IoTeX
Децентрализованная сеть для Интернета Вещей основанная на конфиденциально-ориентированном блокчейне

Команда IoTeX (support@iotex.io)
Последнее обновление:12 июля, 2018
Версия 1.5

Отказ от ответственности Этот документ предназначен для технического обзора. Он не предназначен быть исчерпывающим или иметь окончательный дизайн; таким образом, неосновные аспекты не охватываются, такие как API, привязки или языки программирования.

Аннотация

На сегодняшний день, большинство устройств Интернета Вещей (IoT) применяются централизованным образом, несмотря на то, что по своей природе они децентрализованные. Было выявлено множество проблем: масштабируемость, высокие эксплуатационные расходы, проблемы конфиденциальности, риски безопасности и недостаток функциональных свойств. Блокчейн, умышленно имеющий децентрализованную структуру, может быть отличным решением данных проблем. Во-первых, блокчейн достаточно эластичен для того, чтобы решить проблему масштабируемости IoT экономически эффективным способом. Во-вторых, сохраняя данные в пределах масштабов блокчейна - устраняется проблема хранения данных IoT в облаке и, возможно, утечка и злоупотребление данными. В-третьих, блокчейн со смарт-контрактом и токенами имеет огромный потенциал для обеспечения автономной координации устройств для создания функциональных значений. Однако, существующие блокчейны имеют ограничения, связанные с проблемами IoT из-за особенных характеристик IoT, таких как большое количество и неоднородность устройств, ограничение в расчетах, хранении и мощности и т. д.

Этот документ представляет IoTeX - децентрализованная сеть для IoT, основанная на конфиденциально-ориентированном блокчейне с четырьмя основными нововведениями:

- Блокчейн в блокчейне, для хорошо сбалансированной распределенной сети, которая максимизирует масштабируемость и конфиденциальность экономически эффективным способом;
- Настоящая конфиденциальность на блокчейне, основанная на передаваемом платежном коде, кольцевой подписи с постоянным размером без надежной настройки и первой реализации bulletproof;
- Быстрый консенсус с мгновенным завершением, который значительно улучшает пропускную способность сети и снижает стоимость транзакций;
- Гибкая и легковесная системная архитектура, основанная на IoTeX, специально предназначенная для ключевых IoT приложений в различных отраслях промышленности.

Содержание

Список иллюстраций

Список таблиц

1 Интернет Вещей (Internet of Things, IoT)

Интернет Вещей (IoT) – быстро прогрессирует как проявление сетевого объединения общества, все, что приносит пользу от соединения - соединяется. Тем не менее, эта далеко идущая трансформация – только начало. Ожидается, что количество подключенных устройств IoT будет расти на 21% ежегодно, увеличившись до 18 миллиардов к 2020 году [10] и ожидается рост мирового рынка IoT от 170 миллиардов USD в 2017 году до 560 миллиардов USD к 2022 году [15], при совокупном годовом приросте в 26,9%. Несмотря на то, что многие эксперты в индустрии и потребители связали IoT со следующей промышленной революцией или со следующим интернетом, существует три основных проблемы, которые сдерживают массовое развитие и принятие IoT.

1.1 Проблема масштабируемости

На сегодняшний день, большинство устройств IoT подключены и контролируются централизованно. Устройства IoT подключены к серверным инфраструктурам на общедоступных облачных сервисах или на серверных фермах, для передачи данных и приема команд управления. На данный момент масштаб IoT упирается в масштабируемость и эластичность этих серверных (back-end) инфраструктур, серверов и центров обработки данных. Существенно высокие эксплуатационные расходы масштабного использования IoT, вряд ли будут покрыты за счет прибыли от продажи устройств. В результате этого, многие поставщики IoT не смогут обеспечить экономически выгодные устройства и приложения, которые достаточно масштабируемые и надежные для реальных сценариев использования [35].

