

Блокчейн третьего поколения

Блокчейн



Оглавление

Введение	3
Словарь терминов	3
Трилемма блокчейна	4
Децентрализация и безопасность	5
Масштабируемость	5
Решение масштабируемости на разных уровнях	7
Примеры решений первого уровня	7
SegWit	8
Шардинг	9
Примеры решений второго уровня	12
Роллапы	13
Сайдчейны	15
Примеры решений нулевого уровня	17
Polkadot	18
Avalanche	18
Cosmos	18
Chainlink	19
Wormhole	19
LayerZero	19
Hyperlane	20
BTC Relay	20
Axelar	20
Каким будет блокчейн третьего поколения	20
Дополнительные материалы	21
Использованная литература	22

Введение

Всем привет! Мы продолжаем курс о блокчейне, на котором изучаем технические основы этой технологии и знакомимся с решением прикладных задач, как в сфере финансов, так и в разработке приложений.

На прошлых лекциях мы рассмотрели первые два поколения блокчейнов. В 2009 году был запущен Биткоин — первый в мире блокчейн. Он привнёс децентрализацию в систему денежных переводов. В 2015 году появился Ethereum, который стал первым блокчейном второго поколения. Он позволил запускать любые децентрализованные приложения на одной и той же платформе.

На этой лекции мы поговорим о блокчейнах третьего поколения. Технологическая гонка сейчас в самом разгаре, поэтому рассматривать один центральный пример, как мы это делали ранее, будет некорректно. После лекции вы сможете самостоятельно оценивать новые проекты, разбираться в современных блокчейн-инновациях и выбирать, какие блокчейны лучше всего соответствуют концепции третьего поколения.

На этой лекции вы узнаете:

- В чём проблема второго поколения и почему возникла необходимость в третьем.
- Какие есть уровни блокчейн-экосистемы и наиболее перспективные технологии в них.
- Каким будет блокчейн третьего поколения.

Словарь терминов

Масштабируемость — способность блокчейна увеличивать число обрабатываемых транзакций в секунду.

Нулевой уровень (Layer 0) — базовая инфраструктура, на которой может быть построено множество блокчейнов первого уровня.

Первый уровень (Layer 1) — базовые блокчейны, используемые разработчиками для создания приложений, таких как децентрализованные приложения.

Второй уровень (Layer 2) — решения для масштабирования, переносящие активность сети за пределы блокчейнов первого уровня, чтобы облегчить их транзакционную нагрузку.

Третий уровень (Layer 3) — уровень приложений на основе блокчейна, включая игры, кошельки и другие DApp.

Форк — создание копии программного обеспечения и его модификация.

Хардфорк — создание копии программного обеспечения, несовместимого с предыдущими версиями.

Софтфорк — создание копии программного обеспечения с обратной совместимостью.

Роллап — популярное решение второго уровня. Оно объединяет транзакции вне блокчейна для ускорения их обработки.

ZK-роллап — это тип роллапа, в котором используется криптографическая техника под названием «доказательство с нулевым разглашением».

Цифровая подпись — хеш, созданный на основе приватного ключа и самих подписываемых данных.

Доказательство с нулевым разглашением (zero knowledge proof) — это криптографический инструмент, с помощью которого одна сторона может доказать другой стороне, что утверждение истинно, не раскрывая подробностей об этом утверждении.

Сайдчейн — параллельный блокчейн, который работает независимо от основного.

