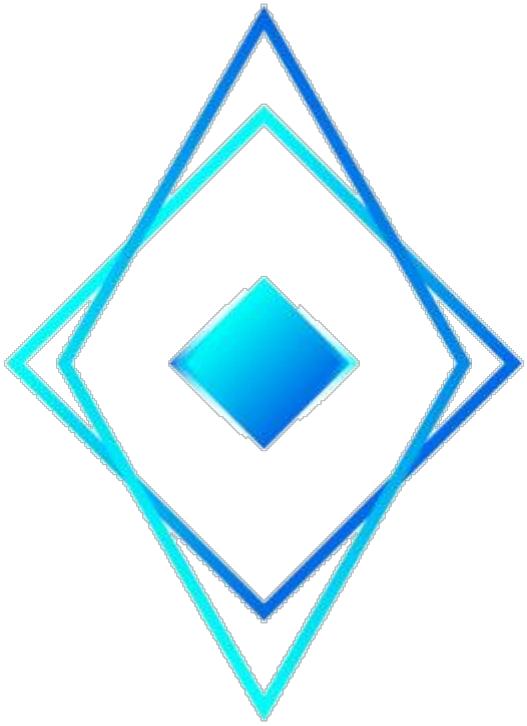
EtherZero – хард-форк Ethereum и платформа общего назначения для смарт-контрактов



Техническая документация EtherZero

V2.0

15 января 2018 года

Аннотация

EtherZero, сокращенно ETZ, является хард-форком Ethereum, платформой с высокой степенью расширяемости, предоставляющая без комиссионные транзакции в реальном времени или операции с сервисами подтверждения выполнения. Стремясь быть универсальной платформой для выполнения смарт-контрактов, ETZ помогает разработчикам создавать DAPP (децентрализованные приложения), которые ничем не ограничены в применении в сфере финансов и бизнеса, и создаются для того, чтобы популяризировать децентрализованные сервисы для большего числа людей и отраслей.

ETZ исключает систему комиссионных платежей (gas fee system) сети Ethereum и включает в себя протокол правил ограничения транзакций (Transaction Restriction Policy Protocol), который помогает предотвратить любые DDOS атаки.

ETZ также использует двухуровневую сетевую архитектуру DASH, реализованную с помощью системы верификации транзакций основанной на Мастернодах (Masternodes transaction verification network) и ETZ блокчейне (blockchain ledger layer) – встроенной автономной системы, предоставляющей пользователям информацию об операциях в режиме реального времени с возможностью проводить много параллельных транзакций (high transaction concurrency), что исключает долгое ожидание подтверждения проведенной операции.

Оглавление

Глава I. Предисловие

Стоит обратить внимание, что Ethereum, бета-версия которого была выпущена в мае 2015 года, потерял свою конкурентоспособность в сравнении с платформами нового поколения по аспектам производительности обработки транзакций и удобства пользования в следствии изобретения и применения различных новых виртуальных “пост-биткоин” валют и механизма консенсуса DPOS и его производных решений.

Недостаток конкурентоспособности проявляется в следующих аспектах: низкая масштабируемость и долгое время подтверждения транзакций, вызванная большим количеством узлов в обработке транзакции; проблема отсутствия поддержки реализации общего назначения (general-purpose development support) и использование транзакционных комиссий в качестве своего рода механизма защиты от DDOS-атаки.

ETZ использует проверенный на опыте механизм Ethereum-а выполнения смарт-контрактов, но устраняет его низкую масштабируемость и систему комиссионных платежей, реализует комплексную систему учета торговых лимитов и систему безопасности против атак типа DDOS. Созданная двухуровневая сеть, состоящая из основного узла (main node) и консенсусного слоя подтверждения выполнения работы (pow consensus layer), дает основу для выполнения бесплатных транзакций, с высоким уровнем параллелизма, в реальном времени и реализации многих других возможностей.

Глава II. Изначальный план

Раздел 2.01. Рынок

Несмотря на то, что общая рыночная капитализация криптовалют превысила 600 млрд. долларов США (к концу 2017 года) и продолжает расти, удивительно, что большинство инвесторов не знают о криптовалютах и о том, как технология блокчейн с транзакциями, не требующими доверия, может изменить мир. Другими словами, есть огромная потребность специализированных приложений в области блокчейна и криптовалют, чтобы снизить порог понимания и помочь обычным людям узнать какое колоссальное влияние эти технологии могут оказать на их повседневную жизнь. Очевидно, что подобные приложения не создаются независимо и не появляются в единичном экземпляре, а разрабатываются на базе универсальной DAPP платформы.

Раздел 2.02. Чем являет ся DAPP плат форма общего назначения?

Такая платформа (General-purpose DAPP Platform) должна включать, но не ограничиваться следующий функциональностью:

Основные операции должны выполняться бесплатно: Для того чтобы иметь возможность поддерживать разработку и бизнес операции децентрализованных приложений, различные базовые операции, такие как регистрация, логин, запись, поиск и просмотр транзакций в блокчейне, предоставление ссылки на информацию о транзакции и связанные логические операции, должны выполняться без комиссий.

Высокая параллельность и масштабируемость: Чтобы обслуживать смарт-контракты с пользователями по всему миру и данными в едином блокчейне в одно и тоже время – это достаточно сложная задача. Поэтому данная платформа для децентрализованных приложений также должна обладать достаточной масштабируемостью.

Мгновенная обратная связь: Подавляющее большинство пользовательских операций должны проводиться в реальном времени насколько позволяют условия по безопасности – это является основным требованием для децентрализованных приложений, что не сопоставимо с традиционными приложениями.

