование дизайна	54
7.2.	Общее пространство блоков и валидаторов	55
7.3.	Компоненты ioDDK и высокоуровневый рабочий процесс	57
7.3.1.	Компоненты ioDDK	57
7.3.2.	Рабочий процесс высокого уровня	58
7.4.	Рынок аренды блочного пространства	58
7.5.	Влияние на IoTeX L1	59
8.	Новая дорожная карта	60
9.	Заключение	60

Глава 1

DePIN сегодня

IoTeX был основан в 2017 году, чтобы дать людям возможность владеть и контролировать свои интеллектуальные устройства, а также данные и ценность, которые производят их устройства, путем подключения Интернета вещей (IoT) к блокчейну. Наш основополагающий тезис заключался в том, что аранжировка миллиардов интеллектуальных устройств с использованием децентрализованных блокчейнов решит основные проблемы существующего Интернета вещей, такие как доверие, безопасность и суверенитет, а также позволит процветать новой парадигме сетей устройств, принадлежащих пользователям. За последние 6 лет мы стали пионерами в синтезе реального мира и блокчейнов, исследовав и разработав несколько основных вариантов использования:

- **Микроплатежи (2017-2018):** Используйте блокчейн в качестве глобального уровня цифровых расчетов для облегчения автоматизированных и дешевых платежей между устройствами, машинами и людьми. Блокчейны служат объединяющим слоем для ранее несовместимых друг с другом устройств для связи и транзакций.
- **Происхождение и отслеживаемость (2018-2020):** Используйте блокчейн в качестве надежного бухгалтерского учета и реестра прав собственности, обеспечивая возможность происхождения интеллектуальных устройств и децентрализованных сценариев использования в цепочке поставок (например, Pebble трекер [1,2]). Блокчейн собирает данные с доверенных устройств для проверки реальных действий, а также запускает новые события и рабочие процессы.
- **Владение данными и конфиденциальность (2020–2021):** Используйте блокчейн в качестве децентрализованного уровня идентификации, чтобы люди могли владеть и контролировать свои устройства и данные (например, Ucam [3,6]), включающий передовую криптографию, такую как сквозное шифрование, многосторонние вычисления и конфиденциальные вычисления. Децентрализованные решения для обеспечения конфиденциальности, разработанные в сотрудничестве с такими крупными предприятиями, как Arm [7,8].
- **DePIN (2021 – настоящее время):** Используйте блокчейн в качестве основы для децентрализованных сетей физической инфраструктуры (DePIN), новую модель формирования капитала и координации действий людей, которая позволяет людям вносить свой вклад и создавать капитал в реальных инфраструктурных сетях. Данные и услуги, которые производят DePIN, могут также служить входными данными для других категорий вариантов использования, а именно искусственного интеллекта (ИИ) и активов реального мира (RWA).

Оригинальный White paper IoTEx [5], опубликованная в 2017 году, продемонстрировала наше видение безопасного, масштабируемого, многоцелевого и децентрализованного уровня L1, который включает в себя технологии сохранения конфиденциальности и ориентированное на устройства промежуточное программное обеспечение для соединения физического и цифрового миров. За прошедшие годы мы реализовали многие из амбициозных целей, которые мы поставили перед собой в нашем первоначальном техническом документе:

- Основная сеть IoTEx обработала около 120 миллионов транзакций без каких-либо простоев или взломов;

- Первые аппаратные устройства, совместимые с блокчейном (например, Ucam, Pebble Tracker), были разработаны и изготовлены IoTeX как готовые комплекты разработчика оборудования для разработчиков;
- В платформу IoTeX были интегрированы различные интеллектуальные устройства третьих сторон, что дает фундаментальное понимание того, как безопасно подключить реальный мир к блокчейну;
- На IoTeX была запущена целая экосистема проектов DePIN, которая включает в себя реальные данные со смарт-устройств;
- Было создано глобальное сообщество сетевых валидаторов, разработчиков и пользователей, которое представляет собой жизненную силу сети IoTeX.

Но это только начало. С 2017 года сфера блокчейна выросла в геометрической прогрессии, и теперь у нас есть более глубокое понимание того, что необходимо DePIN для достижения массового внедрения. Параллельно с созданием нашей первоначальной концепции IoTeX, основной разработчик IoTeX был занят исследованием и разработкой новых инноваций, которые выведут DePIN на новый уровень, таких как доказательства с нулевым разглашением, масштабирование вне цепочки, самостоятельная идентификация для устройств и общественные блага, которые приводят вперед весь сектор DePIN. Концепция IoTeX 2.0, которую мы представляем, описывает наш трехлетний план по расширению сети IoTeX. Мы стремимся внедрить новую модульную конструкцию платформы, обновить нашу токеномику и многое другое, чтобы удовлетворить растущие потребности разработчиков в пространстве DePIN и за его пределами. Благодаря этому обновленному видению мы наконец сможем реализовать нашу конечную цель — расширение прав и возможностей “**DePIN для всех!**”.

1.1 Почему важен DePIN

Прежде чем мы углубимся в IoTeX 2.0 и наше видение будущего DePIN, мы хотели бы начать с рассказа о том, что такое DePIN и почему вас это должно волновать. Сегодня многие из наиболее важных отраслей и коммунальных предприятий нашего мира, таких как телекоммуникации, энергетика и вычисления, являются монополиями и олигополиями, которые принадлежат и контролируются централизованными корпорациями и правительствами. Эти триллионные отрасли созданы с чрезвычайно высокими входными барьерами, как финансовыми, так и логистическими; например, AT&T ежегодно тратит 24 миллиарда долларов и требует более 160 000 сотрудников для управления своей телекоммуникационной империей. Из-за этих огромных барьеров для входа на рынок существует лишь несколько «поставщиков услуг» для товаров и услуг, которые могут выбирать обычные люди. Это означает, что конкуренция ограничена, инновации подавлены, а потребителям приходится мириться с некачественным обслуживанием клиентов и чрезмерно завышенными ценами, потому что у них нет другого выбора. Предоставляя услуги миллионам клиентов, корпоративные гиганты также тайно извлекают конфиденциальные и ценные данные от людей ради собственной выгоды. Проблемы, вытекающие из этого, еще более выражены в странах с формирующимся рынком, еще больше углубляя разрыв в уровне благосостояния и ограничивая возможности для обычных людей.

DePIN — это революционная концепция, которая изменит статус-кво. DePIN, построенные на децентрализованных блокчейнах с открытым исходным кодом, могут обеспечить прозрачность, доверие и инновации в физической инфраструктуре и коммунальных услугах, которые обслуживают миллиарды людей по всему миру, с низкими затратами или вообще без них. Но исправление сегодняшнего мира —

это лишь часть истинного потенциала DePIN. Реальная возможность состоит не в том, чтобы просто исправить то, что не так с нынешним миром, а в том, чтобы построить новый мир с утилитами, которыми владеют, управляют и используют обычные люди. DePIN позволит любому внести свой вклад и создать капитал в реальных инфраструктурных сетях, преодолевая вышеупомянутые финансовые и логистические барьеры для входа. Используя новые методы формирования капитала, популяризированные децентрализованными финансами (DeFi) для краудсорсинга сетевых ресурсов, DePIN могут объединять предоставленное пользователями оборудование, рабочую силу и региональный опыт, чтобы стимулировать создание новых инфраструктурных сетей и вознаграждать участников акциями в сетях, которые они используют. Наконец, DePIN могут использовать неизменяемые смарт-контракты в блокчейне для проверки и координации действий участников в направлении того, что лучше для сети.

DePIN не только открывает путь к улучшению нашего нынешнего мира, но также дает возможность создать лучший мир. Мы находимся на пороге новой промышленной революции, когда устаревшая инфраструктура, такая как ископаемое топливо и проводной Интернет, будет заменена инновационной инфраструктурой, такой как возобновляемые источники энергии и беспроводная связь. С помощью DePIN каждый может внести свой вклад в модернизацию нашей глобальной инфраструктуры и получить свою справедливую долю от триллионов долларов стоимости, которую представляет эта инфраструктура. Новый мир, созданный людьми и для людей — вот обещание DePIN. DePIN — для всех!

1.2 DePIN Ландшафт

DePIN — это коллективная работа сотен проектов по всему миру, направленных на децентрализацию и улучшение нашей физической инфраструктуры. Хотя термин DePIN был создан в 2023 году, сектор DePIN активен гораздо дольше, а такие проекты, как IoTeX, Helium и Filecoin, стали пионерами с 2017 года. Сегодня ландшафт DePIN разнообразен и состоит из проектов, создающих специфичную для DePIN инфраструктуру, а также приложения DePIN в нескольких вертикалях. DePIN в настоящее время является одним из наиболее многообещающих вариантов использования блокчейнов и может быть разделен на сети физических ресурсов и сети цифровых ресурсов, которые обозначаются типом услуги, предоставляемой сетью. Сети физических ресурсов производят невзаимозаменяемые ресурсы (т. е. данные/услуги с любых устройств уникальны), которые более осозаемы по своей природе и обычно полагаются на аппаратное обеспечение, зависящее от местоположения. С другой стороны, сети цифровых ресурсов создают рынки для взаимозаменяемых ресурсов (т. е. 1 ГБ хранилища — это 1 ГБ хранилища), которые более виртуальны по своей природе и полагаются на оборудование, не зависящее от местоположения. Сектор DePIN также включает в себя инфраструктуру и инструменты, которые способствуют росту этой категории и предоставляют готовые возможности для приложений DePIN. Полная картина DePIN [9] показана на рисунке 1.1.



DePIN Ландшаф

Апрель 2024 Децентрализованная Сеть Физической Инфраструктуры

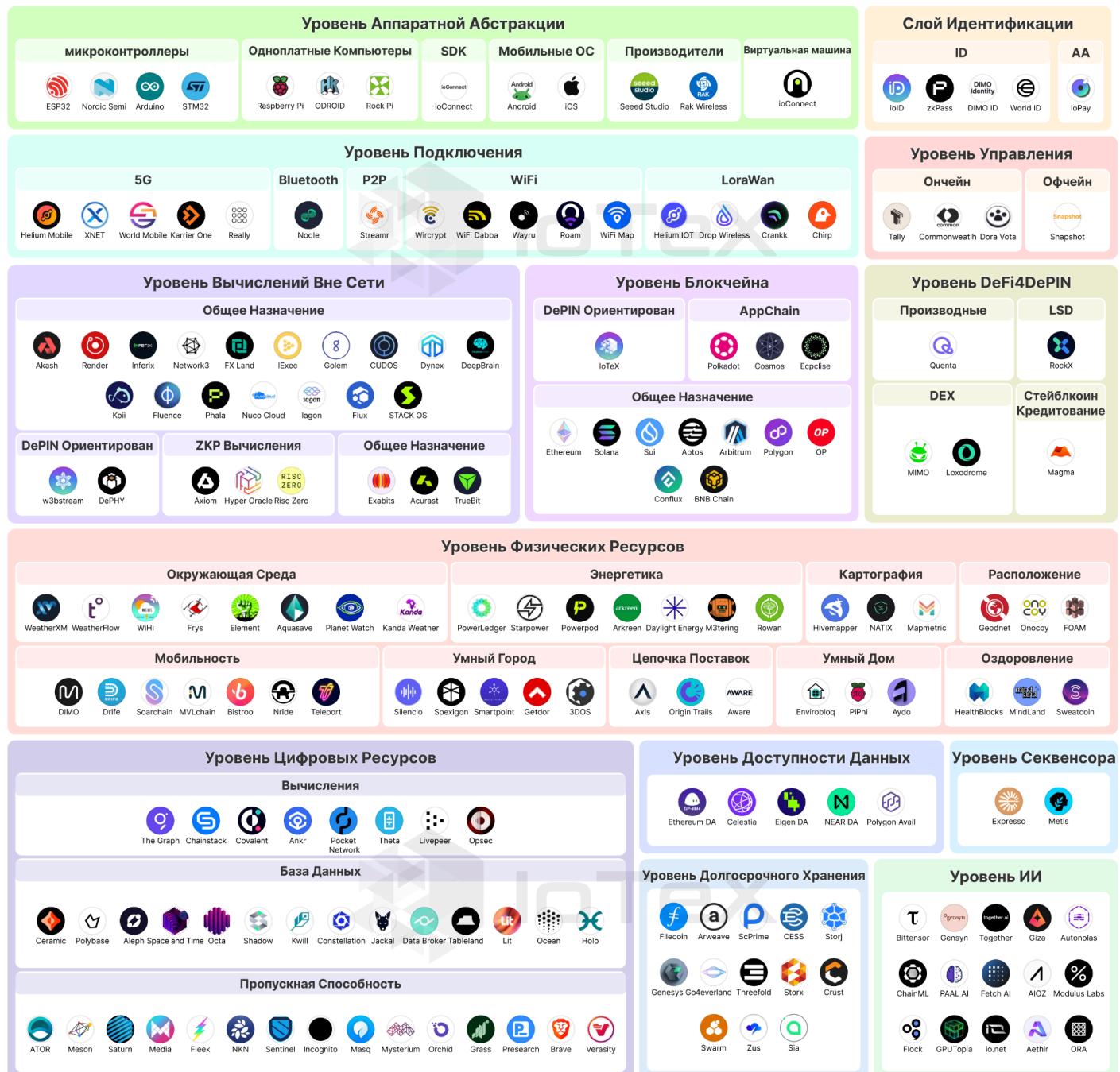


Рис 1.1: Ландшафт DePIN

1.3 Технический стек DePIN и его проблемы

Независимо от того, фокусируется ли DePIN на физических ресурсах или цифровых ресурсах или на какую конкретную вертикаль они нацелены, необходима потребность в комплексном технологическом стеке, который соединяет реальный мир с миром блокчейна. В отличие от сценариев использования блокчейна, которые облегчают обмен цифровыми активами, такими как NFT, и финансовыми активами, такими как стейблкоины, DePIN должны взаимодействовать с реальными интеллектуальными устройствами, которые генерируют невероятное количество данных. Блокчейн, как неизменяемый реестр, является идеальной основой для документирования фактов о том, что произошло в реальном мире; однако, прежде чем записывать «доказательства активности в реальном мире» с устройств в блокчейн на постоянной основе, необходимо выполнить ряд шагов, чтобы убедиться, что активность в реальном мире действительно произошла и данные заслуживают доверия. Устройства должны быть зарегистрированы в цепочке, необработанные данные должны собираться, анализироваться и храниться, а вычисления над данными должны выполняться проверяемым способом, прежде чем любое «доказательство активности в реальном мире» может быть зафиксировано в блокчейне. В эталонной архитектуре ниже представлены девять основных уровней, которые следует учитывать в проектах DePIN.



Рис 1.2: Технический стек DePIN

- **Уровень аппаратной абстракции:** обеспечивает безопасное соединение широкого спектра интеллектуальных устройств, больших и малых, с объектами на уровне подключения;
- **Уровень подключения:** надежно передает данные, создаваемые интеллектуальными устройствами, на уровень секвенсора;

- **Слой секвенсора:** сортирует пакеты данных от интеллектуальных устройств перед отправкой их на уровень доступности данных;
- **Уровень доступности данных:** временно хранит данные для немедленного использования, разделяя доступ к данным с уровнем вычислений вне цепочки для получения аналитической информации на основе необработанных данных;
- **Уровень долгосрочного хранения:** архивирует необработанные данные и аналитическую информацию для использования в будущем, к которым могут получить доступ третьи лица через API для обеспечения соответствия требованиям, аналитики, искусственного интеллекта и многое другое;
- **Уровень внесетевых вычислений:** применяет бизнес-логику к данным, хранящимся на уровне доступности данных, для получения информации и доказательств, связанных с реальной деятельностью;
- **Уровень блокчейна:** служит якорем доверия для идентификаторов и данных устройств, проверяя достоверность вычислений вне сети и распределяя вознаграждение в виде токенов заинтересованным сторонам DePIN;
- **Уровень идентификации:** управляет идентификацией внутри и/или вне цепочки для всех задействованных объектов (например, интеллектуальных устройств, пользователей, серверов, производителей, валидаторов);
- **Уровень управления:** обеспечивает соблюдение сетевых политик и процедур (например, стимулов) децентрализованным способом, обычно посредством процесса голосования сообщества.

Обширные уровни технологического стека DePIN могут оказаться непосильными для одной команды, которая может разрабатывать монолитно. Эта сложность создает высокий барьер для строителей, желающих экспериментировать с инновационными идеями в DePIN. За последние несколько лет хорошо финансируемые проекты преодолели эти проблемы за счет привлечения значительного венчурного капитала и разработки собственных монолитных технологических стеков. Однако для того, чтобы DePIN действительно процветал и достигал всех уголков мира (например, Латинской Америки, Африки и Юго-Восточной Азии), большой набор технологий и сложность высоких технологий создают дополнительные проблемы:

- **Скорость запуска:** скорость, с которой DePIN могут достичь минимального порога предложения для стимулирования первоначального спроса, ограничена из-за аппаратных ограничений и требований к первоначальным капитальным затратам;
- **Рост спроса:** DePIN борются с наращиванием спроса из-за долгого пути к началу поставок и трудностей в достижении паритета с существующими решениями по пользовательскому опыту, надежности и стоимости;
- **Ликвидность токена:** DePIN используют стимулы в виде токенов для стимулирования роста сети и финансирования операций инфраструктуры, но сталкиваются с трудностями при закрытии маxовика и создании ликвидности в цепочке;
- **Осведомленность:** DePIN часто фокусируются на конкретных отраслях, где цель проекта и показатели успеха не всегда очевидны, особенно для тех, кто еще не участвует в отрасли напрямую.

Из-за этих проблем DePIN все еще находится в зачаточном состоянии и еще не превзошел DeFi и другие криптографические отрасли с точки зрения рыночной стоимости и распространения. DeFi и DePIN во многом схожи, особенно в том, что они краудсорсингуют ресурсы людей («сторона

предложения») для создания продукта, который другие люди желают и используют («сторона спроса»). Однако путь к получению и поддержанию спроса и предложения сильно различается между DeFi и DePIN. На высоком уровне спрос и предложение DeFi легче настроить, но они быстротечны, в то время как спрос и предложение DePIN сложнее настроить, но он более способен выдержать испытание временем. Кроме того, DePIN часто должны агрегировать большой запас ресурсов для создания первоначального спроса, в отличие от DeFi, где небольшое количество агрегированных средств может иметь немедленный спрос. Сравнивая DePIN и DeFi с проблемами, отмеченными выше, мы можем увидеть следующие подробные различия:

1.4 Наша философия DePIN

Мы твердо убеждены, что DePIN должен развиваться так же, как DeFi, и предназначен для всех: каждого разработчика, каждого участника и каждого пользователя. Это убеждение подчеркивает, что:

- Небольшие команды с большим сердцем должны иметь возможность создавать эффективные продукты DePIN для обслуживания своих местных сообществ и регионов.
- Проекты DePIN должны быстро повторяться без высоких первоначальных затрат, чтобы выявить настоящие инновации.
- Проекты в рамках DePIN должны быть компонуемыми как по функциям (например, агрегирование данных о звонке, машине, телефоне для отдельного человека), так и по региону (например, городская модель Uber).
- Участники сети, обеспечивающие ценность или полезность сети, должны иметь низкую планку входа и получать стабильное и долгосрочное финансовое вознаграждение.
- Пользователи должны иметь возможность пользоваться общедоступными и инновационными утилитами из этих сетей DePIN с минимальными затратами или вообще бесплатно.

Эта вера не является просто принятием желаемого за действительное. Ее можно практически перевести в технический проект, известный как IoTeX 2.0, как показано ниже.

	DeFi	DePIN	Проблемы для DePIN	Частичные Решения
Технический Стек	Просто и только в цифровом формате: например, в основном Solidity + JS, легко развертывается для запуска	Сложный и затрагивает физический мир: C/C++ + Golang/Python/Rust + Solidity + JS + опционально Swift, сложно развернуть	Проблема 1: проекты DePIN сложнее создавать, и для их запуска требуется больше капитала из-за их аппаратного компонента. Разведка идет медленно и дорого	<ul style="list-style-type: none"> Запускайте проекты централизованно, чтобы «проверить» рынок и ускорить принятие решений Отсутствие децентрализации и недоверия может отпугнуть вкладчиков и инвесторов
Скорость Запуска	Быстро: например, запустите dApp по всему миру; несколько майнеров с капиталом быстро наладили линию предложения	Медленно: например, поставка и развертывание оборудования для конкретного проекта, пороговый масштаб поставок, при котором сеть может обслуживать спрос, может быть высоким	Проблема 2: проекты DePIN медленно запускаются (устанавливают сторону предложений) из-за их аппаратных ограничений, что может привести к несоответствию с криптоциклами	<ul style="list-style-type: none"> Работа с существующим партнером Web2, например T-Mobile, для более быстрого достижения порогового масштаба Не применяется к инновационным сетям DePIN, где не существует партнера Web2
Рост Спроса	Легко привлечь пользователей, если спроектировано правильно, выращивание урожая, длится недолго	Медленная загрузка, например, привлечение клиентов с тарифным планом сотовой связи, но может быть более эффективным в долгосрочной перспективе	Проблема 3: Криптовалюта может обеспечить излишне сложный UX, замедляя внедрение со стороны спроса	<ul style="list-style-type: none"> Использование токенов для стимулирования обычных людей к принятию и использованию DePIN Большинство людей не являются крипто-нативными и не понимают токены, кошельки, ...
Ликвидность Токена	Ликвидность токенов легко приобрести и является естественным побочным продуктом финансового применения	Ликвидность токенов зачастую трудно достичь, поскольку основатели и участники имеют больше опыта работы с аппаратным обеспечением и Web2, чем финансового опыта	Проблема 4: Ликвидность токенов важна для любого криптопроекта, но особенно для DePIN, которые обеспечивают рост сети с помощью стимулов в виде токенов	<ul style="list-style-type: none"> Команды DePIN могут работать с СЕХ и маркет-мейкерами для достижения ликвидности токенов Это может быть дорогостоящим и длительным процессом
Рост Сети Обмена	Показатели успеха понятны, например TVL, их легко получить и отобразить	Показатели успеха зависят от проекта и должны быть получены с физических устройств	Проблема 5: командам DePIN приходится тратить драгоценное время и усилия на создание информационных панелей для отображения показателей своего проекта	<ul style="list-style-type: none"> Данные в цепочке можно извлечь и отобразить с помощью таких инструментов, как Dune Однако многие DePIN начинаются централизованно и не имеют большого количества данных в цепочке, которые можно было бы показать.

