

Layer 2

в мире блокчейна



**Путеводитель в будущее
децентрализации**

Артем Демиденко / ИИ

Артем Демиденко

**Layer 2 в мире блокчейна:
Путеводитель в будущее
децентрализации**

«Автор»

2023

Демиденко А.

Layer 2 в мире блокчейна: Путеводитель в будущее
децентрализации / А. Демиденко — «Автор», 2023

Эта книга представляет собой исчерпывающий путеводитель в мире Layer 2 технологий в блокчейне. Она исследует инновационные методы решения проблем масштабируемости, долгих подтверждений транзакций и высоких комиссий в современных блокчейнах. Читатели узнают о разнообразных технологиях Layer 2, включая Sidechains, Plasma, State Channels и Rollups, и их применении в различных областях, от децентрализованных финансов до игр и смарт-контрактов. Кроме того, книга предоставляет практические руководства по созданию собственных проектов на базе этих технологий. Через подробное рассмотрение преимуществ и ограничений Layer 2, а также обсуждение будущего развития данной области, читатели получают глубокое понимание того, как эти инновации изменят ландшафт блокчейна и форму децентрализованного будущего.

© Демиденко А., 2023

© Автор, 2023

Содержание

Глава 1: Введение в Layer 2	5
Глава 2: Sidechains – Когда блокчейн встречается блокчейн	11
Глава 3: Plasma – Масштабируемость на основе смарт-контрактов	14
Конец ознакомительного фрагмента.	17

Артем Демиденко

Layer 2 в мире блокчейна: Путеводитель в будущее децентрализации

Глава 1: Введение в Layer 2

1.1 Зачем нам Layer 2?

Проблемы блокчейна и необходимость Layer 2

Для полного понимания необходимости Layer 2 в мире блокчейна, давайте более подробно рассмотрим основные проблемы, с которыми сталкиваются основные блокчейн-сети, такие как Bitcoin и Ethereum, и почему Layer 2 является решением для этих проблем:

Масштабируемость: Одной из главных проблем блокчейна является его ограниченная пропускная способность. Это означает, что блокчейн сети могут обрабатывать ограниченное количество транзакций в секунду. Например, Bitcoin может обрабатывать приблизительно 7-10 транзакций в секунду, а Ethereum – около 15-30 транзакций в секунду. При росте числа пользователей и децентрализованных приложений, это ограничение становится серьезной преградой для масштабирования и массового принятия.

Высокие комиссии: При повышенной загрузке блокчейна пользователи вынуждены платить высокие комиссии за обработку своих транзакций. Это происходит из-за ограниченной емкости в блоках и конкуренции за включение транзакций в следующий блок. Эта проблема стала очень актуальной в периоды пиковой активности, когда комиссии могут существенно возрастать, делая многие виды транзакций неэффективными.

Сложность разработки: Создание смарт-контрактов и децентрализованных приложений на блокчейне может быть сложным и затратным процессом. Это связано с необходимостью учитывать особенности протоколов блокчейна, обеспечивать безопасность и протестировать код. Эти ограничения могут замедлить разработку и ограничивают количество разнообразных проектов и DApps, доступных в блокчейн-экосистемах.

Layer 2 как решение

Layer 2 представляет собой надстройку над основным блокчейном (Layer 1), созданную для решения описанных выше проблем. Вот как Layer 2 решает эти проблемы:

Масштабируемость: Layer 2 позволяет обрабатывать гораздо больше транзакций в секунду, чем Layer 1. Это достигается путем переноса большей части транзакций и операций на второй уровень, где они могут выполняться быстрее и более эффективно. Только результаты этих операций периодически записываются на Layer 1 благодаря механизмам безопасности, обеспечивающим целостность данных.

Снижение комиссий: Поскольку Layer 2 позволяет обрабатывать множество транзакций без необходимости включения каждой из них в блок Layer 1, комиссии на Layer 2 часто намного ниже, чем на Layer 1. Это делает использование блокчейна более доступным и эффективным для различных видов транзакций и приложений.

Повышенная эффективность разработки: Layer 2 упрощает разработку DApps и смарт-контрактов, так как многие задачи могут быть выполнены вне Layer 1. Разработчики получают больше свободы и гибкости в создании своих приложений, что способствует росту экосистемы блокчейна.

Таким образом, Layer 2 представляет собой мощное решение для устранения ограничений, с которыми сталкиваются блокчейн-сети, и является ключевым компонентом, способ-

ствующим более широкому принятию блокчейна в различных областях, начиная от финансов и заканчивая играми и децентрализованными приложениями.

