The Nervos Network Positioning Paper

1. Цель написания данной статьи

Сеть Nervos состоит из ряда протоколов и инноваций. Важно иметь четкую документацию и технические спецификации по разработке и реализации ключевых протоколов, для которых мы используем процесс RFC (запрос комментариев). Однако мы считаем, что не менее важно, чтобы мы помогали нашим сообществам понять, чего мы пытаемся достичь, каких компромиссов, и как мы пришли к нашим текущим проектным решениям.

Мы начнем этот документ с подробного изучения проблем, с которыми сегодня сталкиваются публичные (неразрешенные permisionless) блокчейны, и существующих решений, пытающихся эти проблемы решить. Мы надеемся, что это обеспечит необходимый контекст для наших читателей, чтобы понять наше собственное обоснование того, как наилучшим образом решить эти проблемы, и наши основополагающие проектные решения. Затем мы предоставим высокоуровневый обзор всех частей Nervos Network с акцентом на то, как они работают вместе для поддержки общего видения сети.

2. Предыстория

Масштабируемость, устойчивость и функциональная совместимость являются одними из самых больших проблем, с которыми сегодня сталкиваются публичные (неразрешенные) блокчейны. Хотя многие проекты утверждают, что имеют решение этих проблем, важно понимать, откуда эти проблемы возникают, и рассматривать решения в контексте возможных компромиссов.

2.1 Масштабируемость

Биткойн [1] был первым публичным (permissionless) блокчейном, разработанным для использования в качестве электронных денег в одноранговой (peer-to-peer) сети. Ethereum [2] сделал возможным большее количество вариантов использования и создал децентрализованную вычислительную платформу общего назначения. Тем не менее, обе эти платформы накладывают ограничения на свои транзакционные возможности: биткойн ограничивает размер блока, а Ethereum ограничивает лимит газа. Это необходимые шаги для обеспечения долгосрочной децентрализации, однако они также ограничивают возможности обеих платформ.

Сообщество блокчейнов предложило множество решений по масштабируемости в последние годы. В общем, мы можем разделить эти решения на две категории: масштабирование по цепочке и масштабирование вне цепочки.

Решения масштабирования по цепочке нацелены на увеличение пропускной способности согласованного процесса и создание блокчейнов с собственной пропускной способностью, которая конкурирует с централизованными системами. Решения для автономного масштабирования используют блокчейн только в качестве безопасной платформы активов и расчетов, в то время как почти все транзакции перемещаются на верхние уровни.

2.1.1. Цепное масштабирование с помощью единой цепочки блоков

Самый простой способ увеличить пропускную способность блокчейна - увеличить запас пространства блока. С дополнительным пространством блоков больше транзакций может проходить через сеть и обрабатываться. Увеличение предложения пространства блока в ответ на возросший спрос на транзакции также позволяет удерживать комиссию за транзакции на низком уровне.

Bitcoin Cash (BCH) применяет этот подход для масштабирования своей одноранговой платежной сети. Протокол Bitcoin Cash начался с максимального размера блока 8 МБ, который впоследствии был увеличен до 32 МБ, и который будет продолжать увеличиваться бесконечно по мере увеличения спроса на транзакции. Для справки: после реализации Биткойном (BTC) Segregated Witness в августе 2017 года, протокол Биткойн теперь позволяет использовать средний размер блока около 2 МБ.

В масштабе центра обработки данных математика работает. Если 7,5 миллиардов человек создают по 2 транзакции в день, сети потребуется производить 26 ГБ блоков каждые 10 минут, что приведет к росту числа блоков в 3,75 ТБ в день или 1,37 ПБ в год [3]. Сегодня эти требования к хранилищу и пропускной способности являются разумными для любого облачного сервиса.

Однако ограничение работы узла средой центра обработки данных приводит к единой жизнеспособной топологии сети и требует компромиссов в безопасности (скорость разветвления блокчейна будет увеличиваться по мере увеличения требований к передаче данных по сети), а также децентрализации (полное число узлов будет уменьшаться по мере увеличения стоимости консенсусного участия).

С экономической точки зрения, постоянно увеличивающийся размер блока смягчает нагрузку на пользователей. Анализ сети Биткойн показал, что плата остается неизменной до тех пор, пока блок не заполнится примерно на 80%, а затем возрастет в геометрической прогрессии [4].

И хотя перенесение стоимости управления растущей сети на ее пользователей может показаться разумным решением, оно может быть недальновидным по двум причинам:

- Подавление сборов за транзакции вынуждает майнеров полагаться преимущественно на компенсацию от выпуска новых монет (блок вознаграждений). Если инфляция не является постоянной частью протокола, выпуск новой монеты в конечном итоге прекратится (когда будет достигнут общий хард-кеп монеты), и майнеры не получат ни вознаграждение за блок, ни значительные комиссионные за транзакции. Экономический эффект от этого серьезно скомпрометирует модель безопасности сети.
- Стоимость полного узла становится чрезмерно дорогой. Это устраняет возможность обычных пользователей независимо проверять историю и транзакции блокчейна, заставляя провайдеров услуг, таких как биржи и платежные системы, обеспечивать целостность блокчейна. Это требование доверия сводит на нет основную ценность общедоступных неразрешенных блокчейнов как одноранговых, публичных распределенных систем.

Платформы с оптимизированной стоимостью транзакций, такие как Bitcoin Cash, сталкиваются со значительной конкуренцией со стороны других блокчейнов (разрешенных и неразрешенных), а также традиционных платежных систем. Проектные решения, которые улучшают безопасность или устойчивость к цензуре, повлекут за собой связанные с этим расходы и, в свою очередь, увеличат стоимость использования платформы. Принимая во внимание конкурентную среду а также заявленные цели сети, можно заключить, что более низкие затраты будут являться главной целью сети, которая должна будет быть достигнута даже в ущерб другим свойствам.

Эта цель согласуется с нашими наблюдениями за использованием транзакционной сети. Пользователи этих систем безразличны к значительным долгосрочным компромиссам, потому что они будут использовать сеть только в течение короткого времени. После того, как их товары или услуги получены и оплата произведена, эти пользователи больше не беспокоятся об эффективности работы сети. Принятие этих компромиссов очевидно в широко распространенном использовании централизованных обменов крипто-активами, а также в более централизованных блокчейнах. Эти системы популярны прежде всего за их удобство и эффективность транзакций.

Некоторые платформы смарт контрактов используют аналогичные подходы для масштабирования пропускной способности блокчейна, позволяя лишь ограниченному набору валидаторов «суперкомпьютера» участвовать в процессе согласования и независимо проверять блокчейн.

Хотя компромиссы в отношении децентрализации и сетевой безопасности позволяют осуществлять более дешевые транзакции и могут быть удобны для ряда пользователей, скомпрометированная модель долгосрочной

безопасности, барьер затрат для независимой проверки транзакций и вероятная концентрация и закрепление операторов узлов приводят нас к заключению, что это неправильный подход для масштабирования публичных блокчейнов.

2.1.2 Цепное масштабирование через несколько цепочек

Масштабирование по цепочке через несколько цепочек может быть достигнуто с помощью шардинга, как это видно в Ethereum 2.0, или цепочек приложений, как это видно в Polkadot. Эти схемы эффективно разделяют глобальное состояние и транзакции сети на несколько цепочек, позволяя каждой цепочке быстро достигать локального консенсуса, и всей сети, достигать глобального консенсуса с помощью «цепочки маяка» (Beacon Chain) или «цепочки реле» (Relay Chain).

Эти конструкции позволяют нескольким цепочкам использовать модель общей безопасности, одновременно обеспечивая высокую пропускную способность и быстрые транзакции внутри шардов (Ethereum) или пара-цепочек (Polkadot). Хотя каждая из этих систем представляет собой сеть взаимосвязанных цепочек блоков, они различаются по протоколам, работающим в каждой цепочке. В Ethereum 2.0 каждый шард запускает один и тот же протокол, а в Polkadot каждая парацепь может запускать настраиваемый протокол, созданный через структуру субстрата.

В этих многоцепочечных архитектурах каждое dApp (или экземпляр dApp) находится лишь в одной цепочке. Хотя сегодня разработчики привыкли создавать dApps, которые легко взаимодействуют с любым другим dApp на блокчейне, шаблоны проектирования должны будут адаптироваться к новым многоцепочечным архитектурам. Если приложение dApp разделено между разными шардами, механизмы должны будут поддерживать синхронизацию состояний между различными экземплярами dApp (находящимися в разных сегментах). Кроме того, несмотря на то, что механизмы уровня 2 могут быть развернуты для быстрой связи между различными шардами, транзакции между ними потребуют глобального консенсуса и введут задержку подтверждения.

С этими асинхронными транзакциями возникает печально известная проблема «поезда и гостиницы». Когда две транзакции должны происходить атомически (например, бронирование билета на поезд и номера в отеле на двух разных шардах), требуются новые решения. Ethereum вводит контракт «янкирование» (yanking), в котором зависимый контракт удаляется на одном шарде, создается на втором шарде (который содержит другой зависимый контракт), и обе транзакции затем выполняются на втором шарде. Однако в такой ситуации, “вырванный” контракт недоступен в исходном шарде, что приводит к проблемам с использованием, а значит - требованием новых шаблонов проектирования.

У шардинга есть свои преимущества и проблемы. Если фрагменты могут быть действительно независимыми, а потребности между фрагментами минимальны, блокчейн может линейно масштабировать свою пропускную способность, увеличивая количество фрагментов. Это лучше всего подходит для автономных приложений, которым не требуется внешнее состояние или совместная работа с другими приложениями.

Шардовая архитектура может быть проблематичной для приложений, которые разрабатываются путем составления вместе «строительных блоков» приложений (это называется «проблемой компоновки»). Композиционность особенно актуальна в пространстве децентрализованных финансов (DeFi), где более продвинутые продукты, как правило, строятся поверх других продуктов, составляющих стандартные блоки.

На техническом уровне, для шардинга обычно требуется топология «1 + N», в которой N цепочек подсоединяются к одной мета-цепочке, вводя верхнюю границу для количества сегментов, которые мета-цепочка может поддерживать, не сталкиваясь с проблемами масштабируемости.

Мы наблюдаем значительную ценность в объединенном глобальном состоянии (global state), позволяющем появиться экосистеме взаимозависимых приложений; разработчикам - внедрять инновации на грани, по аналогии с использованием веб-разработчиками библиотек для задач более низкого уровня и открытых API для интеграции служб. Гораздо более простой опыт разработки возможен, когда разработчикам не приходится учитывать синхронность (при передаче активов между разделениями или передаче сообщений). Возможным становится и превосходный пользовательский опыт, обусловленный согласованностью архитектурных аспектов взаимодействия блокчейна.

Мы признаем, что шардинг является многообещающим решением для масштабируемости (в частности, для менее взаимозависимых приложений), однако мы считаем, что выгодно иметь дизайн, который концентрирует наиболее ценное состояние на одной цепочке блоков, обеспечивая возможность компоновки. При такой конструкции используются подходы масштабирования вне цепочки, чтобы обеспечить более высокую пропускную способность.

2.1.3 Масштабирование вне цепи через второй уровень

В протоколах уровня 2 блокчейн базового уровня действует как уровень расчета (или фиксации), тогда как сеть второго уровня маршрутизирует криптографические доказательства, которые позволяют участникам «принимать доставку» криптовалюты. Все действия второго уровня криптографически защищены базовым блокчейном, а базовый уровень используется только для расчета сумм, входящих / выходящих из сети второго уровня, а также для разрешения споров. Такие проекты работают без

делегирования хранения (или риска потери) средств и обеспечивают мгновенные, почти бесплатные транзакции.