Рис. Проблемы DePIN по сравнению с DeFi

Глава 2

IoTeX 2.0

2.1 Введение

IoTeX 2.0 определяет грандиозное видение и дорожную карту сети IoTeX на следующие несколько лет, расширяя нашу миссию по обеспечению «DePIN для всех» и основанную на многолетнем опыте пионера индустрии DePIN. Наша цель — не только решить технические и нетехнические проблемы, с которыми сегодня сталкиваются проекты DePIN, но и реализовать весь потенциал DePIN в будущем, сделав IoTeX крупнейшей экосистемой DePIN в мире. Для достижения этой цели мы рады представить IoTeX 2.0, который сочетает в себе новую философию, технологии, токеномику, общественные блага и инициативы, которые позволяют обычным людям вносить свой вклад в DePIN и дают разработчикам возможность по-настоящему соединить реальный мир с миром блокчейна.

С IoTeX 2.0 сеть IoTeX превратится из простого блокчейна L1 в открытую инфраструктуру DePIN, Dapps и L2, которые будут привязаны через токен IOTX. Это значительно увеличит количество и типы участников сети IoTeX, что в конечном итоге расширит сферу действия IoTeX и DePIN на новые горизонты. DePIN должен быть доступен каждому, поэтому IoTeX 2.0 отдает приоритет вовлечению разработчиков и пользователей на каждом этапе жизненного цикла. Независимо от того, являетесь ли вы признанным децентрализованным приложением, которое хочет расширить свою собственную цепочку L2, или традиционной компанией, стремящейся реализовать бизнес-модель на основе DePIN, или просто небольшой командой с большой идеей, IoTeX 2.0 предоставляет полный набор возможностей, которые актуально для всех разработчиков DePIN.

Наша основная методология — модульная инфраструктура: проекты DePIN могут создавать стек технологий, соответствующий их конкретному этапу и требованиям, выбирая из меню модульных предложений. Эти предложения включают в себя собственные продукты, созданные IoTeX coredev, и партнерские продукты из лучших проектов. Основное преимущество модульного подхода заключается в том, что разработчики инфраструктуры могут сосредоточиться на функциях, которые у них лучше всего выполняются, и сотрудничать для достижения общей цели. Наши модульные предложения включают в себя передовые технологии, такие как автономное масштабирование, доказательства с нулевым разглашением и искусственный интеллект, чтобы привнести уникальные инновации в сектор DePIN. Эти модули создаются не только специалистами IoTeX coredev, но и специализированными разработчиками инфраструктуры, использующими IoTeX для обеспечения их безопасности и доверия. Этот подход предоставляет крупнейшим командам DePIN комплексные решения, а также предлагает более мелким командам специальные решения, которые они могут использовать для быстрого и безопасного создания новых проектов DePIN.

С архитектурной точки зрения IoTeX 2.0 подчеркивает следующие перспективы:

- **Модульный пул безопасности (MSP):** Основой модульности является единый, надежный уровень, поддерживаемый IOTX и другими основными ресурсами, который мы называем MSP. Это набор смарт-контрактов, развернутых на IoTeX L1. И IoTeX L1, и MSP служат якорем доверия

и неизменяемым регистром для всех действий на уровне модулей инфраструктуры DePIN (DIM) и уровнях Dapp/L2. В общих чертах, MSP позволяет IoTeX L1 обеспечивать безопасность «доказательства доли» для модулей DIM, которые охватывают различные части технологического стека DePIN. Поставщики DIM делают ставку на IOTX и другие основные активы, чтобы присоединиться к MSP. Более того, DIM, получившие безопасность и доверие от MSP, будут периодически якорить свои состояния в IoTeX L1, открывая возможность разработчикам dApp внедрять инновации на основе проверенной реальной деятельности.

- **Инфраструктурные модули DePIN (DIM):** Новый уровень DIM в IoTeX 2.0 предлагает модульный набор функций, охватывающий весь стек технологий DePIN. Содействуя вкладу глобальных разработчиков, основная разработка IoTeX обеспечит собственные реализации для нескольких уровней. Дополнительные DIM, такие как вывод искусственного интеллекта, хранилище, вычисления с сохранением конфиденциальности, анализ данных, RPC и системы доменных имен, будут предоставлены партнерами и разработчиками, которые будут использовать IOTX для MSP. Обратите внимание, что при необходимости каждый DIM может иметь свой собственный токен.
- **Общественные блага:** Цель IoTeX — вывести DePIN на новые горизонты, что требует общественных благ, которым каждый может доверять и которые может свободно использовать. Наша цель — возглавить движение DePIN, создав набор ресурсов с открытым исходным кодом, с которыми разработчики могут легко интегрироваться и предложить своим пользователям для стимулирования открытого участия. К этим общественным благам относятся инструменты, ориентированные на пользователей (например, проводники, кошельки, мосты), инструменты, ориентированные на разработчиков (например, IDE), а также общесетевые ресурсы (например, управление, финансирование).
- **Меритократическая токеномика:** Добавление новых уровней в сеть IoTeX приводит к появлению новых заинтересованных сторон, которые внесут свой вклад в различные категории. Цель нашей обновленной токеномики — не только расширить полезность токена IOTX, но и сделать это меритократическим способом, при котором вознаграждения распределяются в зависимости от значимости вкладов заинтересованных сторон. Расширение масштабов сети IoTeX обеспечит новую полезность токена IOTX, сделав его основной валютой сектора DePIN.
- **DePIN Dapps и DePIN L2:** На вершине технологического стека будет экосистема DePIN Dapps и L2, которые используют некоторые или все DIM IoTeX 2.0. Хотя многие децентрализованные приложения предпочтут запустить свои собственные токены на IoTeX L1 и использовать все предложения DIM, некоторые децентрализованные приложения могут выбрать использование только одного или нескольких DIM. Модульная ориентация на IoTeX 2.0 позволяет децентрализованным приложениям использовать различные модули в зависимости от их текущих потребностей, одновременно предоставляя новые возможности для их будущих потребностей. Кроме того, новым компонентом уровня DIM является ioDDK, SDK цепочки L2, который позволит проектам запускать свои собственные L2 поверх IoTeX L1. Это позволит DePIN создавать свою собственную суверенную токеномику и размещать свои собственные Dapps, пользуясь при этом широкими возможностями уровня DIM и получая безопасность и доверие со стороны IoTeX L1.

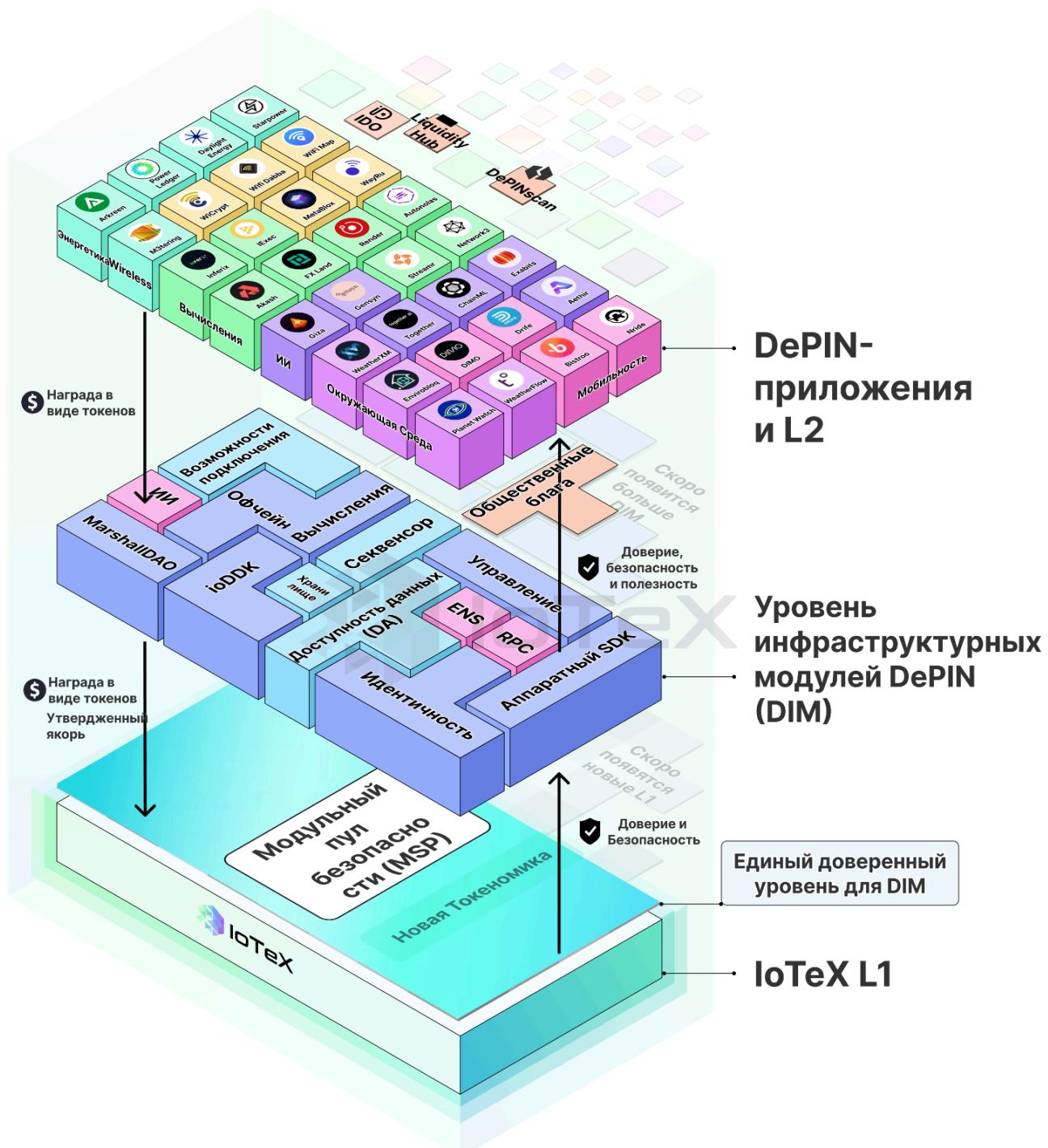
2.2 Что мы (не) строим

Как упоминалось в разделе 1.3, создание DePIN требует многоуровневого технологического стека, охватывающего широкий спектр возможностей. Недавно представленный уровень DIM IoTeX 2.0 предлагает решения для каждого из этих элементов технологического стека. Этот уровень DIM полностью открыт, что позволяет любому разработчику инфраструктуры включать свои реализации. Это предоставляет проектам DePIN широкий спектр возможностей для создания собственного технологического стека.

Наряду с основными модулями, разработанными внутри IoTeX coredev, многочисленные модули будут получены из ведущих проектов в пространстве блокчейнов со специализированными возможностями. Например, уровень доступности данных находится в центре внимания таких проектов, как Celestia и NEAR, тогда как уровень долгосрочного хранения находится в центре внимания таких проектов, как Filecoin и Arweave. Поскольку IoTeX 2.0 подчеркивает модульность и возможность компоновки, мы приглашаем все проекты интегрироваться в уровень DIM, что позволяет проектам DePIN разрабатывать технологический стек по своему усмотрению.

Хотя мы открыто приветствуем предложения в любой части уровня DIM, IoTeX coredev исследовали и разработали современные решения для нескольких критически важных модулей, ориентированных на единый доверенный уровень для DIM, аппаратного обеспечения, идентификации, автономных вычислений, L2. SDK и общественные блага, которые мы суммируем ниже и подробно рассмотрим в следующих разделах.

- **MSP (унифицированный доверенный уровень для DIM):** Это единый доверенный уровень, состоящий из набора смарт-контрактов на IoTeX L1. Он принимает ставки IOTX и другие основные активы и сдает свою безопасность в аренду другим DIM.



Область Применения IoTEx 2.0

DIM, которые мы строим

Сборка команды DIMs 3Р

Общественные Блага

Новая Токеномика

Рис 2.1: Область применения IoTeX 2.0

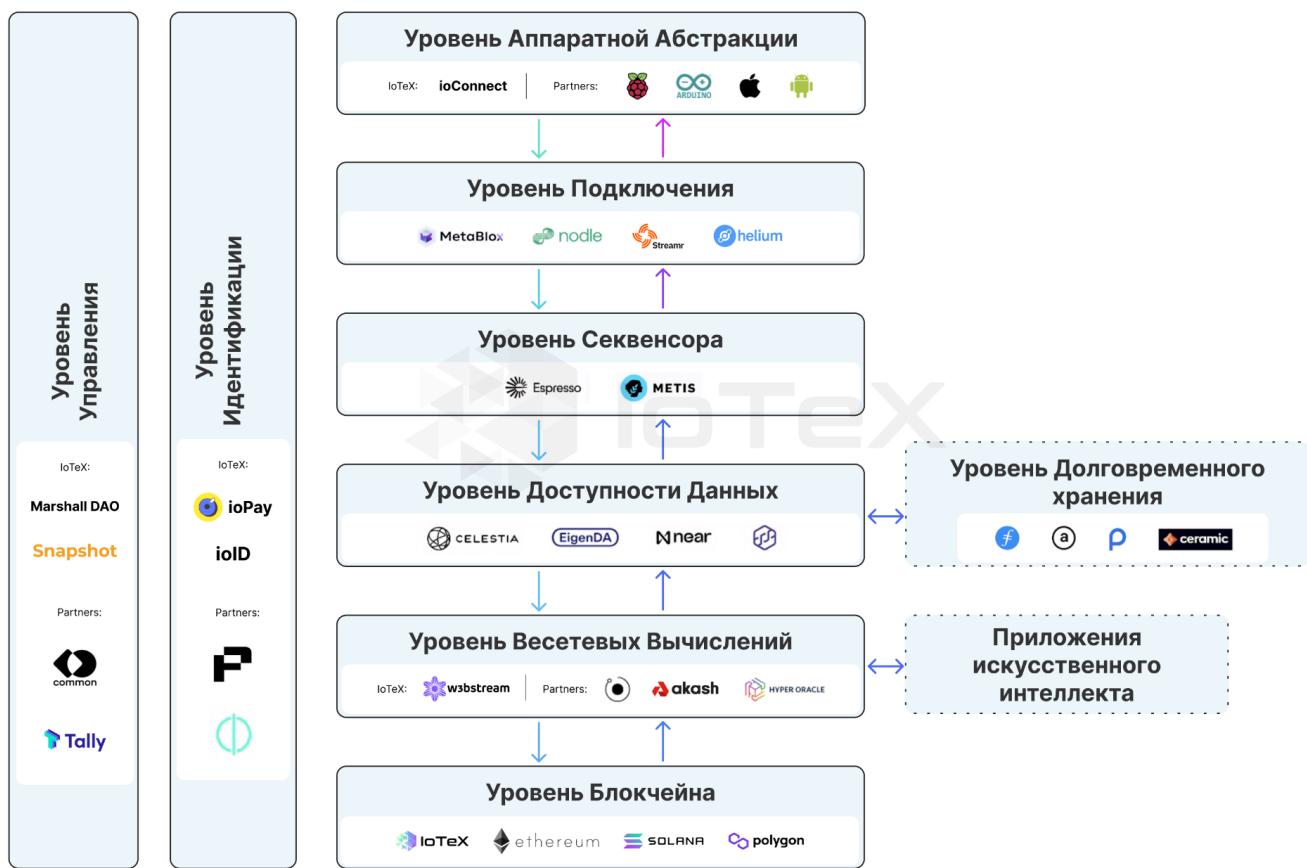


Рис 2.2: Инфраструктурные модули DePIN (DIM)

- **W3bstream (DIM для внесетевых вычислений):** Первая в мире децентрализованная автономная вычислительная сеть, в которой используются проверяемые вычислительные технологии, такие как доказательства с нулевым разглашением (ZKP), полностью гомоморфное шифрование (FHE), доверенные среды выполнения (TEE) и многосторонние вычисления (MPC) для разных поставщиков (включая нас самих) для генерации «доказательств активности в реальном мире» в режиме реального времени и передачи этих доказательств в блокчейн для вознаграждения владельцев устройств.
- **ioID (идентификационный DIM):** Набор самостоятельных цифровых удостоверений внутри и вне цепочки, которые позволяют людям и машинам устанавливать широкие цифровые отношения и взаимодействовать друг с другом, не полагаясь на централизованных поставщиков удостоверений.
- **ioConnect (DIM аппаратной абстракции):** SDK, который позволяет различному оборудованию подключаться к W3bstream и различным уровням L1/L2. Он служит уровнем абстракции оборудования, который безупречно работает на основных аппаратных платформах, таких как Raspberry Pi, ESP32 и Arduino, упрощая работу с оборудованием. Другими словами, устройства на базе ioConnect можно легко интегрировать в различные приложения DePIN, выступая в качестве мультиплексора.

- **ioDDK (DIM L2 SDK):** Цепной SDK, который позволяет разработчикам DePIN беспрепятственно запускать собственный суверенный блокчейн, наслаждаясь безопасностью IoTeX L1. Он изначально поддерживает модули IoTeX, такие как W3bstream, ioID и DePINscan.
- **IoTeX L1:** Блокчейн IoTeX L1 совместим с EVM и использует наш собственный механизм консенсуса Roll-DPoS для достижения более 1000 TPS. Объем и полезность IoTeX L1 будут расширены в IoTeX 2.0: ioID будут зарегистрированы в IoTeX L1, MSP будет развернут как смарт-контракты на IoTeX L1, а ioDDK привяжет цепочки L2 к IoTeX L1.
- **Общественные блага:** Мы продолжим развивать существующие общественные блага, такие как DePINscan [23] и DePIN Liquidity Hub [21], а также создавать общественные блага для разработчиков DePIN.

2.3 Токеномика

Токен IOTX был представлен в 2019 году в качестве базовой валюты для IoTeX L1. С момента запуска Mainnet токен IOTX эффективно сбалансировал стимулы между валидаторами (или «дегелатами»), разработчиками Dapp и пользователями. Делегаты, которые делают ставку IOTX и проверяют транзакции блокчейна в рамках сетевого консенсуса, получают вознаграждения IOTX, в то время как разработчики и пользователи, включая Dapps, держатели токенов и многие другие, платят IOTX за отправку транзакций и взаимодействие со смарт-контрактами. Токены IOTX также используются различными типами держателей токенов для участия в управлении всей сетью.

Поскольку IoTeX расширяется от простого уровня L1 до модульной платформы взаимосвязанной инфраструктуры, токеномика, связанная с токеном IOTX, также будет расширена, чтобы соответствовать нашему видению IoTeX 2.0. Это включает в себя новые формы полезности токена IOTX, которые будут включены в новые технологические предложения IoTeX 2.0. Кроме того, еще одна важная цель токеномики IoTeX 2.0 — сбалансировать инфляционные вознаграждения за ставки, дефляционное сжигание токенов в зависимости от использования платформы и стимулировать DePIN Dapps и L2 к использованию нашей модульной инфраструктуры. Это означает, что наша обновленная токеномика не только привнесет новую полезность и ценность токена IOTX, связав его с W3bstream, ioID, ioDDK и другими DIM, но также будет поддерживать стабильное предложение токенов за счет балансирования инфляционных и дефляционных механизмов. Благодаря более широкому внедрению предложений модульной инфраструктуры IoTeX, токен IOTX приобретет новую ценность в качестве валюты сети IoTeX 2.0.

2.3.1 Полезность IOTX в IoTeX 2.0

Токены IOTX будут использоваться во всей инфраструктуре и экосистеме IoTeX 2.0, и их можно рассматривать с разных точек зрения, как описано ниже.

Собственный Токен L1

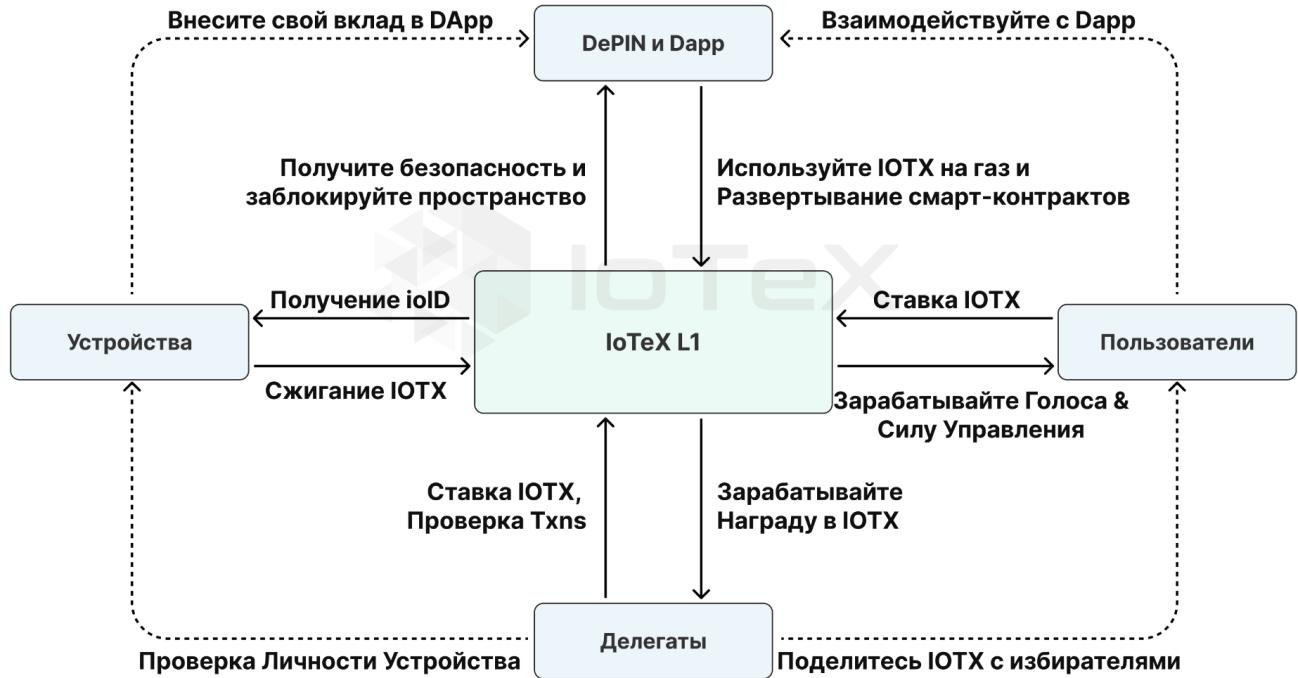


Рис 2.3: Маховик DePIN и полезность токенов IOTX

- **С точки зрения IoTeX L1:** Делегаты будут делать ставки IOTX, чтобы иметь право проверять сетевые транзакции и участвовать в консенсусе, а также будут получать токены IOTX в качестве вознаграждения за свои услуги. Владельцы токенов также могут делать ставки IOTX, чтобы голосовать за делегатов и получать вознаграждения IOTX. Токен IOTX продолжит служить внутренней валютой блокчейна IoTeX L1 в IoTeX 2.0, где Dapps, которые хотят развертывать смарт-контракты и обрабатывать транзакции в блокчейне IoTeX L1, будут тратить IOTX в качестве платы за газ. Помимо размещения IOTX для участия в управлении, пользователи также могут тратить IOTX в качестве платы за газ для обработки транзакций на IoTeX L1 и взаимодействия с Dapps, внося свой капитал и ресурсы для получения вознаграждений. В IoTeX 2.0 владельцы устройств также могут записать IOTX, чтобы зарегистрировать свои устройства в IoTeX L1 и получить ioID, которые обеспечивают надежную привязку для участия в DePIN. Наконец, чтобы создать маховик, IoTeX L1 будет использовать DAO, где держатели токенов смогут голосовать за то, как распределяются сетевые стимулы для различных инициатив с целью стимулирования новых устройств, DePIN, Dapps и пользователей. Чем больше устройств, DePIN, Dapps и пользователей подключено, тем больше пользы IOTX будет иметь на IoTeX L1 за счет сжигания, размещения и расходования IOTX.