1.2 Основные проблемы блокчейна

Блокчейн – это инновационная и обещающая технология, но он также сталкивается с несколькими ключевыми проблемами, которые затрудняют его широкое принятие и использование.

1.2.1 Масштабируемость

Одной из наиболее острых проблем блокчейна является масштабируемость, что означает способность сети обрабатывать большое количество транзакций за короткое время. В классических блокчейнах, таких как Bitcoin и Ethereum, есть ограничения по пропускной способности, что ограничивает количество транзакций, которые можно включить в блоки. Это приводит к следующим проблемам:

- **Задержки в обработке транзакций:** Поскольку блокчейн обрабатывает транзакции по очереди, с высокой загрузкой сети возникают задержки в выполнении транзакций. Пользователи вынуждены ждать длительное время, пока их транзакции будут подтверждены.

- **Высокие комиссии:** При ограниченной пропускной способности пользователи, желающие ускорить обработку своих транзакций, устанавливают высокие комиссии. Это приводит к высоким затратам на отправку даже небольших сумм.

- **Ограничения масштабируемости DApps:** Для децентрализованных приложений, работающих на блокчейне, масштабируемость становится серьезным ограничением. Если блокчейн не способен обрабатывать большое количество транзакций, то DApps также ограничены в своей производительности.

1.2.2 Высокие комиссии

Высокие комиссии – это прямое следствие ограниченной масштабируемости. Пользователи вынуждены предлагать более высокие комиссии для включения своих транзакций в следующий блок. Это создает конкуренцию за место в блоке и может сделать отправку транзакций дорогостоящей. Высокие комиссии могут иметь следующие последствия:

- **Неэффективность микроплатежей:** Микроплатежи, как правило, страдают от высоких комиссий, что делает их нерентабельными на блокчейне.

- **Ограничение доступности:** Пользователи с низкими доходами могут столкнуться с трудностями в доступе к блокчейн-сервисам из-за высоких комиссий.

1.2.3 Сложность разработки

Разработка смарт-контрактов и DApps на блокчейне может быть сложной задачей:

- **Языковые ограничения:** Многие блокчейны используют специфические языки программирования (например, Solidity для Ethereum), что делает разработку более сложной и ограничивает выбор разработчиков.

- **Отладка и тестирование:** Отладка смарт-контрактов может быть сложной, и ошибки могут привести к серьезным последствиям, включая потерю средств.

- **Ограниченная степень гибкости:** Блокчейн предоставляет ограниченную степень гибкости в реализации бизнес-логики, что может быть ограничивающим фактором для разработчиков.

Layer 2 представляет собой ряд инновационных решений, которые призваны решить или смягчить эти проблемы, улучшив производительность и удобство использования блокчейна.

1.3 Что такое Layer 2?

Layer 2 (Уровень 2) представляет собой концепцию, которая внедряется в мир блокчейна для улучшения его масштабируемости, производительности и функциональности, без изменения основного блокчейн-протокола, который является Layer 1 (Уровень 1).

Понятие Layer 2 аналогично добавлению второго уровня в архитектуре компьютерной сети. Он служит дополнительным слоем над основным блокчейн-протоколом и позволяет обра-

батывать большое количество транзакций и данных более эффективно. Вот ключевые аспекты Layer 2:

Второй уровень над основным блокчейном (Layer 1): В мире блокчейна, Layer 1 представляет собой основной протокол, такой как Bitcoin или Ethereum. Это первичная блокчейн-сеть, которая обеспечивает децентрализацию и безопасность, но она может иметь ограниченную масштабируемость и скорость транзакций из-за своей природы. Layer 2 строится поверх Layer 1, как дополнительный слой, дополняющий и расширяющий функциональность блокчейна.

Использует основную сеть для обеспечения безопасности и децентрализации: Одним из ключевых аспектов Layer 2 является его зависимость от безопасности и децентрализации Layer 1. Это означает, что Layer 1 остается конечным авторитетом, который обеспечивает безопасность и подтверждает транзакции, происходящие на Layer 2. Это дает уверенность пользователям, что их активы защищены и могут быть перенесены обратно на Layer 1 в случае необходимости.

Выполняет большинство транзакций и вычислений на своем собственном уровне: Layer 2 разгружает Layer 1, выполняя большую часть операций и вычислений на своем уровне. Это позволяет увеличить пропускную способность и скорость обработки транзакций без необходимости изменения основного блокчейна. Например, множество микротранзакций может быть обработано на Layer 2, и только итоговые результаты будут регистрироваться на Layer 1. Это существенно снижает нагрузку на Layer 1 и повышает эффективность всей системы.