Эти технологии демонстрируют, как можно использовать такую сеть хранения ценностей как Биткойн для ежедневных платежей. Наиболее типичным примером решения уровня 2 на практике является канал оплаты между покупателем и кафе. Давайте предположим, что Алиса посещает Биткойн-кафе каждое утро. В начале месяца она переводит средства в канал платежей Lightning (“Молния”), который она открыла в кафе. Когда она посещает каждый день, она криптографически подписывает право кофейни взять часть средств в обмен на свой кофе. Эти транзакции происходят мгновенно и являются полностью одноранговыми, «вне цепочки», что обеспечивает бесперебойное обслуживание клиентов. Канал Lightning не заслуживает доверия, Алиса или кафе могут закрыть канал в любое время, забрав средства, которые им причитаются.

Такие технологии канала оплаты, как Lightning, являются лишь одним примером техники масштабирования вне цепочки. Есть много технологий для развития, которые могут безопасно масштабировать пропускную способность блокчейна таким образом. В то время как платежные каналы включают в себя соглашения вне цепи для передачи остатков между двумя сторонами, каналы состояния (state channels) включают внеплановые соглашения в произвольное состояние между участниками канала. Это обобщение может стать основой масштабируемых, ненадежных (trustless), децентрализованных приложений. Канал одного состояния может использоваться даже несколькими приложениями, что обеспечивает еще большую эффективность. Когда одна сторона готова выйти из канала, она может предоставить согласованное криптографическое подтверждение блокчейну, который затем выполнит согласованные переходы состояний.

Боковая цепь - это еще одна конструкция, которая позволяет увеличить пропускную способность через доверенных сторонних операторов блокчейна. Благодаря двусторонней привязке к блокчейну с надежным и недоверенным консенсусом средства могут перемещаться между главной цепью и боковой цепью в обоих направлениях. Это позволяет сформироваться большому объему доверенных транзакций в боковой цепочке с последующим чистым расчетом в основной цепочке. Транзакции с боковой цепью имеют минимальные комиссии, быстрое подтверждение и высокую пропускную способность. Хотя боковые цепи предлагают превосходный опыт в некотором отношении, они действительно идут на компромисс касаемо безопасности. Тем не менее, существует множество исследований в отношении ненадежных боковых цепей, которые могут обеспечить такие же улучшения производительности без ущерба для безопасности.

Примером технологии ненадежных боковых цепей является Plasma (описанная в пункте 5.4). Архитектура боковой цепочки, которая использует корень доверия в блокчейне с широким глобальным консенсусом. Плазменные цепи

предлагают те же улучшения производительности, что и централизованные боковые цепи, но делают это, предлагая гарантии безопасности. В случае, если оператор плазменной цепи является злонамеренным или работает со сбоями, пользователям предоставляется механизм, который позволяет им безопасно выводить свои активы боковой цепи в основную цепь. Это делается без сотрудничества с оператором цепочки Plasma, что предлагает пользователям удобство транзакций с боковой цепью, а также безопасность блокчейна уровня 1.

Масштабирование вне цепочки обеспечивает децентрализацию, безопасность и масштабируемость. С помощью перемещения всего кроме расчетных транзакций и споров за пределы цепочки, эффективно используется ограниченный глобальный консенсус публичного блокчейна. Разнообразные протоколы уровня 2 могут быть реализованы на основе требований приложений, обеспечивая гибкость для разработчиков и пользователей. Производительность не меняется по мере того, как в сеть добавляется больше участников, и все стороны могут разделить гарантии безопасности, предлагаемые консенсусом первого уровня.

2.2 Устойчивость

Поддержание долгосрочной работы автономного, бесхозного (ownerless) публичного блокчейна представляет собой довольно сложную задачу. Стимулы (incentives) должны быть сбалансированы между различными заинтересованными сторонами, а система должна быть спроектирована таким образом, чтобы обеспечить широкоформатные полноценные операции узла и публичную проверку. Требования к оборудованию должны оставаться разумными при поддержке открытой глобальной сети.

Стимулы и средства управления собственным активом блокчейна должны быть в состоянии сбалансировать требования оценки долгосрочных держателей и требования компенсации майнеров или валидаторов, защищающих сеть.

Ко всему прочему, как только открытая цепочка блоков готова к работе, очень трудно изменить основные правила, регулирующие протокол. Поэтому с самого начала система должна быть устойчивой. В этом отношении мы провели тщательную инвентаризацию проблем в создании устойчивых, неразрешенных блокчейнов.

2.2.1 Децентрализация

Одной из самых больших долгосрочных угроз, с которыми сталкиваются публичные блокчейны, является постоянно растущий барьер независимого участия и проверки транзакций, что отражается на стоимости работы полного узла. Отказываясь маршрутизировать недопустимые блоки, полные узлы

позволяют привлекать к ответственности майнеров или валидаторов сети. Помимо этого, они позволяют участникам блокчейна независимо проверять состояние / историю в цепочке. По мере того, как стоимость полных узлов увеличивается а их количество уменьшается, участники сети все чаще вынуждены полагаться на профессиональных операторов услуг для предоставления как истории, так и текущего состояния, что подрывает фундаментальную модель доверия открытых и недопустимых блокчейнов.

Чтобы полный узел не отставал от прогрессии блокчейна, он должен иметь достаточную вычислительную пропускную способность для проверки транзакций; пропускную способность для приема транзакций и емкость для хранения всего глобального состояния. Чтобы контролировать эксплуатационные расходы полного узла, протокол должен принять меры для ограничения пропускной способности или увеличения емкости всех трех из этих ресурсов. Большинство протоколов блокчейна ограничивают их вычислительную или пропускную способность, но очень немногие ограничивают рост глобального состояния. По мере увеличения размера и продолжительности работы этих цепочек, затраты на полную эксплуатацию узла будут необратимо возрастать.

2.2.2 Экономические модели

Несмотря на то, что в последние годы было проведено множество исследований в отношении согласованных протоколов, мы считаем, что криптоэкономика является недостаточно изученной областью. Вообще, современные криптоэкономические модели для протоколов уровня 1 в первую очередь ориентированы на стимулы и наказания для обеспечения консенсуса в сети, а нативные (native) токены в основном используются для оплаты сборов за транзакции или для удовлетворения требований к ставкам, которые обеспечивают сопротивление Сибил (Sybil).

Мы считаем, что правильно разработанная экономическая модель должна выходить за рамки процесса консенсуса и обеспечивать долгосрочную устойчивость протокола. В частности, экономическая модель должна быть разработана с учетом следующих целей:

- сеть должна иметь устойчивый способ увеличения доходов для компенсации провайдеров услуг (обычно майнеров или валидаторов), гарантирующий, устойчивую защищенность сети
- сеть должна иметь устойчивый способ поддерживать низкий барьер для участия, обеспечивая, децентрализованность сети на протяжении длительного времени
- ресурсы публичной сети должны быть эффективно и справедливо распределены
- родной (нативный) токен блокчейна должен иметь убедительную внутреннюю ценность (intrinsic value)

2.2.3 Анализ экономической модели Биткойна

Протокол Биткойна ограничивает размер блоков и обеспечивает фиксированное время блока. Это делает пропускную способность сети дефицитным ресурсом, на который пользователи должны делать ставки путем платы за транзакции. Биткойн-скрипт не допускает циклов, что делает длину скрипта хорошим приближением к его вычислительной сложности. В целом, более высокий спрос на пространство блоков приводит к более высокой плате за транзакции для пользователей. Кроме того, чем больше входов, выходов или вычислительных шагов, участвующих в транзакции, тем больше пользователь будет платить за транзакции.

Внутренняя ценность Биткойна почти полностью обусловлена его денежной премией (готовностью общества относиться к нему как к деньгам) и, в частности, желанием удерживать его в качестве накопителя стоимости. Поскольку доход майнеров выражен в BTC, это восприятие должно быть устойчивым, чтобы экономическая модель Биткойна была устойчивой. Другими словами, модель безопасности Биткойна является круговой - она зависит от коллективного убеждения, что сеть является надежно защищенной и поэтому может использоваться в качестве денежного накопителя стоимости.

Ограничение размера блоков в биткойнах эффективно устанавливает барьер для участия в сети - чем меньше ограничение размера блоков, тем проще для непрофессионалов работать с полными узлами. Глобальное состояние Биткойн - это его набор UTXO (unspent transaction output) или набор выходов неизрасходованных транзакций, скорость роста которого также ограничена лимитом размера блока. Пользователи заинтересованы в том, чтобы эффективно создавать и использовать UTXO; создание большего количества UTXO приводит к более высокой плате за транзакцию. Тем не менее, нет никаких стимулов для поощрения объединения UTXO и уменьшения размера глобального состояния; после создания, UTXO будет занимать глобальное состояние бесплатно до тех пор, пока не будет израсходован.

Экономическая модель Биткойна, основанная на платных транзакциях, является справедливой моделью для распределения пропускной способности и дефицитного ресурса, налагаемого протоколом. Это подходящая экономическая модель для одноранговой платежной системы, но плохой выбор для платформы хранения реальной ценности. Пользователи биткойнов, которые используют блокчейн для хранения стоимости, платят комиссионные за транзакции только один раз, но затем могут занимать состояние навсегда, пользуясь постоянной безопасностью, обеспечиваемой майнерами, которые обязаны постоянно инвестировать ресурсы.

Биткойн обладает жестким ограничением общего предложения, и его новая эмиссия через награды за блок в конечном итоге упадет до нуля. Это может вызвать две проблемы:

1) Во-первых, если Биткойн продолжит преуспевать в качестве накопителя стоимости, единичная стоимость BTC будет продолжать увеличиваться, и

общая стоимость, которую защищает сеть, также будет увеличиваться (по мере того, как больше денежной стоимости поступает в сеть). Платформа «хранилище ценностей» должна иметь возможность увеличить свой бюджет безопасности, поскольку ценность, которую она защищает, со временем увеличивается. В противном случае она напрашивается на то, чтобы злоумышленники удвоили расходы и украли активы сети.

Когда цена за нарушение безопасности протокола меньше прибыли, которую они могут получить, действуя честно, злоумышленники всегда будут атаковать. Это аналогично городу, который должен увеличивать свои военные расходы по мере увеличения богатства внутри города. Без этих инвестиций рано или поздно город будет атакован и разграблен.

С существованием вознаграждений за блокировку Биткойн может масштабировать безопасность до совокупного значения, которое он хранит - если цена Биткойна удваивается, доход, который майнеры получают от вознаграждений за блоки, так же удваивается, поэтому они могут позволить себе производить удвоенную скорость хэширования, что вдвое увеличивает стоимость атаки сети.

Это, однако, меняется, когда предсказуемое вознаграждение за блок падает до нуля. Майнеры должны будут полностью полагаться на комиссию за транзакции; их доход больше не будет масштабироваться до стоимости актива Биткойн, но будет определяться требованием транзакции сети. Если потребность в транзакции недостаточно высока для заполнения доступного пространства блока, общая сумма комиссии за транзакцию будет минимальной. Поскольку комиссионные за транзакции строго зависят от спроса на блочное пространство и не зависят от цены Биткойна, это окажет глубокое влияние на модель безопасности Биткойна. Чтобы Биткойн оставался безопасным, мы должны были бы принять за условие постоянный спрос на транзакции с избыточной емкостью, который также зависит от цены Биткойна. А это очень сильные предположения.