MSP и DIM

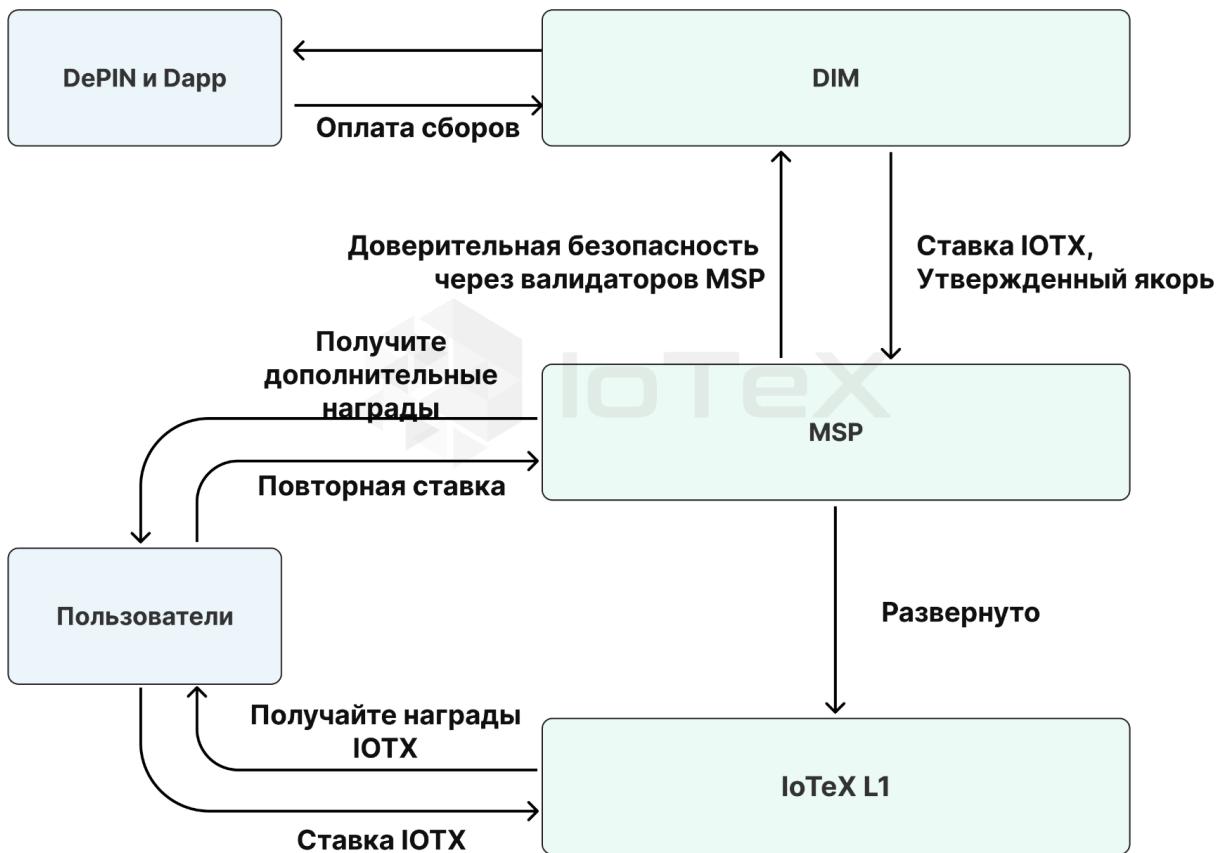


Рис 2.4: Полезность токенов IOTX в MSP и DIM

- **С точки зрения модульного пула безопасности (MSP):** IoTeX 2.0 позволит пользователям перепрофилировать свои ставки IOTX путем повторной ставки или перезакладывания их в Модульный пул безопасности (MSP), который предназначен для расширения безопасности блокчейна IoTeX L1 на DIM, которые интегрируют свои предложения с IoTeX 2.0. Используя MSP, разработчики DIM могут стимулировать участников IOTX выделять свои повторные ставки IOTX для обеспечения безопасности своих решений. Это вводит новую экономику, включающую стейкинг IOTX, где MSP будет эффективно «сдавать в аренду» безопасность и доверие DIM, которые будут необходимы для стейкинга IOTX. Это также открывает новые возможности заработка для стейкеров IOTX, которые будут получать те же базовые вознаграждения за ставку IOTX, а также дополнительные вознаграждения за повторную стейкинг своих токенов IOTX, а также потенциальные взятки от проектов DIM.
- **С точки зрения инфраструктурных модулей DePIN (DIM):** DIM должны будут сделать стейк IOTX, чтобы присоединиться к модульному пулу безопасности (MSP), получить безопасность от пула перераспределенных активов и предлагать свои услуги в поддающейся проверке форме Dapps, L2 и пользователям. DIM также могут использовать IOTX в качестве оплаты от

децентрализованных приложений, использующих их услуги, или использовать свои собственные токены. Например, поставщик долгосрочного хранилища, такой как Filecoin, или поставщик доступности данных, такой как NEAR, сделает ставку на IOTX, чтобы присоединиться к IoTeX 2.0 в качестве DIM, после чего они смогут взимать плату с Dapps за свои услуги передачи данных в своих собственных токенах. Для некоторых модулей DIM IoTeX 2.0, созданных командой IoTeX, таких как ioID и ioConnect, оплата за эти услуги будет номинирована в токенах IOTX.

- **С точки зрения DePIN Dapps и DePIN L2s:** Dapps и L2, запускаемые на технологическом стеке IoTeX 2.0, будут платить IOTX за обработку транзакций и взаимодействие со смарт-контрактами. Кроме того, Dapps и цепочки L2 могут выбирать свой собственный модульный технологический стек и платить одному или нескольким DIM за такие услуги, как подключение, хранение данных, вычисления вне сети и т. д., в токене DIM. Чтобы замкнуть цикл, большинство Dapps будут иметь свои собственные токены, которые пользователи будут приобретать и тратить для доступа к сервисам Dapps.

В дополнение к полезности токена IOTX, описанной выше, для IoTeX 2.0 также есть новые разработки, касающиеся того, как токены IOTX будут сжигаться в зависимости от использования инфраструктуры, как IOTX будет передаваться децентрализованным приложениям и разработчикам через программы стимулирования и как будут выпускаться новые IOTX, заинтересованным сторонам в будущем. Мы рассмотрим эти новые конструкции в следующих подразделах.

Эмиссия IOTX, Дефляция и Повторная Ставка

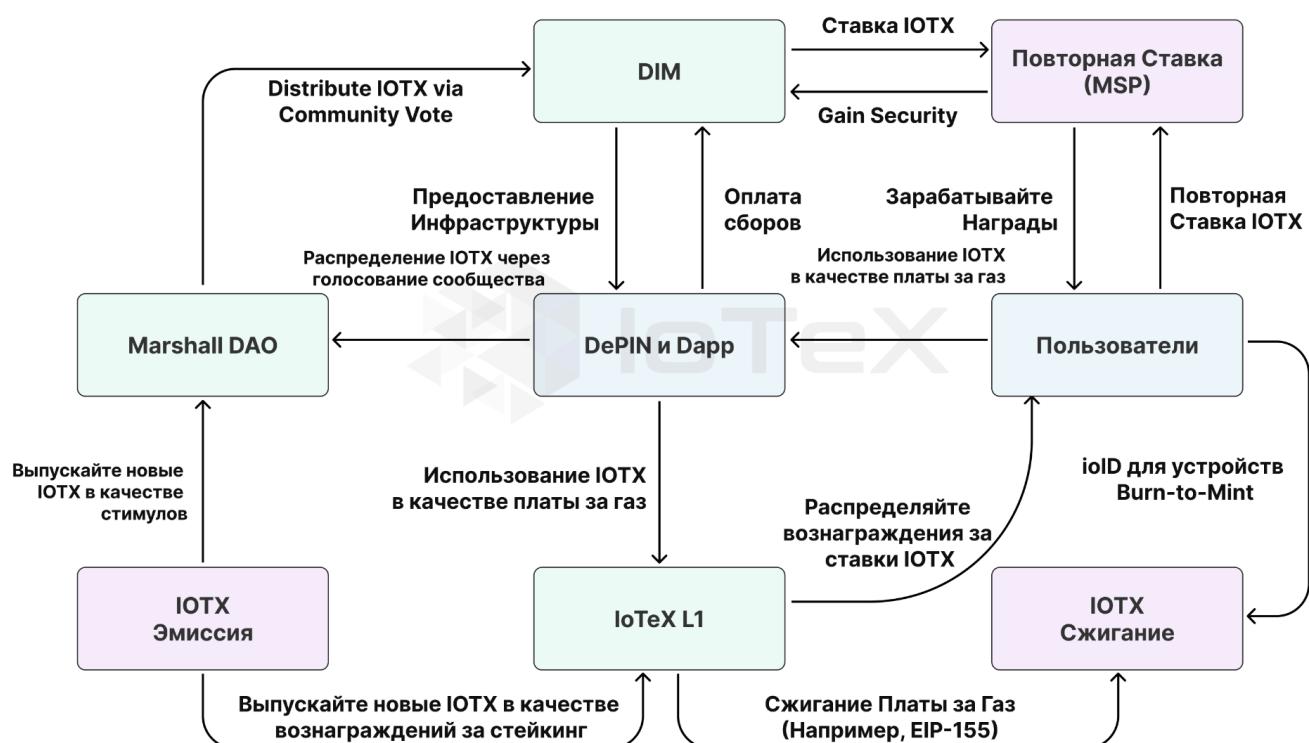


Рис 2.5: Эмиссия, дефляция и рестейкинг токенов IOTX в IoTeX 2.0.

2.3.2 Вознаграждения за инфляционные ставки

Когда в 2019 году была запущена основная сеть IoTeX, 12% от общего объема поставок IOTX (т. е. 1,2 млрд IOTX) было выделено на вознаграждения за ставки для делегатов. Владельцы токенов стейкуют IOTX, чтобы голосовать за делегатов, которые делят часть вознаграждений за стейкинг со своими избирателями. С 2019 года около 200 миллионов IOTX в год распределяются среди делегатов и избирателей в виде вознаграждений за блоки и наград за эпохи. Награды за блоки доставлялись делегатам консенсуса (т. е. 36 делегатам с наибольшим количеством голосов, имеющим право производить блоки) за каждый новый созданный блок, а награды за эпохи распределялись пропорционально между 100 делегатами с наибольшим количеством голосов каждую эпоху (т. е. каждый час). После более 4 лет работы Mainnet первоначально выделенный запас IOTX для вознаграждений за ставки приближается к полному распределению. Таким образом, инфляционные вознаграждения за ставки будут введены как часть IoTeX 2.0, чтобы стимулировать делегатов продолжать проверять сетевые транзакции и обеспечивать безопасность сети.

Вознаграждения за инфляционные ставки определяются как новые IOTX, добавленные к поставке токенов, доставленные делегатам, которые участвуют в консенсусе, и держателям токенов, которые делают ставку IOTX. По сути, это означает, что только те, кто ставит токены IOTX, получат недавно выпущенные токены IOTX, что обеспечивает более высокий коэффициент ставок IOTX и более высокую безопасность для сети IoTeX в целом. Распределение инфляционных вознаграждений за стейкинг будет следовать той же структуре, что и предыдущее распределение IOTX, выделенных на вознаграждения за стейкинг: делегаты консенсуса, производящие блоки, будут получать вознаграждения за блоки, а 100 лучших делегатов будут пропорционально делить вознаграждения за эпохи.

Хотя это новая концепция сети IoTeX, инфляционные вознаграждения за ставки встроены почти во все L1, включая Ethereum, Solana, Cosmos и другие. Например, Solana начала с уровня инфляции в 8%, который снижается на 15% каждый год. По состоянию на первый квартал 2024 года инфляция в сети Solana составляет ~5,5%. Хотя фактический процент годовой инфляции для сети IoTeX будет определяться общесетевым управлением, цель будет состоять в том, чтобы ввести умеренную инфляцию, которая обеспечит конкурентоспособные годовые вознаграждения за ставки для делегатов IoTeX L1 по сравнению с другими экосистемами блокчейнов, а также стимулировать приложения DIM и DePIN расти, сохраняя при этом стабильное предложение токенов с учетом дефляционного сжигания токенов, что подробно описано в разделе ниже.

2.3.3 Дефляционное сжигание

Чтобы сбалансировать необходимую инфляцию в криптосетях, обычно реализуется дефляционное сжигание токенов на основе использования сети для поддержания стабильного предложения токенов (например, таким шаблоном проектирования является «Равновесие сжигания и монетизации»).

Например, сеть Ethereum выдает валидаторам примерно 1700 новых ETH в день, но уравновешивает эту инфляцию дефляционным сжиганием комиссий за газ (т. е. EIP-1559), чтобы поддерживать в целом стабильное или дефляционное предложение токенов ETH с течением времени. С 2020 года сеть IoTeX использовала программу Burn-Drop для стимулирования дефляционного сжигания IOTX в зависимости от количества новых устройств, зарегистрированных в сети, в результате чего на сегодняшний день сжигается примерно 4% от общего количества или 400 миллионов IOTX. С введением IoTeX 2.0 и

прекращением программы Burn-Drop в сеть IoTeX на уровне протокола будут добавлены новые источники дефляционного сжигания на основе использования нашей модульной инфраструктуры:

- На уровне L1 IoTeX 2.0 представит сжигание комиссий за газ, аналогично EIP-1559 Ethereum. Это будет стимулировать и перераспределять ценность среди держателей токенов IOTX на основе более широкого использования IoTeX L1. Ставка IOTX для участия в управлении и голосовании за делегатов останется неизменной, сохраняя важный эффект от ставок активов, снижающих скорость токена IOTX.
- Для ioID создание новых идентификаторов устройств в цепочке потребует сжигания определенного количества IOTX, при этом скорость сжигания будет динамической в зависимости от общего количества устройств, зарегистрированных в сети IoTeX. Кроме того, в конструкцию ioID будет включен дополнительный механизм дефляционного сжигания для получения проверяемых учетных данных (VC) для DID. По аналогии: ioID похож на пустой паспорт, а VC — на штампы в паспорте, которые позволяют людям получать доступ к различным странам. В IoTeX 2.0 идентификаторы ioID будут зарегистрированы в IoTeX L1, а один или несколько виртуальных машин для устройств будут получены путем записи токенов IOTX для доступа к DIM, например, W3bstream. Этот дизайн будет перераспределять ценность среди держателей токенов IOTX на основе роста числа «оборудованных» устройств в сети IoTeX, аналогично Burn-Drop, но переработанный, чтобы лучше соответствовать модульной конструкции IoTeX 2.0.
- Для W3bstream, ioConnect и ioDDK сетевые эффекты, вызванные ростом и внедрением этих модульных продуктов Dapps и компаниями, будут способствовать дефляционному сжиганию IOTX из-за необходимости устройств напрямую взаимодействовать с каждым соответствующим DIM. Кроме того, может быть установлено периодическое сжигание токенов IOTX на основе пороговых значений принятия, определенных сообществом IoTeX, для перераспределения стоимости между держателями токенов.

Токеномика IoTeX 2.0 предназначена для вознаграждения за более широкое использование различных модульных компонентов платформы IoTeX за счет дефляционного сжигания токенов IOTX.

Первоначально это дефляционное сжигание будет уравновешивать упомянутые выше инфляционные вознаграждения за ставки, чтобы поддерживать чистое стабильное общее количество токенов, а в будущем массовое внедрение платформы IoTeX может привести к тому, что общее количество токенов IOTX станет чистым дефляционным. Чтобы стимулировать массовое внедрение, необходимое для достижения этой цели, токеномика IoTeX 2.0 будет распределять токены IOTX среди различных разработчиков через программы стимулирования роста, описанные ниже.

2.3.4 Стимулы роста

Важным столпом IoTeX 2.0 является The Marshall DAO (IIP-23) [10], децентрализованной автономной организации (DAO), которая позволит заинтересованным сторонам IoTeX вносить предложения относительно того, как распределять стимулы IOTX для развития экосистемы IoTeX, включая внедрение авторитетных проектов DePIN и финансирование общесетевых инициатив. Это создает прозрачную и меритократическую систему, в которой лучшие идеи финансируются с помощью IOTX. Первоначально Marshall DAO будет финансироваться за счет более чем 500 миллионов IOTX, которые были перепрофилированы из ассигнованного Burn-Drop, решение о которых было принято сообществом IoTeX посредством общесетевого голосования в первом квартале 2024 года. В будущем возможно

дополнительное финансирование Marshall DAO будет добавлено посредством дальнейшего общесетевого голосования для добавления вновь выпущенных IOTX в пул.

Marshall DAO использует модель управления в цепочке с депонированием голосов, что означает, что чем больше IOTX задействовано в DAO, тем больше прав голоса имеет пользователь. Это гарантирует, что решения о финансировании проектов и инициатив будут приниматься теми, кто больше всего заинтересован в долгосрочном успехе IoTeX. Владельцы токенов, делающие ставку в течение как минимум 91 дня, получают veIOTX, непередаваемый сетевой токен, который можно использовать для предложения и голосования по распределению финансирования с помощью датчиков, которые представляют конкретные предложения. Это означает, что долгосрочные участники могут голосовать, используя свой veIOTX, чтобы определить, как IOTX из DAO финансирует различные проекты, включая, помимо прочего, повышение ликвидности для торговых пар DEX на IoTeX, спонсирование проектов DePIN на ранних стадиях через панели запуска, ускорение проектов DePIN через двойной майнинг, выдача грантов на общественные блага и общесетевые инструменты и многое другое.

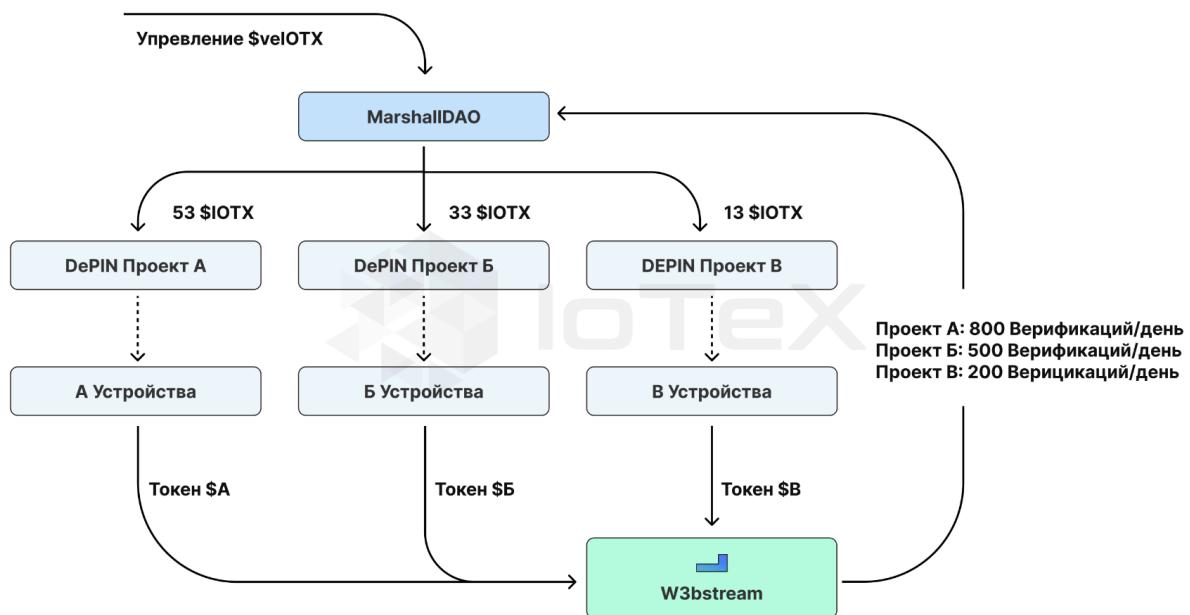


Рис 2.6: Модель управления Marshall DAO

2.4 Общественные блага

В дополнение к возможностям, предоставляемым блокчейном IoTeX и DIM, важной частью IoTeX 2.0 также являются общественные блага, которые решают многие краткосрочные и среднесрочные проблемы проектов DePIN. Эти общественные блага обеспечивают осведомленность, удобство использования и ликвидность проектов DePIN посредством простой интеграции, а также предоставляют сообществу IoTeX возможность контролировать более широкую индустрию DePIN, а также глубоко погружаться в конкретные проекты.