Концепция Layer 2 стала ключевой для решения проблем масштабируемости и производительности блокчейна, и она представляет собой мощный инструмент для расширения возможностей этой технологии, делая ее более привлекательной и практичной для различных приложений и пользователей.

Повышение масштабируемости в Layer 2

Проблема низкой масштабируемости в Layer 1 блокчейн-сетях, таких как Bitcoin и Ethereum, долгое время была главной преградой на пути их массового использования. Эта проблема заключается в том, что основные блокчейны обладают ограниченной способностью обработки транзакций в секунду, что может привести к следующим проблемам:

1. Задержки и перегрузки: Когда блокчейн сеть перегружена, транзакции могут задерживаться на неопределенный срок, что снижает общую производительность и делает использование блокчейна неэффективным.

2. Высокие комиссии: Чтобы обеспечить приоритетное включение своих транзакций в блок, пользователи вынуждены платить высокие комиссии. Это становится особенно проблематичным в периоды активного использования сети.

3. Ограничения для масштабируемых приложений: Блокчейн-приложения, такие как децентрализованные финансы (DeFi) и онлайн-игры, требуют высокой пропускной способности и низкой задержки, чтобы предоставлять удовлетворительное пользовательское взаимодействие. Layer 1 ограничивает возможности этих приложений.

Роль Layer 2 в решении проблемы масштабируемости

Layer 2 призван решить эти проблемы, предоставляя дополнительный уровень масштабируемости поверх Layer 1. Вот как это работает:

1. Оффчейн транзакции: Layer 2 обрабатывает большинство транзакций вне основной блокчейн-сети. Это означает, что транзакции могут выполняться мгновенно и с минимальными комиссиями на уровне Layer 2, а не Layer 1.

2. Агрегация данных: Layer 2 может агрегировать несколько транзакций в одну, которая затем записывается на основной блокчейн. Это снижает нагрузку на Layer 1 и увеличивает пропускную способность.

3. Смарт-контракты на Layer 2: Некоторые решения Layer 2, такие как Rollups, позволяют выполнять смарт-контракты на втором уровне. Это значит, что вычисления и выполнение смарт-контрактов могут происходить быстро и эффективно, без привлечения Layer 1.

4. Платежные каналы и State Channels: Технологии, такие как Lightning Network для Bitcoin и Raiden Network для Ethereum, представляют собой примеры Layer 2, которые позволяют пользователям устанавливать приватные каналы для мгновенных и недорогих транзакций.

В результате использования Layer 2, блокчейн-сети становятся более масштабируемыми, производительными и доступными для широкого спектра приложений и пользователей. Это решение проблемы масштабируемости оказывает существенное воздействие на развитие блокчейна и его способность изменить различные отрасли, от финансов до цифровых искусств.

Снижение комиссий

Снижение комиссий является одним из ключевых преимуществ Layer 2 в мире блокчейна. Для более подробного понимания, давайте разберемся, как именно Layer 2 помогает снизить комиссии в сравнении с использованием только Layer 1.

Высокие комиссии на Layer 1:

На основном уровне блокчейна (Layer 1), когда сеть перегружена большим количеством транзакций, пользователи конкурируют за приоритет обработки своих транзакций. Для повышения шансов на быструю обработку, они готовы платить более высокие комиссии майнерам. В периоды пиковой активности комиссии на Layer 1 могут значительно возрасти, делая маленькие и обычные транзакции дорогими.

Layer 2 как решение:

Layer 2 позволяет снять большую часть нагрузки с Layer 1, перенося множество транзакций и вычислений на свой собственный уровень. Это снижает конкуренцию за обработку транзакций на Layer 1, и, следовательно, комиссии на Layer 1 становятся менее завышенными.

Как это работает:

1. Большинство транзакций обрабатываются внутри Layer 2: Вместо того, чтобы отправлять каждую транзакцию напрямую на Layer 1, пользователи проводят множество своих операций на Layer 2. Эти транзакции обрабатываются быстро и с низкими комиссиями, так как они не создают конкуренцию на Layer 1.

2. Фиксация на Layer 1 только при необходимости: Layer 2 периодически фиксирует свой баланс и состояние на Layer 1. Это происходит гораздо реже, чем бы это было в случае, если бы все транзакции проводились непосредственно на Layer 1. Фиксация на Layer 1 может быть дорогостоящей, но так как она выполняется редко, это несравнимо с постоянными высокими комиссиями на Layer 1.