Система версий: Должна поддерживаться система версионности приложений, которая будет помогать разработчикам быстро выполнять исправления ошибок и проводить тестирование (A/B test).

Развитие платформы: Обработка предложений в сообществе и механизм голосования основных нод помогают стимулировать эволюцию ETZ, что способствует достижению быстрого консенсуса в итерациях технологии и правил платформы.

Основные компонентные функции: Децентрализованное хранилище, такое как протокол IPFS, безопасная процедура быстрого исправления, общие базовые службы, такие как аутентификация, анонимная связь, система уведомлений и т. д.

ETZ, как это уже понятно, решает все вышеуказанные задачи. Учитывая, что Ethereum наиболее технологически и экологически проверенная платформа в таких областях как смарт-контракты и выпуск токенов, мы решили реализовать платформу без платы за транзакцию и применить двухуровневую сетевую архитектуру монеты Dash для достижения высокой масштабируемости и получении информации по транзакциям в реальном времени.

Мы планируем добавить больше новаторских технических решений, такие как протокол IPFS, DAG и иерархическая сеть Plasma в будущем. Это долгосрочная работа, которая потребует усилий блокчейн- и криптовалютного сообщества в целом, и мы будем продолжать увлеченно изучать и исследовать всё это до того момента, пока не будут выполнены вышеуказанные задачи.

Глава III. Бесплатная DAPP платформа

Раздел 3.01. Использование без комиссии

Первой особенностью EtherZero является разделение валидации транзакций с системой формирования блоков, трансляции и синхронизации. Чтобы расширить возможности использования блокчейн DAPP-разработчикам и создателям смарт-контрактов нужны экономически дружелюбные технологии в отличие от текущих проектов на Биткойн и Эфириуме, реализация которых значительно снижает популярность блокчейн приложений.

Простой пример:

Алиса купила чашку кофе по цене 6 долларов, она должна заплатить комиссию за транзакцию в десять раз больше цены самой чашки при текущей рыночной ситуации. Очевидно, что это необоснованно. EtherZero исключает подход Ethereum в оплате газом за транзакцию приняв стратегию нулевой комиссии. Поскольку применение Ethereum Gas является важным механизмом для предотвращения DDOS-атак, ETZ будет использовать Proof of Stake (POS) для решения подобных проблем. Для получения подробной информации о политике безопасности, разработанной для системы с нулевыми комиссиями, обращаясь к разделу DDOS-Атака.

Раздел 3.02. Газ в Эфириуме

В Эфириуме значение газа рассчитывается в ETH и выплачивается майнерам как транзакционная комиссия после выполнения работы. Количество газа и ETH проявляется так:

а) Вознаграждение за работу майнера

б) Метод защиты системы от DDOS-атак

в) Метод повышения ликвидности

г) Базовая валюта для обмена токенами в Эфириуме

Как обеспечить мотивацию майнеров после исключения комиссий?

Даже если сбор за обработку транзакций будет исключен майнеры будут по-прежнему будут получать награду в валюте сети за формирование блоков. Бонус за монету, добытую майнерами, будет делиться на три части: 45% самому майнеру, 45% мастерноде и 10% в бюджет сообщества.

Раздел 3.03. Что означает отсутствие комиссий для DAPP-разработчиков?

В качестве простого примера децентрализованной реализации может выступать процесс декомпозиции задачи команды проекта, что требует от всех участников, чтобы они знали задачи других членов. Каждая последующая задача – это командный консенсус и результат с требованием прослеживаемости.

Приложение включает в себя регистрацию членов, добавление, удаление и изменение задач. Согласно требованиям разработки Ethereum, все эти операции потребляют газ, что явно необоснованно для пользователей приложения. При этом в EtherZero частота инициирования транзакции и глубина выполнения смарт-контрактов будет положительно связана с балансом счета. Этот механизм похож на POS, он объективно учитывает использование пропускной способности и устанавливает относительно высокий порог капитала, что является преградой для запуска DDOS-атака злоумышленниками при предоставлении бесплатных услуг. Этот вид ограниченного и экономически эффективного без комиссионного механизма поможет распространению децентрализованных приложений в жизни.

Раздел 3.04. Техническая реализация

а) Добавление дополнительного протокола верификации транзакций (Transaction Verification Protocol layer) для устранения атак DDOS, который могут возникнуть в сети без комиссий

б) Ограничение частоты инициирования транзакций на основе баланса счета

в) Размер данных, переносимых по транзакции, прямо пропорционален балансу счета

г) Введение ожидающего пула

д) Алгоритм настройки вышеупомянутой числовой системы с соответствующими элементами

содержащие частоту торговли, баланс счета и т. д.

Глава IV. Высокая параллельность и выполнение транзакции в реальном времени на базе двухуровневой сети