- DePINScan [23] является общеотраслевым исследователем сектора DePIN. Он предназначен для того, чтобы дать пользователям, майнерам и инвесторам DePIN возможность отслеживать рост

проектов DePIN и обнаруживать проекты на ранней стадии. Он предоставляет в режиме реального времени количество устройств и профили проектов, служа способом обнаружения проектов и получения цен, объема и рыночной капитализации активов DePIN в реальном времени.

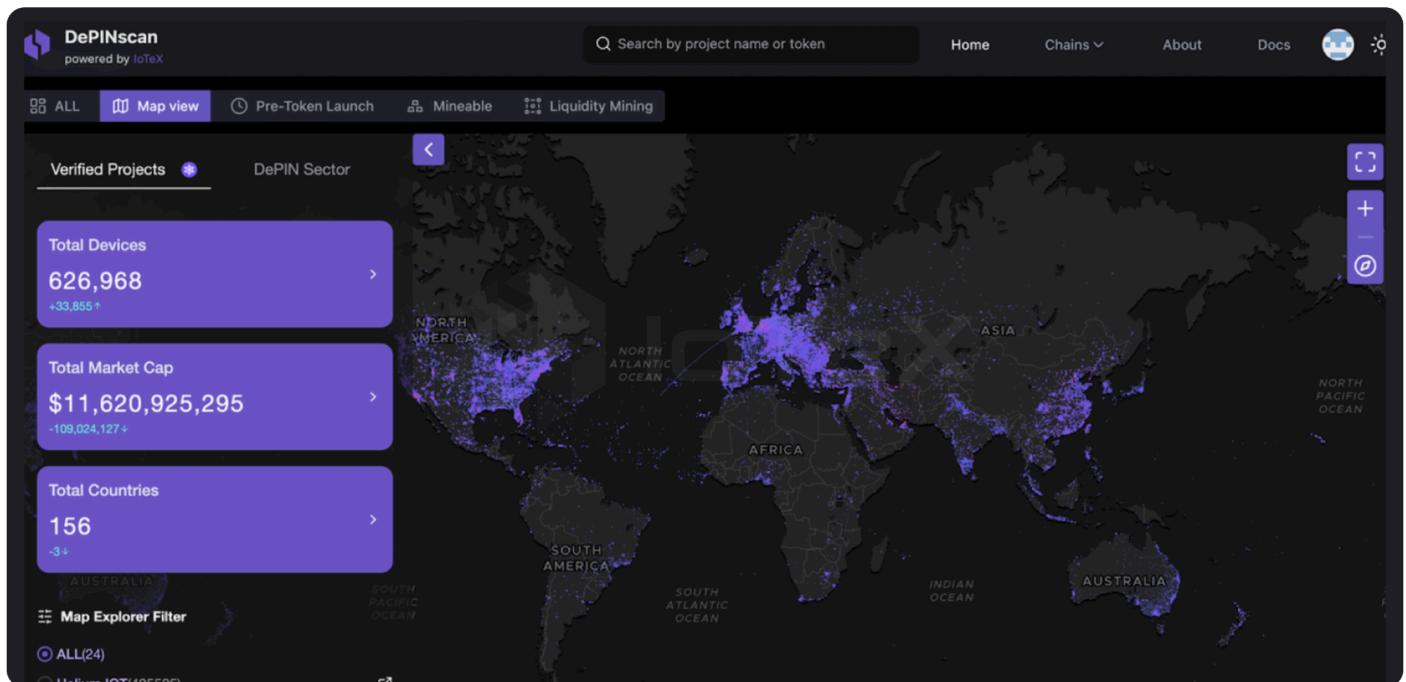


Рис 2.7: DePINScan Explorer

- DePIN Liquidity Hub [21] — это DEX типа Uniswap v3 с концентрированной ликвидностью, который обеспечивает автоматизированных менеджеров диапазона (маркет-мейкеров) и позволяет пользователям торговать токенами DePIN (см. Рисунок 2.8). Ликвидность токенов очень важна для любого криптообъекта, особенно для DePIN, поскольку они активно используют свои токены в качестве механизма стимулирования для развития своей сети. К сожалению, многие DePIN на ранних стадиях с трудом создают и поддерживают здоровый уровень ликвидности в цепочке. Для поддержки новых проектов IoTeX запустил DePIN Liquidity Hub [24] для увеличения ликвидности проектов DePIN, которые могут переносить свои токены из любой другой цепочки L1 в IoTeX L1, создавать двусторонний пул ликвидности на различных децентрализованных биржах (DEX) и проводить кампании по добыче ликвидности, чтобы стимулировать инвесторов к загрузке своей сети ликвидность.

	Name	Symbol	Liquidity ↓	Volume (24hrs)	Price	Price Change (24hrs)
1	Wrapped iOTX	WIOTX	\$13,948,780	\$95,531	\$0.0463	+4.34%
2	WEN	WEN	\$1,473,287	\$5,274	\$1.03	+2.86%
3	Dimo	DIMO	\$146,790	\$1,812	\$0.47	+4.00%
4	WiFi Map	WIFI	\$56,501	\$3,569	\$0.13	+24.56%
5	Geodnet	GEOD	\$39,699	\$5,038	\$0.0953	-11.88%
6	Wicrypt Network...	WNT	\$35,731	\$1,005	\$0.31	+3.52%
7	CRUST	CRU	\$20,337	\$0	\$1.59	+4.34%
8	Drop Wireless I...	DWIN	\$19,132	\$142.07	\$0.0722	+7.61%
9	XNet Mobile	XNET	\$16,383	\$302.29	\$0.0366	-2.77%
10	DRIFE	DRF	\$12,050	\$1,229	\$0.0024	-3.81%

Рис 2.8: Центр ликвидности DePIN

В дополнение к вышеперечисленным общественным благам, которые уже доступны разработчикам, есть и другие, которые будут созданы командой IoTeX, а также глобальными разработчиками в ходе разработки IoTeX 2.0. Примерами могут служить стартовая площадка для проектов DePIN, позволяющая донести свои проекты до страстных инвесторов, рынки устройств, предоставляющие майнерам оборудование, ориентированное на DePIN, а также инструменты управления, обеспечивающие децентрализованное голосование за проекты DePIN. Благодаря тому, что общественные блага легко доступны для строителей, IoTeX 2.0 предоставит проектам полный набор возможностей, которые сделают запуск и развитие проекта DePIN проще, чем когда-либо.

2.5 Поддержка разработчиков на протяжении всего жизненного цикла проекта

IoTeX 2.0 предлагает полный спектр инфраструктуры, инструментов и общедоступных ресурсов, регулируемых меритократической токеномикой. Они предназначены для помощи разработчикам DePIN на каждом этапе жизненного цикла проекта.

- На начальных этапах проекты DePIN в основном сосредоточены на развитии своего технологического стека и повышении осведомленности о своих проектах. Чтобы облегчить это, IoTeX 2.0 предоставляет общедоступные ресурсы, такие как DePINscan и Liquidity Hub, для привлечения внимания, ликвидности и пользователей, как показано на рисунке 2.9.

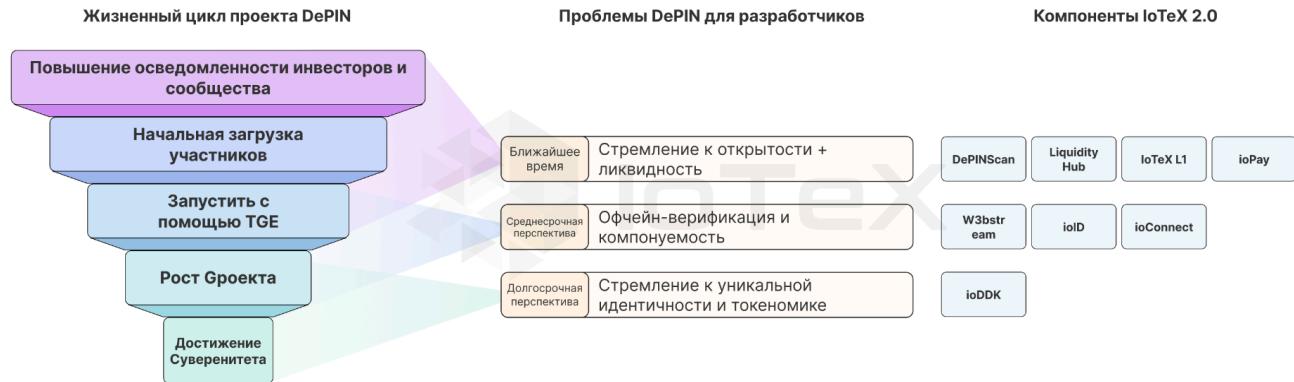


Рис 2.9: Поддержка разработчиков на протяжении всего жизненного цикла проекта DePIN

- По мере развития проектов растет спрос на более совершенную и адаптированную инфраструктуру, особенно по мере того, как проекты децентрализуют свои технологические стеки и стремятся к большей масштабируемости. Чтобы удовлетворить эти потребности, IoTeX 2.0 предлагает такую инфраструктуру, как W3bstream, ioID и ioConnect, чтобы предоставить передовые технологии для разработчиков DePIN.
- В долгосрочной перспективе проекты DePIN должны создавать и расширять свои собственные суверенные сети спроса и предложения. IoTeX 2.0 продолжает поддерживать эти проекты даже на более поздних стадиях, позволяя им запускать собственный L2 через ioDDK.

2.6 Будущее

С IoTeX 2.0 мы отправляемся в новый путь, чтобы оснастить устройства по всему миру всеми инструментами, необходимыми для обеспечения их независимости, сбора данных из реального мира для создания инновационных Dapps и предоставления пользователям возможности монетизировать уникальные услуги и данные своих устройств. Продолжающаяся конвергенция искусственного интеллекта, блокчейна и интеллектуальных устройств теперь вызывает технологическую революцию, которая фундаментально изменит то, как устроен наш мир. Хотя эти технологии со временем развивались независимо, они все больше переплетаются и объединяются в новый продуктивный актив: сети DePIN, состоящие из доверенных и принадлежащих пользователям устройств.

Умные устройства будут предоставлять услуги и генерировать данные. Блокчейн добавит доверия и проверяемости этим данным и услугам. И, наконец, ИИ будет извлекать пользу из данных и автоматизировать эти услуги. То, что всего несколько лет назад казалось научной фантастикой, сегодня становится реальностью. В ближайшем будущем развивающаяся машинная экономика будет опираться на эту технологическую троицу и станет самой ценной отраслью в мире. Благодаря блокчейну у нас будет возможность запрограммировать эту новую машинную экономику с помощью проверенных технологий, которые не только приносят пользу обществу, но также обеспечивают ценность и равенство для обычных людей. Возможности безграничны, но некоторые из самых захватывающих возможностей:

- Коллективный разум и искусственный интеллект:** IoTeX станет крупнейшим концентратором устройств и, следовательно, реальным концентратором данных для агрегирования информации в реальном времени. Перехватывая потоки данных с устройств и проверяя события реального мира в сети, мы можем использовать коллективный разум масс, чтобы совершить революцию в отдельных отраслях, таких как связь, умный город и возобновляемые источники энергии. Еще большая возможность заключается в использовании ИИ для анализа межотраслевых отношений и извлечения реляционной информации, которая может улучшить наше понимание мира. IoTeX 2.0 станет децентрализованной платформой, которая записывает историю реального мира глазами наших интеллектуальных устройств, позволяя нам понять наше прошлое и оптимизировать наше будущее.
- Экономика автономной машины:** В настоящее время интеллектуальные устройства не только генерируют ценные данные, но и развиваются, чтобы предоставлять людям надежные и ценные услуги. Автономные такси обеспечивают первые беспилотные поездки, спутники обеспечивают связь с людьми по всему миру, на складах используются роботы, которые превосходят ловкость людей, а солнечная и ветровая энергия производится с помощью устройств, использующих возобновляемые источники энергии следующего поколения. Оркестрацию этих устройств предоставления услуг лучше всего осуществлять с помощью блокчейнов и интеллектуального искусственного интеллекта. Мы предвидим будущее, в котором IoTeX сможет позволить системам искусственного интеллекта отслеживать и управлять ресурсами Земли с беспрецедентной точностью и полным доверием.
- Торговые площадки цифровых ресурсов:** В то время как некоторые DePIN фокусируют данные и услуги на оборудовании, зависящем от местоположения, другие агрегируют цифровые ресурсы с оборудования, не зависящего от местоположения. Они могут включать в себя цифровое хранилище, вычисления с помощью процессоров и графических процессоров, пропускную способность и другие цифровые ресурсы, традиционно предлагаемые облачными конгломератами. В эпоху, когда «данные — это новое золото», а «вычисления — это новая нефть», IoTeX 2.0 позволит размещать ценные цифровые ресурсы на рынках, где каждый сможет обмениваться ими в одноранговой сети с другими людьми по всему миру.
- Децентрализованное управление и принятие решений:** За счет безопасной и прозрачной интеграции данных реального мира в блокчейны IoTeX 2.0 может помочь создать основу для децентрализованного принятия решений с использованием поддающихся проверке фактов о событиях в реальном мире. Поскольку люди коллективно определяют процессы посредством децентрализованного управления, мы можем использовать неизменяемые смарт-контракты и безопасные устройства для надежного управления основными аспектами жизни общества. IoTeX 2.0 предоставляет каждому возможность поделиться своим опытом и участвовать в открытом управлении новым миром.

Глава 3

Модульный пул безопасности (MSP) — единый доверенный уровень для модулей инфраструктуры DePIN.

3.1 Проблема

DePIN имеет комплексный технологический стек, который включает в себя как элементы цепочки, такие как DePIN L2 для конкретных сценариев, так и элементы вне цепочки, такие как потоки данных, оракулы, процессы, проверка, хранение и автоматизация. Эта сложная структура требует большего количества модулей и сборщиков для создания собственных децентрализованных архитектур доверия с нуля. Задачи могут включать в себя разработку токена для ставок, создание ликвидности, привлечение стейкеров, набор валидаторов и получение признания на рынке, что приводит к потенциальной фрагментации безопасности и децентрализации.

Для создания единого и сквозного доверия децентрализованным образом крайне важно обеспечить, чтобы каждая часть была максимально безопасной и децентрализованной, следуя принципу самого слабого звена. Поскольку разработчики продолжают разрабатывать инфраструктурные модули DePIN (DIM), сохранение целостности безопасности и децентрализации без фрагментации является приоритетом. Такой подход позволяет быстро интегрировать DIM в существующий технологический стек для использования в проектах DePIN.

Модульный пул безопасности (MSP) обеспечивает единый уровень доверия, поддерживающий DIM. Он собирает обеспечение ставок от различных установленных L1/L2 и может предоставлять их обеспечение новым DIM в обмен на компенсацию. Эта система позволяет новым модулям инфраструктуры получать выгоду от безопасности базовых уровней L1/L2 без создания собственной инфраструктуры безопасности. Например, новый DIM может присоединиться к MSP посредством предложения по управлению. В случае одобрения DIM примет меры безопасности и децентрализации уровней L1/L2. Стейкеры, которые поддерживают определенный DIM, направляя свои доли в MSP, могут получить компенсацию в виде токенов сети DIM.

3.2 Открытый Рынок для безопасности и доверия

MSP уверенно представляет собой механизм открытого рынка, мастерски управляя поставками и потреблением своей объединенной безопасности заинтересованными сторонами и DIM. MSP объединит безопасность, ориентированную на DePIN, во всех DIM, вместо того, чтобы фрагментировать безопасность между многочисленными DIM. Конкретно в MSP есть три типа участников:

- **Разработчики DIM** создают DIM, такие как DePIN L2 для конкретных сценариев, автономные сервисы, такие как потоковая передача данных, Oracle, обработка (например, общего назначения, на основе ZKP, на основе TEE и т. д.), хранение данных, автоматизация (например,

автоматическая выплата, цена каналы), модули идентификации и аутентификации. Разработчики DIM должны стимулировать участников распределять свои активы по своим модулям. MSP предоставит механизм взяток, чтобы гарантировать, что заинтересованные стороны получают достаточную мотивацию от DIM.

- **Стейкеры** — это участники сети, которые делегируют свои активы из хорошо зарекомендовавших себя блокчейнов одному или нескольким валидаторам. Они способствуют сетевой безопасности без необходимости запуска узла самостоятельно. В обмен на свое делегирование они получают часть гонораров и вознаграждений сети. Стратегическое распределение определяет модули, заслуживающие дополнительной объединенной безопасности, с учетом возможности большего сокращения. Стейкеры согласились, позволив MSP прилагать дополнительные условия сокращения их активов, повышая экономическую безопасность. Здесь важно отметить, что инфраструктура MSP, которую мы создаем, имеет открытый исходный код и сможет использовать безопасность всех основных блокчейнов, включая Bitcoin, Ethereum и IoTeX. Хотя эта идея все еще находится на ранней стадии, мы потенциально могли бы сотрудничать с такими протоколами, как Eigenlayer или Babylon, чтобы облегчить межсетевое взаимодействие.
- **Валидаторы** предоставляют постоянно работающий набор узлов, доступных разработчикам DIM, которые будут напрямую обслуживать проекты DePIN.

Реализация MSP должна включать следующие ключевые принципы:

- **Открытый вход и выход:** Стейкеры и DIM должны иметь свободу входа и выхода из рынка без каких-либо ограничений. Это обеспечивает конкурентоспособные цены, отражающие истинную ценность услуг.
- **Сетевые эффекты:** По мере увеличения числа участников каждый участник находит рынок более ценным. Эта петля положительной обратной связи может привлечь на рынок больше покупателей и продавцов.
- **Децентрализация:** Рынок не контролируется центральной властью. Вместо этого он действует на основе законов спроса и предложения.

3.3 Архитектура

Архитектура модульного пула безопасности (MSP) предназначена для обеспечения оптимизированного и безопасного процесса создания новых сетей, в частности DePIN и DIM, на основе унаследованной безопасности от существующих систем ставок на хорошо зарекомендовавших себя блокчейнах L1. Вот подробное описание того, как работает MSP:

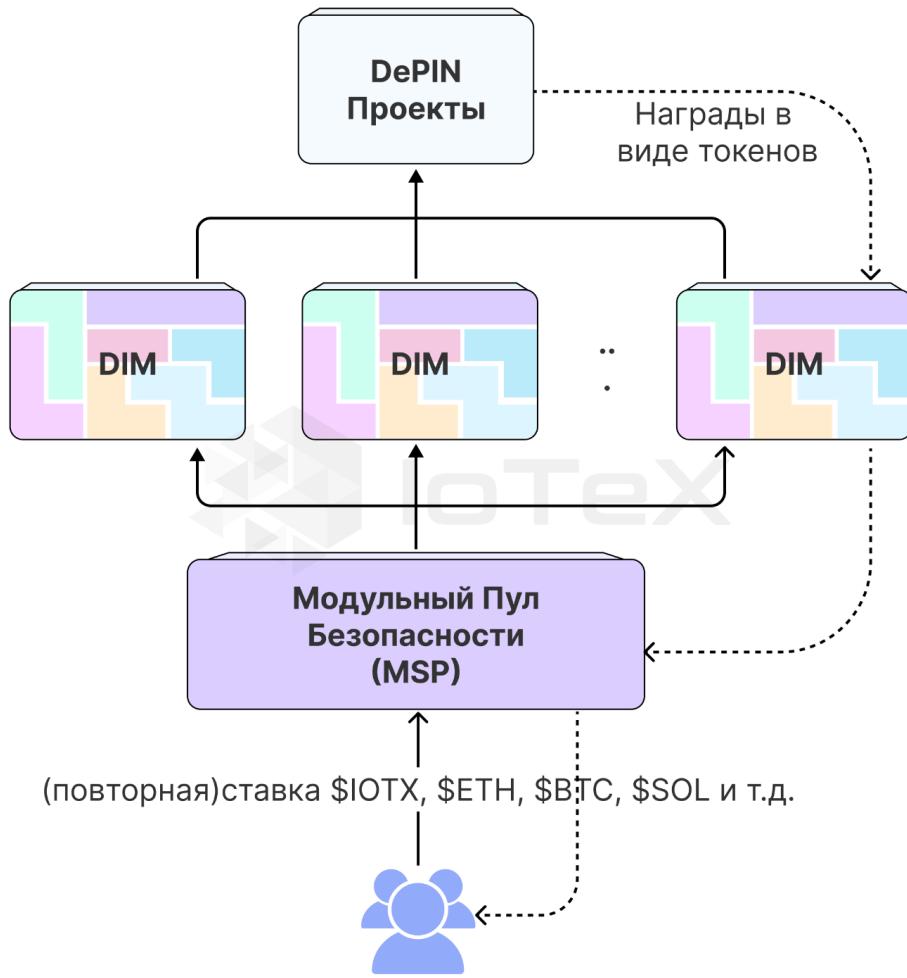


Рис 3.1: Архитектура модульного пула безопасности (MSP)

- Стейкеры делегируют активы:** Стейкеры, являющиеся участниками существующих L1, таких как Bitcoin, Ethereum и IoTeX, делегируют свои активы MSP. Тем самым они способствуют безопасности сетей на базе MSP.
- Стейкеры выбирают валидаторов:** В сети MSP заинтересованные лица имеют возможность выбирать валидаторов из пула опций, предоставляемых сетями DIM, с которыми они связаны. Валидаторы отвечают за работу узлов для защиты сети и проверки транзакций.
- Валидаторы запускают узлы:** после выбора стейкерами валидаторы управляем узлами в сети MSP. Эти узлы играют решающую роль в обеспечении целостности и безопасности транзакций в сети.
- Разработчики DIM создают сети:** Тем временем разработчики DIM работают над развитием своих сетей.
- Стимулирование стейкеров:** Разработчики DIM стимулируют участников распределять свои активы по модулям в сети MSP. Это стимулирование может принимать различные формы, такие как вознаграждения, сетевые токены или другие преимущества. MSP обеспечивает достаточную мотивацию заинтересованных сторон с помощью таких механизмов, как механизм взяток, для поощрения участия.