1.2 Отсутствие конфиденциальности

Ожидается, что IoT создаст возможности для массового участия конечных потребителей в критически важных услугах, таких как энергетика, мобильность, юридическая и демократическая стабильность. Проблемы конфиденциальности возникают из-за того факта, что IoT взаимодействует автоматически и напрямую с физическим миром и объем собранных данных будет увеличиваться при развитии и дальнейшем росте. Существует несколько распространенных угроз конфиденциальности, как указано в [37]:

1. Идентификация: связанный (постоянный) идентификатор, например, имя и адрес или любой псевдоним, с физическим лицом;

2. Локализация и отслеживание: получение местоположения человека различными средствами;

3. Профилирование: составление информационного профиля о физических лицах для

того, чтоб сделать выводы путем объединения с другими профилями и источниками данных;

4. Нарушение конфиденциальности и изложение/презентация: передача личной информации через публичного посредника и процесс ее раскрытия нежелательной аудитории;

5. Жизненный цикл перехода: устройства часто хранят большое количество информации об их собственной истории на протяжении всего их жизненного цикла, что может стать причиной утечки при изменении сферы управления в жизненном цикле устройства;

6. Инвентарная атака: несанкционированный сбор информации о существовании и характеристиках личных вещей, например, взломщики могут использовать данные инвентаризации для того, чтоб проверить имущество и найти безопасное время для взлома;

7. Связь: соединение разных ранее разделенных систем, таких как сочетание источников данных, показывает (правдивую или ошибочную) информацию о том, что субъект не раскрывал ранее изолированные источники и, что самое важное, не хотел их раскрывать.

Все они являются распространенными угрозами связанными с утечкой данных на уровне устройств; или утечка данных во время связи; или, чаще всего, утечка данных благодаря централизованным сторонам.

1.3 Отсутствие функциональных значений

Большинство существующих решений IoT испытывают недостаток в создании значимых решений. «Быть соединенным» - самое распространенное значимое решение. Однако простая возможность подключения не делает устройство умным или полезным. Значительная часть пользы, которые производит IoT, происходят от интеграции, сотрудничества и, в итоге, автономной координации неоднородных объектов. Вот пример, нескольких хороших аналогий: отдельные клетки взаимодействуют для создания многоклеточных организмов, насекомые строят общество, люди стоят города и государства. Сотрудничая, все эти особи объединяются для того, чтоб построить что-то имеющее большую ценность, нежели их собственное. К сожалению, согласно [29], 85% устаревших устройств не имеют возможности взаимодействовать или сотрудничать друг с другом из-за проблем с совместимостью. Обмен данных для деловых и эксплуатационных идей практически невозможен.

2 Блокчейн

Технология блокчейн была представлена в 2008-м году и ее первое внедрение т.е. биткойн, произошло год спустя, в 2009-м и было опубликовано в работе *Bitcoin: A Peer-*

to- Peer Electronic Cash System [21] написанной Satoshi Nakamoto (псевдоним). По существу, блокчейн - это распределенная, транзакционная база данных, которая доступна всем узлам участвующим в сети. Это главная техническая инновация биткойна, и она действует как общественный регистр для транзакций. У каждого узла в системе есть полная копия текущего состояние цепи, которое содержит каждую транзакцию, когда-либо выполненную. Каждый блок содержит хэш предыдущего блока, тем самым соединяя их вместе. Связанные блоки становятся цепью из блоков, таким образом формируя, блокчейн.

2.1 Составляющие

Блокчейн можно представить, как четырёхмерное пространство, у которого есть три горизонтальных слоя включающие: транзакции и блоки, консенсус, вычислительный интерфейс, и один вертикальный слой - управление.

Транзакции и блоки

На самом нижнем горизонтальном слое, подписанные транзакции распространяются среди всех узлов и блоков, создаваемых полными узлами. Это является основой блокчейна, где передача цифровых активов (как неотъемлемых ценностей) и безопасности аккаунта, достигаются через крипто примитивы, такие как подпись с использованием эллиптических кривых, хэш-функция и Дерево Меркла.