Это позволяет пользователям экономить на комиссиях и делает более доступными как маленькие, так и большие транзакции. Снижение комиссий стимулирует развитие децентрализованных приложений, улучшая пользовательский опыт и облегчая принятие блокчейна в повседневной жизни.

Большая гибкость и функциональность

Layer 2 открывает перед разработчиками блокчейн-приложений огромные возможности в области гибкости и функциональности. Этот аспект чрезвычайно важен, так как он способствует созданию разнообразных децентрализованных приложений (DApps) и расширяет границы того, что можно сделать на блокчейне. Вот несколько ключевых аспектов:

Разнообразие DApps:

- *Децентрализованные финансы (DeFi):* Сегодня DeFi считается одним из самых динамично развивающихся сегментов в мире блокчейна. Layer 2 предоставляет DeFi-проектам возможность выполнять транзакции и операции с активами более быстро и с меньшими

комиссиями. Это включает в себя децентрализованные обменники, кредитные протоколы, стейблкоины и другие финансовые инструменты.

- *Игры и NFT*: Layer 2 также открывает новые горизонты для игровой индустрии и коллекционирования цифровых активов. Игры на блокчейне могут стать более интересными и масштабируемыми благодаря возможности проводить моментальные и дешевые транзакции. Кроме того, некоторые Layer 2 решения обеспечивают более широкую поддержку для нефунгибельных токенов (NFT), что способствует развитию рынка NFT и совместимости с различными блокчейнами.

- *Интернет вещей (IoT)*: Layer 2 также может быть применен для расширения возможностей Интернета вещей. Это позволяет создавать децентрализованные системы управления и обмена данными между устройствами, повышая безопасность и эффективность IoT-решений.

Улучшенная производительность и пользовательский опыт:

- *Скорость и комиссии*: Layer 2 снижает задержки и уровень комиссий, что делает блокчейн более доступным для широкой аудитории. Это значительно улучшает пользовательский опыт и способствует массовому принятию технологии.

- *Больше операций за секунду*: Layer 2 может поддерживать гораздо большее количество транзакций и операций в секунду, что важно для приложений, требующих высокой производительности.

Инновационные решения:

- *Эксперименты и инновации*: Layer 2 стимулирует конкуренцию и инновации среди разработчиков, поскольку они могут экспериментировать с новыми идеями и проектами без значительных инвестиций в сетевую безопасность и обслуживание.

- *Устранение ограничений*: С увеличением функциональности Layer 2, разработчики могут устранять ограничения, которые ранее ограничивали их возможности на блокчейне.

Layer 2, таким образом, создает плодородную почву для инноваций и развития экосистемы блокчейна, делая эту технологию более привлекательной для различных отраслей и бизнес-сценариев.

Технологии Layer 2

Layer 2 представляет собой многофункциональный набор технологий, предназначенных для оптимизации работы блокчейна. Каждая из этих технологий решает конкретные проблемы, стоящие перед блокчейном, и обладает своими уникальными характеристиками. Давайте более подробно рассмотрим основные технологии Layer 2:

Sidechains (Подсети)

Описание: Sidechains – это независимые блокчейны, связанные с основным блокчейном (Layer 1), который называется главной цепью. Они предоставляют большую гибкость и масштабируемость, позволяя пересылать активы между главной цепью и подцепями.

Преимущества:

- **Масштабируемость**: Подсети могут обрабатывать большое количество транзакций независимо от главной цепи.

- **Гибкость**: Разработчики могут настраивать подсети под конкретные нужды приложений.

- **Интероперабельность**: Активы могут свободно перемещаться между главной цепью и подцепями.

Plasma (Плазма)

Описание: Plasma – это концепция, предложенная Джозефом Пуном (Joseph Poon) и Виталиком Бутериным (Vitalik Buterin), которая позволяет создавать подцепи (плазменные цепи) для увеличения производительности и масштабируемости. Эти подцепи могут быть дочерними к главной цепи.

Преимущества:

- **Высокая масштабируемость:** Плазменные цепи могут обрабатывать большое количество транзакций внутри себя, передавая только суммарные результаты на главную цепь.

- **Снижение комиссий:** Транзакции внутри плазменных цепей могут быть более дешевыми, чем на главной цепи.

- **Гибкость и инновации:** Разработчики могут создавать разнообразные приложения и смарт-контракты в плазменных цепях.

State Channels (Каналы состояния)

Описание: State Channels – это механизм, который позволяет двум или более участникам установить частные каналы связи между собой и проводить неограниченное количество транзакций внутри этих каналов, не записывая каждую транзакцию на главную цепь.

Преимущества:

- **Моментальные транзакции:** Транзакции внутри каналов обрабатываются моментально, без задержек.