6. **Распределение ставок безопасности:** MSP играет ключевую роль в распределении безопасности ставок между новыми DIM. Используя объединенную безопасность, полученную от установленных L1/L2, а также участие стейкеров и валидаторов, MSP обеспечивает безопасность и децентрализацию этих новых сетей.

В целом эта архитектура обеспечивает более эффективный и безопасный процесс запуска новых модулей DIM. Используя безопасность существующих уровней L1/L2 и интегрируя различных заинтересованных сторон, таких как заинтересованные стороны, валидаторы и разработчики, MSP создает надежную экосистему, способствующую инновациям и росту децентрализованных трастовых архитектур. Такой подход не только экономит время и ресурсы для новых разработчиков сетей, но также повышает общую безопасность и устойчивость экосистемы DePIN.

Глава 4

W3bstream — децентрализованная сеть мультипруверов для проверки DePIN

Приложения DePIN обычно содержат специальный сценарий обработки данных (например, вывод искусственного интеллекта, вычисление оценки, обнаружение устройства, обнаружение мошеннических устройств и т. д.), который способен извлекать ценную информацию на основе данных, собранных устройствами DePIN из реального мира. Полученные данные затем используются для запуска смарт-контрактов для действий, связанных с токенами. Из-за большого объема машинных данных их долгосрочная обработка и хранение в цепочке является непомерно высокой и неэффективной. В результате оффчайн-вычисления стали многообещающим решением проблем масштабируемости DePIN.

4.1 Архитектура W3bstream

W3bstream — это управляемая блокчейном сеть с несколькими проверочными устройствами, разработанная IoTeX, целью которой является использование возможностей гетерогенных проверочных устройств глобального масштаба для ускорения развития новых приложений DePIN. Вкратце, W3bstream — это децентрализованная автономная вычислительная сеть, состоящая из разнородных узлов, выполняющих проверяемые вычисления, как показано на рисунке ниже. Доказательства, генерированные W3bstream, проверяются внутрисетевыми верификаторами, а затем используются DePIN Dapps.

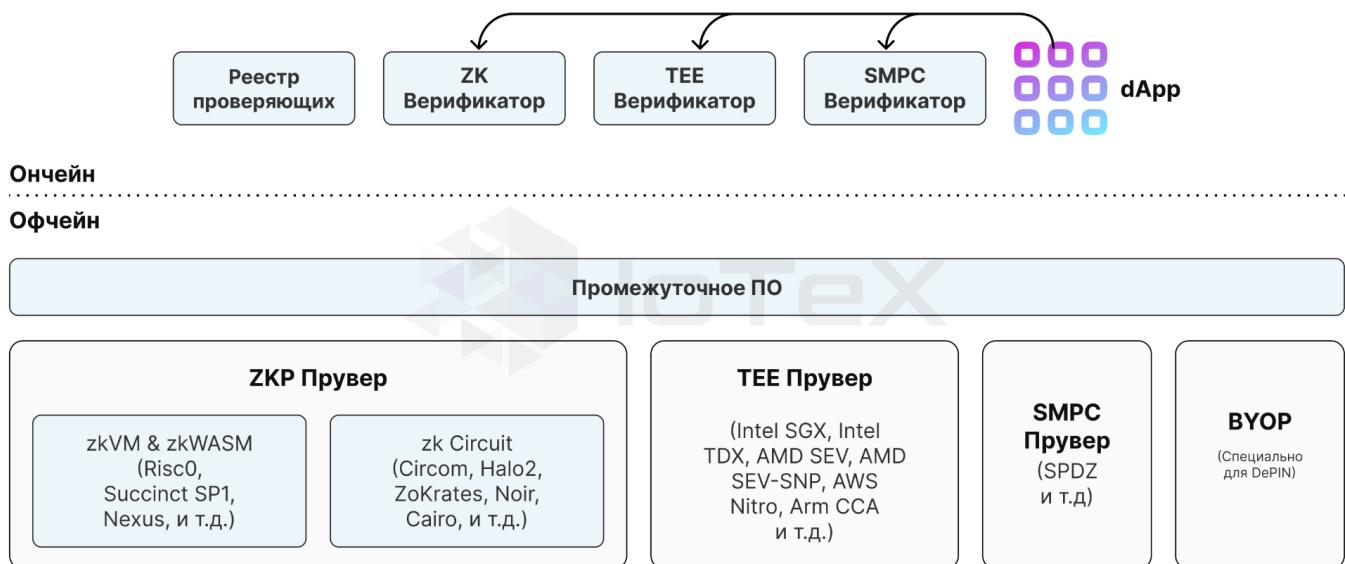


Рис 4.1: Коротко о W3bstream

4.1.1 Четыре типа пруверов

В прошлом был разработан ряд методов для подтверждения целостности обработки данных и обеспечения публичной проверки, включая доказательства с нулевым разглашением (ZKP), доверенные среды выполнения (TEE), безопасные многосторонние вычисления (SMPC). Эти технологии основаны на различных предположениях о безопасности и имеют разные последствия на практике. W3bstream может использовать четыре категории проверяющих устройств для реализации проверяемых вычислений для приложений DePIN, а именно проверяющее устройство с доказательством с нулевым разглашением (ZKP), проверочное средство доверенной среды выполнения (TEE), проверяющее устройство для безопасных многосторонних вычислений (SMPC) и собственное проверяющее устройство (BYOP) через хорошо продуманный уровень промежуточного программного обеспечения.

- **ZKP Prover:** ZKP позволяет одной стороне (т. е. доказывающий) доказать другой стороне (т. е. доказывающему), что данное утверждение верно, без раскрытия дополнительной информации, помимо того факта, что утверждение верно. ZKP должны удовлетворять формальным требованиям *полноты, надёжности, и с нулевым разглашением*, что позволяет создавать надежные приложения. На практике средство доказательства ZKP может быть реализовано с использованием либо виртуальной машины общего назначения с нулевым разглашением (zkVM), либо настраиваемой системы ограничений (т. е. схемы). Типичная системная архитектура приложения на основе SNARK, построенного на zkVM (соответственно, настроенной схеме), показана ниже.



Рис. 4.2: Системная архитектура приложения на основе SNARK, построенного на zkVM

В то время как средство доказательства общего назначения на основе zkVM инкапсулирует сложность создания ZKP и позволяет разработчикам кодировать свою бизнес-логику с использованием языков программирования высокого уровня, таких как C/C++, Rust и т. д., для создания средства доказательства ZKP с настраиваемой схемой требуется более глубокое понимание рабочего процесса создания ZKP, а также предметно-ориентированных языков (DSL). Однако прувер ZKP с настроенной схемой обычно может обеспечить более высокую производительность по сравнению с прувером на базе zkVM. Средство проверки ZKP позволяет разработчикам DePIN использовать мощную технологию ZKP для проведения надежных вычислений вне сети. W3bstream постепенно будет поддерживать ведущие проекты zkVM/zkWASM (например, Risc0 [28], Succinct SP1 [29], Nexus [30], zkWASM [31] и т. д.), а также

популярные DSL (например, Circom [32], Halo2 [33], ZoKrates [34], Noir [35], Cairo [36] и т. д.) для создания индивидуальных схем zk.



Рис. 4.3: Системная архитектура приложения на основе SNARK, построенного по индивидуальной схеме.

- **TEE Prover:** Согласно определению Консорциума конфиденциальных вычислений (CCC), доверенная среда выполнения (TEE) — это выделенная аппаратная (и программная) среда, которая обеспечивает уровень гарантии следующих трех свойств: 1) **Конфиденциальность данных:** Неавторизованные объекты не могут просматривать данные, пока они используются в TEE; 2) **Целостность данных:** Неавторизованные объекты не могут добавлять, удалять или изменять данные, пока они используются в TEE; и 3) **Целостность кода:** Неавторизованные объекты не могут добавлять, удалять или изменять код, исполняемый в TEE. Эти важные свойства безопасности обеспечивают конфиденциальность и целостность как данных, так и программы, тем самым позволяя удаленной стороне доверять результатам вычислений на аппаратной платформе с поддержкой TEE (например, Intel SGX, AMD-SEV, Arm CCA, AWS Nitro, NVIDIA H100, и т. д.). Системы на базе TEE обеспечивают безопасность аппаратного обеспечения, и пользователи должны быть уверены, что оборудование не было взломано или сломано незамеченным образом. Ниже показана типичная системная архитектура приложения на основе TEE, которая основана на механизме удаленной аттестации аппаратной платформы на основе TEE. Удаленная аттестация — это процесс, посредством которого одна сторона (т. е. проверяющая сторона) оценивает надежность потенциально недоверенного удаленного узла (т. е. аттестатора). Цель аттестации — позволить проверяющему получить уверенность в надежности аттестатора путем получения достоверного, точного и своевременного отчета о состоянии программного обеспечения и данных аттестатора. С помощью службы аттестации можно получить отчет о аттестации, содержащий криптографические измерения среды выполнения (т. е. аппаратного обеспечения, программного обеспечения, пользовательских данных и т. д.).

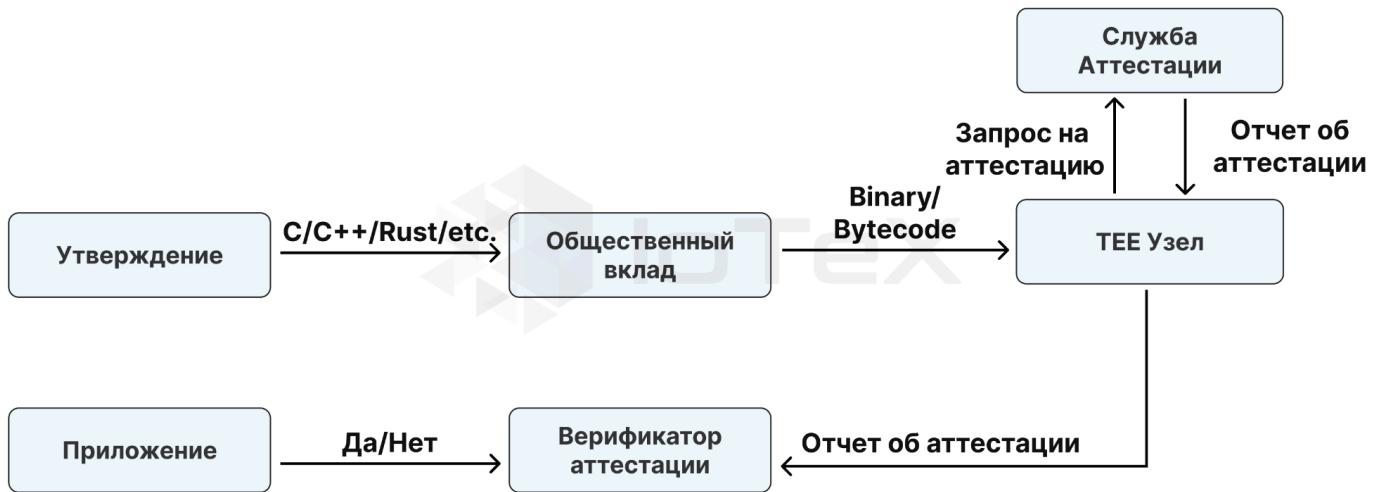


Рис. 4.4: Системная архитектура приложения на базе ТЕЕ

Средство проверки ТЕЕ можно реализовать, следуя общему процессу разработки определенного поставщика ТЕЕ. Средство проверки ТЕЕ помогает разработчикам DePIN использовать современную технологию конфиденциальных вычислений для выполнения автономных вычислений с сохранением конфиденциальности. W3bstream будет постепенно поддерживать поток разработки ведущих аппаратных платформ на базе ТЕЕ, таких как Intel SGX [37], Intel TDX [38], AMD SEV [39], AMD SEV-SNP [40], AWS Nitro [41], Arm CCA [42] и т. д.

- **SMPC Prover:** MPC представляет собой набор методов для совместных вычислений с сохранением конфиденциальности над распределенными данными и не раскрывает ничего, кроме результата вычислений. Учитывая различные предположения безопасности и модели угроз (например, получистные злоумышленники, злонамеренные злоумышленники, скрытые злоумышленники), протокол SMPC должен удовлетворять как минимум трем свойствам, а именно: **конфиденциальность входа**, **правильность** и **независимость входов**. Ниже показана типичная системная архитектура приложения на основе SMPC, построенного на модели предварительной обработки.

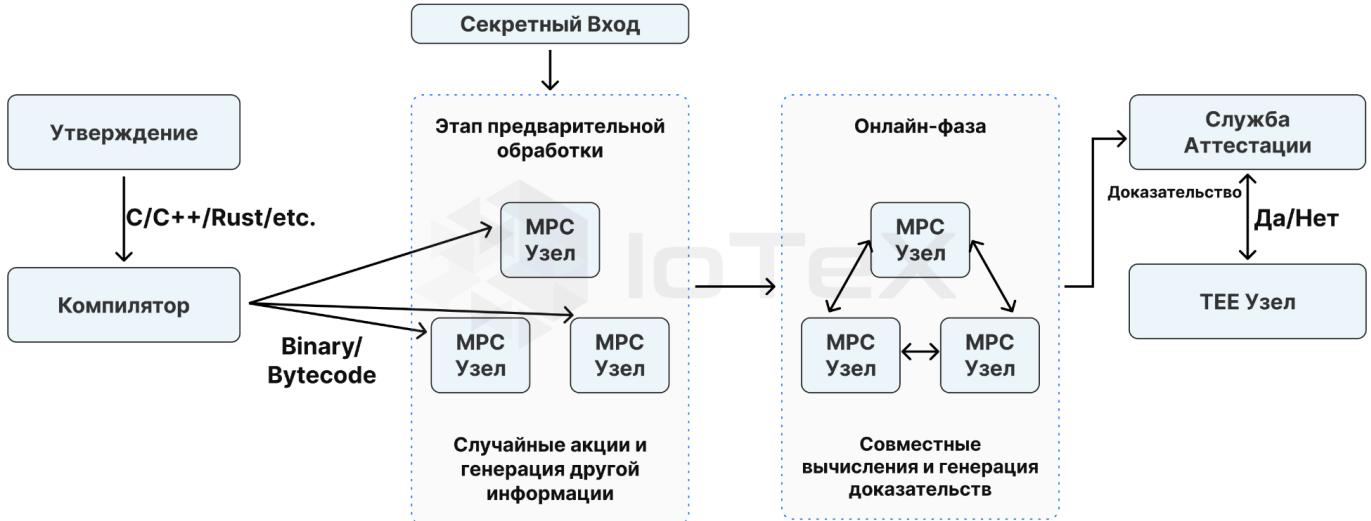


Рис. 4.5: Системная архитектура приложения на базе SMPC

Средство проверки SMPC можно реализовать, следуя общему процессу разработки конкретного протокола SMPC (например, SPDZ). Однако эффективное достижение публичной верифицируемости по-прежнему остается постоянным направлением исследований. Средство проверки SMPC позволяет разработчикам DePIN использовать несколько узлов в сети для проведения совместных распределенных вычислений вне сети с сохранением конфиденциальности.

- **Bring Your Own Prover (BYOP):** BYOP предлагает большую гибкость разработчикам DePIN, которые развертывают оптимизированные средства проверки, адаптированные к конкретным проектам DePIN, или изучают новые эффективные методы проверяемых вычислений в контексте DePIN.

4.1.2 Наши собственные инновации в области ZKP

Мультискалярное умножение (MSM) является одним из основных компонентов многих систем доказательства с нулевым разглашением и основным узким местом производительности для генерации доказательств в этих схемах. Одной из основных стратегий ускорения MSM является использование предварительных вычислений. В этом направлении было предложено несколько алгоритмов (например, Pippenger [11, 12] и BGMW [13]) и их вариантов. В нашем недавнем исследовании [15] мы возвращаемся к недавнему методу расчета MSM на основе предварительных вычислений, предложенному Луо, Фу и Гонгом на конференции CHES 2023 [14] и обобщаем их подход. В частности, мы представили общую конструкцию оптимальных ведер. Это улучшение приводит к повышению производительности примерно на 15–40 %, что подтверждается как теоретическим анализом, так и экспериментами. Мы также внедрили запись с возможностью сегментирования с использованием быстрых эндоморфизмов на эллиптических кривых $j = 0$ для деления требуемого объема памяти на 3 практически без потери производительности по сравнению с нашим уже оптимизированным алгоритмом LFG.

4.2 Рабочий процесс W3bstream

4.2.1 Регистрация и управление пруверами

Подключение устройства, которое проверяет, основано на ioID и следует процессу, описанному в разделе 5.2.2 — Регистрация и привязка ioID. Контракт на управление автопарком в сети отвечает за планирование задач и отслеживание жизненного цикла всех проверяющих узлов. Каждый проверяющий узел может находиться в статусе «Занят», «Не Активен» или «Не в сети», и статус узла будет постоянно обновляться в контракте на управление автопарком. Обозреватель W3bstream можно использовать для проверки состояния всех узлов проверки.

4.2.2 Рабочий процесс

В модульной инфраструктуре DePIN W3bstream представляет собой реализацию уровня автономных вычислений (OCCL) с несколькими проверочными устройствами, как описано в разделе 4.1. Webstream — это децентрализованный гетерогенный пул проверяющих, который способен выполнять специфичную для проекта бизнес-логику данных, хранящихся на уровне доступности данных (DAL), и генерировать доказательства достоверности (например, доказательства с нулевым разглашением, отчеты об аттестации и т. д.) вычисления выполнены. W3bstream работает как компонент вычислений без сохранения состояния в модульной инфраструктуре DePIN и следует рабочему процессу OCCL высокого уровня, как показано на рисунке ниже.



Рис. 4.5: Высокоуровневый рабочий процесс уровня оффчайн вычислений.

1. Координационный узел в оффчайн-вычислениях уровень извлекает данные из уровня доступности данных на основе конфигурации проекта DePIN;
2. Узел-координатор передает данные на простаивающий узел проверки или выбранный набор простаивающих узлов на уровне автономных вычислений;

3. Узел(узлы) проверяющего устройства выполняет вычисления, указанные в проекте DePIN, и генерирует результат вычисления и соответствующее доказательство достоверности;
4. Результат вычисления и подтверждение достоверности возвращаются в узел-координатор;
5. Узел-координатор отправляет результат вычисления и подтверждение действительности в смарт-контракт для дальнейшей обработки.

Как только доказательство будет успешно проверено в цепочке, результату вычисления можно будет доверять и использовать dApp проекта DePIN.

4.3 Проверка DePIN и искусственный интеллект вне сети

Комплексный набор средств проверки, доступный в W3bstream, позволяет разработчику доказывать целостность автономных вычислений в блокчейне уровня 1 для широкого спектра приложений DePIN. В частности, разработчик может выбрать наиболее подходящую проверяемую методику вычислений для конкретного приложения.

4.3.1 Проверка DePIN

Как отметил Гай Вуллет из a16z [43], успех DePIN зависит от решения ключевой проблемы: обеспечения надежной проверки географически рассредоточенных сервисных узлов без необходимости использования центрального органа власти. Текущую технологию проверки DePIN можно грубо разделить на три категории [44]: подход, основанный на доверенном оборудовании, статистический подход и подход, основанный на подтверждении достоверности. Каждый подход к проверке имеет свои плюсы и минусы, и на практике может потребоваться комбинация нескольких подходов. W3bstream помогает различным проектам DePIN развертывать и впоследствии обновлять алгоритм проверки на платформе. Эти алгоритмы проверки могут быть написаны на языках программирования высокого уровня, таких как Rust, Golang, C++ и т. д. Используя один из средств проверки, предоставленных в W3bstream, можно гарантировать надежность алгоритмов проверки DePIN.

4.3.2 ИИ вне блокчейна

Приложения DePIN открывают новые возможности для обучения ИИ и получения выводов в различных отраслях промышленности. С одной стороны, приложения DePIN способны надежно передавать огромные объемы реальных данных в Web3, что может значительно повысить точность моделей ИИ. С другой стороны, приложения DePIN могут эффективно организовывать вычислительные ресурсы и ресурсы хранения для обучения и вывода ИИ в глобальном масштабе. Однако приложения искусственного интеллекта часто требуют больших вычислительных ресурсов и создают серьезные проблемы при развертывании в сети.

W3bstream позволяет разработчику проводить вычисления искусственного интеллекта вне сети и одновременно обеспечивает надежность процесса вычислений. Хотя доказательства с нулевым разглашением способны обеспечить надежную интеграционную защиту для вычислений вне сети, применение доказательств с нулевым разглашением для ИИ (например, ZKML) может легко повлечь за собой накладные расходы в 10 000–100 000 раз по сравнению с непроверяемыми вычислениями ИИ [45]. Вместо использования средства проверки ZKP разработчик может переключиться на более эффективное средство проверки TEE для вычислений ИИ вне цепочки в W3bstream. Наша первая

работа [7, 8], построенная на платформе Arm Veracruz и анклаве AWS Nitro, показала очень многообещающие результаты.

Глава 5

ioID — унифицированная система идентификации для DePIN

Приложения DePIN включают в себя обширные внутрисетевые (т. е. размещение ставок, передачу активов, кредитование и т. д.) и оффчайновые (т. е. межмашинные и межмашинные) взаимодействия между различными участниками системы. Уровень идентификации в модульной инфраструктуре DePIN является важным компонентом для управления взаимоотношениями различных объектов и обеспечения безопасного взаимодействия между ними. В результате для приложений DePIN крайне желательно разработать единый уровень идентификации, способный удовлетворить требования взаимодействия как внутри, так и вне цепочки.

5.1 Идентификация внутри и вне цепочки

5.1.1 Ончейн-идентификация

Основная цель ончейн-идентификации — подтвердить право собственности на криptoактивы и выполнить различные операции, связанные с криptoактивами, такие как передача, размещение ставок, кредитование и т. д. Для этой цели хорошо подходит адрес блокчейна внешней учетной записи (EOA) или кошелька смарт-контракта (SCW), как указано в ERC-4337 [25]. В частности, SCW, допускающий произвольную логику проверки, способен абстрагировать сложности транзакций блокчейна (например, проверку подписи, увеличение попсе, оплату газа, совместимость цепочки и т. д.) и сделать взаимодействие с блокчейном более интуитивным для конечных пользователей. Дополнительные атрибуты (например, участие в мероприятии, голосование за предложения и т. д.) также могут быть связаны с идентификатором в цепочке (т. е. адресом блокчейна) через Non-Fungible Tokens (NFTs) [26] или Soulbound Tokens (SBTs) [27]. Эти атрибуты могут потребоваться для определенных децентрализованных приложений (например, для раздачи токенов).