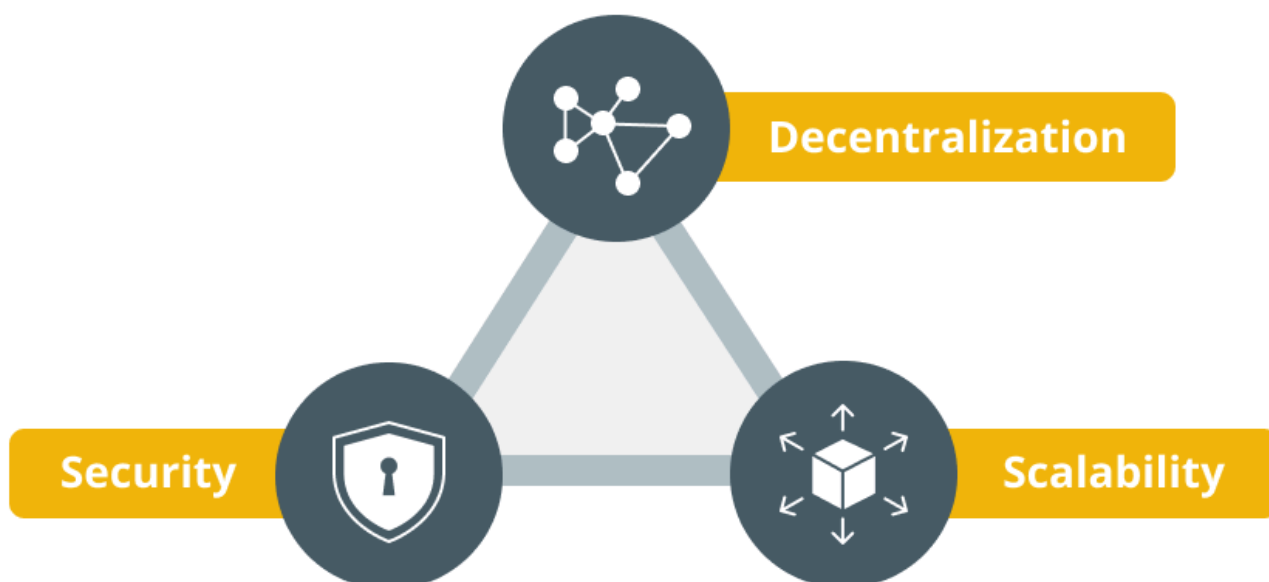
Трилемма блокчейна

Блокчейны второго поколения в теории могут использоваться для создания любых сетей без вмешательства третьих лиц. Но широкому распространению этой технологии препятствует проблема, которую называли трилеммой блокчейна.

Термин «трилемма блокчейна» введён Виталиком Бутериным и связан с тремя ключевыми характеристиками блокчейна:

- децентрализацией;
- безопасностью;
- масштабируемостью.

Трилемма указывает на то, что сложно достичь высокого уровня всех этих характеристик одновременно. Усиление одной, часто ослабляет другую.



Трилемма блокчейна. Источник: habr.com

Чтобы понять суть трилеммы блокчейна, разберём каждую характеристику и их взаимосвязи. Это поможет нам ответить на вопрос «Почему, третье поколение необходимо?».

Децентрализация и безопасность

Децентрализация означает, что сеть работает без центрального контроля. Чем больше в сети узлов, тем децентрализованней блокчейн. Однако степень децентрализации не имеет значения, если она не гарантирует безопасность.

В блокчейне безопасность обусловлена использованием криптографии и алгоритмов консенсуса. Чем выше уровень децентрализации, тем эффективнее работают эти инструменты и выше уровень безопасности. Простыми словами, злоумышленнику сложно захватить контроль над блокчейном, в котором очень много узлов.

Масштабируемость

Децентрализация и безопасность являются ключевыми характеристиками блокчейна, потому на прошлых лекциях мы их детально рассматривали. В эпоху первого и второго поколения большинство проектов активно работали именно над улучшением этих качеств. Например, в 2022 году Ethereum перешёл на более совершенный алгоритм консенсуса Proof of Stake. Сегодня основной фокус внимания стал переключаться на то, чтобы привлечь в блокчейн-технологии

широкую аудиторию и миллиарды потенциальных пользователей. Именно с этим у многих блокчейнов возникают трудности.

В блокчейнах, чтобы подтвердить достоверность данных, требуется время на обмен информацией между участниками. Чем больше участников, тем больше нужно времени на обмен информацией между ними. Другими словами, чем децентрализованней блокчейн, тем сильнее замедляется обработка транзакций в нём.



Масштабируемость — способность блокчейна увеличивать число обрабатываемых транзакций в секунду.

При повышении уровня децентрализации и безопасности страдает масштабируемость. В результате этого значительно сокращается количество транзакций, которое может обрабатывать блокчейн. Рассмотрим конкретный пример.

Блокчейн Ethereum способен проводить до 15 транзакций в секунду, что в 2 раза быстрее, чем у Биткоина. Для сравнения — платёжная система Visa обрабатывает 24 000 транзакций в секунду.

Чем больше становится пользователей в Ethereum, тем больше операций конкурируют между собой за включение в блокчейн. Из-за этого растёт нагрузка на узлы, которые проверяют и генерируют новые блоки. Поэтому количество обрабатываемых транзакций может падать до 10-ти в секунду.

Наиболее очевидным решением описанной проблемы является сокращение числа участников, подтверждающих и добавляющих данные в сеть, ради увеличения масштабирования и скорости. Однако это приведёт к ослаблению децентрализации, поскольку сеть будет контролировать меньше людей. Будет ослаблена и безопасность, ведь чем меньше пользователей, тем выше риск атаки.

В этом и заключается трилемма: усиление одной стороны треугольника ослабляет противоположный угол.

Не существует единого универсального решения этой трилеммы. Множество проектов разрабатывают собственные решения этой проблемы. Вероятно, одно из них станет основой для блокчейнов третьего поколения. А пока давайте рассмотрим наиболее популярные технологии, чтобы понять как и куда развиваются современные блокчейны.


Решение масштабируемости на разных уровнях

Тысячи специалистов работают над созданием решений масштабирования. Некоторые из этих решений направлены на изменение архитектуры основного блокчейна, другие нацелены на протоколы, работающие поверх основной сети. Чтобы не запутаться в них, давайте разберём, из чего состоит экосистема блокчейна.