Раздел 4.01. Причина введения Маст ернод

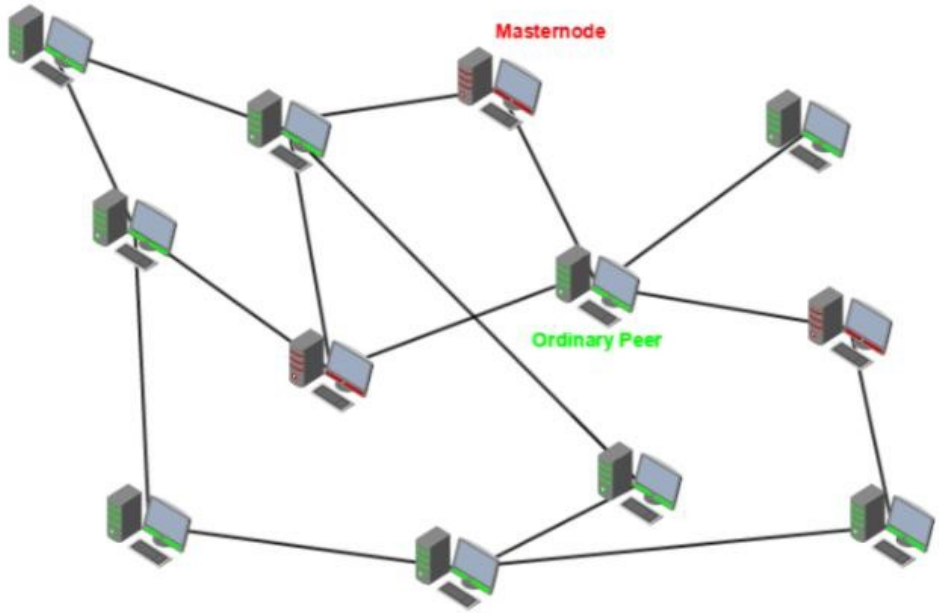
Что такое Мастернода (Master Node)

Мастерноды, первоначально уникальные для сети Dash, являются полными узлами. Мастернодой является сервер, подключенный к сети, который гарантирует определенный уровень производительности и функциональности для выполнения требуемых задач. Используя концепцию, известную как доказательство обслуживания (Proof of Service), Мастернода в дополнение к доказательству работы, выполненной майнерами, предоставляет результаты в двухуровневую сеть.

Мастерноды предоставляют критически важные сервисы для всей сети. Фактически вся сеть контролируется матернодами, которые имеют право отклонять ненадлежащим образом сформированные блоки майнеров. Если майнер попытался взять всю награду за блок сам или попытался запустить старую версию программного обеспечения Dash, мастернода заблокирует этот блок, и он не будет добавлен в блокчейн.

Отделив асинхронную проверку транзакции и формирование блокчейна, ETZ способен достичь высокого параллелизма и получение информации по транзакциям в реальном времени. Кроме того, Матерноде разрешено голосовать за предложения по управлению и финансированию и участвовать в процессе итераций развития технологий сообщества.

Следует отметить, что при физическом сетевом соединении основной узел не является особенным по отношению к обычным узлам.



Каждому обычному узлу в сети P2P необходимо синхронизировать текущий активный список мастернод (masternode list) в первый раз при присоединении к блокчейну.

Ответственность Мастернод

Первоначальные и основные обязанности мастернод:

а) Проверка (верификация) транзакций: достижение согласия (консенсуса) с другими мастернодами, отобранными по алгоритму, и трансляция результатов, обеспечение второуровневого предоставления информации по транзакциям в режиме реального времени. Этот сервис предоставления информации (feedback service) в реальном времени отличается от “мгновенной оплаты DASH” и не ограничивается областью специальных сервисов, а является общим базовым сервисом, открытым для всех операций и всех пользователей по умолчанию.

б) Автономия сообщества: Мастерноды должны голосовать на предложения. Предложение будет отражать дискуссию сообщества о тенденциях и на чем сфокусироваться, будет охватывать все аспекты EtherZero, включая, помимо прочего, направление технологической итерации, корректировку операционного плана, разрешение споров участников, изменение в экономических параметрах.

в) Выделенный сервис: в отличие от DASH, в котором основным действием приложения является платеж, EtherZero ориентирован на более широкий спектр децентрализованных приложений, которые требуют, чтобы услуги, предоставляемые мастернодой, могли быть разделены (subdivided) и специализированы в будущем для удовлетворения конкретных потребностей приложений.

Права и интересы мастернод

Для создания и поддержания мастернод требуется финансирование, время, энергия и технологии для предоставления все более и более качественных услуг пользователям во всей

цепи. Принимая на себя вышеуказанные обязанности, они будут получать вознаграждение от системы. Награда поступает из вознаграждения, которое зарабатывают майнеры путем формирования блока. Майнеры получают 45% вознаграждения, другие 45% достаются мастернодам, а остальные 10% используются для автономии сообщества и бюджетов предложений.

Алгоритм распределения бонусов между мастернодами можно описать как: чем больше работы, тем больше вознаграждение. Большее вознаграждение получат мастерноды, которые обработают больше сделок. Большее вознаграждение получат мастерноды, голосования которых соответствует окончательному результату предложения.

Содержание Мастерноды

Порог финансирования

Каждая Мастернода должна быть обеспечена 20 000 ETZ, которые находятся под полным контролем владельца, и он может в любое время свободно всё это потратить. Средства не заблокированы.

Однако, если средства будут перемещены или потрачены, связанная с ними мастернода будет отключена и прекратит получать вознаграждение. Назначение данного порога:

а) Обеспечить условие, чтобы у учредителя или владельца мастерноды было достаточно денег для поддержания долгосрочной работы сервиса.

б) Уменьшить предложение ETZ на рынке для поддержания стоимости ETZ на относительно высоком уровне

в) Защитить систему от DDOS атак, которые обычно запускаются путем создания большого количества мастернод.

Технический порог

Создание мастерноды требует определенного уровня знаний о блокчейне и серверной операционной системе Linux. Серверу нужен выделенный IP-адрес, 24 часа онлайн и максимальное оффлайн время менее часа. Организатор мастерноды может развернуть ее самостоятельно или обратиться за поддержкой к членам профессионального сообщества предлагающим специальные решения для хостинга. Вскоре после этого команда EtherZero предоставит подробный рабочий документ на официальном сайте, в котором будет описана концепция мастерноды, модель дохода, подробные процедурные и командные строки операционного руководства, операционный комплект (operations kits), планы сопровождения и часто задаваемые вопросы.

Раздел 4.02. Двухуровневая сет ь

Арбитражный слой состоит из мастернод вместе с последующим POW консенсусным слоем образуя архитектуру двухуровневой сети. Значение двухуровневой сети в целях обеспечения высокого параллелизма заключается в отделении проверки транзакции в блоке от процесса записи в блокчейне – эти два шага выполняются почти асинхронно. В любой момент транзакция может быть зафиксирована и подтверждена на уровне арбитража, обратная связь поступает

напрямую клиенту, без ожидания получения согласия pow-консенсуса для завершения формирования учета в блокчейне.

В связи с принятием консенсусного pow-алгоритма, майнеры по-прежнему имеют решающее значение для развития платформы. Платформа сохраняет вознаграждение за формирование блока.

Команда ETZ предоставит различные версии программного обеспечения майнинга для разных платформ.

В долгосрочной перспективе удаление комиссий может быть негативным для майнеров.

Учитывая, что майнеры владеют большим количеством ETZ, у них есть потенциал быть мастернодами и на самом деле консолидация майнеров и мастернод – одно из наших решений для достижения более высокого параллелизма. Основываясь на успешном опыте работы DASH, мы имеем повод полагать, что двухуровневая сеть будет гармоничной для симбиотического отношения. Для более долгосрочного консенсусного уровня наша команда рассмотрит DAG и Plasma технологии.

Раздел 4.03. Двухуровневая сеть в сравнении с DPOS

На самом деле все консенсусные механизмы DPOS можно просто объяснить как «богатые игры».

Создатель EOS BM дал полное представление об этом в своей дискуссии с Виталиком Бутериным, основателем Эфириума. Эта особенность проистекает из того факта, что существует вероятность того, что кандидат избранный в качестве принципала, положительно связан с балансом счета кандидата. Если взять EOS в качестве примера, его алгоритм голосования состоит в том, чтобы избрать 20 основных агентов из всех узлов и затем выбрать дополнительного агента с помощью этих 20 основных агентов. Результат голосования зависит от баланса учетной записи и 21 представителя, выбранных опросом, используя прокси формирования блоков для почти одноминутного цикла.

Для EtherZero алгоритм генерации на мастерноде требует, чтобы все транзакции генерировались клиентом случайным образом после синхронизации списка мастернод, и агенты, делегирующие каждую транзакцию, в принципе не могли повторно быть использованы, что обеспечивает более высокую скорость децентрализации.

Раздел 4.04. Высокое масштабирование в двухуровневой сети

Мы определяем масштабируемость как поддержку для массивных пользователей, огромных запросов, так и случайных ответов в реальном времени или почти в реальном времени.

Простой процесс транзакции от пользователя A к пользователю B выглядит так:

а) Пользователь A отправляет ETZ пользователю B с использованием блокировки транзакции

б) Блокировка транзакции передается по всей сети и, наконец, достигает N выбранных узлов (N> 2) для проверки

в) Избранная мастернода (главный узел) подписывает сообщение транзакции с транзакционной блокировкой для формирования сообщения о консенсусе, которое затем транслируется в сеть

г) Когда узел получает согласованное сообщение, можно считать, что транзакция была подтверждена и платеж завершен. Если пользователь A снова пробует инициировать платеж,

который уже существует в сети, второй платеж будет отклонен, чтобы предотвратить атаку повтора.

Подход

а) Двухуровневая сеть: отделение мастерноды от узла майнера позволяет верификации транзакции быть отделенной от процесса формирования блоков в блокчейне. Вместе с блокировкой транзакций, обработка транзакций почти в режиме реального времени может быть безопасно реализована в подобной асинхронной манере.

б) Механизм прокси. Существование мастерноды гарантирует, что не все узлы в цепочке должны быть ответственны за проверку транзакции, транзакция должна быть подтверждена только пятью мастернодами. В результате, чем больше мастернод, тем сильнее способность одновременной обработки транзакций в сети.

Дальнейшие планы

Увеличение емкости блока также является мерой для повышения масштабируемости. EtherZero будет поддерживать емкость 2 МБ и будет инициировать предложения сообществу в зависимости от количества пользователей и транзакций.

С более высокими требованиями к масштабируемости аппаратного обеспечения, будущие мастерноды и майнеры могут формировать единый узел для интеграции ресурсов. Опираясь на профессиональные сервисы, унифицированный узел достигнет специализации узла, как писал Сатоши:

«Текущая система, в которой каждый пользователь является узлом сети, не является конфигурацией больших масштабов. Это будет похоже на то, что каждый пользователь Usenet запускает собственные NNTP-сервер. Дизайн сети должен позволять пользователям просто быть пользователями. Чем больше усилий потребуется чтобы запустить узел, тем меньше будет узлов. Те немногие узлы будут большими владельцами серверов. Остальные будут клиентскими узлами, которые выполняют транзакции и не генерируют» – Сатоши, 2010”

Ссылка: https://medium.com/@eduffield222/how-to-enabling-on-chain-scaling-2ffab5997f8b

Это может быть революция в том плане, что традиционные услуги централизации переходят в децентрализованный профессиональный сервис. Роль такого совместного узла несколько схожа с существующими поставщиками облачных услуг. Анализируя исследования текущих поставщиков услуг облачных сервисов, разработчиков и операционных компаний, мы постоянно изучаем, как улучшить возможности сервиса этих комбинированных узлов в будущем в следующих трех областях:

а) Кастомизированное высокопроизводительное оборудование, включая процессор, оперативную память и жесткий диск

б) Адекватная пропускная способность для поддержки основного узла в трансляции по всей цепи

в) Стабильность сети мастернод соединяться и транслировать друг другу наиболее быстрым способом.