5.1.2 Идентификация вне блокчейна

В приложениях DePIN для установления доверенных отношений между человеком и машиной и между машинами требуется автономная идентификация. Хотя цифровой сертификат (например, X.509), который связывает личность с открытым ключом, широко используется для обеспечения доверия к централизованной системе, самостоятельная личность (SSI) [48] предоставляет многообещающее решение для идентификации для защиты связи между двумя объектами в децентрализованной среде. Как показано на рисунке ниже, SSI состоит из трех ключевых столпов, а именно: децентрализованные идентификаторы (DID) [49], проверяемые учетные данные (VCs) [51] и Обмен сообщениями DIDComm [50]. Как только каждый участник (то есть человек или машина) в децентрализованной системе регистрирует свой DID в поддающемся проверке реестре данных (например, в блокчейне), два объекта могут установить безопасный канал связи и аутентифицироваться друг с другом путем обмена сообщениями DIDComm. VC пригодятся, когда дополнительные атрибуты идентичности должны быть подтверждены определенными организациями (например, эмитентами VC).

5.2 Генерация ioID на устройстве

ioID, который использует адреса кошельков блокчейна (либо внешние учетные записи (EOA), либо кошелек абстракции учетных записей (AA)) в качестве идентификаторов в цепочке, а DID в качестве идентификаторов вне цепочки, представляет собой унифицированную систему идентификации, разработанную IoTeX для управления цифровыми отношениями внутри и вне цепочки между участниками приложений DePIN. Мы предполагаем, что в качестве системы идентификации общего назначения ioID может использоваться на разных уровнях модульной инфраструктуры DePIN, как показано на рисунке ниже. В типичном приложении DePIN ioID позволяет машинам устанавливать безопасные каналы связи и аутентифицироваться друг с другом вне сети. Более того, проект DePIN может полагаться на ioID для распределения вознаграждений в токенах и проведения детального контроля доступа и выставления счетов для конкретного проекта.

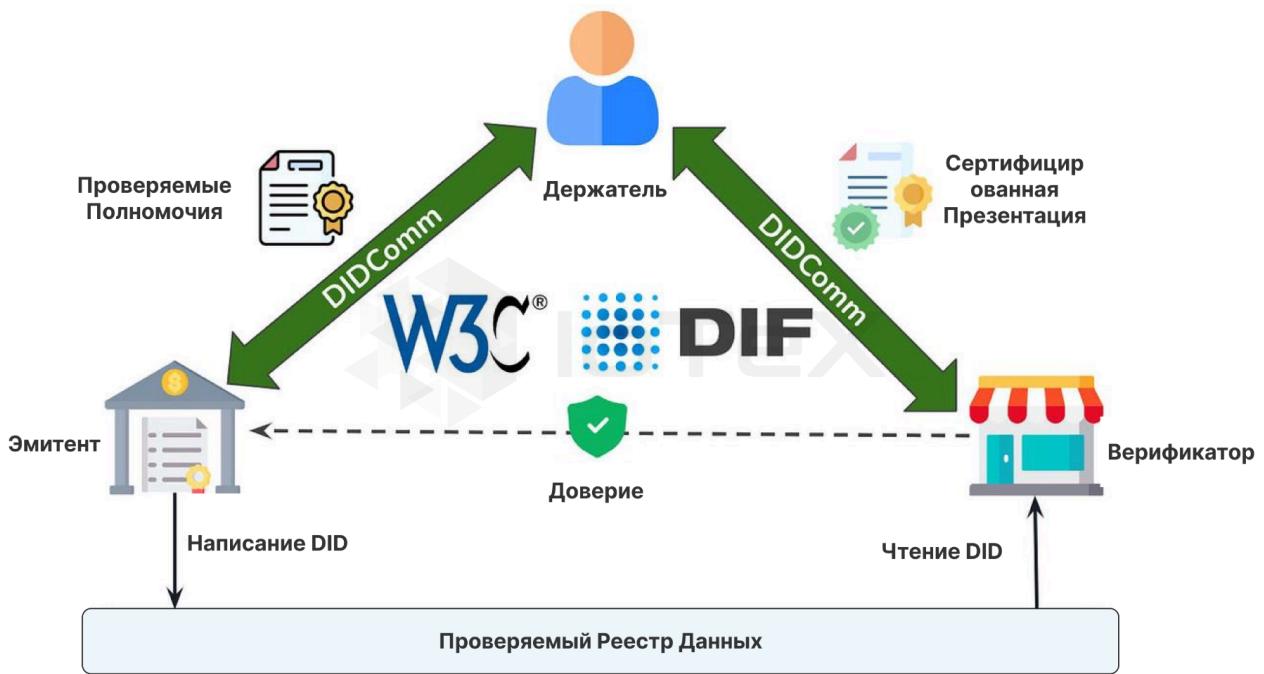


Рис. 5.1: Три ключевых столпа SSI

5.2.1 Генерация ioID на устройстве

Устройство DePIN способно генерировать DID и соответствующий документ DID «на лету» внутри устройства за счет интеграции IoTeX ioConnect SDK [16]. Для узла DePIN, развернутого для поддержки работы определенного централизованного или децентрализованного уровня в модульном стеке DePIN, оператор узла может генерировать DID и документ DID, используя интерфейс командной строки (CLI). Для встроенных устройств DePIN производители могут интегрировать ioConnect SDK в прошивку

устройства и позволить пользователям читать DID и документ DID (например, через последовательные порты) с устройств.

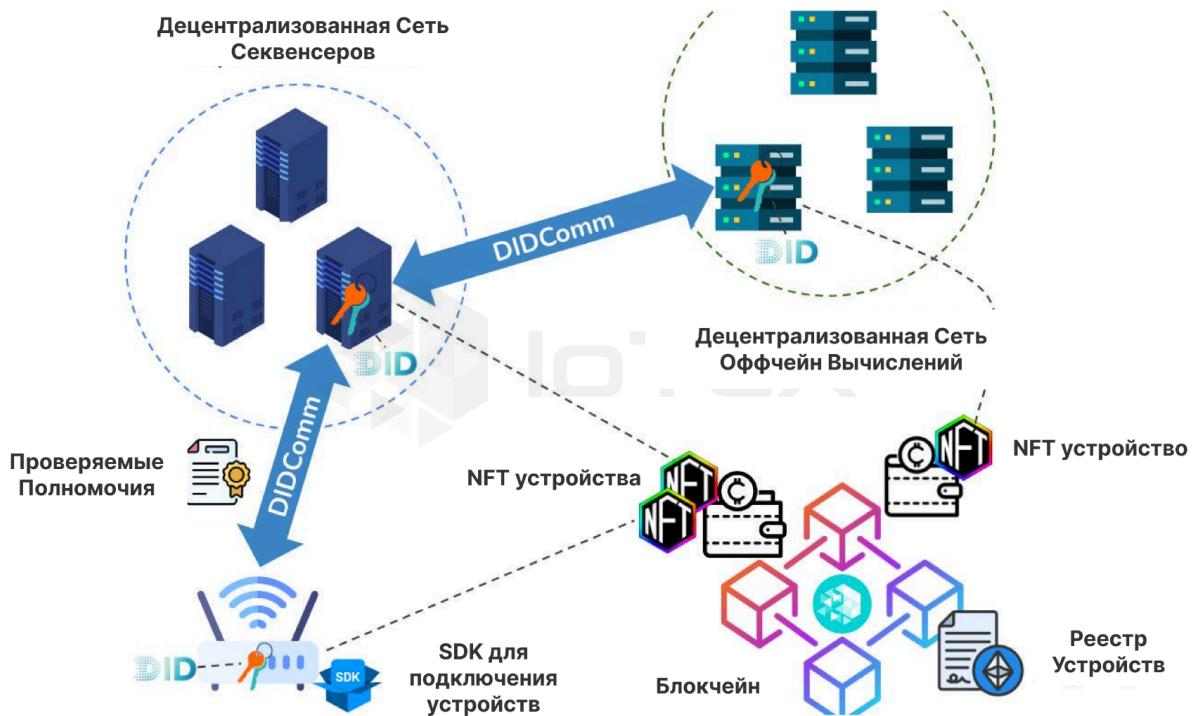


Рис. 5.2: Обзор системы идентификации ioID

5.2.2 Регистрация и привязка ioID — путь владельца устройства к подключению устройств DePIN

Владелец устройства DePIN может подключить устройство через веб-портал (например, IoTEx's [Портал MachineFi](#)). Процесс подключения показан на рисунке ниже.

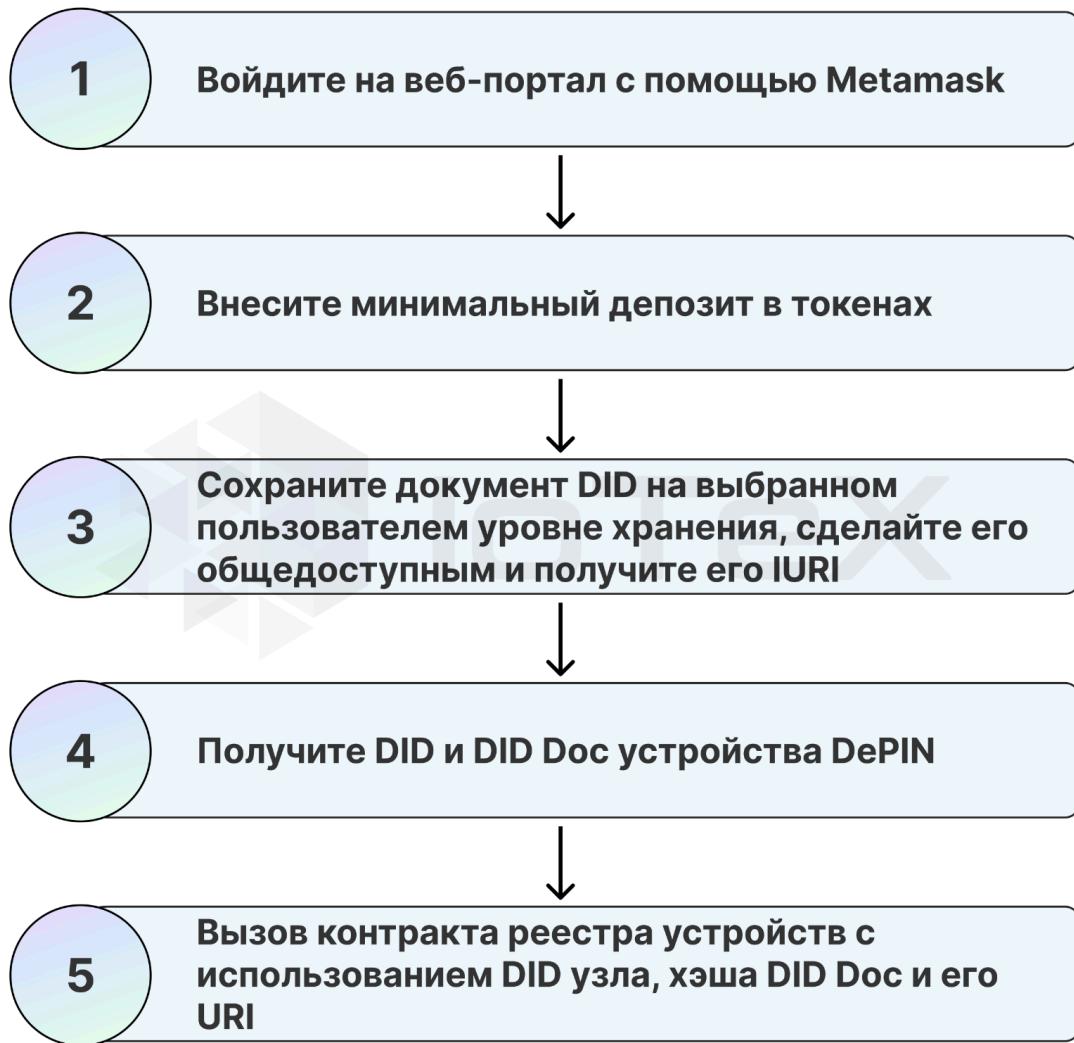


Рис. 5.3: Путь майнера по внедрению устройств DePIN

1. Владелец устройства сначала входит на веб-портал, используя [Metamask](#);
2. Владелец устройства вносит минимальный депозит токенов (например, 10 токенов IOTX) на веб-портале. Эти токены используются для оплаты газа во время процесса подключения устройства;
3. Владелец устройства получает DID и DID-документ устройства DePIN:
 1. Для узла DePIN владельцу устройства (т. е. оператору узла) необходимо войти в узел локально или удаленно и использовать CLI для создания DID и соответствующего документа DID на узле;
 2. Для встроенного устройства DePIN владельцу устройства необходимо
 1. Подключите устройство к ПК через USB;

2. Нажмите кнопку «Прочитать DID и DID-документ устройства» на веб-портале, чтобы получить DID и DID-документ устройства через последовательный порт;
4. Владелец устройства выбирает централизованного или децентрализованного поставщика уровня хранения (например, AWS S3, IPFS и т. д.), сохраняет документ DID, делает его общедоступным и получает его URI;
5. Владелец устройства вызывает контракт реестра устройства, используя DID устройства, хэш документа DID и URI документа DID.

После успешного процесса подключения устройства владелец устройства DePIN может увидеть NFT устройства, отображаемый в его/ее кошельке с блокчейном, который представляет собой владение устройством DePIN в сети.

5.2.3 Безопасное взаимодействие между машинами

После того, как DID устройства DePIN зарегистрирован в цепочке во время процесса подключения устройства, оно может осуществлять безопасную связь вне цепочки с другими объектами в сети на основе стандартизированного протокола обмена сообщениями DIDComm.

5.3 Интеграция ioID в проект DePIN

Прежде чем использовать модуль ioID, проект DePIN должен выполнить ряд настроек.

5.3.1 Смарт-контракты в ioID

Набор смарт-контрактов ioID обеспечивает надежную основу для децентрализованного управления идентификацией в блокчейне IoTeX. Эти контракты в совокупности обеспечивают надежную основу для управления идентификацией и взаимодействия в экосистеме IoTeX.

- **Реестр проектов DePIN:** Реестр проектов DePIN — это реестр на основе NFT, который управляет всеми проектами DePIN. Это гарантирует, что каждый проект однозначно идентифицирован и аутентифицирован в сети.
- **ioID NFT-контракт:** Контракт ioID NFT является важной частью платформы ioID для децентрализованного управления идентификацией в блокчейне IoTeX. Он напрямую управляет реестром проектов и отвечает за создание и назначение уникальных токенов ioID для устройств. Это включает в себя привязку устройств к идентификаторам проектов и владельцам, а также создание связанных адресов кошельков в соответствии со стандартом ERC6551.
- **Магазин ioID:** Магазин ioID отвечает за управление приложением и активацию ioID во всех проектах. Он управляет жизненным циклом приложений управления идентификацией, гарантируя правильную настройку и обслуживание удостоверений.
- **Реестр ioID:** Контракт реестра ioID используется для регистрации устройств в цепочке и активации их ioID. Он также служит преобразователем DID, предоставляя надежные средства проверки личности устройств в различных проектах.

5.3.2 Развёртывание контракта NFT устройства

Чтобы интегрировать проект DePIN с модулем IoTeX ioID, владелец проекта начинает с развертывания «Устройство NFT» контракт на токенизацию каждого устройства в рамках своего проекта. Пользователь, владеющий NFT устройства из проекта DePIN, имеет право зарегистрировать новый идентификатор

ioID для физического устройства и привязать его к своему блокчейн-кошельку. Когда для устройства регистрируется новый ioID ioID NFT создается в кошельке владельца, а соответствующее NFT устройство передается в кошелек ERC-6551 ioID. Этот процесс эффективно “активирует” ioID, связывая физическое устройство с его цифровой идентификацией и его владельцем на блокчейне.

5.3.3 Регистрация проекта DePIN

Любой проект DePIN, намеревающийся использовать идентификаторы ioID, должен подать заявку на определенное количество ioID, заплатив необходимую сумму. ioID могут запрашиваться только зарегистрированными проектами DePIN в блокчейне IoTeX. Владелец проекта может либо выполнить прямой вызов смарт-контракта, либо использовать интерфейс командной строки IoTeX (т. е. ioctl) для регистрации проекта DePIN. После завершения транзакции вы получите NFT проекта с определенным идентификатором токена, представляющим ваш идентификатор проекта DePIN в блокчейне IoTeX.

5.3.4 Настройка контракта NFT устройства

После регистрации проекта DePIN следующим шагом будет установка контракта NFT устройства для этого проекта в магазине ioID. Этот контракт должен быть установлен до того, как устройство попытается зарегистрировать ioID для вашего проекта. Владелец проекта может либо выполнить прямой вызов смарт-контракта, либо использовать интерфейс командной строки IoTeX (т. е. ioctl) для выполнения этого шага.

5.3.5 Запрос ioID

Владельцу проекта необходимо подать заявку на получение ioID, заплатив необходимое количество токенов IOTX. Сумма определяется количеством запрошенных ioID. Владелец проекта может либо выполнить прямой вызов смарт-контракта, либо использовать интерфейс командной строки IoTeX (т. е. ioctl) для запроса ioID. После транзакции количество запрошенных ioID будет связано с проектом DePIN.

5.3.6 Регистрация устройства

После настройки контракта NFT устройства и запроса определенного количества ioID для проекта DePIN физические устройства теперь можно *активировать* для проекта, зарегистрировав их в контракте ioIDRegistry. Этот процесс выполняется владельцем устройства и создает новый ioID NFT для учетной записи владельца устройства, привязывает его к DID устройства и к NFT устройства.

Глава 6

ioConnect — универсальный встроенный SDK, абстрагирующий аппаратную сложность устройств.

Приложения DePIN включают в себя разнообразные аппаратные устройства с различными возможностями и функциями. Основная цель уровня абстракции оборудования (HAL) в модульной инфраструктуре DePIN — абстрагировать сложность и неоднородность широкого спектра интеллектуальных устройств (больших или маленьких) и облегчить их подключение к централизованному или децентрализованному уровню подключения (CL) безопасным способом, как показано на рисунке ниже. Сложным вопросом является разработка универсального встроенного SDK, который позволит производителям устройств легко подключать свои устройства к серверной части DePIN.



Рис 6.1: Безопасное соединение между HAL и CL

6.1 Варианты подключения

6.1.1 Подключение к уровню централизованного подключения

Подключение интеллектуального устройства к централизованному уровню подключения (например, облачному шлюзу Интернета вещей) тщательно исследовалось в традиционных отраслях Интернета вещей и было принято во многих ранних проектах DePIN из-за его технологической зрелости.

Цифровые сертификаты (например, X.509) часто используются для обеспечения безопасной связи между интеллектуальными устройствами и уровнем централизованного подключения. Используя облачный шлюз IoT (например, AWS IoT Core [46]) в качестве примера (см. рис. 6.2), пользователь может сначала создать цифрового двойника в облаке и сгенерировать сертификат устройства. После установки сертификата на интеллектуальное устройство оно может установить безопасное соединение TLS с облачным шлюзом Интернета вещей. Затем цифровой двойник взаимодействует с другими облачными сервисами от имени интеллектуального устройства.

Уровень централизованного подключения, упрощая подключение и управление устройствами, представляет собой единую точку отказа в приложении DePIN, и будущим проектам DePIN следует серьезно рассмотреть вопрос о принятии уровня децентрализованного подключения.

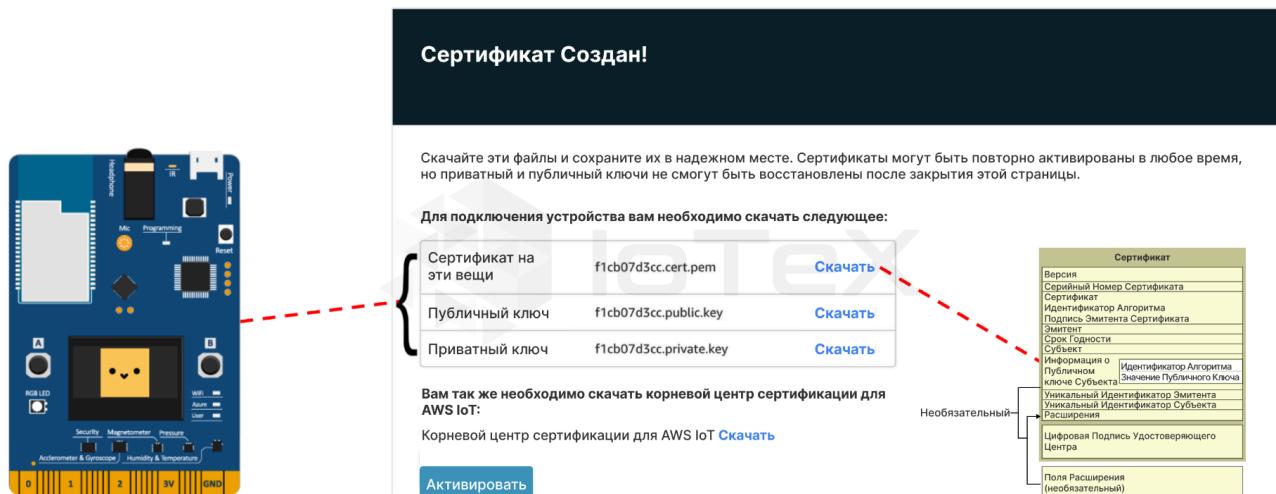


Рис 6.2. Подключение устройств с помощью AWS IoT Core

6.1.2 Подключение к децентрализованному уровню подключения

Хотя уровень децентрализованного подключения обеспечивает более надежное сетевое соединение для приложения DePIN, подключение к нему интеллектуального устройства сопряжено с рядом технических проблем:

- Как интеллектуальное устройство может безопасно подключаться к узлам на уровне децентрализованного подключения, не полагаясь на централизованный центр сертификации (СА) и цифровые сертификаты?
- Как интеллектуальное устройство может взаимно аутентифицироваться с узлами на уровне децентрализованного подключения?
- Как интеллектуальное устройство может установить безопасный канал с узлами на уровне децентрализованного подключения?