2) Во-вторых, когда предсказуемое вознаграждение за блок прекращается, разница в доходе за блок для майнеров увеличивается, и это дает стимулы майнерам переходить на форк, вместо продвижения блокчейна. В экстремальном случае, когда майнерская «шахта» пуста, и они получают блок, загруженный гонорарами, их стимул состоит в том, чтобы раскошелиться на цепь и украсть комиссионные, а не в продвижении по цепочке и производстве блока, потенциально без дохода [5]. В сообществе биткойнов это называется проблемой «стрельбы гонораров» (fee sniping), для которой пока не найдено удовлетворительное решение без снятия хард кэпа Биткойна.

2.2.4 Анализ экономической модели умных контрактных платформ

Типичная экономическая модель смарт контрактных платформ сталкивается с еще большими проблемами. Возьмем Ethereum в качестве примера. Скрипты Ethereum допускают циклы, поэтому длина скрипта не отражает его

вычислительную сложность. По этой причине Ethereum ограничивает не размер блока или пропускную способность, но вычислительную пропускную способность (выраженную в предельном значении газа блока).

Чтобы записывать свои транзакции в блокчейне Ethereum, пользователи предлагают цену за расчеты, которую они готовы платить в виде комиссий за транзакции. Ethereum использует концепцию «газа» в качестве измерения вычислительных затрат, оцениваемых в ETH, а управление скоростью «цены на газ» гарантирует, что цена за шаг вычислений не зависит от ценовых движений нативного токена. Внутренняя ценность токена ETH заключается в его положении в качестве платежного токена децентрализованной вычислительной платформы; это единственная валюта, которую можно использовать для оплаты вычислений в Ethereum.

Глобальное состояние Ethereum представлено с помощью структуры состояния EVM, структуры данных, которая содержит балансы и внутреннее состояние всех учетных записей. Когда создаются новые счета или значения контракта, размер глобального состояния увеличивается. Ethereum взимает фиксированное количество газа за внесение новых значений в свое хранилище состояний и предлагает фиксированную «газовую стипендию», которая компенсирует затраты на транзакцию за газ при удалении значений.

Модель хранения «заплати один раз, займи навсегда» не соответствует текущей структуре затрат майнеров и полных узлов, и эта модель не дает стимула пользователям добровольно удалять состояние или удалять состояние раньше. В результате, Эфириум испытал быстрый рост размера своего состояния. Больший размер состояния замедляет обработку транзакций и повышает эксплуатационные расходы на полные узлы. Без сильных стимулов для очищения состояния эта тенденция продолжится.

Как и в случае с биткойнами, ценообразование в Эфире, основанное на спросе, является справедливой моделью распределения вычислительной пропускной способности - дефицитного ресурса платформы. Модель так же служит целям Эфириума как децентрализованной вычислительной системы. Однако его модель платы за хранение в состоянии не соответствует его потенциальному предложению в качестве децентрализованной платформы хранения состояния или активов. Без платы за долгосрочное использование состояния, в интересах пользователей всегда будет бесплатно занимать его. Без дефицита хранилищ состояния невозможно установить ни динамику рынка, ни динамику спроса и предложения.

В отличие от биткойнов, которые определяют лимит размера блока в своем базовом протоколе, Ethereum позволяет майнерам динамически регулировать лимит газа блока, когда они производят его. Майнеры с современным оборудованием и значительной пропускной способностью способны производить больше блоков, эффективно доминируя в этом процессе голосования. Их интерес состоит в том, чтобы отрегулировать лимит газа блока вверх, поднять планку участия и вытеснить более мелких майнеров из

конкуренции. Это еще один фактор, который способствует быстрому росту стоимости полной работы узла.

Такие платформы смарт-контрактов как Ethereum являются платформами нескольких активов (multi-asset platforms). Они поддерживают выпуск и транзакции всех типов криптоактивов, обычно представляемых как «токены». Они также обеспечивают не только безопасность своих собственных токенов, но и стоимость всех криптоактивов на платформе. «Хранение стоимости» в контексте нескольких активов, следовательно, означает свойство сохранения стоимости, которое приносит пользу как собственным токенам платформы, так и криптоактивам, хранящимся на ней.

Со своей блочной системой вознаграждений, Биткойн обладает отличной экономической моделью «хранения стоимости». Майнеры получают вознаграждение фиксированным блоком, выраженное в BTC, и, следовательно, их доход увеличивается вместе с ценой BTC. Таким образом, платформа может повысить доходы майнеров для повышения безопасности (измеряемой стоимостью атаки) при сохранении устойчивой экономической модели.

Для платформ с несколькими активами становится намного сложнее выполнить это требование, потому что «ценность» может быть выражена с помощью криптоактивов за пределами собственного токена. Если ценность криптоактивов, защищенных платформой, возрастает, но ценность собственного токена не увеличивается, безопасность сети, не повышается, и становится выгоднее атаковать консенсусный процесс платформы, чтобы удвоить затраты хранящихся на платформе криптоактивов.

Чтобы платформа интеллектуальных контрактов с несколькими активами функционировала в качестве накопителя стоимости, спрос на собственные активы в цепочке должен иметь четкий способ генерировать спрос на владение собственным нативным токеном. Другими словами, родной токен платформы должен быть выигрышным для захвата совокупной стоимости активов платформы. Если внутренняя стоимость собственного токена платформы ограничена оплатой комиссии за транзакцию, ее стоимость будет определяться исключительно требованием транзакции. Цена нативного токена не будет соответствовать спросу на право владения хранимыми на платформе крипто-активами.

Платформы интеллектуальных (смарт) контрактов, не предназначенные для функционирования в качестве средств сохранения стоимости, должны полагаться на денежную премию нативного токена (готовность людей удерживать токены за пределами их внутренней стоимости) для поддержания постоянной безопасности. Это возможно только в том случае, если одна платформа доминирует благодаря уникальным функциям, которых нет в других местах, или превосходит другие, благодаря обеспечению минимально возможной стоимости транзакций.

Эфириум в настоящее время обладает таким доминированием и поэтому может поддерживать свою денежную премию. Однако с ростом числа конкурирующих платформ, многие из которых предназначены для более высоких TPS (transactions per second) или скоростей транзакций в секунду и предоставляют аналогичные функциональные возможности, остается открытым вопрос о том, может ли опора только на денежную премию поддерживать безопасность платформы блокчейна, особенно если нативные токены не явно разработаны денежными, или не считаются деньгами. Более того, даже если платформа может предоставлять уникальные функции, ее денежная премия может быть удалена пользовательским интерфейсом посредством эффективных обменов (что очень вероятно, когда массовое принятие блокчейна наконец-то наступит). Пользователи будут владеть активами, с которыми они наиболее знакомы, такими как биткойны или стабильные монеты, и приобретать токены платформы как раз вовремя, чтобы оплачивать комиссию за транзакции. В любом случае фундамент криптоэкономики платформы рухнет.

Платформы с несколькими активами уровня 1 должны обеспечивать устойчивую безопасность для всех криптоактивов, которые они защищают. Другими словами, они должны иметь экономическую модель, разработанную для хранения стоимости.

2.2.5 Финансирование разработки основного протокола

Публичные неразрешенные блокчейны являются общественной инфраструктурой. Первоначальная разработка этих систем требует значительного финансирования, и в процессе эксплуатации им требуется постоянное техническое обслуживание и модернизация. Без преданных людей, обслуживающих эти системы, они могут совершать катастрофические ошибки и работать неоптимально. Протоколы Биткойн и Эфириум не предоставляют нативный механизм для обеспечения финансирования текущего развития, поэтому полагаются на постоянное участие компаний со схожими интересами и альтруистическими сообществами открытого кода.

Dash был первым проектом, который использовал казначейство, чтобы гарантировать финансирование текущей разработки согласно протоколу. Устойчиво поддерживая развитие протокола, этот дизайн предлагает компромисс в отношении устойчивости стоимости криптовалюты. Как и большинство казначейских облигаций блокчейн, эта модель опирается на инфляционное финансирование, которое подрывает стоимость долгосрочных активов.

Сеть Nervos использует казначейскую модель, которая обеспечивает устойчивое финансирование для основного развития. Казначейские фонды поступают от целевой инфляции краткосрочных держателей токенов, в то время как последствия этой инфляции смягчаются для долгосрочных держателей. Более подробная информация об этом механизме предоставлена в пункте (4.6).

2.3 Совместимость

Функциональная совместимость блокчейнов является часто обсуждаемой темой, и многие проекты были предложены специально для решения этой проблемы. С помощью надежных транзакций через блокчейны, истинные сетевые эффекты могут быть реализованы в децентрализованной экономике.

Первым примером функциональной совместимости блокчейнов были атомные перестановки между биткойнами и лайткойнами. Ненадежный обмен биткойнов на Litecoin и наоборот возможен не через протокольные механизмы, а через общий криптографический стандарт (в частности, использование хеш-функции SHA2-256).

Точно так же дизайн Ethereum 2.0 позволяет соединять множество цепочек сегментов, которые работают по одному и тому же протоколу и используют одни и те же криптографические примитивы. Это единообразие будет полезно при настройке протокола межсегментной связи, однако Ethereum 2.0 не будет совместим с другими цепочками блоков, которые не используют те же криптографические примитивы.

Такие сети блокчейнов как Polkadot и Cosmos, идут на шаг впереди, позволяя блокчейнам, построенным на одной и той же основе (Cosmos SDK для Cosmos и Substrate для Polkadot), общаться и взаимодействовать друг с другом. Эти инфраструктуры предоставляют разработчикам некоторую гибкость при создании собственных протоколов и обеспечивают доступность идентичных криптографических примитивов, позволяя каждой цепочке анализировать блоки друг друга и выполнять перекрестную проверку транзакций. Однако оба протокола используют мосты или «зоны разметки» для подключения к блокчейнам, которые не созданы с их собственными структурами, создавая дополнительный уровень доверия. Проиллюстрируем: хотя Cosmos и Polkadot поддерживают «сети блокчейнов», сети Cosmos и Polkadot не предназначены для взаимодействия друг с другом.

Криптоэкономика сетей с перекрестными цепями также может нуждаться в дальнейшем изучении. Как для Cosmos, так и для Polkadot, нативные токены используются для оплаты ставок, управления и транзакций. Если оставить в стороне криптоэкономическую динамику, основанную на ставках, которая сама по себе не может дать внутреннюю ценность токена (обсуждаемую в 4.2.4), то зависимость от транзакций между цепочками для захвата ценности экосистемы может быть слабой моделью. В частности, транзакции с несколькими цепочками - это слабость, а не сила сетей с несколькими цепями, так же как межсегментные транзакции - это слабость защищенных баз данных. Они вводят латентность, а также потерю атомарности и композитности. Существует естественная тенденция для приложений, которым необходимо взаимодействовать друг с другом. В конечном итоге они переходят в одну и ту же цепочку блоков, чтобы уменьшить издержки между цепями, уменьшив потребность в транзакциях между цепями и, следовательно, спрос на нативный токен.

Взаимосвязанные сети выигрывают от сетевых эффектов: чем больше взаимосвязанных цепочек в сети, тем более ценна сеть и тем привлекательнее она для потенциальных новых участников сети. В идеале, мы бы хотели, чтобы это значение росло по отношению к собственному токену, что будет способствовать дальнейшему развитию сети. Однако в объединенной сети безопасности, такой как Polkadot, более высокая собственная цена токена повышает стоимость участия и становится сдерживающим фактором для увеличения стоимости сети. В слабо подключенной сети, такой как Cosmos, более высокая цена токена повышает стоимость капитала для получения комиссионных сборов за транзакции, снижая ожидаемый доход на вложенный капитал и препятствуя дальнейшему участию в ставках.