Консенсус

Средний горизонтальный уровень проявляет одноранговую природу блокчейна, где все узлы в сети достигают консенсуса по всем внутренним состояниям цепи через такие методы как: Доказательство работы (PoW), Доказательство доли (PoS) и их варианты, задача византийских генералов (BFT) и его варианты и т.д. Уровень консенсуса влияет на масштабируемость больше всего. PoW обычно считают менее масштабируемым по сравнению с PoS. Кроме того, этот уровень в большой степени влияет на безопасность с точки зрения двойных расходов и других атак, связанных с видоизменением состояний блокчейна непредвиденным способом.

Вычислительный интерфейс

Первые два горизонтальных уровня формируют форму блокчейна, в то время как уровень вычислительного интерфейса критичен для придания блокчейну полезных качеств, которые включают в себя расширяемость и удобство пользования. Для примера, смарт-контракт был впервые реализован *Ethereum* для включения программируемости, где для выполнения условий контракта можно было рассчитывать на распределенный ”всемирный компьютер”. Боковая цепь (sidechain), вместе с объединенным майнингом, были также разработаны для интенсивной поддержки программируемости. Протоколы второго слоя, такие как сеть Raiden [25], утверждают

что канал был разработан для расширения масштабируемости блокчейна на этом уровне. Кроме того, инструменты, SDKs, схемы и GUIs также чрезвычайно важны для удобства пользования. Уровень вычислительного интерфейса даёт разработчикам возможность разрабатывать децентрализованные приложения (DApp), которые являются основой для того чтобы блокчейн был полезен и имел ценность.

Управление

Как и с организмами, самые успешные блокчейны будет те, которые смогут лучше всего адаптироваться к окружающей среде. Предполагая, что эти системы должны будут развиваться, чтобы выжить, первоначальный дизайн имеет важное значение, но в долгосрочной перспективе, механизмы изменения являются наиболее важными, в их задачу входит управление вертикальным слоем. Существует два важнейших компонента управления:

- Стимул: у каждой группы в системе есть их собственные стимулы. Эти стимулы не всегда на 100% согласованы со всеми другими группами в системе. С течением времени, группы будут предлагать изменения, которые выгодны для них. У организмов в приоритете - собственное выживание. Это обычно проявляется в изменениях в премиальной структуре, денежно-кредитной политике или равновесиях сил.
- Координация: Так как маловероятно, что у всех групп есть 100%-е стимулы на протяжении всего времени, способность каждой группы скоординироваться вокруг их общих стимулов очень важна для того чтобы они могли влиять на изменение. Если одна группа может скоординироваться лучше, чем другая, она создает неравноправие в свою пользу. На практике решающий фактор - то, сколько координации может быть сделано на цепочке (пр., голосование по правилам системы, как в сети Tezos [34], или даже откатить обратно реестр, если большинству заинтересованных сторон не нравится изменение) по сравнению с изменениями вне цепи (такое как Проект развития Биткойна (BIPs) [3]).

2.2 Эксплуатационные модели

Блокчейны можно классифицировать как инклюзивные (permissionless) и эксклюзивные (permissioned), в зависимости от того как они эксплуатируются. Например, биткойн инклюзивный и это означает, что любой может создать адрес и начать взаимодействовать с сетью, идея заключается в “построении доверия между ненадежными”. Напротив, эксклюзивный блокчейн - это закрытая и контролируемая экосистема, где доступ каждого участника определяется и дифференцируется на основе роли, идея заключается в “построении доверия между менее надежными”.

У каждого подхода есть свои преимущества и недостатки. Несмотря на это, все эти конфликты сводятся к фундаментальным компромиссам между доверием, масштабируемостью, сложностью и совместимостью. Например, биткойн и эфириум -

это блокчейны, построенные поверх ненадежных узлов, потому что масштабируемость очень желательна. Следовательно, требуется либо много вычислений (в случае PoW), либо более сложный механизм консенсуса. Например, Fabric [14] - это эксклюзивный блокчейн, где все узлы считаются доверенными и имеют криптографические идентификаторы, например, выданные службами-членами, такими как инфраструктура открытого ключа (PKI), что делает их легко масштабируемыми с низкими вычислениями и относительно простым механизмом консенсуса.

