EOS.IO, техническая белая бумага

26 июня 2017, переведено @blockchained (https://steemit.com/@blockchained)

Аннотация: EOS.IO представляет собой программный комплекс, реализованный в новой блокчейн-архитектуре и позволяющий осуществлять вертикальное и горизонтальное масштабирование децентрализованных приложений. Возможность масштабирования достигается путем создания схемы, аналогичной операционной системе, поверх которой предполагается разработка самих приложений. Разрабатываемый программный комплекс включает в себя управление аккаунтами и аутентификацией, базы данных, асинхронный обмен данными, а также управление очередями выполнения для приложений с возможностью распределения задач между сотнями процессорных ядер или целыми [серверными] кластерами. Результатом является технология, представляющая собой блокчейн-архитектуру, масштабируемую до миллионов транзакций в секунду, не требующую от пользователей комиссионных платежей за использование, а также позволяющую развертывать децентрализованные приложения легко и быстро.

Замечание: криптографические токены, о которых идет речь в данной белой бумаге это криптографические токены уже работающего под управлением EOS.IO блокчейна. Эти токены не являются ERC-20 совместимыми токенами блокчейна Ethereum, связанными с процессом распределения токенов EOS.

Отказ от ответственности: Настоящий драфт технической белой бумаги EOS.IO публикуется исключительно в информационных целях. block.One не гарантирует точность или выводы, сделанные в этом документе, и этот документ предоставляется «как есть». block.one не гарантирует точность заключений, сделанных в этой бумаге, выпускает ее "как есть", без гарантий полноты покрытия и явного или неявного гарантирования перечисленных (но не ограниченных ими) условий: (i) коммерческая пригодность, возможность конкретного применения, именования или несоблюдения (прав); (ii) отсутствие ошибок в тексте, возможность использования по конкретному назначению; а также (iii) ненарушение содержимым данной бумаги прав третьих лиц. block.one и любые аффилированные структуры отказываются от любых обязательств и возможного ущерба, причиной которых может стать использование, упоминание или полагание на информацию, содержащуюся в данной бумаге, а также любые рекомендации относительно возможности наступления таких последствий. Ни в коем случае block.one или ее аффилированные лица не несут ответственность ни перед какими лицами или организациями за любой ущерб, убытки,

обязательства, издержки или расходы любого рода, будь то прямые или не прямые, косвенные, компенсационные, случайные, фактические, примерные, или понесенные из-за обоснования или планирования работ на основе этой белой бумаги или любого содержания настоящего документе, включая, без ограничений, любые потери бизнеса, доходов, прибыли, данных, доступности, доброй воли или другие нематериальные убытки.

Вступление

Технология блокчейн была представлена в 2008 году вместе с запуском валюты биткойн, и с этого момента предприниматели и разработчики пытались обобщить технологию с целью реализации поддержки более широкого спектра приложений в рамках единой блокчейн платформы.

В то время как многие блокчейн-платформы старались реализовать поддержку функциональных децентрализованных приложений, специализированные платформы, такие как децентрализованная биржа BitShares (2014) и социальная медиа-платформа Steem (2016), превратились в интенсивно используемые сообществом блокчейны с десятками тысяч активных пользователей ежедневно. Такие результаты были достигнуты благодаря увеличению производительности до тысяч операций в секунду, снижению задержки ответа до 1.5 секунд, снижению комиссий, а также предоставлению пользователям тех же возможностей, к которым они уже успели привыкнуть в существующих централизованных сервисах.

Высокие комиссии и ограничения, накладываемые потребностями в вычислительных мощностях, препятствуют широкому распространению технологии блокчейн и ее адаптации под нужды сообщества.

Требования к приложениям на блокчейне

Для широкого распространения блокчейн-приложений необходима платформа, достаточно гибкая для того, чтобы удовлетворять следующим требованиям:

Поддержка миллионов пользователей

Выдающиеся компании, такие как Ebay, Uber, AirBnB и Facebook, испытывают потребность в блокчейн-технологии, позволяющей обслуживать миллионы активных пользователей ежедневно. В отдельных случаях приложение просто не может работать до достижения определенного критического количества пользователей, а следовательно, платформа, способная справиться с массовым наплывом пользователей, крайне востребована.

Возможность бесплатного использования

Разработчикам прийдется быть гибкими и предлагать пользователям бесплатные сервисы; пользователи не должны платить за использование платформы или получать доход от ее сервисов. Бесплатная в использовании платформа, вероятно, сможет получить более широкое распространение. В результате у разработчиков и предпринимателей появится возможность построения эффективных стратегий монетизации.

Возможность простого обновления и восстановления после сбоев

Предприятиям, разрабатывающим приложения на блокчейне, требуется гибкость для расширения и улучшения функциональности.

Любое, кроме тривиального, программное обеспечение может содержать ошибки даже после тщательнейших проверок. Платформа должна позволять справляться с неизбежными в процессе ее функционирования проблемами.

Скорость отклика

Удобство использования диктует потребность в устойчивой обратной связи с задержкой, не превышающей нескольких секунд. Длительные задержки ухудшают впечатление пользователей о блокчейн-приложении в сравнении с существующими аналогами, не базирующимися на блокчейн.

Последовательная производительность

Некоторые приложения не могут реализовывать параллельные алгоритмы из-за наличия последовательно зависимых шагов. Например, биржевые приложения должны обеспечивать достаточную производительность последовательных вычислений для поддержания высоких объемов [торгов]. Поэтому и

разрабатываемая платформа должна иметь высокую производительность последовательных вычислений.

Параллельная производительность

Крупномасштабным приложениям необходимо распределять нагрузку на несколько процессоров и компьютеров.