Один из способов разделить части экосистемы — классифицировать их по уровням:

- **Нулевой уровень.** Базовая инфраструктура, на которой может быть построено множество блокчейнов первого уровня.
- **Первый уровень.** Базовые блокчейны, используемые разработчиками для создания приложений, таких как децентрализованные приложения.
- **Второй уровень.** Решения для масштабирования, переносящие активность сети за пределы блокчейнов первого уровня, чтобы облегчить их транзакционную нагрузку.
- **Третий уровень.** Уровень приложений на основе блокчейна, включая игры, кошельки и другие DApp.

Однако не все экосистемы блокчейнов делятся на эти категории. В одних могут отсутствовать определённые уровни, а другие можно отнести к разным уровням в зависимости от контекста.

 Биткоин по своей сути является блокчейном первого уровня. Однако его часто не включают в данную классификацию, так как его консервативная архитектура не предполагает создания каких-либо других уровней.

Примеры решений первого уровня

Ethereum, который мы уже рассматривали в рамках этого курса, относится к первому уровню.

Другие примеры:

- BNB Smart Chain.
- Solana.
- Cardano.

Все они служат главными сетями в своей экосистеме и обрабатывают транзакции в собственном блокчейне.

Возможные решения для масштабирования первого уровня включают:

- **Форки.** Это создание копии программного обеспечения и его модификация. Например, увеличение размера блока в блокчейне для обработки большего числа транзакций в каждом блоке.
- **Смена алгоритма консенсуса.** Одна из причин существования трилеммы блокчейна заключается в сути алгоритма Proof of Work. Он обеспечивает безопасность за счёт майнеров и огромных вычислительных мощностей, которые замедляют сеть. Современные механизмы позволяют достигать нужного уровня безопасности без ущерба масштабируемости.
- **Шардинг.** Формы разделения баз данных.

Реализовать улучшения для первого уровня достаточно сложно, поскольку не все пользователи сети на них согласятся. Это может привести к расколу сообщества или хардфорку, как это произошло с Биткоином и Bitcoin Cash в 2017 году.



Хардфорк — создание копии программного обеспечения, несовместимого с предыдущими версиями.

Работа с первым уровнем может обеспечить наиболее эффективные решения для масштабных улучшений протокола, однако потребуются одобрение валидаторов на изменения через хардфорк.

В некоторых случаях валидаторы могут не захотеть принимать эти изменения, например, в случае перехода от Proof of Work к Proof of Stake. Майнеры потеряют доход от этого перехода на более эффективную систему, что лишает их стимула к улучшению масштабируемости.

SegWit

Один из примеров решения для масштабирования сетей первого уровня — обновление протокола SegWit. Оно освободило место для транзакций в блоках, не повлияв на безопасность сети. Рассмотрим SegWit немного подробнее.

Обновление SegWit было разработано в 2015 году биткоин-разработчиком Питером Уиллом и другими участниками Bitcoin Core. В августе 2017 года обновление было реализовано как софтфорк с обратной совместимостью. Это означает, что даже ещё не прошедшие обновление ноды Биткоина способны обрабатывать транзакции.



Софтфорк — создание копии программного обеспечения с обратной совместимостью.

Одно из самых основных преимуществ SegWit является увеличение вместительности блока. Благодаря удалению подписей из данных о транзакциях на выходе, появляется возможность вместить большее количество транзакций в одном блоке.

Транзакции состоят из двух основных компонентов: входящие данные и исходящие. Входящие данные содержат публичный адрес отправителя, а исходящие – публичный адрес получателя. Отправитель должен доказать, что он обладает необходимым количеством средств для их перевода другому пользователю, и подтвердить это с помощью цифровой подписи.



Цифровая подпись — хеш, созданный на основе приватного ключа и самих подписываемых данных.

Без SegWit данные подписи могут занимать до 65% всего блока. SegWit позволяет удалять подписи из входных данных о транзакциях. Это приводит к увеличению вместительности блока с 1 МБ до примерно 4 МБ.

Обратите внимание, что SegWit не предполагает увеличение размера самого блока. Это инженерное решение, позволяющее задействовать весь потенциал блока без необходимости увеличения его текущего размера (что возможно только в случае хардфорка). Фактический размер блока по-прежнему остаётся 1 МБ, но эффективный предельный размер составит 4 МБ.

SegWit поспособствовал увеличению пропускной способности, поскольку блок Биткоина стал вмещать в себя больше транзакций. Увеличенная скорость также помогла снизить операционные расходы в сети Биткоина. До обновления обычным делом было заплатить более 30\$ за транзакцию. SegWit резко снизил стоимость комиссии до менее чем 1\$.

Шардинг

Концепция шардинга была заимствована из традиционного управления базами данных. Она представляет собой разделение большой базы данных на более мелкие, управляемые – шарды.

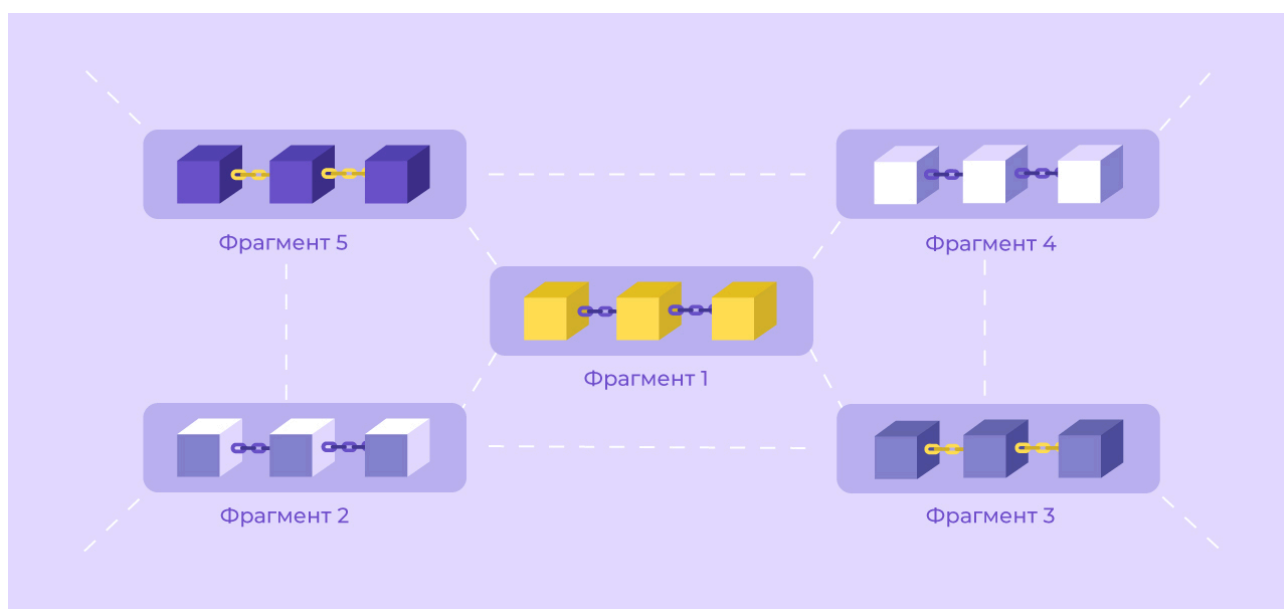
💡 Шардинг — это разделение блокчейн-сети на более мелкие части (шарды), каждая из которых способна параллельно обрабатывать транзакции и смарт-контракты.

Давайте вспомним, как хранятся и обрабатываются данные на блокчейне.

Способ, при котором каждый узел блокчейна отвечает за обработку всего объёма транзакций в сети, называется **последовательной обработкой данных**. Каждый узел должен хранить всю информацию, включая балансы на аккаунтах и историю транзакций, а также обрабатывать все операции, данные и транзакции в сети.

Хотя такая модель повышает безопасность блокчейна за счёт регистрации каждой транзакции всеми нодами, она значительно замедляет обработку данных. В качестве альтернативы выступает **параллельная обработка данных**, позволяющая одновременно выполнять несколько операций.

Шардинг решает эту проблему, разделяя и распределяя нагрузку по обработке транзакций по всей блокчейн-сети. В результате нодам не приходится обрабатывать абсолютно все операции на блокчейне или управлять ими. Простыми словами, цепочки блокчейна в каждом шарде (фрагменте) работают независимо и сообщаются друг с другом только в случае необходимости. Так удаётся ускорить время подтверждения транзакций.



Пример шардинга блокчейна на пять шардов. Источник: maff.io

Рассмотрим преимущества шардинга:

- **Повышенная скорость транзакций.** Вместо последовательной обработки транзакций, шардинг позволяет обрабатывать их одновременно, но в разных шардах. Каждый шард работает независимо, что значительно увеличивает скорость транзакций, а также позволяет всей сети обслуживать больше пользователей, способствуя массовому внедрению.



В качестве примера блокчейн-сети, использующей шарды для решения проблемы масштабируемости, можно привести [Ziliqa](#). Механизм шардинга позволяет Ziliqa обрабатывать тысячи транзакций в секунду.

- **Минимальные затраты на обработку и хранение данных.** При шардинге каждая нода отвечает за обработку и хранение лишь части данных, что сокращает ресурсы, необходимые для работы ноды в сети.
- **Улучшенная производительность сети.** В традиционных блокчейнах рост числа нод снижает производительность, из-за увеличения обмена данными и необходимости синхронизации между ними. При шардинге, когда к сети присоединяется новый узел, он может быть добавлен в шард, а не ко всей сети.

Развитие технологии шардинга в будущем, вероятно, принесёт новые преимущества и поможет усовершенствовать экосистему блокчейна.

Потенциальные уязвимости шардинга:

- **Атаки с захватом шарда.** В системе с шардингом, для управления шардом необходимо гораздо меньше вычислительных мощностей, чем для управления всей сетью. Это повышает уязвимость отдельных шардов для так называемых атак одного процента, когда злоумышленник с небольшим количеством ресурсов (относительно всей сети) может захватить шард.
- **Транзакции между шардами.** Осуществление операций между шардами представляет ещё одну проблему. Они довольно сложны и при неосторожном управлении могут привести к двойному расходованию. Если один шард не точно отслеживает состояние другого во время транзакции, пользователи могут воспользоваться этим с целью двойного расходования.
- **Проблемы с доступом к данным.** Шардинг упрощает поддержание стабильного состояния сети. Если определённые шарды будут недоступны (ввиду перехода узлов в автономный режим), это может привести к проблемам с доступностью данных и нарушит работу всей сети.
- **Безопасность сети.** В системах с шардингом необходим надёжный протокол распределения нагрузки между шардами. Его отсутствие может привести к


неравномерному распределению данных, дисбалансу ресурсов и нестабильности всей сети.

- **Синхронизация узлов.** Синхронизация узлов может вызывать задержки в сети из-за обмена и обновления информации между друг другом. Кроме того, узлы с меньшей вычислительной мощностью или плохим сетевым подключением будут замедлять весь процесс синхронизации и снижат общую производительность блокчейн-сети.

Шардинг — это важный шаг на пути к решению трилеммы блокчейна. Хотя это решение создаёт новые сложности и имеет определённые недостатки, его потенциал увеличивает масштабируемость без ущерба для децентрализации и открывает огромные перспективы для будущего развития блокчейнов третьего поколения.

Примеры решений второго уровня

Внедрение шардинга, изменение размера блоков и смена алгоритма консенсуса — всё это решения первого уровня. Они стремятся изменить фундаментальную конструкцию базовой сети. Некоторые разработчики предлагают решения, которые строятся поверх существующей сетевой структуры. Другими словами, они предлагают решения второго уровня.

 Пользователь может даже не знать, работает ли он в блокчейне первого или второго уровня. Но разработчику всегда необходимо разбираться в системе какого уровня он работает.

Второй уровень обеспечивает более быстрый способ повышения масштабируемости. Некоторые методы могут привести к ослаблению безопасности оригинального блокчейна. Пользователи доверяют таким сетям, как Ethereum и Биткоин, за их проверенную временем надёжность. Избавляясь от некоторых аспектов первого уровня, приходится полагаться на команду и сеть второго уровня для обеспечения безопасности.

Один из главных вопросов — зачем вообще нужны решения второго уровня, если решения первого уровня становятся более масштабируемыми? Существующие блокчейны улучшаются, а новые сети создаются уже с высокой масштабируемостью. Для улучшения масштабируемости крупных систем потребуется много времени, а успех не гарантирован. Вероятно, в эпоху блокчейнов третьего поколения более старые проекты сосредоточатся на безопасности и

позволят решениям второго уровня адаптировать свои сервисы для конкретных задач.


Рассмотрим некоторые наиболее перспективные и распространённые решения второго уровня.

Роллапы

Роллапы позволяют блокчейнам объединять данные о транзакциях и обрабатывать их вне блокчейна (оффчейн). После обработки конечный результат фиксируется в базовой сети. Одновременная обработка такого количества транзакций устраняет вероятность перегрузки блокчейна и позволяет ускорить вычисления, сократив затраты.

Роллапы делятся на две категории:

- **Оптимистические роллапы.** В них все транзакции считаются действительными. Перед отправкой в блокчейн они проходят период ожидания, во время которого сеть может оспорить сомнительные транзакции. Примерами оптимистических роллапов являются Optimism, Arbitrum и opBNB.
- **ZK-роллапы.** Они проверяют каждую транзакцию с помощью доказательств достоверности с нулевым разглашением. Их сложнее реализовать, но они позволяют обойтись без периода разрешения споров и в теории могут быстрее обрабатывать транзакции.

 **Доказательство с нулевым разглашением** (zero knowledge proof) — это криптографический инструмент, с помощью которого одна сторона (доказывающий) может доказать другой стороне (проверяющему), что утверждение истинно, не раскрывая подробностей об этом утверждении.

Сходства и различия оптимистических роллапов и ZK-роллапов представлены в таблице.

	Оптимистические роллапы	ZK-роллапы
Отношение к транзакциям	Транзакции считаются действительными	Все транзакции проверяются с помощью доказательств с нулевым разглашением

Система проверки	Есть период проверки транзакций, чтобы сеть могла оспорить мошеннические транзакции	Нет периода проверки
Механизм доказательства	Доказательство мошенничества	Доказательства достоверности
Сложность	Проще реализовать	Сложнее реализовать из-за доказательств с нулевым разглашением
Распространение	Широко распространены из-за меньшей сложности	Не так широко распространены
Примеры	Optimism, Arbitrum и opBNB	zkSync и Starknet

Сходства и различия роллапов. Источник: academy.binance.com

Роллапы с нулевым разглашением — самый распространённый тип. Давайте подробнее рассмотрим их подробнее. Они состоят из двух основных компонентов:

- **Ончейн-контракты.** Смарт-контракты определяют правила, по которым работает протокол ZK-роллапа. Он состоит из основного контракта и контракта проверяющего. Основной контракт хранит блоки роллапов, отслеживает депозиты и осуществляет важные обновления. Контракт проверяющего проверяет сгенерированные ZKP.
- **Виртуальные офчейн-машины.** Они исполняют транзакции вне базового блокчейна на втором уровне. Виртуальные офчейн-машины работают независимо от основной сети.

ZK-роллапы неразрывно связаны с блокчейном, хотя и находятся в отдельном месте. Они не перегружают сеть деталями транзакций. Вместо этого они предоставляют связанные обзоры, обеспечивая порядок и эффективную работу базового уровня.

Преимущества ZK-роллапов:

- **Повышенная пропускная способность.** ZK-роллапы переносят исполнение транзакций с базового уровня в более эффективную вычислительную среду. Это позволяет повысить пропускную способность, поскольку транзакции не обрабатываются по отдельности в блокчейне.

- **Снижение перегрузки.** Уменьшая нагрузку на блокчейн, ZK-роллапы повышают эффективность операций первого уровня. Кроме того, полным нодам нужно хранить только доказательства с нулевым разглашением, а не все данные.
- **Снижение комиссий.** Благодаря снижению перегрузки, ZK-роллапы помогают уменьшить комиссии.
- **Меры безопасности.** ZK-роллапы используют меры безопасности, позволяющие пользователям выводить средства даже при сбоях в сети роллапов. Это важное преимущество по сравнению с сайдчейнами, в которых во время сбоев можно потерять средства.
- **Ускоренный период проверки транзакций.** При использовании ZK-роллапов в проверке нуждаются только доказательства достоверности внутри роллапов.

Недостатки ZK-роллапов:

- **Сложность.** Главный недостаток заключается в том, что ZK-роллапы намного сложнее реализовать, чем оптимистические роллапы.
- **Ограничения базового уровня.** Несмотря на свою эффективность, ZK-роллапы действуют в рамках ограничений базового уровня.
- **Фрагментация ликвидности.** Любое решение второго уровня приводит к разделению ликвидности в экосистеме. Недостаточная ликвидность в протоколах базового уровня может привести к потенциальным проблемам.

Сайдчейны

Идея сайдчейна появилась в октябре 2014 года в статье под названием [«Внедрение блокчейн-инноваций с помощью привязки сайдчейнов»](#). Работа была опубликована Адамом Бэком в сотрудничестве с другими криптографами и разработчиками Биткойна, включая Мэтта Коралло, Люка Дэшра, Эндрю Поэлстра и Питера Вилле.

Сайдчейн — это параллельный блокчейн, который работает независимо от основного. Обычно связь между ними устанавливается при помощи двустороннего моста, который позволяет быстро передавать токены между основной сетью и сайдчейном.

Ключевая особенность сайдчейнов — их автономность. В отличие от основной сети, сайдчейны могут использовать уникальные алгоритмы консенсуса и параметры блоков, адаптированные под конкретные цели. Такая свобода позволяет

эффективно обрабатывать транзакции, обеспечивая меньшее время подтверждения и низкие комиссии.

Преимущества связаны с определёнными компромиссами. К примеру, гибкие параметры блока могут снизить децентрализацию, так как сократят количество требуемых мощных узлов.

Полезной особенностью некоторых сайдчейнов является их совместимость с виртуальной машиной Ethereum. Она позволяет исполнять смарт-контракты, написанные на Solidity, создавая привычную среду для разработчиков. Если сайдчейн совместим с EVM, он может быстро запускать децентрализованные приложения и исполнять смарт-контракты, разработанные для Ethereum.

Как и любые другие технологические инновации, сайдчейны имеют ряд преимуществ и ограничений. Давайте рассмотрим основные плюсы и минусы сайдчейнов.

Преимущества:

- **Масштабируемость.** Сайдчейны помогают основной сети масштабироваться, снимая с неё нагрузку и повышая производительность.
- **Гибкость.** Автономность сайдчейнов позволяет экспериментировать с различными механизмами консенсуса и параметрами блока, способствуя развитию инноваций и возможностей пользовательской настройки.
- **Совместимость.** Совместимость с EVM обеспечивает быстрый переход для разработчиков, позволяя развёртывать существующие смарт-контракты Ethereum на сайдчейне.

Недостатки:

- **Снижение децентрализации.** Для достижения высокой пропускной способности часто приходится жертвовать степенью децентрализации сайдчейнов. Это может привести к концентрации власти у нескольких нод и поставить под угрозу безопасность блокчейна.
- **Проблемы безопасности.** Сайдчейны сами обеспечивают свою безопасность. И хотя потенциальная атака на сайдчейн не повлияет на основную сеть напрямую, такая независимость может привести к дополнительным рискам.
- **Сложность.** Внедрение и поддержка сайдчейнов требуют значительных усилий и ресурсов. Трудность первоначальной настройки и поддержания работы могут осложнить массовое внедрение решения.

Концепцию сайдчейнов используют несколько проектов, каждый из которых предлагает уникальные функции и решает конкретные задачи в экосистеме блокчейна. Вот несколько примеров:

- **Polygon.** Проект использует несколько сайдчейнов для повышения масштабируемости Ethereum с помощью фреймворка Plasma. Его задача — обеспечить быстрые и недорогие транзакции для децентрализованных приложений.
- **SKALE.** Предоставляя разработчикам платформу для создания децентрализованных приложений с высокой производительностью и масштабируемостью. Он направлен на создание удобной среды для разработчиков.
- **Gnosis.** Использует сайдчейн xDai для обеспечения быстрых и стабильных транзакций. Он удобен в использовании и подходит для приложений, требующих быстрых и доступных транзакций.
- **Loom Network.** Специализируется на создании масштабируемых игр и социальных приложений на блокчейне. Для достижения высокой пропускной способности он использует алгоритм консенсуса Delegated Proof of Stake (DPoS).

Сайдчейны выделяются как перспективное решение проблемы масштабируемости. По мере развития блокчейнов третьего поколения, роль сайдчейнов в создании масштабируемой и универсальной экосистемы, вероятно, будет только расти.

Примеры решений нулевого уровня

Протоколы нулевого уровня — одни из самых современных технологий, которые, вероятнее всего, будут задействованы в блокчейнах третьего поколения. Они помогают решить не только проблему масштабируемости, но и проблему совместимости.

Совместимость — это способность блокчейнов взаимодействовать друг с другом. Концепцию такой инфраструктуры можно назвать «интернетом блокчейнов». В нём смарт-контракты различных блокчейнов могут обмениваться информацией без необходимости отправлять фактические токены из одной сети в другую.

Например, активы, услуги и транзакции записываются на блокчейне в виде документации. Если найти правильное решение для совместимости и воплотить «интернет блокчейнов» в жизнь, все операции одной сети могут быть представлены в другой сети. В результате приложения будут работать с любым активом или услугой независимо от того, на каком блокчейне они находятся.

Как правило, протоколы нулевого уровня служат основным и первичным блокчейном для поддержки данных транзакций в различных блокчейнах первого уровня. Рассмотрим несколько примеров:

Polkadot

Соучредитель Ethereum Гэвин Вуд разработал протокол Polkadot, позволяющий разработчикам создавать собственные блокчейны. Он использует основную сеть, называемую Polkadot Relay Chain. Каждый независимый блокчейн, построенный на Polkadot, называют параллельный чейн, или парачейн.

Relay Chain работает как мост между парачейнами и обеспечивает эффективную передачу данных. Метод, с помощью которого обрабатываются транзакции в разных парачейнах, напоминает шардинг.

Чтобы создать собственный парачейн на Polkadot, разработчики участвуют в аукционах на получение слотов. Первый проект парачейнов Polkadot был одобрен на аукционе в декабре 2021 года.

Avalanche

Блокчейн Avalanche был запущен в 2020 году компанией Ava Labs. Он делает упор на протоколы DeFi и использует инфраструктуру, состоящую из трёх основных блокчейнов: контракта (C-chain), биржи (X-chain) и платформы (P-chain). Они разработаны специально для выполнения основных функций экосистемы, чтобы повысить безопасность и одновременно обеспечить низкую задержку и высокую пропускную способность. X-Chain используют для создания и торговли активами, C-Chain — для создания смарт-контрактов, а P-Chain — для координации валидаторов и подсетей. Гибкая структура Avalanche также позволяет осуществлять быстрые и дешёвые кроссчейн-свопы.

Также разработчики блокчейна создали протокол Avalanche Warp Messaging (AWM), который позволяет создавать собственные параметры обмена сообщениями для обеспечения связи. Цель AWM — облегчить разработку мощных DApp в сети Avalanche.

Cosmos

Сеть Cosmos была основана в 2014 году Итаном Бухманом и Чжэ Квоном. Она состоит из основной сети Cosmos Hub и пользовательских блокчейнов, известных

как зоны. Cosmos Hub передаёт активы и данные между взаимосвязанными зонами и обеспечивает общую безопасность сети.

Каждая зона создаётся в соответствии с потребностями разработчика и позволяет устанавливать собственную криптовалюту, настраивать валидацию блоков и так далее. Все приложения и сервисы Cosmos, размещённые в этих зонах, взаимодействуют через протокол Inter-Blockchain Communication (IBC). Это позволяет свободно обмениваться активами и данными между независимыми блокчейнами.

Inter-Blockchain Communication определяет минимальный набор функций, указанных в стандарте Interchain Standards (ICS) и определяющих способ взаимодействия и обмена данными между блокчейнами. Одним из примеров, работающих с данным протоколом, является Osmosis — децентрализованная биржа, с помощью которой пользователи могут осуществлять своп токенов между разными блокчейнами. Osmosis использует протокол IBC для свободного свопа токенов из разных блокчейнов.

Chainlink

Chainlink разрабатывает протокол Cross-Chain Interoperability Protocol (CCIP) — стандарт с открытым исходным кодом для обеспечения кроссчейн-связи, включая обмен сообщениями и перевод токенов. Цель CCIP — предоставить универсальное соединение между сотнями блокчейнов с помощью стандартизированного интерфейса. В будущем это решение может облегчить создание кроссчейн-приложений и продуктов.

Wormhole

Wormhole — это общий протокол совместимости, который обеспечивает обмен токенами и сообщениями между разными сетями. Он позволяет отслеживать сообщения на исходном блокчейне для проверки и перевода средств на другие блокчейны. Разработчики, использующие Wormhole, могут создавать децентрализованные кроссчейн-приложения, называемые xDapp.

LayerZero

LayerZero — это омничейн-протокол для облегчённой и надёжной передачи сообщений между блокчейнами на основе системы с настройками уровня доверия.

Сверхлегкие ноды LayerZero (ULN) — это смарт-контракты, которые предоставляют заголовки блоков из других связанных блокчейнов для повышения эффективности. ULN срабатывает только по требованию, а смарт-контракт взаимодействует с ретранслятором через конечную точку LayerZero. Такая система обеспечивает лёгкую и эффективную кроссчейн-коммуникацию.

Hyperlane

Hyperlane — это протокол, который проверяет и защищает кроссчейн-коммуникацию с помощью настраиваемых методов консенсуса. Валидаторы Hyperlane отвечают за проверку каждого блокчейна, подключенного к Hyperlane, обеспечивая надёжную и точную кроссчейн-связь.

BTC Relay

BTC Relay — это чейн-ретранслятор для развёртывания приложений в реальных условиях. Он позволяет передавать заголовки блоков Биткоина на Ethereum. Таким образом BTC Relay создаёт мост между двумя сетями на основе не требующей доверия системы, чтобы проверять включение транзакций Биткоина в блокчейн Ethereum.

Axelar

Axelar предлагает решение для кроссчейн-связи с помощью протокола General Message Passing, который позволяет разработчикам создавать децентрализованные приложения, работающие в нескольких блокчейн-сетях. Например, приложение-мост Axelar под названием Satellite подключает BUSD на базе Ethereum к Cosmos, обеспечивая взаимодействие между этими экосистемами.

Каким будет блокчейн третьего поколения

Сейчас блокчейны находятся в таком же положении, как и интернет в начале существования: это множество изолированных экосистем, работающих недостаточно быстро. Блокчейн третьего поколения должен будет решать сразу две проблемы предыдущих поколений — масштабируемость и совместимость.

Для решения проблемы масштабируемости уже существует немало технологий. В Биткойне прошло обновление протокола SegWit, а в Ethereum уже изменился алгоритм консенсуса и внедряется шардинг. Также существует множество решений, функционирующих поверх крупных блокчейнов предыдущих поколений.

Над решением проблемы совместимости сегодня работает множество специалистов, проекты которых можно назвать блокчейнами третьего поколения. Однако до «интернета блокчейнов» ещё далеко. Пока можно говорить лишь о том, что блокчейны, построенные на одном и том же протоколе нулевого уровня, могут взаимодействовать друг с другом по умолчанию без специальных мостов.

Отсутствие совместимости и возможности быстро расширяться препятствует более широкому внедрению блокчейна. Например, пользователям доставляют неудобства разные версии одного и того же приложения, так как в них невозможно легко переводить токены с одного блокчейна на другой. Обычно эта проблема решается уничтожением активов на исходном блокчейне и повторным созданием их на другом блокчейне с помощью кроссчейн-моста. Но часто этот процесс бывает длительным и сложным, а хранить активы на нескольких блокчейнах может быть неудобно и рискованно.

Для вас, как для разработчиков, работа с блокчейнами первых двух поколений тоже будет вызывать неудобства. Каждое развёртывание — это изолированный и независимый проект. Поэтому коды контрактов часто не связаны между собой и не имеют данных друг о друге. Например, если развернуть децентрализованную биржу на сетях Ethereum, BNB Chain и Polygon по отдельности, это приведёт к появлению нескольких изолированных версий.

Однако протоколы нулевого уровня, которые, вероятно, станут основой для блокчейнов третьего поколения, часто предлагают простые в использовании инструменты для разработки программного обеспечения (SDK). У них удобный интерфейс, чтобы стимулировать разработчиков запускать собственные блокчейны и децентрализованные приложения для конкретных целей.

Спасибо, что прошли этот курс. Продолжайте следить за тем, как развиваются и меняются блокчейн-технологии. Желаю вам успехов в том, чтобы внести свой вклад в создание третьего поколения блокчейна!

Дополнительные материалы

1. [Введение в Polkadot](#)
2. [Research Reports | Messari](#)
3. [Официальное русскоязычное сообщество проекта AVA Labs в Telegram](#)

Использованная литература

1. [Что такое трилемма блокчейна](#)
2. [Что такое шардинг и как он работает](#)
3. [Что такое сайдчейны](#)
4. [Что такое ZK-роллапы? Решение второго уровня для масштабирования](#)
5. [Что такое кроссчейн-совместимость](#)
6. [Решения для масштабирования первого и второго уровней блокчейна](#)
7. [Что такое блокчейн первого уровня](#)
8. [Что такое нулевой уровень блокчейна](#)