Чтобы решить вышеупомянутые технические проблемы, устройство DePIN должно реализовывать новые технологии и протоколы, которые можно использовать в такой децентрализованной среде.

6.2 Особенности проектирования для создания универсального встроенного SDK для устройств DePIN

Потенциальные проблемы подключения широкого спектра интеллектуальных устройств к децентрализованному уровню подключения привели к следующим требованиям к проектированию при разработке универсального встроенного SDK для устройств DePIN:

- SDK должен поддерживать популярные аппаратные чипсеты и платформы (например, микроконтроллеры, одноплатные компьютеры, смартфоны и т. д.);
- Производители устройств DePIN должны легко интегрировать SDK в свои устройства;
- SDK должен позволять устройствам DePIN использовать расширенные функции безопасности (например, элементы безопасности, ускорители шифрования и т. д.);
- SDK должен позволить устройству DePIN устанавливать доверительные отношения с другими объектами (например, людьми или машинами) в децентрализованной среде.

Эти требования к дизайну побудили нас изучить новые технологии, такие как сертифицированный PSA криптографический API Arm и самостоятельная идентификация (SSI), а также методология многоуровневого проектирования SDK.

6.2.1 Крипто API, сертифицированный PSA Arm

Крипто API, сертифицированный PSA от Arm [47] определяет стандартизованные и унифицированные интерфейсы для доступа к криптографическим операциям и службам управления ключами на широком спектре аппаратных платформ. Загрузив криптографический программный/аппаратный драйвер, доступный на целевой аппаратной платформе, разработчик может легко получить доступ ко всем функциям, связанным с безопасностью, через криптографический API PSA, как показано на рисунке 6.3.

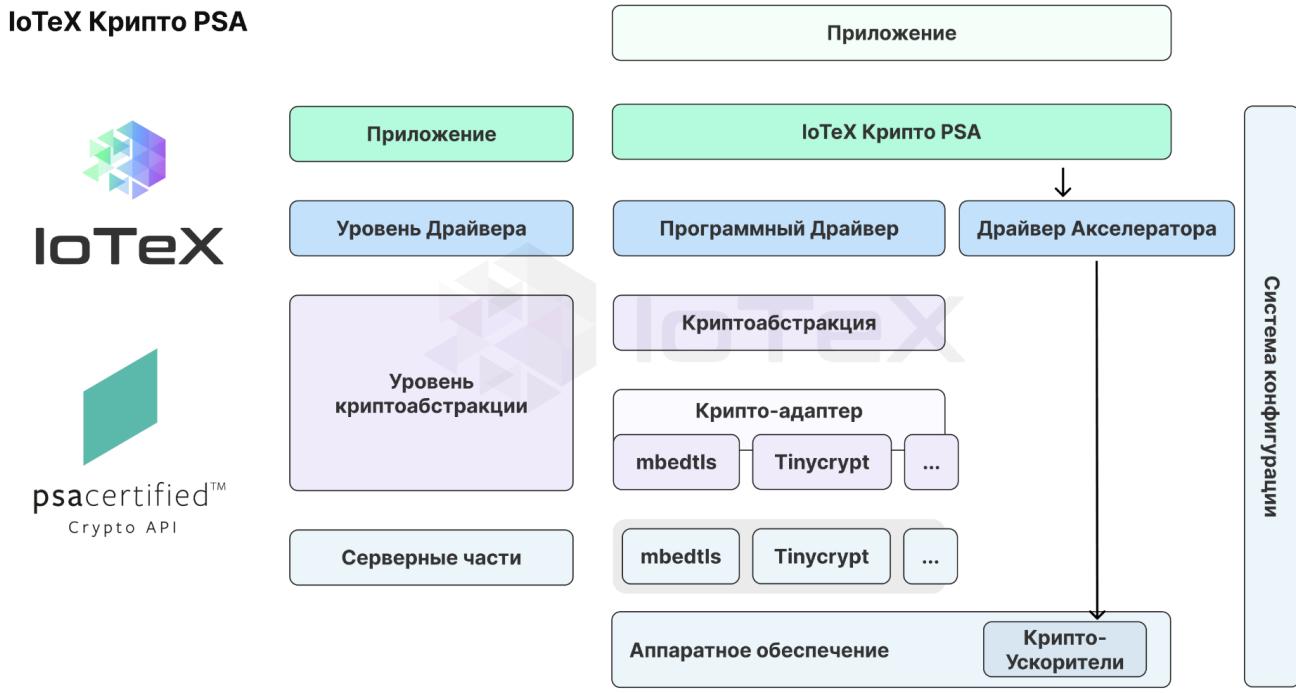


Рис 6.3: Использование Библиотеки PSACrypto от IoTeX в устройствах DePIN

Интеграция сертифицированного PSA криптографического API Arm в устройства DePIN потенциально может повысить безопасность устройств DePIN, тем самым эффективно снижая растущие риски мошенничества в приложениях DePIN.

6.2.2 Самосуверенная идентичность (SSI)

Самостоятельная идентичность (SSI) [48] методы, такие как Децентрализованные идентификаторы (DID) [49], Поддающиеся проверке учетные данные (VC) [51] и Обмен сообщениями DIDComm [50], передают контроль над цифровой идентификацией от традиционных поставщиков удостоверений отдельным лицам и закладывают основу для формирования между людьми, организациями и вещами богатых цифровых отношений. В децентрализованной среде SSI предоставляет многообещающее решение для установления надежных отношений между человеком и машиной и между машинами без необходимости полагаться на сторонних централизованных или федеративных поставщиков удостоверений, как показано на рисунке 6.4.

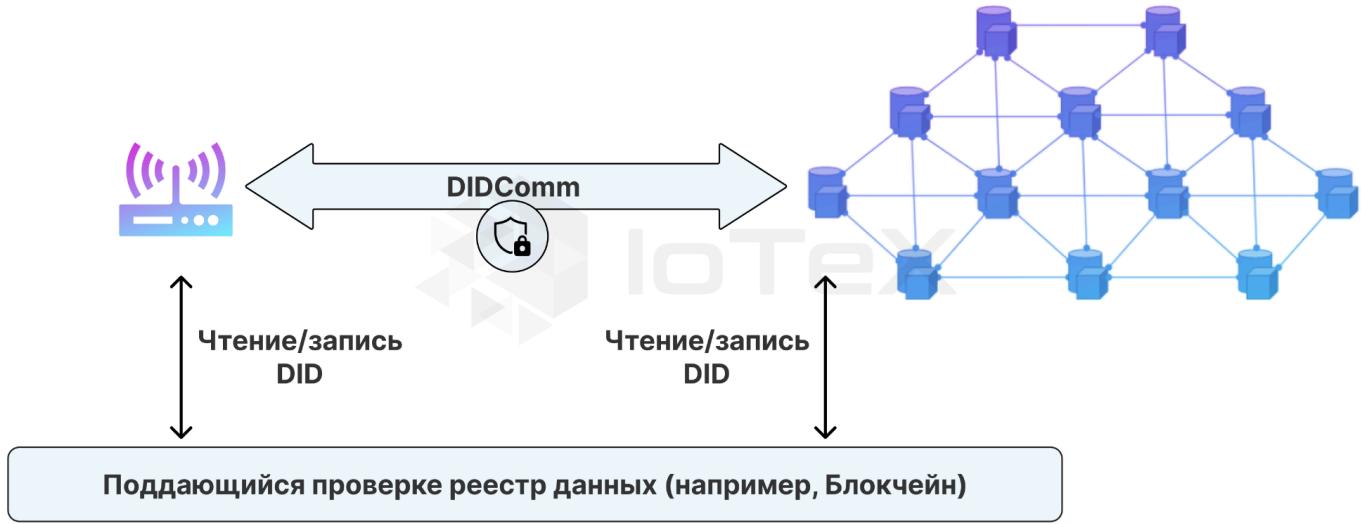


Рис 6.4: Коммуникация на основе SSI в децентрализованной среде

6.3 Спецификация реализации

ioConnect [16] это универсальный встроенный SDK, специально разработанный IoTeX для расширения возможностей устройств DePIN. Для поддержки широкого спектра интеллектуальных устройств и требований приложений SDK имеет ядро SDK и уровень адаптации платформы (PAL).

6.3.1 Ядро SDK ioConnect

Ядро ioConnect состоит из четырех уровней, как показано на рисунке ниже. Два нижних уровня реализуют сертифицированную PSA криптографическую спецификацию API v1.1 от Arm, тогда как два верхних уровня реализуют три ключевых компонента (т. е. DID, VC и DIDComm) в SSI. Все криптографические операции, необходимые в SSI, выполняются посредством вызовов криптографического API PSA.

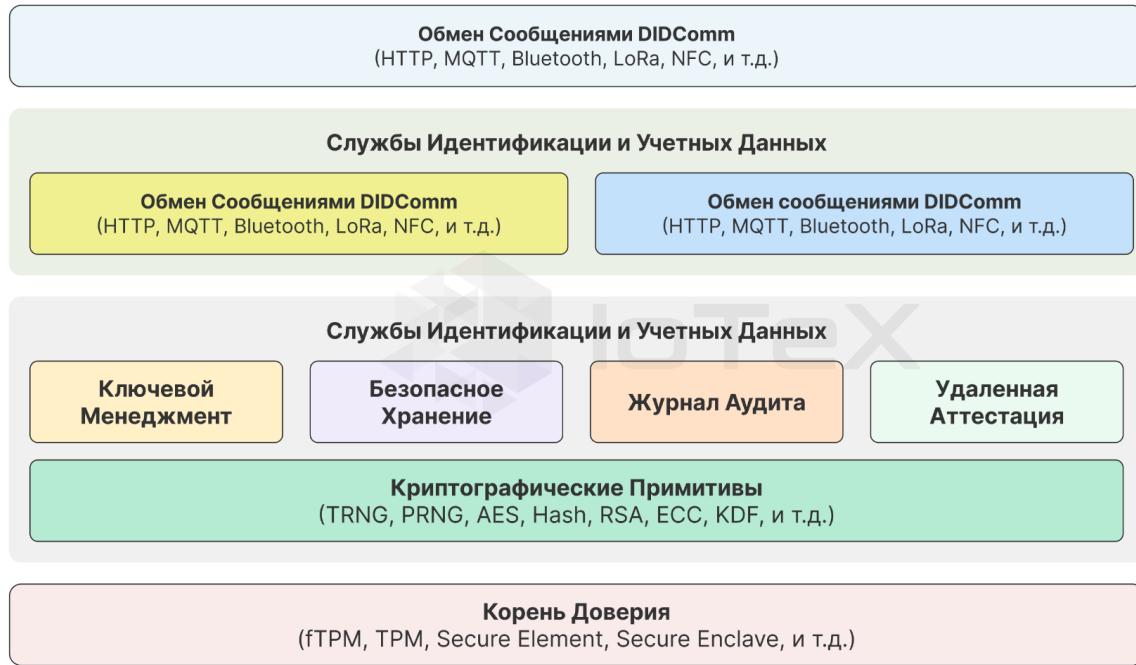


Рис 6.5: Ядро ioConnect SDK

Обратите внимание, что ядро ioConnect SDK не зависит от аппаратных платформ и не привязывается к конкретным компонентам/ресурсам на устройстве DePIN.

6.3.2 Совместимость устройств DePIN

Чтобы обеспечить поддержку широкого спектра устройств DePIN, весь пакет ioConnect SDK использует методологию многоуровневого проектирования, как показано на рисунке ниже. С одной стороны, ядро содержит реализации аппаратно-независимых спецификаций (например, SSI, криптографический API PSA и т. д.), а уровень адаптации платформы (PAL) занимается различиями между различными встроенными системами и платформами (например, правилами компиляции, соглашения о кодировании, дизайн фреймворка и т. д.).

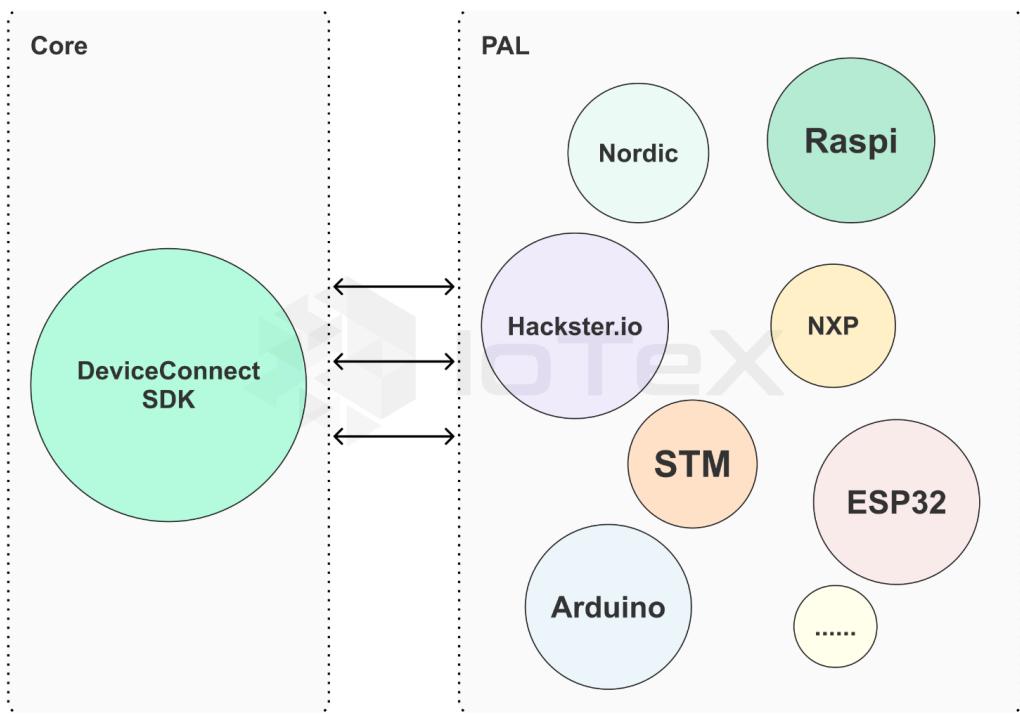


Рис 6.6: Многоуровневая архитектура в ioConnect SDK

Внедрение PAL позволяет разработчикам легко добавлять поддержку нового оборудования, просто разработав еще один компонент PAL всего лишь с 300–500 строками кода, тем самым эффективно решая проблему совместимости устройств DePIN и значительно снижая сложность интеграции производителей устройств DePIN.

Глава 7

ioDDK — включение самостоятельных цепочек приложений DePIN

7.1 Обоснование дизайна

Обоснование включения L2 для конкретных приложений для проектов DePIN на IoTeX L1 обусловлено несколькими убедительными факторами.

- Во-первых, уровни L2 для конкретных приложений имеют решающее значение для проектов DePIN, поскольку они позволяют внедрять уникальную токеномику, индивидуальный пользовательский интерфейс (например, кошелек и браузер) и настраиваемые структуры управления. Эта настройка жизненно важна для оптимизации блокчейна для удовлетворения конкретных потребностей и сценариев каждого приложения DePIN с возможностью масштабирования, гарантируя, что каждый проект сможет полностью раскрыть свой потенциал.
- Кроме того, многим проектам DePIN не хватает опыта и финансовых ресурсов, необходимых для создания и поддержания собственной инфраструктуры блокчейнов.

На данный момент IoTeX L1 защищен пулом из более чем 120 глобально распределенных делегатов (то есть валидаторов) через наш собственный консенсусный протокол рандомизированного делегированного доказательства доли (Roll-DPoS) [52]. Используя безопасное пространство блоков IoTeX L1, эти проекты DePIN могут беспрепятственно запускать свои L2 для конкретных приложений без тяжелой работы, связанной с разработкой блокчейна.

ioDDK — это цепной SDK, который позволяет проектам DePIN создавать самостоятельные цепочки приложений и одновременно наследовать безопасность IoTeX L1, как показано на рисунке 7.1. Проверяя и предлагая блоки IoTeX L1, валидаторы также достигают консенсуса по транзакциям из цепочек приложений DePIN. Сдавая в аренду блочное пространство, IoTeX L1 может предоставить проектам DePIN необходимые ресурсы для эффективного развертывания индивидуальных решений без необходимости значительных первоначальных инвестиций или технических ноу-хау, способствуя созданию более динамичной и инновационной экосистемы.

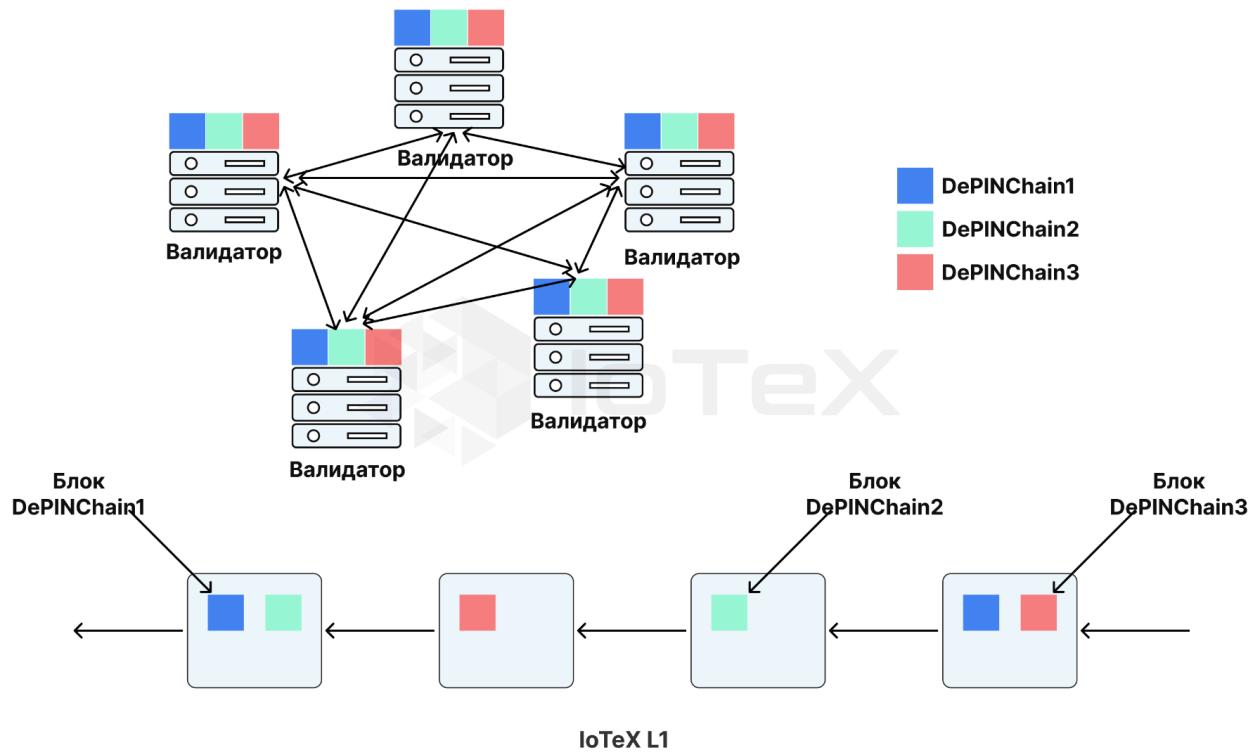


Рис 7.1: Самостоятельные цепочки приложений DePIN, защищенные IoTeX L1

7.2 Общее пространство блоков и валидаторов

Чтобы свести к минимуму сложность разработки, все самостоятельные цепочки DePIN могут использовать совместное пространство блоков и валидаторы с IoTeX L1. На практике можно рассмотреть три варианта реализации, как показано на рисунке ниже.

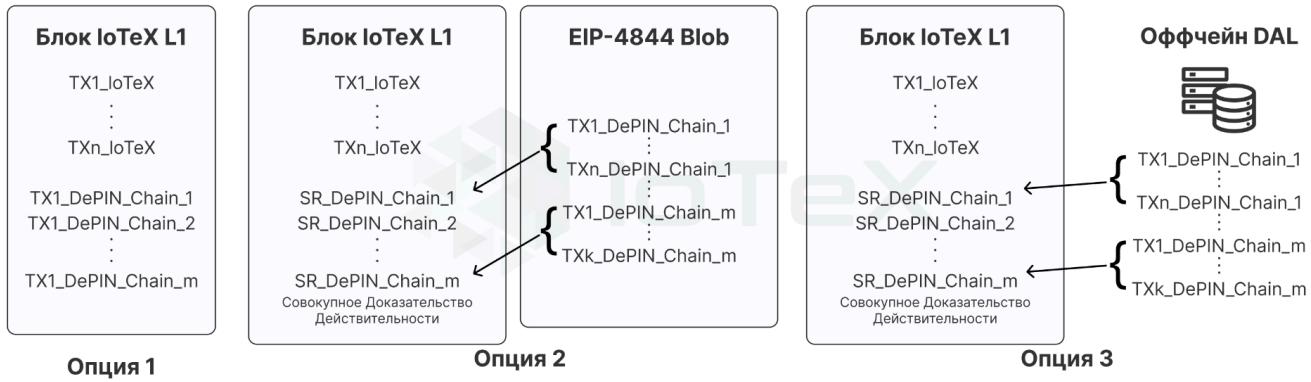


Рис 7.2: Три варианта реализации общего пространства блоков и валидаторов

Вариант 1 – Хранение всех транзакций на IoTeX L1

В этом варианте транзакции из самостоятельных цепочек DePIN вместе с транзакциями в IoTeX L1 используют одно и то же пространство блоков, и все транзакции должны пройти через процесс консенсуса IoTeX L1. Этот подход гарантирует, что все самостоятельные цепочки DePIN достигают той же безопасности, что и IoTeX L1. Однако из-за ограничения размера блока может поддерживаться только определенное количество проектов DePIN. Чтобы определить, какие проекты DePIN имеют право на использование этого подхода, может потребоваться процесс децентрализованного управления.

Вариант 2. Хранение цепочек транзакций DePIN с использованием EIP-4844.