Алгоритм консенсуса (DPOS)

EOS.IO использует единственный децентрализованный алгоритм консенсуса, способный удовлетворить потребности в производительности приложений на блокчейне: Делегированное Доказательство Владения Долей (Delegated Proof of Stake, DPOS). Согласно этому алгоритму, обладатели токенов блокчейна, адаптированного под EOS.IO, могут выбирать производителей блоков в ходе непрекращающегося голосования, и любой может решить участвовать в производстве блоков и получить право произвести количество блоков, пропорциональное полученному количеству голосов относительно всех других производителей. В закрытых блокчейнах руководство могло бы использовать токены для найма и увольнения IT персонала.

В EOS.IO блоки будут создаваться каждые 3 секунды, при этом в каждый момент времени правом создать блок будет обладать только один производитель. Если блок не был создан согласно расписанию, соответствующий отрезок времени пропускается. Если пропущен один или несколько блоков, то в блокчейне остается разрыв в 6 или более секунд.

В EOS.IO блоки создаются раундами. В одном раунде создается 21 блок. Каждый раунд начинается с выбора 21 уникального производителя. 20 лучших из утвержденных производителей автоматически участвуют в каждом раунде, а один выбирается в соответствии с набранным количеством голосов в сравнении с другими производителями. Выбранные для раунда производители выстраиваются в очередь в соответствии с псевдослучайными номерами, полученными из времени блока. Такое перемешивание производителей призвано обеспечить сбалансированность связей между ними.

Если производитель пропускает блок и не производит ни одного блока в течение 24 часов, то он исключается из рассмотрения до специального уведомления, которое такой производитель должен послать в блокчейн для подтверждения намерения продолжения работы. Это обеспечивает слаженную работу сети и минимизирует количество пропускаемых блоков путем исключения ненадежных производителей из расписания.

Обычно DPOS блокчейны не подвержены ветвлению (возникновению форков), т. к. производители блоков не конкурируют между собой, а кооперируются. В случае, если ветвление цепи все-таки происходит, алгоритм консенсуса автоматически переключается на самую длинную последовательность блоков. Эта схема работает, потому что скорость добавления блоков в ветку цепи

напрямую зависит от процента разделяющих текущий консенсус производителей блоков. Другими словами, ветка блокчейна с большим количеством производителей просто растет в длину быстрее в сравнении с веткой с меньшим количеством производителей. Более того, производитель блоков не может производить их для нескольких веток одновременно. Производитель, попавшийся за этим занятием, вероятнее всего будет исключен из процесса путем голосования. Для автоматизации исключения нарушителей могут использоваться криптографические доказательства.

Подтверждение транзакций

В типичных DPOS блокчейнах в работе участвуют все производители блоков. Транзакция может считаться подтвержденной с вероятностью 99.9% в течение 1.5 секунд с момента её отправки.

Есть вероятность возникновения некоторых экстраординарных ситуаций, вызванных сбоем в ПО, отключением от интернета или намеренным вредительством со стороны производителя блоков - в таком случае возникает ответвление (форк). Для абсолютной уверенности в необратимости транзакции узлу сети может потребоваться дождаться подтверждения от 15 из 21 производителей блоков. Для стандартной конфигурации EOS.IO в нормальных условиях на это потребуется 45 секунд. По умолчанию все узлы будут считать блок необратимым после получения подтверждения от 15 из 21 производителей и не станут переключаться на ветку, в которой нет этого блока, независимо от длины ветки.

Узел сети имеет возможность предупреждать пользователей о высокой вероятности нахождения на ветке меньшинства уже в течение первых 9 секунд с момента перехода на такую ветку. После 2-х последовательно пропущенных блоков вероятность нахождения узла на ветке меньшинства равна 95%. После 3-х вероятность достигает 99%. Существует возможность создания надежной модели прогнозирования, которая на основе информации об отключенных узлах, недавних рейтингах участия и других факторов могла бы быстро предупреждать пользователей о проблемах.

Реакция на подобные предупреждения полностью зависит от природы бизнес-транзакций, но самой простой реакцией будет дождаться 15 из 21 подтверждений, после чего предупреждение исчезнет.

Транзакции как Доказательство Владения Долей (TaPoS)

EOS.IO требует включения в каждую транзакцию хеша от заголовка предыдущего блока. Этот хеш выполняет две функции:

1. предотвращает повторение транзакции в ветке, которая не включает в себя упомянутый блок; и

2. уведомляет сеть о нахождении определенного пользователя и его доли на определенной ветке.

С течением времени все пользователи прямо подтвердят блокчейн как основной, что делает затруднительной подделку цепи ввиду отсутствия у злоумышленника возможности переноса транзакций из настоящей цепи.

Аккаунты

EOS.IO позволяет использовать в качестве идентификатора аккаунта уникальные, доступные для человеческого восприятия имена длиной от 2 до 32 символов. Имя выбирается создателем аккаунта. Для обеспечения возможности хранения данных счет аккаунта должен быть пополнен минимальной суммой в момент создания. Кроме того, имена аккаунтов могут содержать указатель на пространство имен (namespace), при этом только владелец аккаунта @domain может создавать аккаунты вида @user.domain.

В контексте децентрализации разработчики приложений будут оплачивать номинальные издержки на создание аккаунтов для своих новых пользователей. Традиционный бизнес уже тратит значительные суммы на привлечение каждого нового клиента, будь то рекламные расходы, бесплатные услуги и т. п. В сравнении с текущими расходами стоимость создания нового аккаунта в блокчейне будет несущественной. К счастью, аккаунты, которые уже были созданы пользователем в других приложениях, регистрировать заново не потребуется.

Сообщения и обработчики

Каждый аккаунт имеет возможность отправлять структурированные сообщения другим аккаунтам, а также может определять процедуры обработки поступающих сообщений (скрипты). EOS.IO выделяет каждому аккаунту защищенную базу данных, доступ к которой имеют только собственные обработчики сообщений этого аккаунта. Обработчики сообщений могут посылать сообщения другим аккаунтам. Сочетание сообщений и их автоматизированных обработчиков и представляет собой смарт-контракты в EOS.IO.

Управление правами доступа на основе ролей

Управление правами доступа включает в себя определение наличия прав доступа у сообщений. Простейшей формой управления правами доступа является проверка наличия у транзакции необходимых подписей, однако это предполпгает, что требующиеся подписи уже известны. Обычно власть привязана к некоторым сотрудникам или группам сотрудников, и зачастую разделена на отдельные ветви. EOS.IO предоставляет декларативную систему управления правами доступа, дающую аккаунтам тщательный многоуровневый контроль над тем, кто, что и когда может делать.

Стандартизация аутентификации и управления правами доступа и отделение их от бизнес-логики приложения являются критически важными факторами. Это делает возможным создание инструментов управления правами доступа в обычных средах разработки, а также обеспечивает широкие возможности для оптимизации производительности.

Каждый аккаунт может контролироваться комбинацией других аккаунтов и приватных ключей, взвешенной по их долям. Это формирует иерархическую административную структуру, отражающую реальную организацию прав доступа, и делает совместное управление средствами проще, чем когда-либо. Совместное управление само по себе вносит наибольший вклад в безопасность и при правильном применении способно значительно снизить риск кражи путем взлома.

EOS.IO позволяет аккаунтам задавать комбинации ключей и/или других аккаунтов, которые могут отправлять сообщения определенных типов другим аккаунтам. Например, существует возможность наличия одного ключа для социальных сетей пользователя и другого - для доступа к бирже. Возможна даже передача прав доступа одного аккаунта другому на выполнение действий от его лица без передачи при этом ключей.

Именованные Уровни прав доступа

Аккаунты EOS.IO имеют возможность задавать именованные уровни прав доступа с возможностью наследования разрешений от более высокого уровня (иерархия прав доступа). Каждый именованный уровень доступа определяет единицу администрирования; такая единица при этом представляет собой процедуру проверки мульти-подписи с указанием порогов действия, ключей и/или именованных уровней доступа других аккаунтов. Например, уровень доступа "Друг" может быть установлен для аккаунта, который может контролироваться в равной степени аккаунтами всех друзей пользователя.

Другим примером может служить блокчейн Steem, имеющий три зафиксированных в коде именованных уровня прав доступа: владелец, активное право, и право на публикацию. Право на публикацию дает возможность осуществлять только социальные действия, такие как голосование и публикация записей, в то время как активное право позволяют делать всё, кроме смены владельца. Право владельца имеет смысл хранить на холодном носителе (не подключенном к сети), т. к. оно дает возможность осуществления с аккаунтом любых действий. Программное обеспечение EOS.IO обобщает такой подход, давая возможность каждому владельцу аккаунта задавать свою собственную иерархию прав доступа, а также группировать действия.

Именованные группы обработчиков сообщений

EOS.IO обеспечивает каждому аккануту возможность объединять обработчики сообщений в иерархические именованные группы. Такие именованные группы

обработчиков могут использоваться другими аккаунтами в процессе конфигурации их настроек уровней доступа.

Обработчики сообщений верхнего уровня именуются по имени аккаунта, а нижнего - по индивидуальным типам сообщений, которые получает аккаунт. Такие группы могут быть вызваны как **@accountname.groupa.subgroupb.MessageType**.

Такая модель позволяет биржевому контракту группировать создание и отмену ордеров отдельно от депозитов и вывода. Подобная группировка по биржевому контракту является общепринятой для пользователей бирж.

Привязка прав доступа

EOS.IO дает возможность каждому аккаунту задавать соответствие Именованных обработчиков сообщений любого аккаунта его Именованному уровню доступа. Например, владелец аккаунта может задать соответствие между своей социальной сетью и группой прав доступа "Друг". С такой привязкой публиковать сообщения в социальной сети владельца аккаунта от его лица имеет право любой друг владельца. И даже несмотря на то, что публикация будет осуществляться от лица владельца, для подписания сообщений друзья будут использовать свои собственные ключи. Это делает возможным определить, кто из друзей использовал аккаунт, и как именно он был использован.

Применение прав доступа

В процессе доставки сообщения типа **Action** от **@Алисы** к **@Бобу** EOS.IO первым делом проверит, обладает ли **@Алиса** соответствующими правами доступа для **@bob.groupa.subgroup.Action**. В случае, если соответствие не найдено, будут последовательно проверены права на **@bob.groupa.subgroup**, затем **@bob.groupa**, и в конечном итоге, на **@bob**. Если не найдено никаких соответствий, предполагается применение именованной группы разрешений **@alice.active**.

Как только соответствие найдено, право подписи проверяется с учетом порога мульти-подписи и права именованного разрешения. Если проверка заканчивается неудачно, проверяются родительские разрешения вплоть до прав доступа владельца, **@alice.owner**.

Исходные группы прав доступа

Технология EOS.IO предоставляет всем аккаунтам возможность содержать группу доступа "владелец", члены которой имеют полный доступ ко всем функциям, и группу "активные права доступа", которая может все, кроме изменения группы "владелец". Все прочие группы прав доступа исходят от группы "активные права доступа".

Параллельный разбор прав доступа

Разбор прав доступа является процессом в режиме "только чтение", а изменение прав осуществляется посредством транзакций, которые вступают в силу только по окончании формирования блока. Это позволяет осуществлять параллельный разбор ключей и разрешений для транзакций. Более того, это также делает возможной проверку всех разрешений до запуска логики самого приложения, результаты работы которой в случае нарушения прав доступа пришлось бы откатить. И наконец, такой подход позволяет проверять разрешения транзакций не в момент их применения, а в момент получения.

С учетом всего вышесказанного проверка разрешений занимает значительную часть общего процесса проверки транзакции. Распараллеливание и отсутствие возможности внесения каких-либо изменений делает процесс проверки разрешений значительно более производительным.

В процессе воспроизведения цепочки блоков по логам сообщений с целью восстановления состояния необходимость в повторной проверке разрешений отсутствует. Сам факт того, что транзакция включена в подтвержденный ранее блок, является достаточным, чтобы пропустить этап проверки прав доступа. Это значительно снижает вычислительную нагрузку, связанную с повторным воспроизведением транзакций всегда растущей цепочки блоков.

Сообщения с отложенной доставкой

Время является критичным компонентом безопасности. В большинстве случаев узнать о том, что приватный ключ был похищен, невозможно до тех пор, пока он не будет использован. Безопасность, основанная на времени, становится еще критичнее в случаях, когда приложение требует хранения ключей на компьютерах, подключенных к сети и использующихся каждый день. EOS.IO дает возможность разработчикам приложений применять определенные сообщения не в момент включения в блок, а с некоторой установленной минимальной задержкой. В течение такой принудительной задержки сообщение может быть отменено.

В момент рассылки таких сообщений пользователи могут получать оповещения по e-mail или sms. В случае, если сообщение не было авторизовано, пользователь может воспользоваться процедурой восстановления аккаунта и отозвать такое сообщение.

Время задержки при этом определяется важностью операции, содержащейся в сообщении. Так, оплата кофе может не иметь задержки и быть необратимой через несколько секунд, в то время как покупка недвижимости может потребовать 72 часа в качестве периода для утверждения. Передача самого аккаунта целиком под чье-то управление может занять до 30 дней. Точное значение времени задержки устанавливается разработчиками приложения и пользователями.

Восстановление украденных ключей

Программное обеспечение EOS.IO дает пользователям возможность восстановить контроль над своим аккаунтом, когда их ключи украдены. Владелец аккаунта может использовать любой ключ владельца, который был активен в течение последних 30 дней, вместе с одобрением своего указанного партнера по восстановлению аккаунта, чтобы переустановить ключ владельца на его аккаунт. Аккаунт партнера по восстановлению не может перезагрузить контроль над аккаунтом без помощи владельца.

У хакеров нет возможности извлечь выгоду, пытаясь пройти через процесс восстановления, потому что они уже “контролируют” аккаунт. Кроме того, если хакер попробует пройти через процесс, партнер по восстановлению скорее всего потребует идентификации и многофакторной проверки подлинности (телефон и электронная почта). Это скомпрометирует хакера или не даст ему никакой выгоды в процессе.

Этот процесс очень отличается от простого соглашения с мульти-подписью. В случае с мульти-подписанной транзакцией есть еще другая сторона, которая является частью каждой проведенной транзакции; но в процессе восстановления агент - это только часть восстановительного процесса, и он не имеет власти над ежедневными транзакциями. Это значительно сокращает расходы и юридические обязательства всех участников.

Детерминированное параллельное выполнение приложений

Консенсус блокчейна зависит от детерминированного (воспроизводимого) поведения. Это означает, что все параллельные выполнения должны быть свободны от взаимоисключений или других блокирующих примитивов. В отсутствии блокировок должен быть какой-то способ гарантировать, что все аккаунты могу только читать и записывать их собственные частные базы данных. Это также означает, что каждый аккаунт обрабатывает сообщения последовательно и что параллельность будет на уровне аккаунта.

В блокчейне на EOS.IO в задачи производителя блоков входит организация доставки сообщений в независимые потоки с целью распараллеливания обработки. Состояние каждого аккаунта зависит только от доставленных ему сообщений. Расписание транзакций - это вывод производителя блоков, оно будет детерминистически выполнено, но процесс его создания не должен быть детерминистическим. Это означает, что производителям блоков можно использовать параллельные алгоритмы для составления расписания транзакций.

Роль параллельного выполнения такова, что когда скрипт создает новое сообщение, оно не доставляется немедленно, вместо этого его доставка запланирована на следующий цикл. Причина, по которой оно не может быть доставлено немедленно, состоит в том, что получатель может активно изменять собственное состояние в другом потоке.

Минимизация коммуникационной задержки

Задержка - это время, требующееся для отправки сообщения от одного аккаунта к другому аккаунту, а затем на получение ответа. Цель состоит в том, чтобы позволить двум аккаунтам совершать двухсторонний обмен сообщениями внутри одного блока без трёхсекундного ожидания между каждым сообщением. Чтобы предоставить такую возможность, программное обеспечение EOS.IO делит каждый блок на циклы. Каждый цикл делится на потоки, а каждый поток содержит список транзакций. Каждая транзакция содержит набор сообщений, которые будут доставлены. Эту структуру можно изобразить в виде дерева, где чередующиеся слои обрабатываются последовательно и параллельно.

```
    Блок

      Циклы (последовательные)

        Потоки (параллельные)

          Транзакции (последовательные)

            Сообщения (последовательные)

              Получатель и уведомленные аккаунты (параллельные)
```

Транзакции, произведенные в одном цикле, могут быть доставлены в любой последующий цикл или блок. Производители блоков будут добавлять циклы в блок, пока время настенных часов не выйдет, или пока не перестанут создаваться новые транзакции для доставки.

Можно использовать статический анализ блока, чтобы убедиться, что в данном цикле нет двух потоков, содержащих транзакции, которые изменяют один и тот же аккаунт. До тех пор, пока такая инвариантность сохраняется, блок может быть обработан параллельным запуском всех потоков.

Только читающие сообщение обработчики

Некоторые аккаунты могут быть в состоянии обрабатывать сообщение по схеме прошло/не прошло без изменения его внутреннего состояния. В таком случае эти обработчики могут выполняться параллельно столь долго, насколько читающие сообщение обработчики для конкретного аккаунта включены в один или более потоков в рамках определенного цикла.

Атомарные транзакции с несколькими аккаунтами

Иногда желательно гарантировать, что сообщения доставлены и приняты несколькими аккаунтами атомарно. В этом случае оба сообщения размещают в одной транзакции, и оба аккаунта будут присвоены одному потоку и сообщения применятся последовательно. Эта ситуация не идеальна для производительности, и когда дело доходит до "выставления счетов" пользователям за использование, они будут начисляться по количеству уникальных аккаунтов, ссылающихся на транзакцию.

Исходя из соображений производительности и стоимости, лучше всего минимизировать атомарные операции с использованием двух или более часто используемых аккаунтов.

Частичная оценка состояния блокчейна

Для масштабирования технологии блокчейн необходимо, чтобы компоненты были модульными. Никто не должен запускать всё подряд, особенно если им необходимо использовать только небольшую часть приложения.

Разработчик биржевого приложения запускает полные узлы с целью отображения состояния биржи для своих пользователей. Этому приложению-бирже не требуется состояние связанности с социальными приложениями. Программное обеспечение EOS.IO позволяет любому полному узлу выбрать любую подгруппу приложений для работы. Сообщения, доставленные другим приложениям, спокойно игнорируются, потому что состояние приложения полностью взято из доставленных ему сообщений.

Это существенно сказывается на связи с другими аккаунтами. Наиболее значительное влияние оказывает невозможность предположения, что состояние другого аккаунта доступно на этой же машине. Это также означает, что как ни заманчиво включение "блокировок", которые позволяют одному аккаунту синхронно вызывать другой аккаунт, такая схема ломается, если другой аккаунт не находится в памяти.

Все состояния связи между аккаунтами должны быть переданы через сообщения, включенные в блокчейн.

Субъективное планирование наилучших результатов

Программное обеспечение EOS.IO не может обязать производителей блоков доставлять любое сообщение любому другому аккаунту. Каждый производитель блоков проводит свою собственную субъективную оценку вычислительной сложности и времени, необходимого для проведения транзакции. Это применяется как для транзакций, созданных пользователем, так и для автоматически созданных скриптом.

Программное обеспечение EOS.IO предусматривает, что на уровне сети все транзакции оплачиваются фиксированной стоимостью пропускной способности, независимо от того, занимает ли их выполнение .01 ms или полные 10 ms. Однако каждый производитель блоков, использующий программное обеспечение, может рассчитать потребление ресурсов, используя свой собственный алгоритм и измерения. Когда производитель блоков делает вывод, что транзакция или аккаунт потребляет непропорциональное большое количество вычислительной мощности, он попросту отказывается от транзакции, когда производит собственный блок; тем не менее, он всё равно

обработает транзакцию, если другие производители блоков сочтут ее действительной.

В целом, пока хотя бы 1 производитель блоков считает транзакцию действительной и не выходящей за лимиты использования ресурсов, то все остальные производители также примут ее, но поиск транзакцией такого производителя может занять до 1 минуты времени.

В некоторых случаях производитель может создать блок, включающий транзакции, на порядок превышающие допустимые лимиты. В таком случае следующий производитель блоков может решить отклонить блок, и равный счет будет нарушен третьим производителем. Это ничем не отличается от того, что происходит, когда большой блок становится причиной сетевых задержек. Сообщество заметило бы злоупотребление и в конечном счете удалило бы свои голоса за производителя-мошенника.

Эта субъективная оценка вычислительных затрат освобождает блокчейн от необходимости четко и детерминировано определять, как долго что-нибудь будет запускаться. Благодаря такой конструкции не нужно четко рассчитывать инструкции, что резко увеличивает возможности для оптимизации без нарушения консенсуса.

Модель токена и использование ресурсов

Замечание: криптографические токены, о которых идет речь в данной белой бумаге это криптографические токены уже работающего под управлением EOS.IO блокчейна. Эти токены не являются ERC-20 совместимыми токенами блокчейна Ethereum, связанными с процессом распределения токенов EOS.

Все блокчейны ограничены в ресурсах и нуждаются в защитной системе. В блокчейне на EOS.IO есть три широких класса ресурсов, потребляемых приложениями:

1. Пропускная способность и хранение логов (диск);
2. Вычисления и вычислительное отставание (CPU); и
3. Хранилище состояния (RAM).

Пропускная способность и вычисления состоят из двух компонентов: мгновенного использования и использования в течение длительного срока. Блокчейн хранит журнал всех сообщений и этот журнал хранится и загружается всеми полными узлами. С журналом сообщений возможно восстановление состояния всех приложений.

Вычислительная задолженность - это расчеты, которые должны быть выполнены для восстановления состояния из журнала сообщений. Если вычислительная задолженность становится слишком большой, тогда возникает

необходимость делать снапшоты состояния блокчейна и отбросить прошлую историю блокчейна. Если вычислительная задолженность растет слишком быстро, то воспроизведение одного года транзакций может занять полгода. Поэтому очень важно, чтобы вычислительный долг тщательно контролировался.

Хранилище состояния блокчейна - это информация, которая доступна из логики приложения. Оно включает в себя такую информацию как реестры ордеров и балансы счетов. Если состояние никогда не читалось приложением, тогда его не следует хранить. К примеру, содержание поста в блоге и комментарии не читаются логикой приложения, значит их не следует хранить в состоянии блокчейна. Между тем существование поста/комментариев, число голосов и другие свойства хранятся как часть состояния блокчейна.

Производители блоков публикуют свой доступный объем пропускной способности, вычислений и состояния. EOS.IO позволяет каждому аккаунту потреблять процент от доступной мощности, пропорциональный количеству токенов, удерживаемых в заключенном 3-дневном контракте. Например, если запущен блокчейн, основанный на программном обеспечении EOS.IO, и если аккаунт держит 1% от общего количества токенов, распространяемых в соответствии с этим блокчейном, тогда этот аккаунт обладает потенциалом использовать 1% емкости хранилища состояния.

При внедрении программного обеспечения EOS.IO в уже запущенный блокчейн пропускная способность и вычислительная мощность распределяются на основе частичного резервирования, потому что они являются преходящими (неиспользуемые мощности не могу быть сохранены для использования в будущем). Алгоритм, используемый программным обеспечением EOS.IO, схож с алгоритмом, который используется в Steem для ограничения использования пропускной способности.

Объективные и субъективные измерения

Как обсуждалось ранее, инструментарий использования вычислений оказывает существенное влияние на производительность и оптимизацию; поэтому, все ограничения на использование ресурсов в конечном счете субъективны и их исполнение контролируется производителями блоков с учетом их индивидуальных алгоритмов и оценок.

Тем не менее, есть определенные вещи, которые поддаются объективному измерению. Количество доставленных сообщений и размер данных, сохраненных во внутренней базе данных, дешевы для объективного измерения. Программное обеспечение EOS.IO позволяет производителям блоков применять тот же самый алгоритм к этим объективным измерениям, но может применить и более строгие субъективные алгоритмы для более субъективных измерений.

Бизнес платит

Традиционно, именно бизнес платит за офисное пространство, вычислительную мощность и другие затраты, необходимые для его работы. Клиент покупает у

бизнеса определенные продукты, и доход от продаж этого продукта используется для покрытия издержек бизнеса. Аналогично, веб-сайт не обязывает своих посетителей производить микроплатежи за посещение этого веб-сайта, чтобы покрыть расходы на хостинг. Поэтому децентрализованные приложения не должны заставлять своих клиентов напрямую платить блокчейну за его использование.

Программное обеспечение EOS.IO не требует, чтобы его пользователи платили непосредственно блокчейну за его использование и, следовательно, не ограничивает и не препятствует бизнесам в определении своей стратегии монетизации продуктов.

Делегирование мощностей

Держатель токенов на блокчейне, запущенном на программном обеспечении EOS.IO, которому не нужно немедленно воспользоваться всей или частью доступной мощности, может отдать или сдать в аренду неиспользуемую пропускную способность другим аккаунтам; производители блоков, работающие на программном обеспечении EOS.IO на таком блокчейне, распознают это делегирование мощности и соответственно распределят пропускную способность.

Отделение стоимости транзакции от ценности токена

Одним из главных преимуществ программного обеспечения EOS.IO является то, что доступная для приложения пропускная способность полностью независима от цены любого токена. Если владелец приложения держит соответствующее количество токенов на блокчейне с внедренным в него программным обеспечением EOS.IO, тогда приложение может работать бесконечно в пределах фиксированного состояния и пропускной способности. В этом случае разработчики и пользователи не зависят от любых колебаний цен на рынке токена и, следовательно, не зависят от котировок. Другими словами, блокчейн, который использует программное обеспечение EOS.IO позволяет производителям блоков естественно увеличивать пропускную способность, вычислительную мощность и имеющееся у токена место для хранения данных независимо от его ценности.

Блокчейн, который использует программное обеспечение EOS.IO также вознаграждает производителей блоков токенами каждый раз, когда они производят блок. Ценность токенов влияет на суммарную пропускную способность, место для хранения и вычислительную мощность, которую производитель может позволить купить. Эта модель естественно использует возрастающую стоимость токенов для повышения производительности сети.

Стоимость хранения состояния

В то время как пропускная способность и вычислительная мощность может быть делегирована, хранение состояния приложения потребует от разработчика приложения держать токены до тех пор, пока состояние не будет удалено. Если состояние никогда не будет удалено, то токены будут эффективно изъяты из обращения.

Каждый пользовательский аккаунт требует определенного места для хранения; таким образом, каждый аккаунт должен поддерживать минимальный баланс. С увеличением емкости хранилища сети этот минимальный требуемый баланс будет уменьшаться.

Вознаграждение за блок

Блокчейн на программном обеспечении EOS.IO будет вознаграждать производителя блоков новыми токенами каждый раз, когда он производит блок. В таких обстоятельствах количество созданных токенов определяется средней желаемой платой, опубликованной всеми производителями блоков. В настройках программного обеспечения EOS.IO можно задать ограничение на вознаграждение производителей, чтобы общее годовое увеличение запаса токенов не превышало 5%.

Полезные сообществу приложения

Помимо избрания производителей блоков, основываясь на блокчейне на программном обеспечении EOS.IO, пользователи могут выбрать 3 полезных сообществу приложения, также известных как смарт-контракты. Эти 3 приложения будут получать токены до заданного процента от общего количества токенов в год минус токены, которые были выплачены производителям блоков. Эти смарт-контракты будут получать токены пропорционально количеству голосов, которое было получено каждым приложением от держателей токенов. Выбранные приложения или смарт-контракты могут быть заменены вновь избранными приложениями или смарт-контрактами владельцами токенов.

Управление

Управление - это процесс, с помощью которого люди достигают консенсуса по субъективным вопросам, которые не могут быть полностью охвачены алгоритмами программного обеспечения. Блокчейн на программном обеспечении EOS.IO реализует процесс управления, который эффективно руководит существующим влиянием производителей блоков. Отсутствие четко определенного процесса управления в предшествующих блокчейнах, как и полагание на специальные, неофициальные и часто противоречивые процессы управления приводит к непредсказуемым результатам.

Блокчейн на программном обеспечении EOS.IO признает, что власть исходит от держателей токенов, которые делегируют эту власть производителям блоков.

Производителям блоков даются ограниченные и проверяемые полномочия по замораживанию аккаунтов, обновлению дефектных приложений и внесению предложений о хардфорках в базовый протокол.

Процесс выбора производителей блоков встроен в программное обеспечение EOS.IO. Прежде чем какое-либо изменение будет внесено в блокчейн, эти производители блоков должны одобрить его. Если производители блоков отказываются вносить изменения по желанию держателей токенов, тогда они могут быть устранены. Если производители блоков вносят изменения без разрешения держателей токенов, тогда все остальные не производящие заверители полных узлов (биржи и т. п.) отклонят изменения.

Замораживание аккаунтов

Иногда смарт-контракт ведет себя аномальным и непредсказуемым образом и не выполняет своего назначения. В других случаях приложение или аккаунт может найти уязвимость, что позволит ему потреблять слишком много ресурсов. На случай неминуемого возникновения таких проблем у производителей блоков есть власть для улаживания подобных ситуаций.

Производители блоков во всех блокчейнах имеют право сами выбирать, какие транзакции включаются в блоки, что дает им возможность замораживать аккаунты. Блокчейн на программном обеспечении EOS.IO формализует это влияние, предлагая процесс замораживания аккаунта при наличии 17 из 21 голоса активных производителей. Если производители злоупотребляют властью, они могут быть устранены, и аккаунт будет разморожен.

Изменение кода аккаунта

Когда всё остальное не возымело результата и “неостановимое приложение” продолжает действовать в непредсказуемой манере, блокчейн на программном обеспечении EOS.IO позволяет производителям блоков заменить код аккаунта без хардфорка всего блокчейна. Подобно процессу заморозки аккаунта, эта замена кода требует 17 из 21 голоса избранных производителей блоков.

Конституция

Программное обеспечение EOS.IO позволяет блокчейнам установить peer-to-peer условия использования или юридически обязывающий для подписавших его пользователей договор, называемый "конституцией". Содержание этой конституции определяет обязательства среди пользователей, которые не могут быть полностью исполнены кодом, и облегчает урегулирование споров путем установления юрисдикции и избранного права наряду с другими взаимно принятыми правилами. Каждая транслируемая в сеть транзакция должна содержать хэш конституции как часть подписи и тем самым явным образом связывать подписавшего с договором.

Конституция также читаемо определяет назначение протокола исходного кода. Это назначение используется для определения разницы между багом и функцией, когда возникают ошибки, и руководит сообществом при выборе метода исправления.

Обновление Протокола & Конституции

Программное обеспечение EOS.IO задает процесс, в котором протокол, определенный каноническим исходным кодом и его конституцией, может быть обновлен следующим образом:

1. Производители блоков предлагают изменения конституции и получают 17/21 голосов одобрения.
2. Производители блоков поддерживают одобрение 17/21 в течение 30 дней подряд.
3. Все пользователи обязаны подписывать транзакции, используя хэш новой конституции.
4. Производители блоков вносят соответствующие изменения в исходный код, чтобы отразить изменения конституции, и предлагают их блокчейну, используя хэш гита изменений кода.
5. Производители блоков поддерживают одобрение 17/21 в течение 30 дней подряд.
6. Изменения в коде вступают в силу 7 дней спустя, давая всем полным узлам одну неделю для обновления после ратификации исходного кода.
7. Все узлы, не перешедшие на новый код, автоматически отключаются.

По умолчанию в конфигурации программного обеспечения EOS.IO процесс обновления блокчейна для добавления новых функций занимает от 2 до 3 месяцев, а время обновления для исправления некритичных ошибок, не требующих изменения конституции, составляет от 1 до 2 месяцев.

Экстренные изменения

Производители блоков могут ускорить процесс, если изменение в программном обеспечении требуется для устранения опасной ошибки или уязвимости в безопасности, которая активно вредит пользователям. Вообще говоря, ускоренные обновления для внедрения новых функций или устранения мелких ошибок могут не соответствовать установленной конституции.

Скрипты & виртуальные машины

Программное обеспечение EOS.IO станет первой и передовой платформой для координации доставки подлинных сообщений аккаунтам. Детали скриптового языка и виртуальной машины относятся к деталями внедрения, которые по большей части независимы от архитектуры технологии EOS.IO. Любой детерминистический язык или виртуальная машина, правильно собранные и

обладающие достаточной производительностью, могут быть интегрированы с API программного обеспечения EOS.IO.

Определяемые схемой сообщения

Все передаваемые между аккаунтами сообщения определяются схемой, которая является частью состояния консенсуса блокчейна. Эта схема позволяет легко выполнять преобразование между двоичной и JSON системами представления сообщений.

Определяемая схемой база данных

Состояние базы данных также определяется аналогичной схемой. Это гарантирует, что все данные, хранимые всеми приложениями, записаны в формате, который может быть интерпретирован в читаемый JSON, но хранятся и обрабатываются с эффективностью двоичного языка.

Отделение аутентификации от приложения

Для максимального использования возможностей распараллеливания и минимизации вычислительного долга, связанного с регенерацией состояния приложения из журнала транзакций, программное обеспечение EOS.IO разделяет логику проверки на три раздела:

1. Проверка того, что сообщение является внутренне согласованным;
2. Проверка того, что все предварительные условия действительны; и
3. Изменение состояния приложения.

Проверка внутренней согласованности сообщения доступна только для чтения и не требует доступа к состоянию блокчейна. Это значит, что она может производиться с максимальным параллелизмом. Проверка предварительных условий, таких как требуемый баланс, доступна только для чтения и поэтому также может выигрывать от параллелизма. Только изменение состояния приложения требует доступа с правом записи и должно обрабатываться последовательно для каждого приложения.

Аутентификация - это доступный только для чтения процесс проверки того, что сообщение может быть применено. На самом деле приложение делает всю работу само. В режиме реального времени должны быть выполнены оба вычисления, однако как только транзакция включена в блокчейн, необходимость выполнять операции проверки подлинности отпадает.

Независимая архитектура виртуальной машины

Замысел блокчейна на программном обеспечении EOS.IO состоит в том, что одновременно может поддерживаться несколько виртуальных машин, и новые

виртуальные машины добавляются по мере необходимости. По этой причине эта бумага не будет предоставлять детали какого-либо языка или виртуальной машины. Тем не менее есть две виртуальные машины, которые в настоящее время рассматриваются для использования в блокчейне на программном обеспечении EOS.IO.