Таблица 1: Преимущества Блокчейна для Интернета Вещей

Свойства Блокчейна	**Преимущества для IoT**
Децентрализация	Масштабируемость, конфиденциальность
Задача Византийских Генералов	Доступность, безопасность
Прозрачность и неизменность	Якорь доверия
Программируемость	Расширяемость

3 Преимущества и проблемы блокчейна и IoT

Чувствительность и восприятие, трансформация, передача и обработка информации являются сутью самых разумных вещей на этой планете. Так как для IoT уровень чувствительности и восприятия распределен случайным образом, к последним двум качествам, пока что, это не относится, поэтому они являются причиной для большинства проблем масштабируемости, конфиденциальности и расширяемости. Мы предполагаем, что технология блокчейн, если она служит спинным мозгом и нервной системой IoT, станет лучшим кандидатом для решения вышеупомянутых проблем, связанных с IoT.

3.1 Преимущества

Используя технологию блокчейн, IoT сразу же получает выгоду от следующих аспектов благодаря свойствам блокчейна, включая децентрализацию, Византийскую толерантность отказоустойчивости, прозрачность и неизменность. В Таблице 1 приведены преимущества блокчейна для Интернета Вещей.

Децентрализация

Децентрализация освобождает пользователей и устройства от централизованного контролируемого и последовательного мониторинга, тем самым частично решая проблему конфиденциальности, навязанную централизованными структурами, которые монополизируют рынок и пытаются отслеживать каждое действие пользователя/устройства для своих собственных выгод, например, рекламы. Децентрализация, в контексте крипто экономики, также указывает на "эластичность”,

которая часто определяется как ”степень, до которой система способна адаптироваться к изменениям рабочей нагрузки путем предоставления и деинициализации ресурсов в автономном режиме, таким образом, чтобы доступные ресурсы в любой момент времени как можно эффективней соответствовали текущему спросу". Блокчейн и лежащая в его основе крипто экономика может быть разработана таким образом, чтобы быть достаточно гибкой и экономически эффективной для сценариев и приложений IoT. Например, больше узлов может быть развернуто на блокчейне, если сеть имеет достаточно вычислительных задач с достаточным количеством стимулов для выполнения.

Задача византийских генералов (BFT)

Задачей византийских генералов является защита от сбоев, при которых компоненты системы выходят из строя произвольным образом, т.е. не только путем остановки или сбоя, но и путем неправильной обработки запросов, искажая их локальное состояние и/или производя неправильные или противоречивые результаты. Задача Византийских Генералов моделирует реальные среды, в которых компьютеры и сети могут вести себя неожиданным образом из-за аппаратных сбоев, перегрузки сети и отключения, а также вредоносных атак. BFT может быть использован для достижения многих желаемых свойств безопасности в контексте IoT, например, устранить возможность атаки посредника (MITM), так как нет ни одного потока связи, которые могут быть перехвачены и подделаны, или сделать атаки DDos (Denial of Service, DoS) почти невозможными.

Прозрачность и неизменность

Блокчейн обеспечивает криптографические гарантии того, что данные, закрепленные на цепочке, всегда являются прозрачными и неизменяемыми, что может быть полезно во многих сценариях, например, в закреплении состояний мира IoT на блокчейне с целью аудита, нотариального заверения и криминалистического анализа, управления идентификацией, аутентификации и авторизации.

Программируемость

Биткойн наделён базовой программируемостью, позволяющей транзакции завершаться успешно только в том случае, если небольшой базовый скрипт выполняется успешно. Эфириум улучшает эту функцию для достижения полноты-по-Тьюрингу (Turning-complete) смарт-контракта, который написан на языке программирования высокого уровня и выполнен на небольшой виртуальной машине (VM), известной как EVM. Эта программируемость может и должна быть распространена на устройства IoT, некоторые из которых на данный момент имеют только простую и жестко запрограммированную логику, которую невозможно перепрограммировать после выпуска.

3.2 Проблемы

Использование общих свойств, предоставляемых блокчейнами, не означает, что каждый блокчейн подходит для использования в IoT. На самом деле, не похоже, что любой существующий публичный блокчейн может быть применён к IoT, поскольку существует довольно много сложных проблем.

Гарантия нативной конфиденциальности недостаточна

Нативные гарантии конфиденциальности от блокчейна могут только решить проблему уязвимых мест конфиденциальности IoT только в той степени, в которой хранятся данные в цепочке, а не на централизованных серверах, использующие псевдо анонимность. Однако, если псевдоним устройства привязан к личности человека, все что делается под этим псевдонимом будут связано с ним.

Не существует универсального блокчейна

Как уже упоминалось выше, IoT представляет собой совокупность разнородных систем и устройств с различными целями и возможностями. Невозможно найти универсальное блокчейн-решение, которое подходит для большинства сценариев. Например, блокчейн для координации миллионов промышленных узлов Интернета Вещей должен быть ориентирован на высокую масштабируемость и пропускную способность транзакций, а блокчейн для координации умных устройств дома - на конфиденциальность и расширяемость. На макроуровне, устройства IoT как одна из его разновидностей, определенно развиваются быстрыми темпами, т.е. интегрируются новые технологии, разрабатываются новые стандарты, производятся новые устройства с новыми возможностями. В отличие от этого, на микроуровне возможности, назначение и рабочая среда отдельного устройства Интернета Вещей также меняются с течением времени.

Эксплуатации в цепи слишком тяжеловесные

В мире IoT многие устройства считаются слабыми узлами, поскольку они:

- Не способны выполнять майнинг на основе PoW из-за ограничений мощности и вычислений;
- Не способны хранить большие объемы данных (например, гигабайты, не говоря уже о терабайтах и петабайтах) из-за ограничений мощности и памяти;
- Не в состоянии проверять все транзакции, обрабатывая весь блокчейн;
- Не могут быть постоянно подключены к другим одноранговым узлам, зависят от времени бесперебойной работы и качества связи.

Таким образом, большинство существующих блокчейн решений слишком тяжеловесные для IoT.

3.3 Аналоги

Недавно запущенная IOTA построена на основе нестандартной технологии, известной как Tangle [24]. IOTA пытается отделить механизм перехода состояния от механизма канонизации консенсуса, отбросив такие понятия, как блоки и цепи. Вместо этого, эмитенты транзакций также являются утверждающими транзакции, а проверка транзакций строится с использованием Направленных Ациклических Граф (DAG), чтобы сделать транзакцию быстрой и без затрат. Эффективность достигается за счет потери глобально определенных состояний, что делает желаемые функции, такие как, простое подтверждение платежа (Simple Payment Verification, SPV) для легких клиентов и смарт-контрактов очень затруднительными. Iot Chain (ITC) [16], еще один IoT блокчейн-проект, основанный в Китае, использует ту же структуру Tangle от IOTA и, следовательно, имеет те же плюсы и минусы. HDAC [13] - еще один недавно предложенный блокчейн для IoT в Корее, который в партнерстве с Hyundai Group сосредоточится на более конкретных областях IoT, таких как аутентификация устройств и транзакции "машина-машина" (M2M).

4 IoTeX: Обзор конструкции и архитектура

4.1 Принципы конструкции

IoTeX стремится стать спинным мозгом и нервной системой для мира IoT, ориентированным на конфиденциальность и масштабируемость. Чтобы достичь этого и решить вышеупомянутые проблемы, наш архитектурный дизайн имеет следующие принципы.

Разделение Полномочий (Separation of Duties)

Непосредственное подключение всех IoT узлов к одному блокчейну - мечта, которая не может стать истиной. Помимо того факта, что различные IoT приложения требуют принципиально разных наборов функций от блокчейна, размещение каждого IoT узла на одном блокчейне заставляет его быстро расти в размерах и вычислениях и в конечном итоге, становится слишком тяжеловесным со множеством IoT устройств. Вместо этого, разделение полномочий гарантирует, что каждый блокчейн взаимодействует с определенной группой IoT узлов, и в то же время, взаимодействует с другими блокчейнами, когда это необходимо. Это аналогично интернет-гетерогенным устройствам, которые сначала образуют внутри связанную группу, интранет. Маленькие интрасети могут в дальнейшем формировать более крупную интрасеть, которые в конечном итоге соединяется с основным Интернетом и связываются друг с другом. «Разделение полномочий» обычно создает хорошо сбалансированную систему для

максимизации эффективности и конфиденциальности.