- **Эффективность:** Использование каналов состояния может существенно снизить комиссии и нагрузку на главную цепь.

- **Приватность:** Транзакции внутри каналов могут быть частными и недоступными для других участников сети.

Rollups (Роллапы)

Описание: Rollups – это технологии, которые объединяют безопасность Layer 1 с масштабируемостью Layer 2. Существует два основных типа Rollups: Optimistic Rollups и Zk-Rollups.

Преимущества:

- **Безопасность Layer 1:** Rollups используют главную цепь для обеспечения безопасности, что делает их надежными.

- **Масштабируемость Layer 2:** Они обрабатывают большое количество транзакций на своем уровне, значительно повышая производительность.

Каждая из этих технологий Layer 2 имеет свои уникальные преимущества и ограничения, и разработчики могут выбирать подходящий инструмент в зависимости от конкретных потребностей своих проектов. Вместе они составляют мозаику решений, которые улучшают эффективность и функциональность блокчейн-экосистемы.

Глава 2: Sidechains – Когда блокчейн встречает блокчейн

Понятие Sidechains

С развитием технологии блокчейн стало очевидным, что существующие блокчейны, такие как Bitcoin и Ethereum, имеют свои ограничения и проблемы. Одной из главных проблем является масштабируемость – способность блокчейна обрабатывать большое количество транзакций в короткие сроки. Это ограничение становится серьезной преградой для массового принятия технологии, так как увеличивается время подтверждения транзакций и возрастают комиссии за транзакции.

Слово "sidechain" переводится как "боковая цепь", и это понятие олицетворяет собой решение, которое было разработано для решения проблем масштабируемости и других ограничений основных блокчейнов. Идея заключается в создании дополнительного блокчейна, который работает параллельно с основным блокчейном (часто называемым Layer 1), но обладает некоторой степенью автономии и способности взаимодействовать с ним.

Ключевые характеристики Sidechains:

1. **Параллельность:** Sidechain существует параллельно с основным блокчейном и имеет свою собственную цепь блоков, независимую от основной цепи.
2. **Совместимость:** Sidechain может быть разработан так, чтобы быть совместимым с основным блокчейном, что облегчает передачу активов между ними.
3. **Гибкость:** Разработчики могут настраивать sidechain под свои нужды, определяя параметры, такие как скорость блоков, размер блоков и механизм согласования.
4. **Интероперабельность:** Sidechain может взаимодействовать с другими sidechains и даже с основными блокчейнами, обеспечивая большую гибкость и функциональность.

Применение Sidechains:

1. **Улучшенная масштабируемость:** Sidechains позволяют обрабатывать большее количество транзакций в секунду, уменьшая задержки и комиссии.
2. **Разработка смарт-контрактов:** Некоторые sidechains предоставляют функциональность смарт-контрактов, позволяя разработчикам создавать децентрализованные приложения.
3. **Конфиденциальность:** Некоторые sidechains могут предоставлять дополнительные уровни конфиденциальности для пользователей и транзакций.
4. **Эксперименты и инновации:** Sidechains предоставляют среду для экспериментов и тестирования новых функций и улучшений без риска нарушения стабильности основного блокчейна.

Итак, понятие sidechains в мире блокчейна представляет собой мощное средство для решения ограничений и проблем, связанных с масштабируемостью и функциональностью основных блокчейнов. Они позволяют блокчейн-экосистеме стать более гибкой, эффективной и способной удовлетворять потребности разных видов пользователей и разработчиков.

Примеры популярных Sidechains

В этом разделе мы рассмотрим несколько популярных sidechains, которые созданы для разных блокчейн-экосистем и выполняют разнообразные функции. Каждый из них представляет уникальные решения и подходы к улучшению масштабируемости, конфиденциальности или другим аспектам блокчейн-технологии.

RSK (Rootstock)

RSK, или **Rootstock**, это один из наиболее известных sidechains, разработанных специально для сети **Bitcoin**. Он интегрируется с Bitcoin, используя собственный токен **RBTC** (Rootstock Bitcoin), который имеет паритет с BTC в соотношении 1:1. Основная цель RSK

– предоставить возможность смарт-контрактов в экосистеме Bitcoin, расширив его функциональность и конкурентоспособность с Ethereum.

Преимущества RSK:

- **Совместимость с Bitcoin:** RSK позволяет пользователям использовать свои Bitcoin на сети RSK для создания и выполнения смарт-контрактов, не теряя своих BTC.
- **Смарт-контракты:** RSK поддерживает смарт-контракты, что делает его привлекательным для разработчиков децентрализованных приложений и услуг.
- **Паритет с Bitcoin:** RBTC имеет 1:1 паритет с Bitcoin, что обеспечивает стабильный курс и сохранение стоимости активов.