С ее многоуровневым подходом Nervos Network также является многоцепной сетью. Архитектурно, Nervos использует модель ячейки и низкоуровневый виртуальный механизм для поддержки истинной настройки и созданных пользователем криптографических примитивов, что обеспечивет взаимодействие между гетерогенными цепочками блоков (см. 4.4.1). Криптоэкономически сеть Nervos (вместо передачи сообщений) концентрирует ценность в своей корневой цепочке. С помощью захвата ценности, собственный токен Nervos Network увеличивается в стоимости, одновременно увеличивая бюджет безопасности сети по мере роста совокупной ценности, защищенной сетью. Наконец, растущая собственная цена токена повышает основную ценность сети, а не ослабляет ее. Это подробно описано в разделе (4.4).

3. Основные принципы работы сети Nervos

Nervos - это многоуровневая сеть, созданная для поддержки потребностей децентрализованной экономики. Есть несколько причин, по которым мы считаем, что многоуровневый подход является правильным способом построения сети блокчейнов. Существует много известных компромиссов в построении блокчейн-систем, таких как децентрализация vs. масштабируемость, нейтральность vs. совместимость, конфиденциальность vs. открытость, экономия от стоимости транзакции vs. криптографическая надежность от взаимодействия с пользователем. Мы считаем, что все эти конфликты возникают из-за попыток решить абсолютно противоположные проблемы с помощью единого блокчейна.

По нашему мнению, наилучший способ построения системы - это не создание единого всеобъемлющего слоя, а разбивка проблем и их решение на различных уровнях. Действуя по такой схеме, блокчейн уровня 1 может сосредоточиться на том, чтобы оставаться защищенной, нейтральной, децентрализованной и открытой публичной инфраструктурой, в то время как меньшие сети уровня 2 могут быть намеренно спроектированы так, чтобы наилучшим образом соответствовать контексту их использования.

В Nervos Network протокол первого уровня (то есть общая база знаний) является уровнем сохранения значений всей сети. Он идейно вдохновлен Биткойном, и является открытым и публичным. Он – доказательство существования основанного на работе блокчейна, разработанного, чтобы быть максимально безопасным и устойчивым к цензуре; чтобы служить децентрализованным хранителем ценностей и криптоактивов. Протоколы уровня 2 используют безопасность блокчейна уровня 1, чтобы обеспечить неограниченную масштабируемость и минимальные комиссионные за транзакции, а также позволяют компромиссы для конкретных приложений в отношении моделей доверия, конфиденциальности и окончательности.

Вот основные принципы, которые привели к созданию Nervos Network:

- Устойчивый блокчейн уровня 1 с несколькими активами должен быть крипто-экономически спроектирован так, чтобы быть средством сохранения стоимости.
- Уровень 2 предлагает лучшие варианты масштабирования, обеспечивая почти неограниченные транзакционные возможности, минимальные транзакционные издержки и улучшенный пользовательский интерфейс. Блокчейны уровня 1 должны проектироваться так, чтобы дополнять решения уровня 2, а не конкурировать с ними.
- Доказательство работы в качестве метода сопротивления Сибил (Sybil) важно для блокчейнов уровня 1.
- Блокчейн уровня 1 должен предоставлять общую модель программирования для интерактивных протоколов и функциональной совместимости блокчейнов, а также обеспечивать максимальную настраиваемость протокола и простоту его обновления.
- Чтобы лучше распределить ресурсы и избежать «трагедии общего достояния», хранилище состояния должно иметь четкую и детализированную модель владения. Чтобы обеспечить постоянное долгосрочное вознаграждение майнерам (независимо от спроса на транзакции), оккупация состояния должна иметь постоянную стоимость.

4. The Nervos база общих знаний

4.1 Обзор

«Общие знания» определяются как знания, которые известны всем или почти всем, обычно со ссылкой на сообщество, в котором используется этот термин. В контексте блокчейнов в целом и Nervos Network в частности, «общее знание» относится к состоянию, проверенному глобальным консенсусом и принятому всеми в сети.

Свойства общих знаний позволяют нам коллективно трактовать криптовалюту, хранящуюся в публичных блокчейнах, как деньги. Например, сальдо и история всех адресов в биткойнах являются общеизвестными для пользователей биткойнов,

поскольку пользователи могут независимо воспроизодить общий регистр, проверять глобальное состояние начиная с блока генезиса и знать, что любой другой может сделать то же самое. Эти общеизвестные вещи позволяют людям совершать одноранговые (peer-to-peer) операции, не доверяя их третьим лицам.

База общих знаний Nervos (CKB) предназначена для хранения всех видов общих знаний, и не ограничивается деньгами. Например, CKB может хранить определяемые пользователем криптоактивы, такие как сгруппированные и несмешиваемые токены, а также ценные криптографические доказательства, которые обеспечивают безопасность для протоколов более высокого уровня, таких как каналы оплаты (5.2) и цепочки фиксации (5.4).

И Биткойн, и Nervos CKB являются общими системами хранения и проверки знаний. Биткойн хранит свое глобальное состояние как набор UTXO и проверяет переходы состояний с помощью жестко закодированных правил и сценариев, встроенных в транзакции. Nervos CKB обобщает структуру данных и возможности сценариев Биткойна, сохраняет глобальное состояние в виде набора активных программируемых ячеек и проверяет переходы состояний с помощью пользовательских сценариев с полным набором Тьюринга, которые выполняются на виртуальной машине.

В то время как Nervos CKB имеет такие же возможности интеллектуального контракта, как Ethereum и другие платформы, его экономическая модель предназначена для сохранения общих знаний, а не для оплаты децентрализованных вычислений.

4.2 Консенсус

Консенсус Накамото (NC) Биткойна хорошо принят благодаря своей простоте и низким расходам на связь. Однако у NC есть два недостатка: 1) пропускная способность обработки транзакций далека от удовлетворительной, и 2) он уязвим для эгоистичных атак майнинга, в ходе которых злоумышленники могут получить дополнительное вознаграждение за блок, отклоняясь от предписанного поведения протокола.

Консенсусный протокол CKB - это вариант NC, который повышает предел производительности и сопротивление эгоистичному майнингу, сохраняя при этом свои достоинства. Выявляя и устраняя узкое место в задержке распространения блоков NC, наш протокол поддерживает очень короткие интервалы между блоками без ущерба для безопасности. Сокращенный интервал между блоками не только увеличивает пропускную способность, но и снижает задержку подтверждения транзакции. Включая все действительные блоки в расчет корректировки сложности, эгоистичный майнинг больше не приносит прибыли в нашем протоколе.

4.2.1 Увеличение пропускной способности

Nervos база общих данных увеличивает пропускную способность PoW Consensus с помощью алгоритма консенсуса, полученного из Nakamoto Consensus. Алгоритм использует коэффициент бесхозных цепочек блоков (процент действительных блоков,

которые не являются частью канонической цепочки) в качестве измерения связности сети.

Протокол нацелен на фиксированную долю “сирот” (orphans). В ответ на низкий процент сирот трудность цели снижается (увеличивается скорость производства блоков), а когда уровень сирот пересекает определенный порог, сложность цели увеличивается (уменьшается скорость производства блоков).

Это позволяет использовать все возможности пропускной способности сети. Низкая скорость передачи сирот означает, что сеть хорошо подключена и может обрабатывать большие объемы данных. Протокол затем увеличивает пропускную способность в этих условиях.

4.2.2 Устранение узкого места распространения блоков

Узким местом в любой сети блокчейна является распространение блоков. Консенсусный протокол Nervos CKB устраняет узкое место в распространении блоков, изменяя подтверждение транзакции в два этапа: 1) предложение и 2) фиксация.

Сначала транзакция должна быть предложена в «зоне предложения» блока (или одного из его “дядей” - uncles). Транзакция будет зафиксирована, если она появится в «зоне фиксации» блока в определенном окне после его предложения. Такая конструкция устраняет узкое место в распространении блоков, поскольку зафиксированные транзакции нового блока будут уже получены и проверены всеми узлами при их предложении.

4.2.3 Смягчение эгоистичных атак майнинга

Одна из самых фундаментальных атак на консенсус Накамото - эгоистичная добыча. В этой атаке злонамеренные майнеры получают несправедливые блок награды, сознательно превращая добытые другими блоки в осиротевшие.

Исследователи отмечают, что возможность получения несправедливой прибыли коренится в механизме корректировки сложности Nakamoto Consensus, который игнорирует осиротевшие блоки при оценке вычислительной мощности сети. Это приводит к снижению сложности майнинга и увеличению усредненных по времени вознаграждений за блок.

Консенсусный протокол Nervos CKB включает блоки “дяди” в расчет корректировки сложности, что делает эгоистичный майнинг неприбыльным. Такая ситуация сохраняется независимо от стратегии атаки или ее продолжительности; майнер не может получить нечестную награду за любую комбинацию честного и эгоистичного майнинга.

Наш анализ показывает, что благодаря двухэтапному процессу подтверждения транзакций, эгоистичный майнинг де-факто также устраняется через ограниченное время атаки.

Для более глубокого понимания нашего согласованного протокола, пожалуйста, прочитайте материалы здесь.

4.2.4 Доказательство труда Proof of Work против доказательства кола Proof of Stake

Системы Proof of Work (PoW) и Proof of Stake (PoS) обе уязвимы для концентрации мощности, однако качества систем обеспечивают очень разные рабочие реалии для тех, кто находится у власти.

PoW майнинг несет реальные расходы, которые могут превышать доходы от майнинга без тщательного контроля затрат. Те, кто находится у власти, должны оставаться инновационными, придерживаться разумных бизнес-стратегий и продолжать инвестировать в инфраструктуру, чтобы оставаться доминирующими. Майнинговое оборудование, операции по майнингу и доступ к дешевой энергии подвержены изменениям в результате технологических инноваций. Трудно поддерживать монополизацию всех трех в течение длительных периодов времени.

С другой стороны, создатели блоков в системах PoS получают вознаграждение детерминированным способом, основанным на ставочной сумме, с очень низкими требованиями к операционному капиталу. По мере развития системы влияние естественных преимуществ, предоставляемых первым движущимся предприятиям и частным лицам, будет расти. В системе PoS возможно такое, что мощность концентрируется в руках нескольких игроков. Хотя системы PoW имеют аналогичную проблему с концентрацией в майнинге, стоимость сохранения могущества в системе PoS значительно ниже.

Кроме того, валидаторы PoS имеют одну уникальную силу: управление набором валидаторов. Принятие транзакции, которая позволяет валидатору присоединиться к группе консенсуса, находится в руках существующих валидаторов. Сговор о попытках влияния на валидатора, установленного посредством цензуры транзакций и манипулирования заказами будет трудно обнаружить, и трудно наказать. В противовес, консенсусное участие в системах PoW действительно открыто и не зависит от текущей структуры власти. Преимущества не предоставляются ранним участникам системы.

Что касается экономики токенов, хотя считается, что ставки могут привлекать капитал, стремящийся получить доход (и, следовательно, увеличивать спрос на нативный токен), это не полноценная картина. Все PoS-проекты в конечном итоге увидят, что их ставка стабилизируется, и капитал входящий и выходящий из пула ставочного капитала будет примерно одинаковым. Механизм разметки сам по себе не увеличит спрос на нативный токен. Другими словами, хотя введение разбивки и обеспечивает спрос на собственный токен на начальном этапе проекта (пока повышается ставка разбивки), само по себе размещение не может обеспечить долгосрочный спрос на нативный токен и, следовательно, не может являться единственной внутренней ценностью нативного токена.

У долгосрочных держателей токенов в системе PoS есть 3 варианта. Они могут: 1) управлять инфраструктурой и самостоятельно запускать проверяющий узел для получения нового выпуска крипто 2) делегировать свои токены третьей стороне и доверять ее целостности и инфраструктуре, или 3) стоимость их токенов “разводится” путем текущей эмиссии. Ни один из этих вариантов не является особенно привлекательным для долгосрочных держателей токенов, ориентированных на сохранение стоимости.

Мы считаем, что безлимитное участие PoW является требованием к инфраструктуре, лежащей в основе глобальной экономической деятельности. Главной целью уровня 1 является обеспечение максимально возможной децентрализации, безопасности и нейтральности блокчейна. Хотя системы PoS играют определенную роль в децентрализованной экономике, по нашему мнению, они не отвечают требованиям действительно открытого и децентрализованного уровня 1.

4.2.5 Функция доказательства работы (PoW)

Nervos блоки CKB могут быть предложены любым узлом при условии, что 1) блок действителен 2) заявитель решил сложную вычислительную задачу, называемую доказательством работы. Головоломка с доказательством работы определяется в терминах предлагаемого блока. Это гарантирует, что решение головоломки однозначно идентифицирует блок.

Доказательство работы Биткойна требует нахождения допустимого одноразового номера, так чтобы результат применения хеш-функции к заголовку блока удовлетворял определенному уровню сложности. Для Биткойна хеш-функция является дважды повторяющейся SHA2–256. Хотя SHA2 был хорошим выбором для Биткойна, то же самое нельзя сказать о криптовалютах, которые следуют за ним. Для майнинга биткойнов было разработано большое количество специализированного оборудования, большая часть которого бездействует, будучи устаревшим из-за повышения эффективности.

Новая криптовалюта, использующая ту же головоломку для проверки работоспособности, снова сделает это устаревшее оборудование полезным. Даже современное оборудование может быть арендовано и переоснащено для добычи новой монеты. Распределение мощности майнинга для монеты на основе SHA2 будет очень трудно предсказать, а также оно будет подвержено внезапным и большим изменениям. Этот аргумент также применяется к алгоритмическим оптимизациям, адаптированным к SHA2, которые были разработаны для того, чтобы сделать программное вычисление функции более дешевым.

Для новой криптовалюты имеет смысл определить загадку доказательства работы в терминах функции, которая еще не использовалась другими криптовалютами. Для Nervos CKB мы пошли еще дальше и решили определить ее в терминах функции проверки работоспособности, которая не могла быть предметом преждевременной оптимизации, поскольку она является новой.

Однако предполагаемая недоступность оборудования для майнинга имеет место быть только в самом начале. В долгосрочной перспективе развертывание специального оборудования для майнинга выгодно, что значительно увеличивает проблемы атаки на сеть. Поэтому, помимо того, что она нова, идеальная функция проверки работоспособности для новой криптовалюты еще и проста, что значительно снижает барьер для разработки аппаратного обеспечения.

Безопасность - очевидная третья цель проекта. В то время как известная уязвимость может использоваться всеми майнерами одинаково и просто приведет к более высокой сложности, нераскрытая уязвимость может привести к оптимизации майнинга, которая обеспечивает обнаружителю (-ям) преимущество, превышающее их долю в майнинге. Лучший способ избежать этой ситуации - привести веский аргумент в пользу неуязвимости.

4.2.6 Eaglesong

Eaglesong - это новая хеш-функция, разработанная специально для проверки работы Nervos CKB (общих баз данных), но она также подходит в других случаях, когда требуется безопасная хеш-функция. Критерии дизайна были в точности такими, как указано выше: новизна, простота и безопасность. Мы хотели создать дизайн, который был бы одновременно достаточно новым и стал небольшим шагом вперед для науки, и достаточно близким к существующим проектам, чтобы привести веские аргументы в пользу безопасности.

Для этого мы решили создать экземпляр “губки” (как в Keccak / SHA3) с перестановкой, построенной из операций ARX (сложение, вращение и xor); аргумент в пользу его безопасности основан на стратегии широкого следа (тот же аргумент, что лежит в основе AES).

Насколько нам известно, Eaglesong является первой хэш-функцией (или, если на то пошло, функцией), которая успешно сочетает в себе все три принципа проектирования.

Вы можете узнать об Eaglesong больше здесь.

4.3 Модель ячейки

Nervos CKB использует Модель Ячейки (Cell Model) - новую конструкцию, которая может обеспечить многие преимущества модели учетной записи (Account Model), используемой в Ethereum. При этом, владение активами и свойства проверенной проверки модели UTXO (используемой в биткойнах) сохраняется.

Клеточная модель фокусируется на состоянии. Ячейки содержат произвольные данные, которые могут быть простыми, такими как количество токена и имя владельца, или более сложными, такими как код, указывающий условия проверки для передачи токена. Конечный автомат CKB выполняет сценарии, связанные с ячейками, для обеспечения целостности перехода состояния.

Помимо хранения собственных данных, ячейки могут ссылаться на данные в других ячейках. Это позволяет разделять пользовательские активы и логику, управляющую ими, что отличается от основанных на учетных записях платформ смарт-контрактов, в которых состояние является внутренним свойством смарт-контракта и должно быть доступно через интерфейсы смарт-контракта. В Nervos CKB ячейки являются независимыми объектами состояния, которыми владеют, и на них можно ссылаться и передавать напрямую. Ячейки могут отражать истинные «ликвидные активы», принадлежащие их владельцам (точно так же, как UTXO являются ликвидными активами для владельцев биткойнов), при этом ссылаясь на ячейку, которая содержит логику, обеспечивающую целостность переходов состояний.

Транзакции модели ячеек также являются подтверждением перехода состояний. Входные ячейки транзакции удаляются из набора активных ячеек, а выходные ячейки добавляются в набор. Активные клетки составляют глобальное состояние Nervos CKB и являются неизменяемыми: после создания ячеек их нельзя изменить.

Модель Ячеек спроектирована так, чтобы быть адаптируемой, устойчивой и гибкой. Она может быть описана как обобщенная модель UTXO и может поддерживать определяемые пользователем токены, смарт контракты и разнообразные протоколы уровня 2.

Для более глубокого понимания модели, прочтите материалы здесь.

4.4 Виртуальная машина

В то время как многие проекты блокчейнов следующего поколения используют WebAssembly в качестве основы виртуальной машины блокчейна, Nervos CKB включает в себя уникальный выбор дизайна виртуальной машины (CKB-VM) на основе набора команд RISC-V.

RISC-V - это архитектура набора команд RISC с открытым исходным кодом, созданная в 2010 году для облегчения разработки нового аппаратного и программного обеспечения. Это набор инструкций, не требующий уплаты роялти, широко понятый и широко проверенный.

Мы нашли многочисленные преимущества использования RISC-V в контексте блокчейна:

- Стабильность: основной набор инструкций RISC-V был доработан и заморожен, а также широко внедрен и протестирован. Базовый набор команд RISC-V является фиксированным и никогда не потребует обновления.
- Открытость и поддерживаемость: RISC-V предоставляется по лицензии BSD и поддерживается такими компиляторами, как GCC и LLVM, с использованием языка Rust и Go в процессе разработки. Фонд RISC-V включает в себя более 235 организаций-членов, занимающихся разработкой и поддержкой набора инструкций.

- Простота и расширяемость: набор команд RISC-V прост. С поддержкой 64-битных целых чисел набор содержит всего 102 инструкции. RISC-V также предоставляет модульный механизм для расширенных наборов команд, позволяющий использовать векторные вычисления или 256-битные целые числа для высокопроизводительных криптографических алгоритмов.
- Точная оценка ресурсов: набор команд RISC-V может быть запущен на физическом ЦП, обеспечивая точную оценку машинных циклов, необходимых для выполнения каждой инструкции, и информируя о ценах на ресурсы виртуального механизма.

CKB-VM - это низкоуровневая виртуальная машина RISC-V, которая обеспечивает гибкое вычисление, полное по Тьюрингу. С помощью широко распространенного формата ELF, сценарии CKB-VM могут быть разработаны на любом языке, который может быть скомпилирован в инструкции RISC-V.

4.4.1 CKB-VM и Модель Ячеек

После развертывания существующие публичные блокчейны более или менее фиксированы. Обновление основополагающих элементов, таких как криптографические примитивы, предполагает многолетние обязательства или просто невозможно.

CKB-VM делает шаг назад и перемещает примитивы, ранее встроенные в пользовательские виртуальные машины, в ячейки поверх виртуальной машины. Хотя сценарии CKB являются более низкоуровневыми, чем «умные» контракты в Ethereum, они несут в себе значительное преимущество гибкости, обеспечивая гибкую платформу и основу для прогрессирующей децентрализованной экономики. Ячейки могут хранить исполняемый код и ссылаться на другие ячейки как на зависимости. Почти все алгоритмы и структуры данных реализованы в виде CKB-скриптов, хранящихся в ячейках. При поддержке виртуальной машины настолько простой, насколько это возможно, и при выгрузке хранилища программ в ячейки, обновление ключевых алгоритмов так же просто, как загрузка алгоритма в новую ячейку и обновление существующих ссылок.

4.4.2 Запуск других виртуальных инструментов на CKB-VM

Благодаря низкоуровневой природе CKB-VM и доступности инструментария в сообществе RISC-V, легко компилировать другие виртуальные машины (такие как EVM Ethereum) непосредственно в CKB-VM. Это имеет несколько преимуществ:

- Смарт контракты, написанные на специализированных языках, работающих на других виртуальных машинах, могут быть легко перенесены для запуска на CKB-VM. (Строго говоря, они будут работать на своей собственной виртуальной машине, скомпилированной для работы внутри CKB-VM.)

- CKB может проверять переходы состояний разрешения споров транзакций уровня 2, даже если правила переходов состояний написаны для запуска на виртуальной машине, отличной от CKB-VM. Это одно из ключевых требований для поддержки недоверенных боковых цепей общего назначения второго уровня.

Техническое описание CKB-VM см. здесь.

4.5 Экономическая модель

Родным токеном Nervos CKB является «Байт общего знания», или сокращенно CKByte. CKBytes дают право владельцу токена занимать часть общего состояния хранилища блокчейна. Например, удерживая 1000 CKBytes, пользователь может создать ячейку емкостью 1000 байтов или несколько ячеек, добавляя до 1000 байтов емкости.

Использование CKBytes для хранения данных на CKB создает альтернативную стоимость для владельцев CKByte. Они не смогут депонировать занятые CKBytes в NervosDAO для получения части вторичной эмиссии. CKBytes имеют рыночную цену, и, таким образом, пользователям предоставляется экономический стимул добровольно освобождать хранилище состояний для удовлетворения высокого спроса расширяющегося состояния. После того, как пользователь освободит хранилище состояний, он получит объем CKBytes, эквивалентный размеру состояния (в байтах), которое занимали его данные.

Экономическая модель CKB позволяет выпускать родной токен для связи роста состояния, поддерживая низкий барьер участия и обеспечивая децентрализацию. Поскольку CKBytes становятся дефицитным ресурсом, они могут быть оценены и распределены наиболее эффективно.

Генезисный блок Nervos Network будет содержать 33,6 млрд CKBytes, из которых 8,4 млрд будут немедленно сожжены. Новый выпуск CKBytes включает в себя две части - базовый выпуск и вторичный выпуск. Базовая эмиссия ограничена конечным общим предложением (33,6 млрд CKBytes), а ее график выпуска аналогичен биткойну. Награда за блок подвергается халвингу примерно каждые 4 года, до того момента, пока новый выпуск не достигнет 0. Все базы выдаются майнерам как стимулы для защиты сети. Вторичная эмиссия имеет постоянную скорость эмиссии 1,334 млрд CKBytes в год и предназначена для наложения альтернативных издержек для заполнения хранилища состояний. После прекращения базовой выдачи будет существовать только вторичная эмиссия.

Nervos CKB включает в себя специальный умный контракт, который называется NervosDAO, и функционирует как «укрытие от инфляции» в результате последствий вторичной эмиссии. Владельцы CKByte могут депонировать свои токены в NervosDAO и получить часть вторичной эмиссии, которая точно компенсирует ее инфляционные эффекты. Для долгосрочных

держателей токенов, пока они фиксируют свои токены в NervosDAO, инфляционный эффект вторичной эмиссии является только номинальным. Благодаря смягчению последствий вторичной эмиссии, эти пользователи эффективно держат жестко ограниченные токены, такие как Биткойн.

Пока CKBytes используются для хранения состояния, их нельзя использовать для получения вознаграждений за вторичные выпуски через NervosDAO. Это делает вторичную эмиссию постоянным налогом инфляции, или «арендной платой состояния» за занятие хранилища. Эта экономическая модель налагает плату за хранение, пропорциональную как пространству, так и времени занятия. Она более устойчива, чем модель «плати один раз, займи навсегда», используемая другими платформами, и более осуществима и удобна для пользователя, чем другие решения об аренде состояния, которые требуют явных платежей.

Майнеры получают вознаграждение как за блок, так и за транзакцию. В качестве наград за блок, когда майнер добывает его, он получает выдачу полной базы блока и часть вторичной эмиссии. Например, эта часть зависит от состояния: если половина всех собственных токенов используется для сохранения состояния, майнер получит половину вторичной выдачи за блок. Дополнительная информация о распространении вторичной эмиссии включена в следующий раздел (4.6). В долгосрочной перспективе, когда выдача базы прекращается, майнеры по-прежнему будут получать доход от ренты, который не зависит от транзакций, но связан с использованием Общей базы знаний Nervos (CKB).

По аналогии, CKBytes можно рассматривать как землю, а криптоактивы, хранящиеся в CKB, можно рассматривать как дома. Земля требуется для строительства дома, а CKBytes требуются для хранения активов в CKB. По мере роста спроса на хранение активов в CKB растет и спрос на CKBytes. По мере того, как стоимость хранимых активов увеличивается, стоимость CKBytes также увеличивается.

При таком дизайне спрос на множество активов переводится в спрос на один актив, и можно использовать ту же систему стимулирования, которая обеспечивает Биткойн. Майнеры получают блок вознаграждения в CKBytes, которые увеличиваются в ценности с ростом спроса и, таким образом, увеличивают бюджет безопасности Nervos Network.

Для более детального описания экономической модели читайте этот материал.

4.6 Казначейство

Часть вторичной эмиссии, которая не направляется 1) майнерам или 2) долгосрочным держателям с токенами, заблокированными в NervosDAO, пойдет в казначейский фонд. Проиллюстрируем: если 60% выпущенных CKBytes используются для хранения состояния, а 30% CKBytes хранятся в

NervosDAO, майнеры получат 60% вторичного выпуска; NervosDAO (долгосрочные держатели) получат 30% вторичной эмиссии, и 10% вторичной эмиссии пойдут в казну.

Казначейский фонд будет использоваться для финансирования текущих исследований и разработок протокола, а также для создания экосистемы Nervos Network. Использование казначейских средств будет открытым, прозрачным и доступным для всех. По сравнению с моделью казначейского финансирования, основанной на инфляции, эта модель не «разбавляет» долгосрочных держателей токенов (которые поместили свои токены в NervosDAO). Финансирование разработки протокола строго зависит от альтернативных издержек для владельцев краткосрочных токенов.

Казначейство не будет активировано сразу же после запуска основной сети знаний Nervos. Оно будет активировано с помощью хард-форка позже, только после того, как Фонд Nervos исчерпает Экосистемный Фонд, включенный в блок Генезиса (Genesis). До активации казначейства эта часть вторичного выпуска будет «сожжена».

4.7 Управление

Управление - это то, как общество или группы в нем организуются для принятия решений. Каждая соответствующая сторона, заинтересованная в системе, должна быть вовлечена в этот процесс. Что касается блокчейна, то сюда должны входить не только пользователи, владельцы, майнеры, исследователи и разработчики, но и поставщики услуг, такие как кошельки, биржи и пулы майнинга. Различные группы заинтересованных сторон имеют разные интересы, и практически невозможно согласовать все стимулы. Вот почему управление блокчейном - сложная и противоречивая тема. Если мы рассмотрим блокчейн как большой социальный эксперимент, управление требует более сложной конструкции, чем любая другая часть системы. После десяти лет эволюции мы все еще не определили общие лучшие практики или устойчивые процессы для управления блокчейном.

В некоторых проектах управление осуществляется через «благожелательного диктатора на всю жизнь» (например, Линус Торвальдс в Linux). Мы признаем, что это делает проект очень эффективным, сплоченным и одновременно очаровательным: люди любят героев. Однако это противоречит децентрализации - основной ценности блокчейна.

Некоторые проекты наделяют отдельный внеплановый комитет широкими полномочиями по принятию решений, например, ECAF (EOSIO Core Arbitration Forum) по EOS. Тем не менее, эти комитеты не имеют достаточных полномочий, чтобы гарантировать участникам выполнение их решений, которые в конкретном случае могли бы сыграть роль в закрытии ECAF в начале этого года.

Некоторые проекты, такие как Tezos, идут дальше и внедряют управление по цепочке, чтобы все участники следовали принятым решениям. Это также позволяет избежать любых разногласий между разработчиками и майнерами (или пользователями полного узла). Обратите внимание, что управление по цепочке отличается от простого голосования по цепочке. Если предложенная функция или исправление набрало достаточное количество голосов посредством управления по цепочке, код цепочки будет обновляться автоматически. Майнеры или полные узлы не имеют никаких средств, чтобы контролировать это изменение. Polkadot использует еще более сложный подход к управлению по цепочке, используя «выборный совет»: процесс референдума для взвешенного по колу голосования и механизмы положительной / отрицательной предвзятости (bias) для учета явки избирателей.

Однако, несмотря на свою прямолинейность, управление на цепочке на практике не так элегантно, как представляется. Прежде всего, голоса отражают только интерес владельцев токенов, просто игнорируя все остальные стороны. Во-вторых, низкий уровень голосования является давней проблемой как в мире блокчейна, так и в реальном мире. Как результаты могут быть в интересах большинства, если голосует лишь меньшинство? И последнее, но самое главное. Хард-форк всегда должен рассматриваться как окончательное решение для всех заинтересованных сторон. Учитывая превосходную доступность данных, обеспечиваемую широкой репликацией неразрешенного блокчейна, всегда должна быть возможность отказаться от существующей цепочки с полным сохранением данных и без прерывания. Хард-форк никогда не может быть реализован через управление по цепочке.

На вопросы управления пока нет жизнеспособных ответов, поэтому для Nervos Network мы будем использовать развивающийся подход. В первые дни Фонд Nervos возьмет на себя роль руководящего органа проекта. Nervos Foundation - это Панамский фонд с управлением, сформированным из независимых советов. Фонду поручены мандаты на дальнейшее развитие Nervos Network, развитие ее экосистемы и внедрение.

Со временем, по мере того, как будет добываться больше токенов, майнинг становиться более распределенным, и все больше разработчиков вовлекутся в процесс, ответственность за управление постепенно перейдет к сообществу. В долгосрочной перспективе именно на уровне сообщества будет проходить управление процессом обновления протокола и распределением ресурсов из казначейства.

Nervos CKB разработана, чтобы быть децентрализованной автономной инфраструктурой, которая могла бы существовать в течение сотен лет, что означает наличие определенных моментов, которые требуют от нас как сообщества усилий, чтобы оставаться преданными сети независимо от того, как она развивается.

Существуют 3 основных инварианта:

- График эмиссии полностью фиксирован, поэтому никогда не изменится.
- Состояние / данные, хранящиеся в ячейках, не должны изменяться.
- Семантика существующих скриптов не должна изменяться.

Основанное на сообществе управление блокчейнами - это очень новая область, и существует множество достойных экспериментов. Мы понимаем, что это не тривиальная тема, и требуется время для полного изучения, наблюдения и повторения, чтобы прийти к оптимальному подходу. Мы придерживаемся консервативного подхода к управлению на уровне сообществ в краткосрочной перспективе, оставаясь полностью приверженными этому направлению в долгосрочной перспективе.

5. Обзор решений уровня 2

5.1 Что такое уровень 2?

Уровень 1 сети блокчейна определяется ограничениями. Идеальный блокчейн уровня 1 не делает никаких компромиссов в отношении безопасности, децентрализации и устойчивости, однако это создает проблемы, связанные с масштабируемостью и транзакционными издержками. Решения уровня 2 построены на основе протоколов уровня 1, что позволяет переносить вычисления за пределы цепочки с помощью механизмов, позволяющих безопасно вернуться к блокчейну уровня 1.

Это похоже на чистые расчеты в современной банковской системе или нормативные документы SEC. Сокращая объем данных, требующих глобального консенсуса, сеть может обслуживать больше участников и способствовать большей экономической активности, чем это было бы возможно в противном случае. При этом и свойства децентрализации сохраняются.

Пользователи уровня 2 зависят от безопасности, обеспечиваемой блокчейном уровня 1, и используют эту защиту при перемещении активов между уровнями или урегулировании спора. Эта функция аналогична судебной системе: суд не обязан отслеживать и проверять все транзакции, а служит только для регистрации основных доказательств и разрешения споров. Точно так же в контексте блокчейна, блокчейн уровня 1 позволяет участникам осуществлять операции вне цепочки, а в случае разногласий предоставляет им возможность доставлять криптографические доказательства в блокчейн и наказывать за нечестность.

5.2 Платежные каналы и каналы состояния

Платежные каналы создаются между двумя сторонами, которые часто совершают сделки. Они обеспечивают немедленную оплату с минимальными задержками, которую транзакции, выполняемые непосредственно в

глобальной цепочке блоков, никогда не смогут обеспечить. Платежные каналы функционируют аналогично вкладке в баре - вы можете открыть вкладку с барменом и продолжать заказывать напитки, но рассчитать вкладку и заплатить окончательную сумму только когда будете готовы покинуть бар. При работе с платежным каналом участники обмениваются сообщениями, содержащими криптографические обязательства для своих балансов, и могут обновлять эти балансы неограниченное количество раз вне цепочки, прежде чем они будут готовы закрыть канал и перенести баланс обратно в блокчейн.

Платежные каналы могут быть однонаправленными или двусторонними. Каналы однонаправленных платежей передаются от Стороны А к Стороне Б, аналогично приведенному выше примеру вкладки. Сторона А вносит максимальную сумму, которую она может потратить со Стороной В, а затем медленно перечисляет средства при получении товаров или услуг.

Двусторонние платежных каналы более сложны, но начинают открывать ряд возможностей для технологий уровня 2. В этих платежных каналах денежные средства движутся между сторонами в обоих направлениях. Это позволяет «перебалансировать» каналы платежей и открывает возможность платежей по каналам через третье лицо. Похожим образом обусловлено существование таких платежных каналов как сеть Биткойн и Лайтнинг. Средства могут быть переведены от Стороны А Стороне Б без прямого канала между ними, если Сторона А сможет найти путь через посредника с соединениями, открытыми для обеих сторон.

Как каналы оплаты могут масштабировать платежи внутри сети, так и каналы состояния могут масштабировать любые транзакции внутри сети. В то время как платежный канал ограничен управлением балансами между двумя сторонами, канал состояния - это соглашение о произвольном состоянии, позволяющее все - от игры в шахматы без доверия до масштабируемых децентрализованных приложений.