В этом варианте транзакции из самостоятельных цепочек DePIN временно сохраняются в IoTeX L1 с использованием больших двоичных объектов EIP-4844. Корни состояний вместе с совокупным доказательством действительности переходов состояний всех самостоятельных цепочек DePIN используют одно и то же пространство блоков с транзакциями IoTeX L1. Агрегированное доказательство действительности проверяется на IoTeX L1 для расчета всех транзакций в самостоятельных цепочках DePIN. Такой подход на основе объединения может эффективно улучшить масштабируемость системы и позволить всем самостоятельным цепочкам DePIN одновременно наследовать безопасность IoTeX L1. Обратите внимание, что для реализации этого подхода следует использовать один из пруверов в сети W3bstream.

Вариант 3. Хранение транзакций цепочки DePIN с использованием DAL вне цепочки.

В этом варианте самостоятельные цепочки DePIN могут выбрать уровень доступности данных вне цепочки (DAL) для хранения своих транзакций. Как и в варианте 2, корни состояний вместе с совокупным доказательством действительности переходов состояний всех самостоятельных цепочек DePIN используют одно и то же пространство блоков с транзакциями IoTeX L1. Агрегированное доказательство действительности проверяется на IoTeX L1 для расчета всех транзакций в самостоятельных цепочках DePIN. Однако в этом подходе корни состояния должны быть привязаны к IoTeX L1 со стороны DAL. Хотя такой подход на основе валидума также может улучшить масштабируемость системы, безопасность зависит от реализации конкретного DAL. Обратите внимание, что для реализации этого подхода следует использовать один из пруверов в сети W3bstream.

Сравнение трех вариантов

В таблице 1 представлено сравнение трех вышеупомянутых вариантов реализации с точки зрения хранения транзакций цепочки DePIN, масштабируемости, требований W3bstream и безопасности.

Таблица 7.1: Сравнение трех вариантов реализации

	Хранилище цепочек транзакций DePIN	Масштабируемость	Необходим W3bstream	Безопасность
Опция 1	цепной блок	Низкая	Нет	Высокая
Вариант 2	большой двоичный объект в цепочке	Высокая	Да	Высокая
Вариант 3	внесетевой DAL	Высокая	Да	Низкая/Средняя

7.3 Компоненты ioDDK и высокоуровневый рабочий процесс

7.3.1 Компоненты ioDDK

ioDDK, который позволяет проекту DePIN использовать существующие делегаты (т. е. валидаторы) и пространство блоков в IoTeX L1 для размещения самостоятельной цепочки DePIN, состоит из следующих компонентов:

- **Конфигурация цепи:** Компонент конфигурации цепочки позволяет разработчику настраивать конкретные параметры (например, начальную высоту, тип транзакции, требования к пространству блоков и т. д.) цепочки DePIN;
- **Развертывание цепочки:** Компонент развертывания цепочки позволяет разработчику управлять процессом развертывания цепочки DePIN среди всех делегатов IoTeX L1;

- **Цепной исследователь:** Компонент обозревателя цепочки позволяет проекту DePIN, а также внешним сторонам отслеживать состояние и ключевые показатели (т. е. высоту блока, TPS, детали транзакций и т. д.) цепочки DePIN;
- **Chain Commander:** Chain Commander — это инструмент командной строки, который предоставляет набор команд для упрощения разработки и управления цепочкой DePIN.

7.3.2 Рабочий процесс высокого уровня

Как только проект DePIN будет одобрен для создания независимой цепочки с использованием общего пространства блоков и валидаторов в IoTeX L1 (например, через процесс децентрализованного управления), проект может использовать ioDDK следующим образом:

- Разработчик использует функцию «Конфигурация цепочки» в ioDDK для указания ряда конкретных параметров цепочки DePIN:
 - **Идентификатор цепи:** идентификатор цепи генерируется автоматически для представления независимой цепочки DePIN;
 - **Тип операции:** различные поля в транзакции;
 - **Максимальное количество транзакций:** максимальное количество транзакций цепочки DePIN, обработанных в блоке IoTeX L1;
 - **W3bstream-доказательство:** выбор прувера W3bstream.
- Разработчик готовит образ докера логики обработки транзакций для цепочки DePIN и использует функцию “Развертывание цепочки” в ioDDK для развертывания образа докера всем делегатам IoTeX L1;

Как только логика обработки транзакций, специфичная для цепочки DePIN, будет развернута на делегатах IoTeX L1, транзакции цепочки DePIN будут обрабатываться соответствующим образом. Разработчик может использовать “Chain Explorer” в ioDDK для проверки статуса предоставленной цепочки DePIN. Более того, разработчик также может использовать “Chain Commander” для управления цепочкой DePIN с помощью ряда вспомогательных команд.

7.4 Рынок аренды блочного пространства

Мы планируем реализовать рынок блоков, позволяющий разработчикам торговать пространством блоков, адаптированным для их конкретных DePIN L2, созданных с помощью ioDDK. Эта ориентированная на рынок стратегия гарантирует, что распределение ресурсов адаптируется к спросу в реальном времени, тем самым оптимизируя общую эффективность сети.

Введение торгуемого пространства блоков также влияет на полезность и ликвидность токена IOTX. Например, разработчики могут застейкать или сжечь IOTX, чтобы получить определенный объем блочного пространства. Доходы, полученные от транзакций, могут распределяться разными способами, включая финансирование казны или сжигание для регулирования поставок токенов.

7.5 Влияние на IoTeX L1

Введение общего пространства блоков в IoTeX L1 приносит множество функций, предназначенных для удовлетворения растущих потребностей проектов DePIN L2:

- **Быстрое время блокировки и завершенность.** Одним из основных требований к DePIN L2 является быстрое время блокировки и быстрая завершенность для оптимизации взаимодействия с пользователем. В настоящее время время блокировки IoTeX L1 составляет 5 секунд. Однако, чтобы удовлетворить потребности высокопроизводительных проектов DePIN, мы стремимся сократить время блока до 2 секунд. Это сокращение значительно повысит скорость реагирования и эффективность приложений L2, обеспечивая более плавную и удобную работу.
- **Повышенная пропускная способность и децентрализация:** общая пропускная способность DePIN L2 по своей сути ограничена мощностью компьютера всех валидаторов в сети IoTeX L1. Чтобы решить эту проблему, крайне важно как увеличить количество валидаторов, так и улучшить общую децентрализацию сети. Расширяя пул валидаторов, IoTeX L1 может поддерживать больший объем транзакций и обеспечивать более надежную безопасность. Это усовершенствование также будет способствовать созданию более децентрализованной и устойчивой сети, необходимой для поддержания доверия и стабильности в растущей экосистеме.

Для выполнения вышеизложенных требований планируется внедрение разделения Proposer-Builder (PBS) [53]. PBS — это концепция, первоначально предложенная исследователями Ethereum, призванная повысить устойчивость к цензуре и общую производительность сетей блокчейнов. Он разделяет роли предлагающих и создателей блоков для оптимизации производства блоков и обеспечения справедливости в процессе проверки.

- **Предлагающие блоки:** отвечают за предложение новых блоков на основе текущего состояния блокчейна и сетевых правил. Они собирают транзакции и создают предложение блока, которое будет проверено сетью. Эту роль, скорее всего, будут выполнять нынешние делегаты консенсуса.
- **Строители блоков:** специализированные организации, занимающиеся созданием блоков путем выбора наиболее ценных транзакций из пула операций, оптимизации использования пространства блоков и потенциального повышения пропускной способности. Они отправляют свои построенные блоки предлагающим, которые затем предлагают эти блоки в сеть для проверки. Это будет новая роль, введенная в сеть IoTeX L1 и предназначенная для работы с пакетными транзакциями, в том числе из DePIN L2.

Разделение этих ролей помогает снизить риск централизованного контроля и цензуры за счет распределения обязанностей между различными организациями. Это повышает пропускную способность сети и сокращает время обработки транзакций, т. е. также позволяет более эффективно производить блоки, поскольку разработчики могут сосредоточиться на выборе транзакций, оптимизации и даже сегментировании, в то время как предлагающие управляют процессами консенсуса и финализации блоков. Этот подход гарантирует, что DePIN L2, основанные на общем пространстве блоков, предоставляемом IoTeX L1, смогут работать эффективно и безопасно, отвечая требованиям конкретных сценариев применения.

8. Новая дорожная карта

IoTeX 2.0 — это набор многочисленных компонентов, которые мы планируем создавать до 2026 года. Дорожная карта представлена ниже. Обратите внимание, что многие из перечисленных компонентов зависят от предложений руководства и голосования и поэтому могут быть изменены.

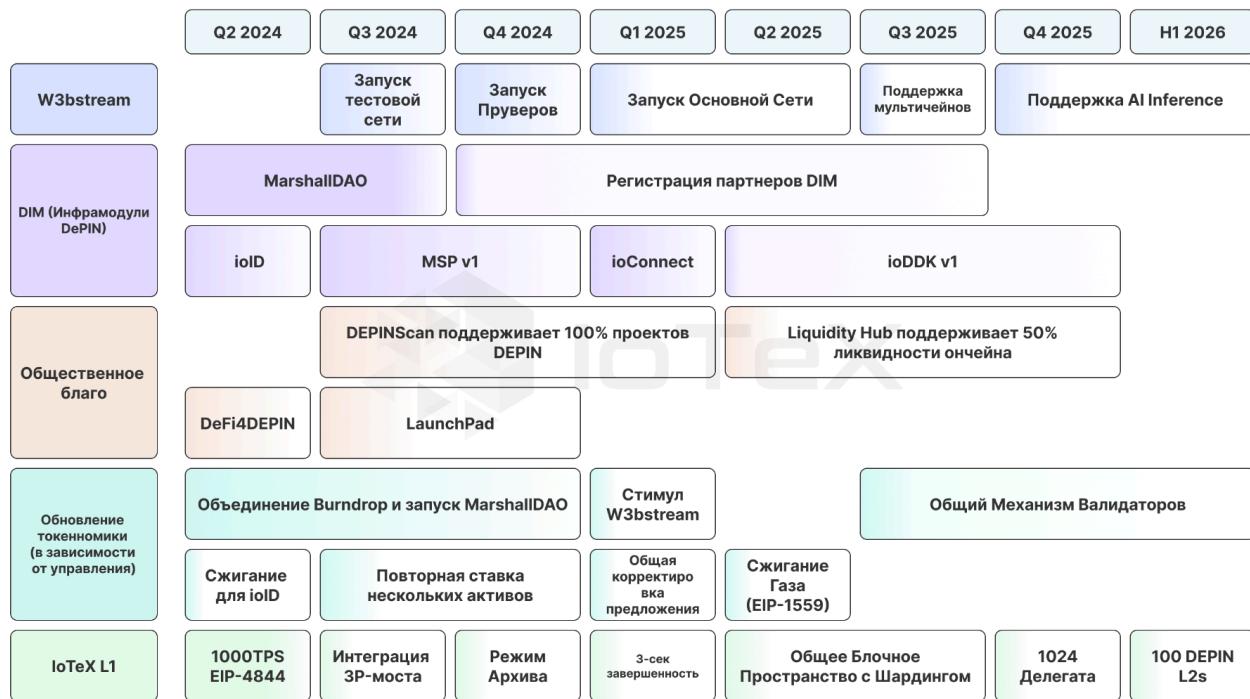


Рис 8.1: Дорожная карта IoTeX 2.0

9. Заключение

IoTeX 2.0 предлагает новое видение сети IoTeX, сохраняя при этом основные принципы, которые привели к ее созданию. С самого начала IoTeX представлял себе будущее, в котором люди смогут владеть и контролировать свои устройства, а также данные и ценность, которые эти устройства производят. IoTeX стремится стать центром реальных данных в реальном времени, обеспечивающим работу сверх интеллектуальной сети искусственного интеллекта. Эта сеть не просто превзойдет человеческий интеллект, но и будет использовать точные и надежные данные, отражающие реальный мир в режиме реального времени. Этот сдвиг предполагает, что абсолютная истина и сила принятия решений будут корениться в осозаемых, динамичных реалиях нашей физической среды. Эта трансформация меняет то, как данные ценятся и используются, влияя на будущее цивилизации. Самое главное, что все, что позволяет IoTeX, будет принадлежать и управляться людьми и для людей.

Спасибо сообществу IoTeX за ваш постоянный вклад, поддержку и отзывы. Отправляясь в это новое амбициозное путешествие, мы знаем, что IoTeX и наше глобальное сообщество осуществляют реальные изменения и принесут DePIN в каждую страну мира. Пришло время строить!

Отказ от ответственности

Эта статья является результатом совместной работы разработчиков IoTeX и членов сообщества IoTeX. В нем изложено предлагаемое направление развития сети IoTeX. Однако содержание не влечет за собой каких-либо обязательств со стороны авторов или их соответствующих организаций. Сообщество IoTeX несет ответственность за адаптацию и принятие мер, предложенных в этом документе. Успех любого предложения в конечном итоге будет зависеть от напряженной работы более широкого сообщества и тех, кто строит сеть IoTeX.

Информация, представленная в настоящем документе, предоставлена перечисленными выше сторонами (СТОРОНЫ) исключительно в информационных целях. Ни СТОРОНЫ, ни какие-либо из их аффилированных лиц, директоров, должностных лиц, менеджеров, сотрудников или представителей не делают каких-либо заявлений или гарантий, явных или подразумеваемых, в отношении каких-либо материалов или информации, содержащихся в настоящем документе. Кроме того, СТОРОНЫ или любые такие лица не принимают на себя и не несут какой-либо ответственности перед вами или вашими аффилированными лицами, а также соответствующими директорами, должностными лицами, менеджерами, сотрудниками или представителями ваших или ваших аффилированных лиц в результате использования содержащейся здесь информации и материалов.

Представленная здесь информация предоставляется добросовестно на основе достоверной информации, но ее точность и полнота не гарантируются. Информацию в этом документе не следует рассматривать как инвестиционный совет, финансовый совет, торговый совет или совет любой другой формы. Рекомендуется провести собственную комплексную проверку и проконсультироваться со своим финансовым консультантом, прежде чем принимать какие-либо инвестиционные решения.

Благодарность

Мы выражаем нашу искреннюю благодарность фирмам венчурного капитала (например, Escape Velocity (EV3), 1kx, 6th Man Ventures (6MV), SNZ Capital, Future Money Group (FMG), Borderless Capital, Lattice, Summer Capital, Pantera Capital, BlueYard. Capital, Spartan Capital, Lemniscap, NGC Ventures, Electric Capital, Stanford Blockchain Accelerator, Foresight Venture и Samsung NEXT), проекты Web3 (например, NEAR Foundation, RISC0, Helium Foundation, The Graph Foundation, Filecoin Foundation и Textile) и фирмы, занимающиеся исследованием криптовалют (например, IntoTheBlock (ITB) и Messari), чьи неоценимые отзывы и непоколебимая поддержка сыграли важную роль в формировании этого технического документа. Ваш опыт, понимание и приверженность значительно повысили глубину и качество нашей работы. Мы глубоко признательны за время и ресурсы, которые вы вложили, и ваш вклад сыграл решающую роль в продвижении миссии IoTeX 2.0.

Библиография

[1] Pebble Tracker. <https://docs.iotex.io/dev-toolkit/web3-smart-devices/pebble-tracker>.

- [2] X. Fan, Q. Chai, Z. Li, and T. Pan, "Decentralized iot data authorization with pebble tracker," in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1-2.
- [3] Ucam. <https://ucam.iotex.io/>.
- [4] DePIN DevKit - SenseCAP Indicator D1.<https://www.seeedstudio.com/SenseCAP-Indicator-D1-p-5643.html>.
- [5] IoTeX - A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain, The IoTeX Team, https://github.com/iotexproject/files/blob/main/publications/IoTeX_Whitepaper_1.5_EN.pdf, July 12, 2018.
- [6] X. Fan, Z. Zhong, Q. Chai, and D. Guo, "Ucam: A User-Centric, Blockchain-Based and End-to-End Secure Home IP Camera System," in Security and Privacy in Communication Networks, N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Eds., Cham: Springer International Publishing, 2020, pp. 311â323.
- [7] M. Brossard, G. Bryant, X. Fan, A. Ferreira, E. Grimley-Evans, C. Haster, D. Miller, D. P. Mulligan, H. J. M. Vincent, S. Xiong, and L. Xu, "Privacy-Preserving Object Detection with Veracruz", PerCom Workshops 2023, pp. 322-324, 2023.
- [8] M. Brossard, G. Bryant, B. El Gaabouri, X. Fan, A. Ferreira, E. Grimley-Evans, C. Haster, E. Johnson, D. Miller, F. Mo, D. P. Mulligan, N. Spinale, E. Van Hensbergen, H. J. M. Vincent, and S. Xiong, "Private Delegated Computations Using Strong Isolation," IEEE Trans. Emerg. Top. Comput, 12(1): 386-398, 2024.
- [9] IoTeX Foundation, The Building Blocks of DePIN, <https://iotex.io/blog/the-building-blocks-of-depin/>.
- [10] IIP-23: The Marshall DAO, <https://community.iotex.io/t/iip-23-the-marshall-dao/11172>.
- [11] N. Pippenger, "On the evaluation of powers and related problems," In 17th Annual Symposium on Foundations of Computer Science (sfcs 1976), pp. 258â263. IEEE Computer Society, 1976.
- [12] D. J. Bernstein, J. Doumen, T. Lange, and J.-J. Oosterwijk, "Faster batch forgery identification," In International Conference on Cryptology in India, pp. 454â473. Springer, 2012.
- [13] E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson, "Fast exponentiation with precomputation: Algorithms and lower bounds," preprint, 1995.
- [14] G. Luo, S. Fu, G. Gong, "Speeding up multi-scalar multiplication over fixed points towards efficient zkSNARKs," IACR Trans. Cryptogr. Hardw. Embed. Syst. 2023(2), pp. 358-380, 2023.
- [15] X. Fan, V. Kuchta, F. Sica, and L. Xu, "Speeding Up Multi-Scalar Multiplications for Pairing-Based zkSNARKs," Cryptology ePrint Archive, Paper 2024/750, 2024, <https://eprint.iacr.org/2024/750>.
- [16] ioConnect - A Universal Embedded SDK for Connecting Smart Devices to Web3. <https://github.com/machinefi/ioConnect>.

- [17] W3bstream. <https://w3bstream.com/>.
- [18] D. Patrick, DePIN Supercharged â Introducing the Worldâs First DePIN Accelerator. <https://iotex.io/blog/depin-accelerator/>.
- [19] ioTube - A Decentralized Multi-Asset Cross-Chain Bridge. <https://bridge.iotex.io/>.
- [20] ioPay - A DePIN Wallet. <https://iopay.me/>.
- [21] DePIN Liquidity Hub. <https://iotex.io/depin-liquidity>.
- [22] mimo - A Decentralized Exchange for Everyone. <https://mimo.finance/>.
- [23] DePINscan. <https://depinscan.io/>.
- [24] A. Basi, DePIN Liquidity Hub - Join the Fastest Growing Sector in Crypto, <https://iotex.io/blog/depin-liquidity-hub/>.
- [25] V. Buterin, Y. Weiss, D. Tirosh, S. Nacson, A. Forshtat, K. Gazso, and T. Hess, ERC-4337: Account Abstraction Using Alt Mempool, Ethereum Improvement Proposals, 2021.
- [26] W. Entriken, D. Shirley, J. Evans, and N. Sachs, ERC-721: Non-Fungible Token Standard, Ethereum Improvement Proposals, 2018.
- [27] T. Daubenschütz and Anders, ERC-5192: Minimal Soulbound NFTs, Ethereum Improvement Proposals, 2022.
- [28] Risc0. <https://www.risczero.com/>.
- [29] Succinct Processor 1 (SP1). <https://succinctlabs.github.io/sp1/>.
- [30] Nexus. <https://www.nexus.xyz/>.
- [31] zkWasm. <https://delphinuslab.com/zk-wasm/>.
- [32] Circom 2. <https://docs.circom.io/>.
- [33] Halo 2. <https://zcash.github.io/halo2/>.
- [34] ZoKrates. <https://zokrates.github.io/>.
- [35] Noir. <https://noir-lang.org/>.
- [36] Cairo. <https://www.cairo-lang.org/>.

[37] Intel Software Guard Extensions (SGX).

<https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html>.

[38] Intel Trust Domain Extensions (TDX).

<https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html>.

[39] AMD Secure Encrypted Virtualization (SEV). <https://www.amd.com/en/developer/sev.html>.

[40] AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More.

<https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/solution-briefs/amd-secure-encrypted-virtualization-solution-brief.pdf>.

[41] AWS Nitro System. <https://aws.amazon.com/ec2/nitro/>.

[42] Arm Confidential Compute Architecture.

<https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture>.

[43] G. Wuollet, Introducing the Nakamoto Challenge: Addressing the Toughest Problems in Crypto.

<https://a16zcrypto.com/posts/article/introducing-the-nakamoto-challenge-addressing-the-toughest-problems-in-crypto>.

[44] IoTeX Foundation, Decentralized Verification in DePIN.

<https://iotex.io/blog/decentralized-verification-in-depin/>.

[45] Modulus Labs, The Cost of Intelligence: Proving Machine Learning Inference with Zero-Knowledge.

https://github.com/Modulus-Labs/Papers/blob/master/Cost_Of_Intelligence.pdf.

[46] AWS IoT Core. <https://aws.amazon.com/iot-core/>.

[47] Arm PSA Certified APIs. <https://arm-software.github.io/psa-api/crypto/>.

[48] Self-Sovereign Identity. https://en.wikipedia.org/wiki/Self-sovereign_identity.

[49] Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations. W3C Recommendation, 19 July 2022. <https://www.w3.org/TR/did-core/>.

[50] DIDComm Messaging. DIF Ratified Specification. <https://identity.foundation/didcomm-messaging/spec/>.

[51] Verifiable Credentials Data Model v1.1. W3C Recommendation, 03 March 2022.

<https://www.w3.org/TR/vc-data-model/>.

[52] IoTeX Research, <https://iotex.io/research>.

[53] Vitalik Buterin, State of research: increasing censorship resistance of transactions under proposer/builder separation (PBS), https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance.