Технологии ZK

UBF

Что такое ZK?

В криптовалютном мире, Zero-Knowledge Rollups (ZK Rollups) и Optimistic Rollups являются двумя видами технологий расширения масштабируемости блокчейна, каждая из которых имеет свои особенности. Сейчас топовые проекты соревнуются в эффективности, самый технологичный и маркетингово-продуманный проект будет очень жирно качать в цикле 2024-2026.

Тема техническая, поэтому давайте разберем в чем смысл этих технологий на простых примерах из жизни. А дальше уже перейдем к технической части, тому, как это работает, отличиям и всему, что позволит одной технологии обойти другую в новом бычьем цикле.

Zero-Knowledge Rollups (ZK-Rollups)

Zero-Knowledge Rollups (ZK-Rollups) — это технология в области криптовалют, которая помогает ускорить транзакции и снизить их стоимость, при этом сохраняя безопасность и приватность. Давайте рассмотрим простой пример из реальной жизни, чтобы объяснить, как это работает.

Представьте, что вы учитель в классе с 30 учениками. Каждый день ученики сообщают вам о своих домашних заданиях. В традиционной системе (аналог блокчейна без ZK-Rollups) вы бы проверяли каждое задание по отдельности, что занимает много времени.

Теперь представьте, что вместо этого у вас есть умный помощник, который может быстро проверить все домашние задания и просто сообщить вам, что все задания выполнены правильно, не раскрывая конкретных деталей каждого задания. Это и есть Zero-Knowledge Rollup. Помощник (ZK-Rollup) собирает все данные о домашних заданиях (транзакциях), быстро и эффективно проверяет их и передает вам только итоговый результат, не раскрывая подробностей. Таким образом, вы экономите время и ресурсы, так как вам не нужно проверять каждую задачу вручную.

То есть, ZK-Rollups позволяют собирать множество транзакций в одну группу, быстро проверять их все вместе, а затем передавать в основную сеть криптовалюты только сводную информацию о них. Это повышает эффективность и скорость обработки транзакций, уменьшая при этом их стоимость и загрузку на сеть.

Optimistic Rollups

Optimistic Rollups — это технология в мире криптовалют, которая направлена на увеличение скорости и снижение стоимости транзакций в блокчейне. Для понимания этой концепции давайте воспользуемся простым примером из повседневной жизни.

Представьте, что вы управляете кафе, где клиенты делают заказы, оплачивают их, а вы выдаёте им чеки. В обычной системе (аналог блокчейна без Optimistic Rollups), вы бы проверяли платёж каждого клиента, прежде чем выдать ему чек. Это занимает время и создаёт очереди.

Теперь допустим, вы решили ускорить процесс. Вы начинаете выдавать чеки клиентам сразу после их заказа, действуя по принципу "доверяю, но проверяю". Это означает, что вы оптимистично предполагаете, что большинство клиентов честные и оплатят свой заказ. Однако, в конце дня вы всё равно проверяете записи, чтобы убедиться, что все оплаты были произведены корректно.

В этом сценарии кафе — это блокчейн, заказы клиентов — это транзакции, а ваша система выдачи чеков без немедленной проверки платежа — это Optimistic Rollup. Вы оптимистично предполагаете, что транзакции действительны и обрабатываете их быстро, но оставляете возможность для последующей проверки на случай обнаружения неправомерных действий. Это ускоряет процесс и снижает нагрузку на вашу систему (блокчейн), но при этом сохраняет безопасность, позволяя впоследствии проверить и исправить любые недочёты.

Сравнение Zero-Knowledge Rollups (ZK Rollups) и Optimistic Rollups по пунктам

А теперь к более продвинутому материалу. Намного легче будет читаться после информации выше, не так ли?

Эффективность и Технологичность:

Zero-Knowledge Rollups: Они используют математические доказательства (zero-knowledge proofs), чтобы подтверждать корректность транзакций. Это обеспечивает высокую степень безопасности и эффективности, так как не требуется проверка каждой транзакции участниками сети.

Optimistic Rollups: Они предполагают, что транзакции верны по умолчанию, и только в случае оспаривания требуется их проверка. Это снижает немедленную нагрузку на вычислительные ресурсы, но может увеличить время ожидания в случае споров.

Сжатие Блоков:

Zero-Knowledge Rollups: Эффективно сжимают данные транзакций, благодаря чему в блок можно включить больше транзакций. Это повышает пропускную способность сети.

Optimistic Rollups: Также позволяют сжать данные транзакций, но в меньшей степени, чем ZK Rollups. Они сосредотачиваются на упрощении процесса верификации.