Как и в случае с платежным каналом стороны открывают канал, обмениваются криптографическими подписями с течением времени и представляют окончательное состояние (или результат) в смарт-контракт на цепочке. Смарт-контракт будет затем выполняться на основе этого ввода, рассчитывая транзакцию в соответствии с правилами, закодированными в контракте.

«Обобщенный канал состояния» - это мощная конструкция канала состояния, позволяющая одному каналу состояния поддерживать переходы между несколькими смарт контрактами. Это уменьшает «раздувание» состояний, присущее архитектуре «один канал на приложение», а также позволяет легко подключиться к сети с возможностью использования каналов состояния, которые уже открыты пользователями.

5.3 Боковые цепи

Боковая цепь - это отдельная цепочка блоков, которая прикреплена к недоверенному блокчейну (основной цепочке) с помощью двусторонней привязки. Чтобы использовать боковую цепь, пользователь отправляет средства по указанному адресу в главной цепи, блокируя эти средства под контролем операторов боковой цепи. Как только эта транзакция подтверждена и период безопасности пройден, операторам боковой цепи может быть передано подтверждение, детализирующее внесение средств. Затем операторы создадут транзакцию в боковой цепочке, распределяя соответствующие средства. Эти средства затем могут быть потрачены на дополнительную сеть с низкими комиссиями, быстрым подтверждением и высокой пропускной способностью.

Основным недостатком боковых цепей является то, что они требуют дополнительных механизмов безопасности и предположений безопасности (security assumptions). Простейшая структура боковой цепи - федеративная боковая цепь - доверяет группе операторов с несколькими сигнатурами. На платформах "умного контракта" модели безопасности могут быть точно настроены с помощью токен - стимулов или сплачивающих / бросающих вызов экономических игр.

По сравнению с другими масштабирующими решениями общего назначения вне цепочки, боковые цепи легче понять и реализовать. Для типов приложений, которые допускают создание модели доверия, приемлемой для их пользователей, боковые цепочки могут быть практическим решением.

5.4 Цепочки фиксации (Commit Chains)

На коммит-цепочках [6], таких как Plasma [7], строится цепочка уровня 2, которая использует доверенный корень в цепочке блоков уровня 1 (корнеую цепочку) с широким глобальным консенсусом. Эти коммит-цепочки безопасны. В случае, если оператор сети является злонамеренным или нефункциональным, пользователи всегда могут вывести свои активы через механизм в корневой цепочке.

Оператору цепочки фиксации доверяют правильное выполнение транзакций и публикацию периодических обновлений в корневой цепочке. При любых условиях, кроме длительной цензурной атаки на корневую цепочку, активы в цепочках фиксации останутся в безопасности. Как и в случае с федеративными боковыми цепями, проекты цепочек фиксации обеспечивают превосходное взаимодействие с пользователем по сравнению с ненадежными цепочками блоков. Тем не менее, они делают это, сохраняя более строгие гарантии безопасности.

Цепочка фиксации защищена набором смарт контрактов, работающих в корневой цепочке. Пользователи вносят активы в этот контракт, и оператор

цепочки коммитов затем предоставляет им активы в ней. Оператор будет периодически публиковать обязательства для корневой цепочки, которые пользователи впоследствии смогут использовать для подтверждения владения активами через доказательства Меркле (Merkle), то есть «выход», при котором активы цепочки фиксации выводятся в корневую цепочку.

Вышеизложенное описывает общее понятие конструкций коммит-цепочек, основу появляющегося семейства протоколов, включающего Plasma. В «Белой книге по Plasma» [7], выпущенной Виталиком Бутериным и Джозефом Пунемом в 2017 году, изложено амбициозное видение. Несмотря на то, что все Плазменные цепочки в настоящее время основаны на активах и могут хранить только владение (и передачи) заменяемых и незамеяемых (fungible and non-fungible) токенов, выполнение недоверенного кода (или смарт контракты) является активной областью исследований.

5.5. Проверяемые вычисления вне цепочки

Криптография предоставляет инструмент, по-видимому, адаптированный к динамике дорогостоящей проверки по цепочке и недорогих вычислений вне цепочки. Это интерактивные системы проверки. Интерактивная система проверки - это протокол с двумя участниками: Проверяющим (Prover) и Верификатором (Verifier). Отправляя сообщения туда и обратно, Проверяющий предоставляет информацию, чтобы убедить Верификатора в том, что определенное утверждение верно, в то время как Верификатор анализирует предоставленное и отклоняет ложные утверждения. Заявления о том, что Верификатор не может отклонить, принимаются как истина.

Основная причина, по которой Верификатор не просто проверяет утверждение, заключается в эффективности. Взаимодействуя с Проверяющим, Верификатор может проверять утверждения, которые непозволительно дороги, чтобы проверить иное. Этот разрыв сложности может происходить из различных источников: 1) Верификатор может работать на легком оборудовании, которое может поддерживать только ограниченные в пространстве или (и) ограниченные во времени вычисления 2) для простой проверки может потребоваться доступ к длинной последовательности недетерминированных решений 3) простая проверка может быть невозможна, поскольку Верификатор не обладает определенной секретной информацией.

Хотя секретность важной информации, безусловно, является серьезным сдерживающим фактором в контексте криптовалют, более важным сдерживающим фактором в контексте масштабируемости является стоимость проверки по цепочке (особенно относительно дешевых вычислений вне цепочки).

В контексте криптовалют значительное внимание было уделено zk-SNARK (нулевым знаниям, кратким неинтерактивным аргументам знания). Это семейство неинтерактивных систем доказательства вращается вокруг арифметической схемы, которая кодирует произвольные вычисления в виде

схемы сложений и умножений в конечном поле. Например, арифметическая схема может кодировать «Я знаю лист на этом дереве Меркля».

Доказательства zk-SNARK имеют постоянный размер (сотни байтов) и могут быть проверены в постоянном времени. Но эта эффективность Верификатора обходится дорого: требуется доверенная установка и структурированная ссылочная строка, в дополнение к арифметике на основе сопряжения (конкретная криптографическая твердость которой остается предметом озабоченности).

Альтернативные системы доказательства предоставляют различные компромиссы. Например, Bulletproofs не имеют надежной настройки и полагаются на гораздо более распространенное предположение о дискретном логарифме. Однако они имеют доказательства логарифмического размера (хотя и довольно маленькие) и Верификаторы с линейным временем zk-STARK предоставляют альтернативу zk-SNARK с точки зрения масштабируемости и без надежной настройки. Также они полагаются только на надежные криптографические предположения, хотя полученные доказательства являются логарифмическими по размеру (и довольно большими: сотни килобайт).

В контексте многоуровневой криптовалютной экосистемы, такой как Nervos Network, интерактивные доказательства предоставляют возможность перенести дорогостоящие вычисления на стороне проверяющего на уровень 2, требуя при этом только скромной работы со стороны Верификатора уровня 1. Например, такой образ мысли фиксируется в протоколе Виталика Бутерина ZK Rollup [8]. Ретранслятор без прав собирает транзакции вне цепочки и периодически обновляет корень Merkle, хранящийся в цепочке. Каждое такое обновление корня сопровождается zk-SNARK, который показывает, что новое дерево Merkle наполняется только допустимыми транзакциями. Смарт контракт проверяет доказательство и позволяет обновлять корень Merkle только в том случае, если доказательство является действительным.

Помимо простых транзакций вышеописанная конструкция должна поддерживать более сложные переходы состояний, включая DEX, множественные токены и вычисления, сохраняющие конфиденциальность.

5.6 Экономическая модель решений уровня 2

В то время как решения уровня 2 обеспечивают впечатляющую масштабируемость, экономическая характеристика этих систем может создавать проблемы при проектировании.

Экономика токенов уровня 2 может включать в себя компенсацию за критически важную инфраструктуру (такую как валидаторы и сторожевые башни), а также разработку стимулов для конкретных приложений. Инфраструктура критического уровня 2 работает лучше с моделью длительной подписки. В Nervos Network эту структуру ценообразования можно легко

внедрить с помощью метода оплаты, основанного на альтернативных затратах CKB. Поставщики услуг могут собирать проценты по «гарантийным депозитам» своих пользователей через NervosDAO. Разработчики уровня 2 могут затем фокусировать экономические модели токенов на стимулах, специфичных для их приложений.

В некотором смысле, эта модель ценообразования в точности соответствует тому, как пользователи платят за хранилище состояний на CKB. По сути, они платят подписчикам плату за майнинг распределением вознаграждений за инфляцию, выданных NervosDAO.

6. The Nervos Network

6.1 Уровень 1 как многокомпонентная платформа хранения ценности

Мы считаем, что блокчейн уровня 1 должен создаваться как хранилище стоимости. Чтобы максимизировать долгосрочную децентрализацию, оно должно основываться на доказательстве консенсуса в работе с экономической моделью, разработанной на основе хранения данных в состоянии, а не комиссионных за транзакции. Общая база знаний (CKB) является доказательством основанной на работе цепочки хранения многих активов с сохранением стоимости. При этом ее программные и экономические модели разработанны вокруг состояния.

CKB является базовым уровнем Nervos Network, с самой высокой безопасностью и самой высокой степенью децентрализации. Владение и передача активов в CKB сопрягаются с самыми высокими затратами, однако обеспечивают самое безопасное и доступное хранилище активов в сети и максимальную возможность компоновки. CKB лучше всего подходит для ценных активов и долгосрочного хранения.

Общая база знаний - это первый блокчейн уровня 1, созданный специально для поддержки протоколов уровня 2:

- CKB предназначена для дополнения протоколов уровня 2 с упором на безопасность и децентрализацию вместо пересекающихся приоритетов уровня 2, таких как масштабируемость.
- CKB моделирует свою бухгалтерскую книгу вокруг состояния, а не счетов.
- Ячейки - это, по сути, автономные объекты состояния, на которые могут ссылаться транзакции и которые передаются между слоями. Это идеально подходит для многоуровневой архитектуры, где объекты, на которые ссылаются и которые передаются между слоями, являются частями состояния, а не учетными записями.

- CKB разработана как обобщенная верификационная машина, а не как вычислительная машина. Это позволяет CKB выполнять функции криптографического суда, который проверяет переходы между цепочками состояний.
- CKB позволяет разработчикам легко добавлять собственные криптографические примитивы. Это заранее проверяет CKB, что позволяет проверить доказательства, сгенерированные различными решениями уровня 2.

Общая база знаний призвана стать инфраструктурой для хранения наиболее ценных в мире общеизвестных знаний. А лучшая в своем классе экосистема уровня 2 обеспечивает наиболее масштабируемые и эффективные транзакции блокчейна.

6.2 Масштабирование с помощью решений уровня 2

Благодаря многоуровневой архитектуре Nervos Network может масштабироваться на уровне 2 для любого количества участников, сохраняя при этом жизненно важные свойства децентрализации и сохранения активов. Протоколы уровня 2 могут использовать любой тип обязательств уровня 1 или криптографический примитив, обеспечивая большую гибкость и креативность при проектировании транзакционных систем для поддержки растущей пользовательской базы уровня 2. Разработчики уровня 2 могут выбирать свои собственные компромиссы в отношении моделей пропускной способности, окончательности, конфиденциальности и доверия, которые лучше всего работают в контексте их приложений и пользователей.

В Nervos Network уровень 1 (CKB) используется для проверки состояния, а уровень 2 отвечает за формирование состояния. Каналы состояний и боковые цепочки являются примерами генерации состояний, однако поддерживается любой тип шаблона генерации-проверки (такой как кластер генерации с нулевым знанием). Кошельки также работают на уровне 2, выполняя произвольную логику, генерируя новое состояние и отправляя переходы состояний в CKB для проверки. Кошельки в сети Nervos очень мощные, потому что они являются генераторами состояний с полным контролем над переходами состояний.