2/3 Атака

Существование финансового порогового значения для мастерноды делает чрезвычайно дорогим формирование атаки, основанной на построении большого числа мастернод.

Например, при использовании сети мастернод DASH, когда общее число мастернод равно 3000, чтобы получить успешный уровень атаки в 1,72%, хакеру нужно контролировать или создать 2000 мастернод, то есть купить 2 миллиона монет DASH при текущих ценовых условиях. Таким образом, атака 2/3 не стоит того, и низкая ликвидность, получаемая за счет блокировки монет мастернод, делает такую атаку нереальной.

Таблица. Вероятность успешной атаки, если атакующий контролирует N узлов

Атакующие мастерноды / Все мастерноды	Вероятность успеха (p)	Количество монет DASH
10/1010	3.44e-24	10,000
100/1100	2.52e-11	100,000
1000/2000	9.55e-03	1,000,000
2000/3000	1.72e-02	2,000,000

Где:

а) $p=\prod_{i=1}^{n} ((r-(i-1))/(t-(i-1)))$

б) n – длина цепи мастернод

c) t – общее количество мастернод в сети

d) r – количество мошенников-мастернод, контролируемых атакующим, и это ≥ n

e) Выбор мастернод является случайным

Ссылка: DASH WHITEPAPER - INSTANT TX

Атака повторного воспроизведения (Replay Attack)

Общей проблемой в большой масштабируемой распределенной сети является обеспечение того, чтобы ресурс был согласован во всей сети. Проблема согласованности обычно решается путем вызова различных алгоритмов соответствия, таких как Paxos.

Биткойн предотвращает атаки повторного воспроизведения с помощью механизма POW (подтверждения выполненной работы) и существенной доли проверенных узлов, вследствие этого ограниченного дизайна для подтверждения транзакции в сети биткойна требуется достаточно большое время. EtherZero представила концепцию блокировки транзакций, когда пользователь инициировал транзакцию то сгенерированная транзакционная блокировка будет транслироваться по всей сети, чтобы заблокировать связанные с транзакцией активы:

Transaction Lock: («txlock», CTransaction, nBlockHeight, Signed Message)

Любая клиентская мастернода не может передавать эти заблокированные активы без получения сообщения подтверждения с выбранных маснетод. Когда существующие транзакции появятся снова в сети, что обычно происходит, когда другой клиентский узел управляет заблокированным активом без получения уведомления о блокировки транзакции, вторая транзакция будет считаться вредоносной атакой повтора, что приведет к отказу от новых выбранных мастернод.

Атака Сивиллы

Это вид атаки в одноранговой сети, в результате которой жертва подключается только к узлам, контролируемым злоумышленником. Такая атака возможна из-за настройки низкого резервного порога и, соответственно, низкой ликвидности, вызванной таким порогом. При создании большого числа мастернод с высоким порогом баланса на счету мастерноды, как в случае EtherZero, такой вид атаки становится чрезвычайно дорогостоящим и сложным.

DDOS-атака

DDOS-атака относится к типу атак, которые инициируются большим количеством мусорных запросов к серверу на создание транзакции за короткий период времени, которые могут привести к выпадению мастерноды из сети и прерыванию обслуживания. В качестве слабого противодействия DDOS атакам используются комиссии за транзакцию, EtherZero учится на POS-механизме. В EtherZero количество транзакций, инициируемых аккаунтом, частота, глубина выполнения контракта и порядок транзакций при упаковке соотносятся с балансом аккаунта и такой механизм приводит к очень высокой стоимости создания большого количества мусорных транзакций. Детальный дизайн для защиты блокчейна от DDOS-атаки:

a) Начальный порог: во избежание злонамеренных атак, только если в учетной записи баланс больше чем 0.1 ETZ, владелец может инициировать транзакцию. Количество транзакций, которые могут быть инициированы учетной записью с фиксированным балансом, ограничены правилами формирования блока (десять секунд).

b) Упорядоченность: чем больше баланс учетной записи, тем более часто транзакции включаются в блоки.

c) Глубина вызова: чем больше баланс учетной записи, тем более сложные контракты, которые могут быть выполнены

d) Емкость: чем больше баланс, тем больше данные транзакций.

e) Максимальная глубина: чтобы предотвратить запуск выполнения контракта в бесконечный цикл, максимальный размер стека будет ограничен 1024.

f) Контрактный счет: только если остаток на счете превышает 100 ETZ и контракт может быть вызван другими учетными записями.

Атака Финни

Атака Финни – это вариант атаки двойного списания. Злоумышленник создает две транзакции – одну кредитующую счет жертвы и одну кредитующую свой счет. Он удерживает первую транзакцию, а вторую пытается включить в блок. Когда он преуспеет в этом (это может занять некоторое время), он быстро совершают покупку по первой транзакции, получает

приобретенные товары, а затем выпускает сформированный блок. Таким образом, первая транзакция станет недействительной, даже если она распространилась по всей сети.

Ссылка: https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack

Эта схема реализуется фактически из-за временной задержки в платежных сервисах в блокчейнах с высоким временем ожидания, таких как BTC. В противовес этому получаемая обратная связь по транзакциям в режиме реального времени в EtherZero значительно сокращает рабочее пространство для таких атак.

Глава V. Автономия сообщества и его развитие

Автономия обусловлена хорошими механизмами управления дефектами и отчетности, с эволюцией, вытекающей из мышления верхнего уровня, технологического и экономического руководства.