Web Assembly (WASM)

Web Assembly является новым веб-стандартом для построения высокопроизводительных веб-приложений. С несколькими небольшими изменениями Web Assembly может быть сделан детерминистическим и стать песочницей. Преимущество Web Assembly - это широкая поддержка со стороны индустрии и то, что он позволяет разработку контрактов на знакомых языках, таких как C или C++.

Разработчики Эфириума уже начали модифицировать Web Assembly для предоставления соответствующей песочницы и детерминизма в их Ethereum flavored Web Assembly (WASM). Этот подход может быть легко адаптирован и интегрирован в программное обеспечение EOS.

Виртуальная машина Ethereum (EVM)

Эта виртуальная машина была использована для большинства существующих смарт-контрактов и может быть адаптирована для работы в блокчейне EOS.IO. Вполне возможно, что EVM контракты могут быть запущены в рамках их собственной песочницы внутри блокчейна на программном обеспечении EOS, и что с некоторой адаптацией EVM контракты смогут связываться с другими приложениями на таком блокчейне.

Межблокчейновая связь

Программное обеспечение EOS.IO создано с мыслью облегчить связь между блокчейнами. Это достигается путем упрощения доказательства существования сообщения и доказательства последовательности сообщений. Эти доказательства в сочетании с архитектурой приложения, разработанной для передачи сообщений, позволяют скрыть детали межблокчейновой связи и проверку действительности от разработчиков приложений.

Доказательство Меркла для проверки легкого клиента (Light Client) (LCV)

Интеграция с другими блокчейнами намного проще, если клиентам не нужно обрабатывать все транзакции. В конце концов, биржа заботится только о входящих и исходящих трансферах биржи, и ни о чем больше. Также было бы идеально, если цепь биржи могла бы использовать легковесные доказательства

депозита меркла вместо того, чтобы обязательно и полностью доверять собственным производителям блоков. По меньшей мере производители блоков этой цепи захотят понести минимально возможные издержки при синхронизации с другим блокчейном.

Цель LCV - позволить генерацию относительно легковесных доказательств существования, которые могут быть проверены любым, кто отслеживает относительно легковесный набор данных. В таком случае цель - доказать, что определенная транзакция была включена в определенный блок, и что блок включен в проверенную историю определенного блокчейна.

Биткоин поддерживает подтверждение транзакций, предполагая, что все узлы имеют доступ к полной истории заголовков блоков, что составляет 4 Мб заголовков в год. С 10 транзакциями в секунду действительное доказательство требует около 512 байт. Это хорошо работает на блокчейне с 10-минутным интервалом между блоками, но это больше не является "легким" для блокчейнов с 3-секундным интервалом.

Программное обеспечение EOS.IO разрешает пользоваться легковесными доказательствами каждому, кто имеет какой-либо необратимый заголовок блока после точки, где была включена транзакция. Используя хеш-связанную структуру, изображенную ниже, можно доказать существование любой транзакции с доказательством, занимающим менее 1024 байт. Если предполагается, что проверяющие узлы шли одновременно со всеми заголовками блоков весь последний день (2Мб данных), то для подтверждения этих транзакций потребуется только доказательство длиной 200 байт.

Существует незначительная дополнительная нагрузка, связанная с производством блоков с надлежащими хэш-ссылками, необходимая для указанных доказательств, что означает, что нет ни одной причины не создавать блоки таким способом.

Когда приходит врем проверить доказательства на других цепях, можно применить множество оптимизаций времени/пространства/пропускной способности. Отслеживание всех заголовков блоков (420 Мб в год) будет сохранять размер доказательств небольшим. Отслеживание же только последних заголовков может предложить компромисс между минимальным долгосрочным хранением и размером доказательств. Аналогично блокчейн может использовать ленивый подход к оценке, где он запоминает промежуточные хэши прошлых доказательств. Новые доказательства должны содержать только ссылки на известное разреженному дереву. Точнее, используемый подход будет обязательно зависим от процента чужих блоков, которые включают транзакции, на которые ссылается доказательство Меркла.

После определенной плотности взаимосвязей становится более эффективным просто иметь одну цепь, содержащую всю историю блоков другой цепи, и вовсе устранить необходимость доказательства. По причинам производительности идеально было бы минимизировать частоту межблокчейновых доказательств.

Задержка связи между блокчейнами

Когда идет коммуникация с другим блокчейном, производители блоков должны ждать до тех пор, пока не будет 100% уверенности, что эта транзакция была необратимо подтверждена другим блокчейном, прежде чем принять ее в качестве действительных входных данных. При использовании блокчейна на программном обеспечении EOS.IO и алгоритма DPOS с 3-секундными блоками и 21 производителем это займет около 45 секунд. Если производители блоков цепи не станут ждать необратимости, то это как если бы биржа приняла депозит, который впоследствии был отменен, что могло бы повлиять на действительность консенсуса блокчейна.

Доказательство целостности

Когда используются доказательства Меркла от других блокчейнов, есть существенная разница между знанием, что все обработанные транзакции являются действительными, и знанием, что ни одной транзакции не было отклонено или пропущено. И если доказать, что все последние транзакции известны, невозможно, то можно доказать, что в истории транзакций не было никаких пробелов. Программное обеспечение EOS.IO облегчает этот процесс, присваивая порядковый номер каждому сообщению, доставленному каждому аккаунту. Пользователь может использовать эти порядковые номера, чтобы доказать, что все сообщения, предназначенные для конкретного аккаунта, были обработаны, и что они были обработаны по порядку.

Заключение

Программное обеспечение EOS.IO разработано с учетом нашего опыта с использованием проверенных концепций и наилучших практик, и представляет собой фундаментально новый уровень в технологии блокчейн. Программное обеспечение является частью цельного плана по построению глобального масштабируемого блокчейн-общества, в котором создавать децентрализованные приложения и управлять ими совсем просто.