Binance Smart Chain

Binance Smart Chain (BSC) – это sidechain, разработанный **Binance**, одной из крупнейших криптобирж в мире. BSC создана с целью предоставить более быстрые и дешевые транзакции по сравнению с Ethereum. Она также поддерживает смарт-контракты, что делает BSC конкурентоспособной альтернативой Ethereum для разработчиков.

Преимущества Binance Smart Chain:

- **Высокая масштабируемость:** BSC спроектирована так, чтобы обрабатывать значительно больше транзакций в секунду, чем Ethereum, что снижает комиссии и уменьшает задержки.
- **Совместимость с Binance:** Пользователи могут легко переносить активы между Binance и BSC, что упрощает взаимодействие с криптовалютной биржей Binance.
- **Децентрализованность сети:** Несмотря на то, что BSC контролируется Binance, она все равно децентрализована, и каждый участник может стать валидатором блоков.

Polygon (Matic)

Polygon, ранее известный как **Matic Network**, представляет собой sidechain для **Ethereum**. Она разработана с целью улучшения масштабируемости и производительности Ethereum, что помогает решить проблемы высоких комиссий и задержек на этой сети.

Преимущества Polygon:

- **Высокая масштабируемость:** Polygon поддерживает множество sidechains, каждая из которых способна обрабатывать множество транзакций в секунду, значительно увеличивая масштабируемость.
- **Смарт-контракты:** Polygon совместим с Ethereum, поэтому смарт-контракты, разработанные для Ethereum, могут быть легко развернуты на Polygon.
- **Низкие комиссии:** Использование Polygon обычно связано с низкими комиссиями за транзакции, что делает его привлекательным для пользователей и разработчиков.

Это лишь несколько примеров популярных sidechains, и существует множество других проектов, каждый из которых направлен на решение конкретных проблем и улучшение определенных аспектов блокчейн-технологии. Sidechains предоставляют инновационные решения для более эффективного использования блокчейн-технологии и ее интеграции в разнообразные экосистемы.

Преимущества и недостатки Sidechains

Sidechains представляют собой уникальное и мощное средство для улучшения функциональности блокчейн-сетей, но они также имеют свои преимущества и недостатки, которые следует внимательно рассмотреть при их реализации и использовании.

Преимущества Sidechains:

Масштабируемость

Один из ключевых аргументов в пользу sidechains – это их способность увеличивать масштабируемость блокчейн-сетей. Sidechains могут обрабатывать собственные транзакции параллельно с основным блокчейном, что позволяет сети обрабатывать гораздо больше опера-

ций в секунду. Это особенно важно для популярных блокчейнов, таких как Bitcoin и Ethereum, которые могут сталкиваться с проблемой перегрузки.

Скорость транзакций

Sidechains предлагают значительно более быстрые транзакции по сравнению с основными блокчейнами. Поскольку sidechain может использовать оптимизированные алгоритмы согласования, время обработки транзакций сокращается до секунд, а не минут или часов, как это иногда бывает на основных блокчейнах. Это позволяет пользователям получать быстрые подтверждения транзакций.

Конфиденциальность

Некоторые sidechains специализируются на повышении уровня конфиденциальности транзакций. Это особенно важно для корпоративных клиентов и институциональных участников, которым может потребоваться большая конфиденциальность в сделках. Sidechains могут предоставлять инструменты для реализации конфиденциальных сделок и обработки данных без их раскрытия всей сети.

Совместимость

Sidechains могут быть разработаны так, чтобы быть совместимыми с разными блокчейнами. Это означает, что активы могут легко перемещаться между различными блокчейнами через sidechains. Это обеспечивает более гибкую интеграцию между разными экосистемами блокчейнов и упрощает обмен активами.

Недостатки Sidechains:

Децентрализация

Один из главных недостатков sidechains – это потенциальная утрата децентрализации. В зависимости от дизайна и механизма согласования, sidechain может быть менее децентрализованным, чем основной блокчейн. Это может создавать риски для безопасности и целостности данных.

Безопасность

Уровень безопасности sidechain зависит от его дизайна и использованных механизмов согласования. Недостаточная безопасность sidechain может привести к утечкам средств и другим проблемам. Поэтому важно тщательно проектировать и аудировать sidechains, чтобы гарантировать их надежность.

Риски централизации

Существует риск, что управление и развитие sidechain может сосредоточиться в руках небольшой группы лиц или организаций. Это может привести к проблемам с централизацией и ущемлению интересов общественности.

