ТРИЛЕММА БЛОКЧЕЙНА

Никита МАКЕЕВ

Департамент Программная Инженерия и Автоматика, группа TI-231M, Факультет Вычислительной Техники, Информатики и Микроэлектроники, Технический Университет Молдовы, Кишинев, Молдова

Автор Корреспондент: Никита МАКЕЕВ, e-mail: nichita.macheev@isa.utm.md

Научный руководитель: **Ирина ЧЕРНЕЙ**

***Аннотация**: Статья освещает одну из ключевых проблем в области блокчейна – трилемме блокчейна, которая включает в себя вопросы безопасности, масштабируемости и децентрализации. Будут рассмотрены определения ключевых понятий, проблема трилеммы в контексте блокчейна, а также потенциальные пути ее решения.*

***Ключевые слова**: блокчейн, трилемма блокчейна, безопасность, масштабируемость, децентрализация.*

Введение

В эпоху цифровых технологий блокчейн представляет собой революционное нововведение, предоставляющее возможность создания защищенных, децентрализованных систем. Однако разработчики блокчейна сталкиваются с фундаментальной проблемой, известной как трилемма блокчейна, которая подразумевает сложность одновременного достижения трех ключевых характеристик: безопасности, масштабируемости и децентрализации.

Трилемма блокчейна определение.

Блокчейн — это децентрализованная технология распределенного реестра, которая обеспечивает надежную и неизменяемую запись транзакций без необходимости в центральном органе управления. Эта технология лежит в основе криптовалют, таких как Bitcoin, и может использоваться в различных приложениях, от финансов до смарт-контрактов и за пределами. (Рисунок 1)

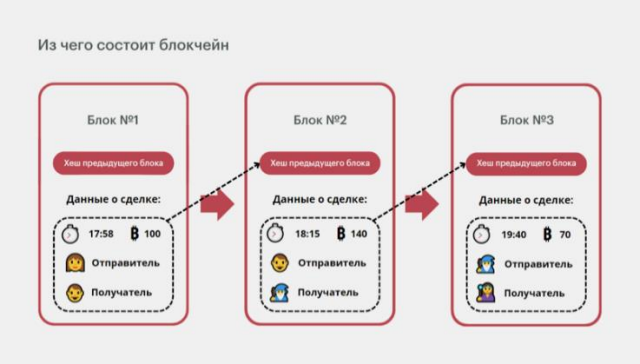

Рисунок 1 – Блокчейн [1]

Трилемма блокчейна – это концепция, согласно которой блокчейн – сеть может обладать максимум двумя из трех качеств: безопасностью, масштабируемостью и децентрализацией. Эта проблема ставит перед разработчиками сложный выбор при проектировании сетей. (Рисунок 2)

Рисунок 2 – Блокчейн [2]

- Безопасность обеспечивает защиту от атак и мошенничества.
- Масштабируемость позволяет сети обрабатывать большое количество транзакций.
- Децентрализация предполагает отсутствие единой контрольной точки, что способствует устойчивости и открытости сети.

Для дальнейшего расширения возможностей блокчейн – платформ и решения проблемы трилеммы, исследуются новые технологические подходы и алгоритмы. Например, используются методы для повышения скорости транзакций и улучшения масштабируемости сетей, такие как Lightning Network для Bitcoin, а также Plasma для Ethereum. Эти технологии стремятся разгрузить основную сеть, перенося часть транзакций на вторичные слои.

Развернутое представление проблемы

Существующие блокчейн – платформы, такие как Bitcoin и Ethereum, демонстрируют различные подходы к решению трилеммы, но каждая из них сталкиваются с ограничениями. Например, Bitcoin обеспечивает высокую степень безопасности и децентрализации за счет масштабируемости, в то время как некоторые новые сети пытаются находить баланс за счет внедрения дополнительных слоев и протоколов.

Пути решения

Среди подходов к решению трилеммы блокчейна выделяются следующие:

- Слоистая архитектура: Разделение функций между различными слоями блокчейна, где один слой может обеспечивать безопасность, другой — масштабируемость. (Пример: Ethereum 2.0, где внедряется слоистая архитектура с использованием шардинга для повышения масштабируемости).
- Сайдчейны и оффчейны: Разработка дополнительных блокчейнов, которые работают параллельно основному блокчейну и способны обрабатывать транзакции вне основной сети. (Примеры: Polygon (MATIC) для Ethereum, обеспечивающий масштабируемость с помощью сайдчейнов).
- Sharding: Разделение данных на части (шарды), чтобы узлы сети обрабатывали только часть данных, что значительно повышает масштабируемость. (Пример: Zilliqa, реализующий шардинг на уровне сети для повышения пропускной способности транзакций).
- Консенсусные алгоритмы: Разработка новых алгоритмов консенсуса, которые могут обеспечить лучший баланс между безопасностью, масштабируемостью и децентрализацией. (Пример: Algorand, использующий алгоритм PPoS (Pure Proof of Stake) для достижения высокой скорости и безопасности транзакций при сохранении децентрализации).

Примеры решений multilayer architecture

Роллапы (Rollups) являются ключевой технологией для протоколов второго уровня в Ethereum. Во многих решениях на основе роллапов используется метод доказательства с нулевым разглашением. Эти технологии объединены под общим названием ZK-Rollups.

Arbitrum, Optimism, и StarkNet представляют собой решения второго уровня (Layer 2), которые направлены на увеличение масштабируемости Ethereum за счет обработки транзакций вне основной цепи. Эти проекты используют различные подходы, такие как оптимистические роллапы и zk-Rollups, для уменьшения нагрузки на основную сеть, сокращения времени обработки транзакций и снижения комиссий.