Простое предложение и голосование могут иметь дело с базовым управлением дефектами. На разных этапах развития могут встретиться разные требования. В EtherZero изменение спроса будет все больше и больше зависеть от мощности сообщества, включая новые открытия, предложения, обзоры, краудсорсинг, вознаграждения и наказания и т.д. Для формирования механизма ответственности с самого начала EtherZero будет руководить сообществом, чтобы сформировать систему рецензирования, и шаг за шагом консолидировать опыт и механизмы как контракты на долгосрочной основе.

Экономические отношения определяют социальную структуру. Системы бюджетирования учитывают 10% от награды за блок, обеспечивая сообщество автономностью и эволюционной системой экономического стимулирования с самого начала.

Раздел 5.01. Разработ чики

Разработчики будут рассматриваться как основное сообщество EtherZero, где они будут играть роль фундаментального поставщика ресурсов, столь же важного, как солнечный свет и вода для растений. Мы будем строить более мотивирующую экономическую систему с самого момента форка и обеспечивать прямое стимулирование в виде ETZ для разработчиков, чтобы создать качественные, творческие и влиятельные приложения для всего сообщества.

Раздел 5.02. Предложение и бюджет ы

Нынешний механизм управления сообществом DASH облегчает процесс создания разнообразия приложений и видов деятельности. Рыночная капитализация DASH также постепенно увеличивается. Будет создана аналогичная система управления сообществом и в EtherZero:

a) Предложение: Каждый может инициировать предложение, и заявитель должен быть известен в сообществе и иметь вклад в развитие сообщества.

b) Проверка: Аудит должен проводиться в цепочке по голосам мастернод (да-нет), предложение будет одобрено или отклонено при наличии разницы в 10% между да и нет голосов.

c) Награда: Награды ETZ будут выпускаться еженедельно на суперблоке, а заявитель будет вознагражден в соответствии с суммой предложения.

Глава VI. Технические характеристики

Раздел 6.01. POW

а) Размер блока: 2M

б) Время формирования блока: 10 секунд

в) Вознаграждение за формирование блока: 4 ETZ

г) Алгоритм настройки сложности: EtHash

Раздел 6.02. Маст ерноды

а) Порог: 20 000 ETZ

б) Вознаграждение: 45% вознаграждения Блока.

Раздел 6.03. Транзакция

а) Число кворума мастернод: 6/10

б) Задержка: почти реального времени, второй уровень

Глава VII. Сценарии применения

Раздел 7.01. DAPPs с поддержкой общего назначения

Основная задача блокчейна состоит в том, чтобы реализовать нерелевантность-доверия, то есть независимо от того, кто контрагент, можно напрямую торговать с ним без какого-либо доверия, а система «Не полагаясь на доверие» реализуется через смарт-контракты. Например, рассмотрим договор ставки на результат матча, упрощенный код которого выглядит следующим образом:

```
matchResult = NBA.matchResultAPI.get ("the final battle")
if(Cavaliers won)
  pay 40 to A
else
  pay 40 to B
```

Исходя из этого примера, сервисы, которые должны использоваться во взаимодействии двух и более сторон требуют посредников, а в случае применения блокчейн технологии смарт-контракт возьмет на себя роль посредника и это будет лучший вариант.

Фактически, смарт-контракт в Ethereum является программой общего назначения, но его функция взимания комиссии делает сложные контракты не эффективными для большого числа пользователей в стоимостном аспекте.

Устранение системы комиссий в EtherZero позволяет пользователям, которые работают со смарт-контрактами, использовать сервисы разумно, не оплачивая какие-либо издержки, обеспечивая экономическую жизнеспособность и устойчивость крупных децентрализованных приложений и предоставляя DAPP естественной способности дифференцировать сервисы на основе балансов счетов.

Раздел 7.02. Промышленное развит ие

Как базовая платформа разработки приложений EtherZero не ограничивается отраслью кооперации. Однако необходимо описать некоторые значимые размышления из того, что мы пытаемся реализовать.

Игры – краудсорсинг, дизайн и обмен продуктов

CryptoKitties, игра с цифровыми кошками, составила от 11% до 15% трафика на Ethereum на 4-ое декабря 2017 г., и позволила людям реализовать огромный потенциал блокчейна в сегменте игр: уникальность такого вида продукта полна возможностей в частной торговле на рынке.

Мы разработаем систему аутсорсинга продуктов и торговую платформу чтобы соединить дизайнеров и писателей, разработчиков числовых систем, производителей игр, игроков и другие группы, для следующих вариантов использования:

a) Производитель: устанавливает требования и блокирует монеты ETZ для интеллектуальных контрактов в качестве предоплаты

b) Дизайнеры: получают задания, создают продукты в соответствии с концепциями игры и требованиями; получают оплату после того, как продукт был признан пользователями и производителями.

c) Проектировщики числовых систем: рассчитывают критический уровень, эффект продукта, условия изменения, правила изменения, и т. д.

d) Пользователи: голосуют за продукт, обмениваются продуктами.

Благодаря такой экологической петле достигается выразительности, распространение и реализация идей и оригинальности.

Электронная коммерция и онлайн-дистрибуция

В скором времени начнут проводиться специализированные семинары в различных индустриях и на них будет обсуждаться с экспертами, что необходимо для создания независимой, основанной на токенах EtherZero, экономики в этих отраслях. Так же исследуются точки слияния между технологиями обработки больших данных (big data) и распределенных и анонимных методов учета, для обеспечения достаточной благоприятной среды для применения ИИ (искусственного интеллекта) в промышленности, основанного на богатых и достоверных данных.

Соединение организация из реального мира с блокчейном

Общество нуждается в различных организациях, централизованных или децентрализованных, больших или маленьких. Вовлеченность и разнообразие самого общества являются проявлением степени социальной свободы. Сравнивая с DAO, мы планируем реализовать

сопоставление приложения, которое мы называем MRO (Map of Real World Organization) в EtherZero, с организацией, которая может быть как анонимная, так и реальная, помогая существующим предприятиям решать задачи внутреннего управления и управления отношениями с контрагентами посредством смарт-контрактов.

Представьте себе следующее:

а) Каждая организация может сопоставить себя с этим приложением

б) Внутреннее управление:

1. Набор персонала и подписание трудового смарт-договора

2. Выплата зарплаты и ее расчет с использованием формализованной структуры типов начислений

3. Покупка сервисов по обработке больших данных, услуг ИИ, предоставляемые разработчиками и юристами на основе стандартных доверенных данных

4. Публикация задач по аутсорсингу и подписание смарт-соглашений об аутсорсинге

5. Проведение голосований или тайных выборов

в) Управление взаимоотношениями

1) Подписание смарт-контрактов с деловыми партнерами или конкурентами

2) Подписание смарт-соглашения о поддержке и обслуживании с партнерами

3) Выплата задолженности, проведение ICO и осуществление различных видов финансирования

4) Другие возможные реализации, которые могут быть виртуализованы для оформления в виде смарт-контрактов.

Глава VIII. Экономическая система

Раздел 8.01. Использование ETZ

Использование монет ETZ во всей экосистеме, классификация по ролям:

а) Майнеры:

-- ETZ в качестве вознаграждения за работу майнера по расчёту и формированию новых блоков

б) Заявители, участвовавшие в ответах на предложения

-- ETZ в качестве бюджета для работы одобренных предложений

в) Мастерноды

-- В качестве порогового значения работы мастерноды

-- В качестве вознаграждения за работу мастерноды по проверке транзакций и предоставлению других сервисов

г) Разработчики

-- Для работы смарт-контракта требуется баланс в 10 ETZ

д) Обычные пользователи

-- 0,1 ETZ требуется для инициации транзакций. Баланс положительно связан с глубиной выполнения транзакции, частотой и т.д.

Экономическая система, построенная на основе вышеуказанной функциональности ETZ, может эффективно поощрять различные роли в экосистеме к достижению общей цели.

Раздел 8.02. Выпуск монет ETZ

EtherZero (абр. ETZ) – это внутренняя монета платформы EtherZero. Первоначальный выпуск ETZ составляет 194 миллиона монет, из которых 97 миллионов будут выделены в качестве вознаграждений для ETH держателей, а другие 97 миллионов будут зарезервированы для частных инвесторов, а также направлены на разработку и эко-развитие.

Ожидаемая ежегодная инфляция составляет 6,5%, при этом большое количество ETZ будет заблокировано для сохранения работы мастернод, смарт-контрактов и обычных счетов, предложение монет на рынке должно быть стабильным или уменьшающимся.

Раздел 8.03. Пороги

Мастерноды (Masternodes)

В настоящее время DASH имеет 4777 мастернод (ссылка 1), каждая из которых должна иметь 1000 DASH, что составляет 61% от общей суммы 7 783 295 DASH.

Планируется что в сети EtherZero, каждая мастернода которой должна иметь 20 000 ETZ, будет работать 4000 основных узлов каждый год, которым потребуется 80 миллионов ETZ, что составляет около 41% от общей суммы первоначальной эмиссии ETZ.

Эккаунты смарт-контрактов

Чтобы обеспечить нормальную работу смарт-контракта разработчикам необходимо иметь 10 ETZ на счете контракта, валюта может быть переведена в любое время, но это повлияет на выполнение контракта, поскольку система ограничивает это: контракты будут вызываться только с балансом выше 10 ETZ.

Внешние счета

Только с балансом 0,1 ETZ или выше может быть инициирована транзакция со стороны внешнего владельца (EOA, external owned account).

Раздел 8.04. Обмен

Информацию о обмене ETZ на другие криптовалюты смотрите в наших объявлениях в Твиттере или Телеграмме.

Раздел 8.05. Денежная политика

Фиксирование сумм ETZ мастернод, учетных записей контрактов и на счетах пользователей приведет к выравниванию рыночного предложения и поддержанию определенной дефляции в течение последующего более длительного периода времени.

По мере развития бизнеса значения порогов могут быть скорректированы посредством голосования в сообществе.

Предполагалось, что половина ETZ в EtherZero будет храниться в мастернодах и на счетах контрактов. Эта эндогенная экономическая система вместе с платежными запросами постоянного потока новых счетов, а также огромные нарождающиеся инвестиции на торговой платформе, будут развивать спрос и предложения, что будет вести к росту цены ETZ беспрерывно.

Глава IX. План и видение

Раздел 9.01 График работ ы

Итерации технических характеристик платформы будут соответствовать постепенной разработке в соответствии с экологическим планированием, в разное время и на основе различных характеристик для руководства разработчиков и пользователей, заинтересованных в соответствующей программе.

См. Экологический рост с точки зрения разработки.

a) Январь 2018 года: в сети EtherZero будет реализована нулевая плата за транзакцию и защита от DDOS-атаки.

b) Февраль 2018: EtherZero завершит полный запуск EtherZero сети, выложит онлайн-кошелек, запустит Mainnet, чтобы получить нулевую комиссию за транзакцию и защиту от DDOS-атаки, будет сформирован первый блок EtherZero

c) Март 2018: Будут выпущены мобильный кошелек и магазин приложений DApp для содействия продвижению и экологического развития пользователей

d) Апрель 2018: Masternode будет успешно протестирован на Testnet

e) Май 2018: Masternode будет успешно протестирован на Mainnet, реализуя более высокую транзакционную параллельность (более 10000TPS)

f) Июнь 2018: Оптимизированная версия Masternode будет подключена к сети, поддерживая десятки тысячи TPS.

g) Январь 2019: Будет запущен конкурс приложений Star DAPP в рамках долгосрочной программы поощрения разработчиков для содействия развития и процветания сообщества разработчиков.

Раздел 9.02 Видение

Мы позиционируем себя как интегратора, промоутера и разработчика блокчейн технологии.

Такая конвергенция является следствием того факта, что большинство текущих инноваций все еще находятся в экспериментальной фазе, сильно отделены друг от друга и имеют неясные сценарии работы приложений. Блокчейн индустрия рекомендует организации выступать в роли наблюдателя и исследовать интеграционный потенциал этих технологий в реальных сценариях, а также предоставить разработчикам операционную систему, которая применяет различные технологии и ориентирована на уровень приложений. EtherZero будет использовать собранные частные средства для привлечения новых блокчейн-специалистов для интеграции

существующих технологий после завершения задачи по развертыванию необходимого количества мастернод. В перспективе технология будет преобразована в практические сценарии работы в параллельном режиме производственной и экспериментальной сетей.

Продвижение и практика нацелены на реальные сценарии работы приложений. Каждая технология должна иметь живую сцену, на которой она имеет прорыв и действительно экономическую выгоду по сравнению с исходной технологической системой, чтобы стать мейнстримом. Мы организуем специальную рабочую группу по применению приложений в различных индустриях, членами которой являются отраслевые эксперты, блокчейн-специалисты и менеджеры продуктов, чтобы исчерпывающим образом исследовать реализуемость сценария и углубить блокчейн революцию.

Слишком много концепций стали серьезным препятствием для обычных пользователей в понимании и получении выгод от использования блокчейн технологий. Мы надеемся защитить пользователей от непосредственного погружения в сложные концепции путем объединения когнитивных и технических аспектов и предоставления итогового зрелого продукта. Мы сделаем все возможное, чтобы помочь разработчикам сообщества создавать осязаемые продукты.

Глава X. Команда

Гари Ло, генеральный директор (Gary Luo, CEO)

Постоянный предприниматель, организовавший первый стартап сразу после колледжа, сделавший много проектов в интернет-маркетинге, мобильных играх и криптовалютах, ответственный за разработку и функционирование нескольких токенов и DAPP. Руководитель проекта в концепции дизайна EtherZero, отвечает за направление развития EtherZero, нацелен на создание общей платформы развития DAPP в течение 5-10 лет.

Ролонг, технический директор (Rolong, CTO)

Имеет более чем 10-летний опыт программирования, ведущий инженер полного цикла разработки (full stack engineer), владеющий C++, GO, JAVA, erlang и серверной разработкой, web3, h5 и другими инструментами разработки клиентских приложений, ведущий разработчик смарт-контрактов и исследователь базовой технологии Ethereum, эксперт по безопасности и защите от DDOS. Им были опубликованы многие технические решения, которые до сих пор используются как технические спецификации для разработчиков.

Роджер Лу (Roger Luo)

Ведущий системный разработчик Ethereum, глубоко исследовал исходные коды Ethereum, имеет десятилетний опыт работы с финансовыми технологиями, большой опыт во взаимодействии с блокчейн энтузиастами, активист сообщества с открытым исходным кодом. Отвечает за разработку ядра системы.

Миа, менеджер по продвижению (Mia, Overseas promotion manager)

Ведущий эксперт по международному маркетингу, в течение многих лет достигал отличных результатов в этой области, несет ответственность за международную рекламу EtherZero.

Фрэнк, менеджер по продукции (Frank, Product manager)

Два года опыта консалтинга в области финансов, трехлетний стаж финансового продакт-менеджера, теперь сосредоточен на технологии шифрования и блокчейн, уделяя особое внимание промышленному применению технологии блокчейн и возможных технических путей реализации.

Глава XI. Резюме

Объединяя преимущества Ethereum и DASH, EtherZero позволяет построить безопасную и надежную платформу предоставления сервисов без транзакционных комиссий, делая экономически целесообразным реализацию крупномасштабных и сложных смарт-контрактов для непрерывной работы, обеспечивая отличные интерактивные возможности, основанные на масштабируемости и обратной связи транзакций в режиме реального времени в сети мастернод. Со временем будет меняться ужасное впечатление людей о чрезвычайно длительном времени подтверждения транзакции.

Учитывая, что индустрия блокчейна все еще находится в начальной экспериментальной стадии, только путем формирования экспертизы и распространения знаний мы можем построить достаточно безупречную техническую среду (technical framework), а посредством интеграции с различными индустриями можем снизить риски, с которыми будем сталкиваться на каждом шагу в достижении цели стать основной блокчейн платформой для разработки и функционирования приложений.

В настоящее время технические ограничения не дают быстрее расширить популярность блокчейна в повседневной жизни, и спекуляции на рынке будут продолжаться еще в течение довольно длительного периода времени. EtherZero будет придерживаться цели улучшения технологии блокчейн, стремясь изучить применение в различных индустриях как наш собственный долг, улучшить социальную эффективность с помощью децентрализованных технологий и идей, снизить социальные операционные расходы и прийти к более справедливому социуму.

Спасибо за Вашу поддержку!