Конфиденциальность и анонимность

Хотя увеличение конфиденциальности может считаться преимуществом, оно также может создавать проблемы в соблюдении законодательства, особенно в финансовой сфере. Регуляторы могут требовать доступа к данным транзакций для борьбы с преступностью и предотвращения отмывания денег.

В заключение, sidechains предоставляют множество преимуществ в улучшении масштабируемости и функциональности блокчейн-сетей. Однако при их использовании следует тщательно взвешивать преимущества и недостатки, уделяя особое внимание децентрализации, безопасности и соблюдению регуляторных норм. Каждый проект sidechain должен быть разработан и реализован с учетом уникальных потребностей и задач, которые он должен решить.

Глава 3: Plasma – Масштабируемость на основе смарт-контрактов

Введение в Plasma

Для понимания Plasma как технологии масштабирования в блокчейне, важно начать с основ и понятий, которые лежат в его основе.

Понятие масштабируемости: Масштабируемость в контексте блокчейна означает способность сети обрабатывать большое количество транзакций или данных без значительного увеличения времени и стоимости их обработки. Традиционные блокчейны, такие как Bitcoin и Ethereum, столкнулись с ограничением в масштабируемости, когда число пользователей и объемы транзакций значительно увеличились, что привело к перегрузке сети и повышенным комиссиям.

Идея Plasma: Plasma представляет собой парадигму, которая предлагает решение для проблемы масштабируемости. Она была предложена Джозефом Пуном и Виталиком Бутериным в 2017 году. Основная идея Plasma заключается в создании дочерних цепей (или подцепей), которые связаны с главной цепью (обычно Ethereum) и позволяют обрабатывать множество транзакций внутри этих дочерних цепей, а затем сжимать эту информацию и хешировать ее на главной цепи. Это позволяет значительно увеличить производительность и масштабируемость блокчейн-сети.

Дочерние цепи: Дочерние цепи – это независимые блокчейны, которые подключены к главной цепи, называемой "родительской цепью" (parent chain). Они могут иметь свои собственные правила и логику, что делает их гибкими в адаптации для различных видов приложений. Эти дочерние цепи могут иметь собственных участников и операторов узлов, но они все равно зависят от безопасности главной цепи.

Обобщенное состояние (Plasma-чейн): Важной концепцией в Plasma является идея "обобщенного состояния" (Plasma chain). Это состояние включает в себя данные о балансах и транзакциях, которые произошли внутри дочерней цепи. Обобщенное состояние периодически фиксируется и хешируется на главной цепи, что обеспечивает безопасность и надежность Plasma.

Преимущества Plasma: Главными преимуществами Plasma являются:

- **Масштабируемость:** Plasma значительно увеличивает пропускную способность сети, позволяя обрабатывать множество транзакций параллельно.
- **Эффективность смарт-контрактов:** Смарт-контракты могут быть выполнены на дочерних цепях, что делает их быстрее и более экономичными.
- **Снижение комиссий:** Использование Plasma может снизить стоимость транзакций для пользователей.

Ограничения Plasma: Несмотря на множество преимуществ, у Plasma есть и ограничения, такие как сложность разработки дочерних цепей, безопасность и риски при выходе активов из дочерних цепей.

В заключении, Plasma представляет собой мощную концепцию масштабирования для блокчейн-систем, которая позволяет сетям обрабатывать больше данных и транзакций, улучшая производительность и снижая стоимость использования. Понимание основных принципов Plasma является ключом к пониманию его потенциальных применений и вызовов.

Plasma MVP

Minimum Viable Plasma (MVP) представляет собой первую и наиболее известную итерацию концепции Plasma, созданную Джозефом Пуном и Виталиком Бутериным. Эта итерация

была разработана на базе Ethereum и служила первым шагом в создании масштабируемого блокчейна с использованием дочерних цепей.

Принцип работы Plasma MVP:

1. **Создание дочерних цепей:** MVP предполагает наличие дочерних цепей, которые связаны с главной цепью Ethereum. Эти дочерние цепи называются "Plasma-цепями" и имеют свои собственные правила и смарт-контракты.

2. **Перевод средств на Plasma-цепь:** Пользователи могут переводить свои средства (ETH и токены) с главной цепи на Plasma-цепь. Этот процесс называется "вкладом" (deposit). Пользователь блокирует свои средства в смарт-контракте на главной цепи, и на их основе создается эквивалентное количество токенов на Plasma-цепи.