В роллапе транзакции объединяются в пакеты, где данные каждого перевода сжимаются. Эти «свертки» отправляют доказательство в основную сеть первого уровня (Ethereum), позволяя подтвердить достоверность всех транзакций пакета без их индивидуальной проверки. После верификации пакет включается в один из блоков. Один пакет роллапа может содержать тысячи транзакций, но в блокчейн первого уровня заносится минимальное количество данных.

Работа ZK-Rollups основана на трех компонентах:

- виртуальная машина протокола второго уровня (L2), группирующая транзакции;
- смарт-контракт верификатора, проверяющий пакеты;
- модуль, отправляющий пакеты в блокчейн первого уровня и обновляющий состояние.

Нода сети второго уровня выполняет первоначальную проверку транзакций. После накопления определенного количества переводов она объединяет их в пакет и создает ZK-доказательство. Пакет проверяется смарт-контрактом в сети первого уровня, который также управляет вводом и выводом средств в L2-блокчейн.Рисунок 3)

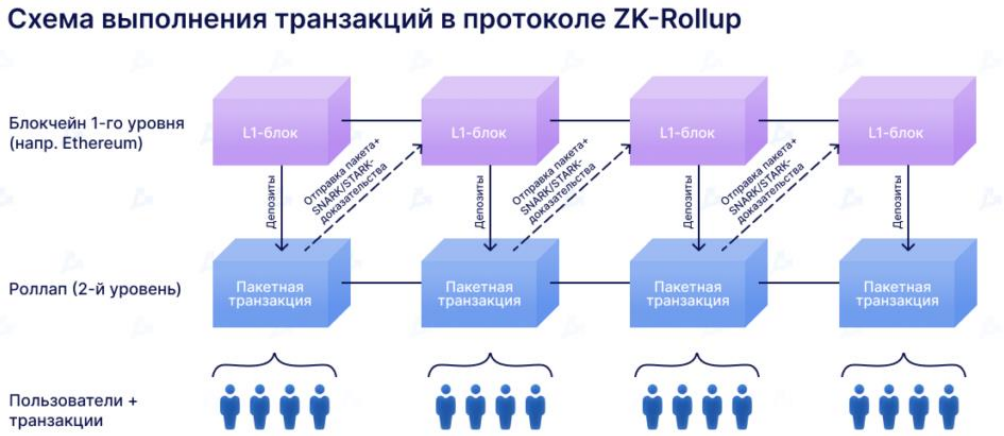

Рисунок 3 – ZK-Rollup [3]

Роллапы также включают в себя балансы пользователей в L2-сети, представленные в виде дерева Меркла, корень которого хранится в смарт-контракте. Это позволяет отслеживать изменения состояния сети. В блокчейн первого уровня также передаются значения, подтверждающие каждую транзакцию, включая корень дерева Меркла, который рассчитывается поэтапно. Промежуточные значения записываются в блокчейн и подтверждают каждый перевод в пакете.

Доказательства с нулевым разглашением сохраняют данные в основной сети после проверки каждого перевода, что обеспечивает актуальное состояние сети. В отличие от ZK-Rollups, при выводе средств из протокола Optimistic Rollups требуется проверка на мошенничество, которая может занять до двух недель, определяя время вывода средств в блокчейн первого уровня. Однако необходимость проверки данных в ZK-Rollups увеличивает потребление ресурсов и финансовые затраты.

Как работают оптимистические роллапы:

Агрегация транзакций: Транзакции собираются в "роллап" блок вне основной цепи. Это позволяет обрабатывать множество транзакций параллельно, существенно снижая затраты на комиссию и повышая пропускную способность сети.

Подача в блокчейн: Сжатый блок транзакций затем отправляется в основную цепь Ethereum как одна транзакция, что значительно снижает нагрузку на сеть.

Оптимистическое предположение: Транзакции считаются действительными по умолчанию. Система предполагает, что все транзакции верны, если только не будет доказано обратное.

Оспаривание и проверка: В случае если кто-то обнаруживает ошибку или мошенничество в одной из транзакций, он может подать фрод-пруф. Система затем проводит проверку, и если мошенничество подтверждается, транзакция отменяется.

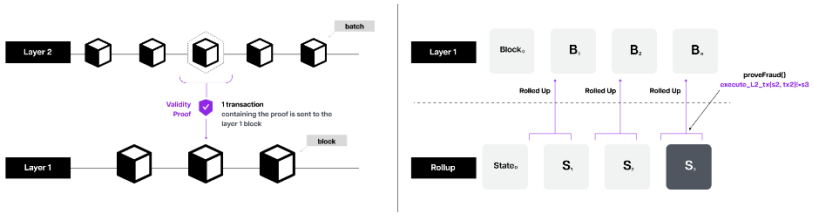

Рисунок 4 – Optimistic Rollups

Заключение

Трилемма блокчейна остается центральной проблемой для разработчиков и исследователей в области криптовалют и блокчейн-технологий. Вопреки этому, существует множество направлений и подходов, которые предлагают потенциальные решения для достижения баланса между безопасностью, масштабируемостью и децентрализацией. Прогресс в этой области будет способствовать развитию более надежных и масштабируемых блокчейн-систем.

Библиография

[1] Технология блокчейн простыми словами. [Электронный ресурс]. – Режим доступа: https://skynet.ru/blog/tekhnologiya-blokchejn-prostymi-slovami/

[2] Что такое трилемма блокчейна простыми словами. [Электронный ресурс]. – Режим доступа: https://www.ixbt.com/live/crypto/chto-takoe-trilemma-blokcheyna.html

[3] Технология Rollup [Электронный ресурс] – Режим доступа: https://forklog.com/cryptorium/chto-takoe-tehnologiya-rollapov-rollups-i-kak-ona-pomogaet-masshtabirovat-ethereum