Боковые цепи удобны для разработчиков и обеспечивают хороший пользовательский опыт. Однако они полагаются на честность своих валидаторов. Если валидаторы ведут себя злонамеренно, пользователи рискуют потерять свои активы. Nervos Network предоставляет открытый и простой в использовании стек боковых цепей для запуска боковых цепей на CKB, состоящей из инфраструктуры цепочки блоков Proof-of-Stake, называемой «Muta», и решения на основе боковых цепей, которое называется «Axon».

Muta - это настраиваемая, высокопроизводительная структура блокчейна, разработанная для поддержки Proof-of-Stake, BFT-консенсуса и умных контрактов. Она обладает высокой пропускной способностью, BFT-консенсусом «Overlord» с низкой задержкой и поддерживает различные виртуальные машины, включая CKB-VM, EVM и WASM. Различные виртуальные машины могут использоваться одновременно в одной цепочке блоков Muta с возможностью взаимодействия между ними. Muta значительно снижает барьер для разработчиков при создании высокопроизводительных блокчейнов, в то же время позволяя максимально гибко настраивать свои протоколы.

Axon - это законченное решение, созданное с помощью Muta, чтобы предоставить разработчикам готовую боковую цепь поверх Nervos CKB с практической экономической моделью токен-безопасности. Решения Axon используют CKB для безопасного хранения активов, а также используют механизм управления на основе токенов для регулирования валидаторов боковой цепи. Также будут встроены перекрестные протоколы для взаимодействия между боковой цепью Axon и CKB и между боковыми цепями Axon. С Axon разработчики могут сосредоточиться на создании приложений, а не на создании инфраструктуры и межсетевых протоколов.
Мута и Аксон в настоящее время находятся в стадии разработки. Скоро мы откроем фреймворки с исходным кодом. RFC для Muta и Axon также находятся в стадии разработки.

Протоколы уровня 2 являются процветающей областью исследований и разработок. Мы предвидим будущее, в котором все протоколы уровня 2 стандартизированы и беспрепятственно взаимодействуют. Тем не менее, мы признаем, что решения второго уровня взрослеют, и мы часто стараемся раздвинуть границы того, что они могут сделать, а также найти их приемлемые компромиссы. Мы видели ранние многообещающие решения, но еще предстоит провести много исследований по таким темам как функциональная совместимость, безопасность и экономические модели в проектах уровня 2. После запуска нашей основной сети мы посвятим большую часть наших исследований протоколам второго уровня.

6.3 Устойчивость

В интересах долгосрочной устойчивости общая база данных Nervos накладывает ограничения на состояние, вводит затраты на хранилище в цепочке и стимулирует пользователей очищать свое хранилище состояния. Ограниченное состояние поддерживает низкие требования к полному участию узлов, обеспечивая работу узлов на недорогом оборудовании. Надежное полное участие узла увеличивает децентрализацию и, в свою очередь, безопасность.

Вводя пропорциональную по времени стоимость «арендной платы за состояние» для хранилища состояний, база общих знаний Nervos смягчает “трагедию общего достояния”, с которой сталкиваются многие блокчейны в

парадигме «плати один раз, храни вечно». Реализованный посредством целевой инфляции, этот механизм арендной платы за состояние обеспечивает бесперебойное взаимодействие с пользователем, в то же время накладывая расходы на хранилище.

Эти инфляционные издержки могут быть целевыми, поскольку пользователи владеют согласованным (консенусным) пространством, которое занимают их данные. Эта модель также включает в себя собственный механизм, позволяющий пользователям удалять свое состояние из согласованного пространства. В сочетании с экономическими стимулами ренты это гарантирует, что размер состояния всегда будет приближаться к минимальному объему данных, требуемому участниками сети.

Индивидуальное состояние также значительно снижает затраты разработчиков. Вместо того чтобы покупать CKBytes в соответствии с требованиями состояния для всех своих пользователей, разработчикам нужно всего лишь приобрести достаточно CKBytes для хранения кода подтверждения, требуемого их приложением. Каждый пользователь будет использовать свои собственные ячейки для хранения своих токенов и будет нести полную ответственность за свои активы.

Наконец, рента обеспечивает постоянное вознаграждение майнерам посредством выпуска новых токенов. Этот предсказуемый доход стимулирует майнеров продвигать блокчейн, вместо того, чтобы раздавать прибыльные блоки и брать комиссионные за транзакции.

6.4 Согласованные стимулы

Экономическая модель Общей базы знаний объединяет стимулы для всех участников экосистемы. В частности, растущая цена токена поддерживает цели каждой из следующих групп:

- Майнеры: рост цен на токены увеличивает доход майнеров
- Пользователи: растущая цена токена привлекает большее участие майнеров и повышает безопасность активов
- Разработчики: рост цен на токены обеспечивает большую безопасность для их пользователей, без существенного увеличения затрат для разработчиков
- Держатели токенов: рост цены токенов увеличивает стоимость их токенов

Общая база знаний Nervos создана специально для безопасного сохранения стоимости, а не для дешевых комиссий за транзакции. Это критическое позиционирование привлечет пользователей со схожими ценностями, подобно сообществу пользователей Биткойн, а не средних пользователей биржи.

Средние варианты использования обмена имеют тенденцию всегда подталкивать сеть блокчейна к централизации, стремясь к большей

эффективности и низким расценкам. Без значительных комиссионных доходов для операторов инфраструктуры, которые защищают сеть (майнеров или валидаторов), безопасность должна финансироваться за счет денежной инфляции или просто недофинансироваться. Денежная инфляция наносит ущерб долгосрочным держателям, а недофинансированная безопасность наносит ущерб любому заинтересованному лицу сети.

Тем не менее, пользователи ценных бумаг предъявляют строгие требования к устойчивости цензуры и безопасности активов. Они полагаются на майнеров, чтобы обеспечить это, и в свою очередь компенсируют их за их роль. В сети создания ценности эти стороны имеют согласованные интересы.

Хотя в других сетях долгосрочные держатели могут считаться «спекулянтами», держатели токенов являются непосредственными участниками общей стоимости Nervos Network. Эти пользователи создают спрос на собственные токены, что способствует увеличению бюджета безопасности сети.

Совмещая стимулы всех участников, объединенное сообщество Nervos сможет расти, а выровненная экономическая система сети также будет устойчивой к хард-форку.

6.5 Захват стоимости и генерация стоимости

Чтобы любой блокчейн оставался защищенным при увеличении стоимости активов, защищаемых платформой, в системе должен быть механизм захвата стоимости по мере увеличения ценности защищаемых активов. Ограничивая состояние, CKB делает пространство консенсуса дефицитным и рыночным ресурсом. По мере роста спроса на хранилище активов в сети, будет увеличиваться и стоимость пространства хранения состояния (и собственных токенов CKB). CKB - это первая мульти-активная платформа, которая напрямую накапливает ценность для своего собственного токена.

В качестве платформы, сохраняющей ценность, внутренняя ценность CKB как платформы определяется степенью безопасности, которую она обеспечивает хранимым активам. По мере роста стоимости защищенных активов механизм захвата стоимости экономической модели CKB способен автоматически повышать бюджет безопасности CKB. Это способствует привлечению большего количества ресурсов для майнинга, делая платформу более безопасной и повышая ее собственную ценность. Это важно не только для того, чтобы сделать платформу устойчивой. Поскольку платформа становится более безопасной, она также становится более привлекательной для более ценных активов, создавая больший спрос, то есть прокладывая путь к увеличению собственной ценности. Очевидно, что это связано с общей совокупной стоимостью, которая в конечном итоге переместится в пространство блокчейна, но мы считаем, что CKB захватит значительную долю этого спроса.

Со временем мы ожидаем, что экономическая плотность CKB увеличится. CKBytes будут использоваться для хранения ценных активов, а малоценные активы будут перемещаться в цепочки блоков, подключенные к CKB (в такие, как боковые цепи уровня 2). Вместо непосредственной защиты активов, CKB можно будет использовать в качестве доверенного корня для защиты всей экосистемы боковой цепи. Например, с помощью нескольких сотен байтов криптографических доказательств. Экономическая плотность таких доказательств необычайно высока, что еще лучше поддерживает кривую спроса на пространство в хранилище, поскольку цена CKBytes значительно повышается. Это аналогично небольшому участку земли, значительно увеличивающему его экономическую плотность за счет поддержки небоскреба.

Наконец, благодаря дизайну NervosDAO и его функции «защиты от инфляции» долгосрочные держатели токенов всегда будут сохранять фиксированный процент от общего объема эмиссии, что делает сам нативный токен отличным средством сохранения стоимости.

6.6 Преодоление регулятивного разрыва

Неразрешенные блокчейны обеспечивают полную децентрализацию при выпуске активов и транзакциях. Это то, что делает их ценными, но также является причиной их несовместимости с реальными финансовыми и судебными системами.

Появление многоуровневой архитектуры дает возможность создавать регулируемые части нерегулируемой, неразрешенной блокчейн цепи. Например, пользователи могут хранить свои децентрализованные активы на уровне 1, иметь абсолютную собственность на эти активы, а также могут обрабатывать бизнес в реальном мире на уровне 2, где они подвергаются нормативным и правовым ограничениям.

Возьмем, к примеру, биржи криптовалют. Такие страны как Япония и Сингапур, выдали лицензии на биржи и создали нормативные требования. Соответствующая биржа или филиал глобальной биржи может создать торговую цепочку уровня 2, импортировать идентификаторы пользователей и активы, а затем вести легальный бизнес в соответствии с местными нормативными требованиями.

Выпуск и сделка с активами реального мира становятся возможными в рамках многоуровневой блокчейн-конструкции. Активы реального мира могут перетекать в экосистему блокчейна через регулируемую боковую цепь уровня 2 к блокчейну без прав доступа уровня 1, предоставляя этим активам доступ к крупнейшей экосистеме компонуемых, децентрализованных финансовых услуг и максимизированной стоимости.

В будущем Nervos Network в сотрудничестве с ведущими компаниями в этой области будет также использовать подобные боковые цепи и приложения второго уровня в качестве основы для широкого принятия пользователями.

Ссылки:

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 31 Oct 2008, https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform". Nov 2013 http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] With an average Bitcoin transaction size of 250 bytes: (2 * 250 * 7,500,000,000) / (24 * 6) = 26,041,666,666 byte blocks (every 10 minutes); 26,041,666,666 * (24 * 6) = 3,750,000,000,000 bytes (blockchain growth each day); 3,750,000,000,000 * 365.25 = 1,369,687,500,000,000 bytes (blockchain growth each year)

[4] Gur Huberman, Jacob Leshno, Ciamac C. Moallemi. "Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System". Bank of Finland Research Discussion Paper No. 27/2017. 6 Sep 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032375

[5] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, Arvind Narayanan. "On the Instabiliity of Bitcoin Without the Block Reward". Oct 2016, https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf

[6] Lewis Gudgeon, Perdo Moreno-Sanchez, Stefanie Roos, Patrick McCorry, Arthur Gervais. "SoK: Off The Chain Transactions". 17 Apr 2019, https://eprint.iacr.org/2019/360.pdf

[7] Joseph Poon, Vitalik Buterin. "Plasma: Scalable Autonomous Smart Contracts". 11 Aug 2017, https://plasma.io/plasma.pdf

[8] Vitalik Buterin. "On-chain scaling to potentially ~500 tx/sec through mass tx validation". 22 Sep 2018, https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477