3. **Смарт-контракты и исполнение:** Вся логика и смарт-контракты находятся на Plasma-цепи, что делает их исполнение быстрым и эффективным. Пользователи могут взаимодействовать с этой цепью так же, как с главной.

4. **Следящие ноды (Watchers):** Это ноды, которые следят за состоянием Plasma-цепи и наблюдают за транзакциями. Они обеспечивают безопасность путем контроля и регистрации состояния Plasma-цепи.

5. **Подведение итогов на главной цепи:** Этот шаг является ключевым в Plasma MVP. По мере выполнения транзакций на Plasma-цепи, следящие ноды регистрируют состояния. Затем они агрегируют эти состояния в блок данных и хешируют их. Этот хеш (или "корень Меркла") регулярно отправляется на главную цепь Ethereum. Это позволяет обеспечить безопасность Plasma-цепи, так как любой пользователь может проверить состояние, сравнивая его с корнем Меркла.

6. **Выходные транзакции и завершение:** Когда пользователь решает выйти из Plasma-цепи и вернуть свои средства на главную цепь, он отправляет специальную "выходную транзакцию" (exit transaction). Следящие ноды мониторят эти транзакции и проверяют, что они корректны. Если транзакция корректна, пользователю возвращаются его средства из смарт-контракта на главной цепи.

Преимущества Plasma MVP:

1. **Масштабируемость:** Plasma MVP позволяет обрабатывать множество транзакций на Plasma-цепи, снижая нагрузку на главную цепь Ethereum.

2. **Эффективность смарт-контрактов:** Исполнение смарт-контрактов на Plasma-цепи происходит быстро и экономично.

3. **Снижение комиссий:** Использование Plasma MVP может снизить стоимость транзакций для пользователей блокчейна.

Однако Plasma MVP также имеет свои ограничения и вызовы, такие как сложность создания и поддержки Plasma-цепей, а также вопросы безопасности и выхода из цепей. Важно учитывать эти факторы при рассмотрении применения Plasma MVP в блокчейн-проектах.

Plasma Cash: Улучшенная масштабируемость и безопасность блокчейна

Plasma Cash представляет собой улучшенную версию Plasma, разработанную для решения некоторых ограничений оригинального Plasma MVP (Minimum Viable Plasma). Подробно рассмотрим особенности Plasma Cash, преимущества и ограничения этой технологии:

Уникальные идентификаторы монет:

Основная особенность Plasma Cash заключается в том, что каждая монета в дочерней цепи имеет уникальный идентификатор, как уникальный номер или хэш. Это существенное отличие от Plasma MVP, где состояние цепи было представлено в виде слитного набора данных, что затрудняло индивидуальное отслеживание монет.

Преимущества Plasma Cash:

1. **Улучшенная безопасность и конфиденциальность:** Поскольку каждая монета имеет уникальный идентификатор, это делает Plasma Cash более безопасной технологией для

пользователей. Они могут легче отслеживать и защищать свои активы, так как монеты не являются взаимозаменяемыми.

2. Быстрые проверки состояния: В Plasma Cash для проверки состояния необходимо только проверить наличие и уникальность конкретной монеты. Это значительно упрощает и ускоряет процесс проверки, по сравнению с проверкой всего состояния цепи, как это делалось в MVP.

3. Упрощенная архитектура: Из-за уникальных идентификаторов монет архитектура Plasma Cash проще и менее подвержена ошибкам. Это делает разработку и обслуживание Plasma Cash-цепей более удобными.

4. Эффективность использования ресурсов: Plasma Cash позволяет более эффективно использовать ресурсы сети блокчейна, так как проверка монеты требует меньше вычислительной мощности, чем проверка всего состояния цепи.

Ограничения Plasma Cash:

1. Сложности выхода из дочерней цепи: Пользователям следует быть осторожными при выходе из Plasma Cash-цепи, так как могут возникнуть проблемы с проверкой уникальных идентификаторов монет. Неверный выход может привести к потере активов.

2. Исследование и разработка: Plasma Cash – это ещё относительно новая технология, и её разработка может потребовать значительных усилий и ресурсов.

3. Безопасность смарт-контрактов: Поскольку смарт-контракты в дочерней цепи исполняются независимо, их безопасность и надежность могут потребовать дополнительного внимания и аудита.

Plasma Cash представляет собой инновационное решение, которое улучшает масштабируемость и безопасность блокчейна, предоставляя уникальные идентификаторы для каждой монеты. Эта технология имеет потенциал стать ключевым элементом будущего блокчейна и позволить масштабировать децентрализованные приложения на новом уровне.

Преимущества и ограничения Plasma

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.