Время Проверки:

Zero-Knowledge Rollups: Требуется меньше времени на проверку благодаря использованию zero-knowledge proofs, которые быстро подтверждают корректность транзакций без необходимости их полного раскрытия.

Optimistic Rollups: Время проверки может быть длиннее, особенно в случае оспаривания транзакций, так как требуется полная проверка данных.

Доверие:

Zero-Knowledge Rollups: Предлагают более высокий уровень доверия из-за математической надёжности zero-knowledge proofs. Они уменьшают зависимость от доверия к операторам сети.

Optimistic Rollups: Требуют большего доверия к операторам, поскольку они предполагают, что транзакции верны, пока не будет доказано обратное.

В общем, ZK Rollups предлагают более высокий уровень безопасности и эффективности, но могут быть более сложными в реализации и интеграции. Optimistic Rollups, с другой стороны, предоставляют более простой подход к масштабированию, но с потенциально более высокими затратами времени и доверия в случае оспаривания транзакций.

Текущее состояние и перспективы развития проектов Optimism, Arbitrum, StarkNet и zkSync

1. Optimism:

Тип Цепи: Строит L2 цепочки (Layer 2 на базе Ethereum).

Применение: Оптимизм используется не только для увеличения количества транзакций в рамках сети Ethereum, но также для построения новых L2 цепочек (например, проекты Manta, OBNB от Binance, GMX).

Отсутствие Собственного Токена: Оптимизм не имеет своего собственного токена, оплата внутри сети происходит в эфире. Governance токены (OP) используются только для функций управления.

2. Arbitrum:

Тип Цепи: Позволяет строить L3 цепочки.

Применение: Arbitrum известен своими дешевыми комиссиями и быстрыми транзакциями в рамках сети Ethereum. Проекты, такие как GMX, используют Arbitrum для построения L3 цепочек.

Недостатки: Может столкнуться с конкуренцией от более новых технологий, таких как StarkNet и zkSync, что может повлиять на комиссии и транзакции.

3. StarkNet:

Тип Цепи: Строит собственные L2 и L3 цепочки.

Применение: StarkNet предоставляет возможность использования собственного токена (STRK) в рамках сети для оплаты комиссий за транзакции, участия в протоколе и управления. Стремится к низким комиссиям.

Конвертация Токена: Существует предположение о конвертации токена STRK в эфиры для оплаты комиссий в момент создания блока. Наценка на STRK может быть плавающей.

4. zkSync

Тип Цепи: zkSync - это решение Layer 2 (L2), построенное на базе Ethereum, предназначенное для увеличения масштабируемости блокчейна. Оно достигается за счет сочетания низких комиссий за транзакции и быстрых операций.

Применение: Разработчики используют zkSync для снижения комиссионных сборов по сравнению с Ethereum. Технология широко применяется в приложениях децентрализованных финансов (DeFi). Среди ключевых проектов на базе zkSync - Syncswap, Mute и Maverick Protocol, которые представляют собой децентрализованные биржи. Также стоит отметить GRVT, первую частную цепочку приложений в ZK Stack, представляющую собой гибридный обмен (HEX), поддерживаемый Matterlabs, создателями zkSync.

Технические особенности: zkSync использует технологию zero-knowledge rollups для обеспечения безопасности и конфиденциальности транзакций. Также оно поддерживает смарт-контракты, написанные на Solidity или Vyper

Анализ и перспективы:

Optimism: Специализируется на построении новых L2 цепочек и позиционирует себя как платформу для новых Layer 2 решений. Основное внимание уделяется развитию Super Chain.

Arbitrum: Известен своей эффективностью и дешевыми комиссиями. Основное преимущество - возможность строить L3 цепочки. Может столкнуться с конкуренцией от более новых технологий.

StarkNet: Позиционирует себя как проект с низкими комиссиями и предоставляет возможность использования собственного токена

zkSync: Является ключевым решением Layer 2 для улучшения масштабируемости Ethereum, привлекая множество DeFi проектов и демонстрируя значительный потенциал для будущего развития в блокчейн-индустрии.

Проекты Optimism, Arbitrum, StarkNet и zkSync находятся в разных фазах развития и предоставляют различные возможности для разработчиков и пользователей. Выбор между ними может зависеть от конкретных потребностей и целей проекта. С развитием технологий и выходом майнетов, станет более ясно, какие из этих проектов будут успешными в будущем.

В качестве заключения:

Старые проекты, такие как Optimism и Arbitrum, могут сохранять свои позиции, но новые технологии, представленные StarkNet и zkSync, считаются технологически более передовыми. Прогнозируется, что они смогут обойти по цене токена и капитализации старые проекты.