Бритва Оккама (Occam's Razor)

Каждый блокчейн имеет разные применения и приложения и должен быть спроектирован и оптимизирован для разных направлений. Например, блокчейн, предназначенный для ретрансляции транзакций между ее субцепями, не нуждается в завершении полноты-по-Тьюрингу (Turing-complete) контракта работающего поверх него; другой блокчейн, который соединяет устройства в одной и той же зоне доверия, не должен излишне заботиться о конфиденциальности транзакций.

IoT Совместимость

Как уже упоминалось, мир IoT полон гетерогенных систем и узлов, более мощных или слабых с точки зрения их ресурсов вычислений, хранения и мощности. Поскольку операции, которые могут выполняться слабыми узлами, могут быть легко выполнены мощными узлами, операции на цепях, должны быть спроектированы и оптимизированы для слабых узлов, т.е. операции должны быть достаточно легковесными, чтобы экономить ресурсы, такие как вычисление, хранение и мощность

4.2 Архитектура: блокчейны в блокчейне

IoTeX - это сеть из множества блокчейнов, которые иерархически расположены, где многие блокчейны могут одновременно взаимодействовать друг с другом, сохраняя при этом совместимость. В мире IoTeX, как показано на Рисунке 1, корневая цепь управляет многими независимыми блокчейнами или субцепями. Субцепь подключается к IoT-устройствам и взаимодействует с ними, чтобы совместно использовать что-то общее, например, они имеют аналогичную функциональную цель, работают в аналогичных средах или имеют одинаковый уровень доверия. Если субцепь плохо функционирует, например, подвергаясь атакам или испытывая ошибки в программном обеспечении, корневая цепь полностью не подвержена влиянию. Кроме того, межблокчейновые транзакции (cross blockchain transactions) привязаны для передачи значения и данных из субцепей в корневую цепь или от одной субцепи к другой через корневую цепь.

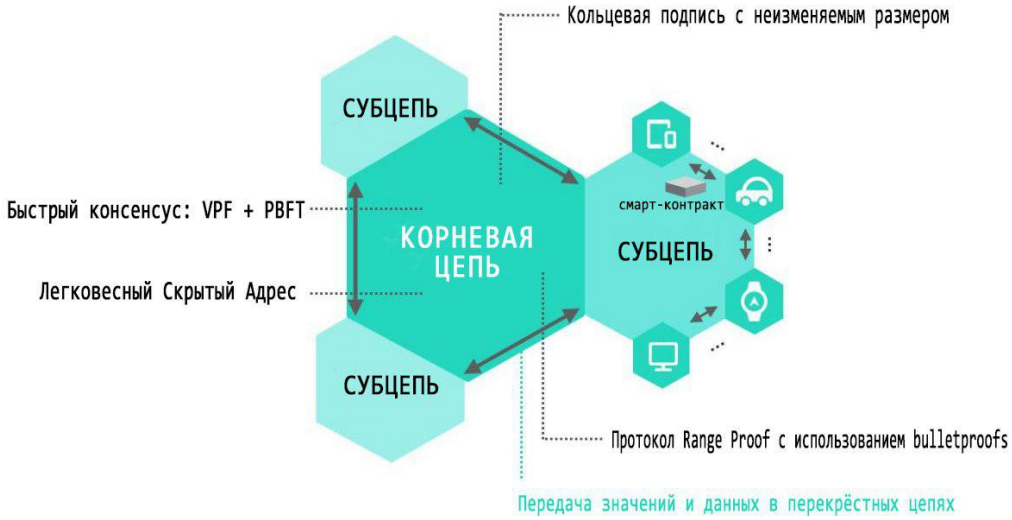

Рис. 1: IoTeX: Блокчейны в блокчейне, архитектура корневой цепи и субцепей.

Корневой блокчейн - это публичная цепь, доступная всем, у которой есть три основные цели:

1. Передача значений и данных по субцепям в режиме конфиденциальности, чтобы обеспечить совместимость между субцепями;

Таблица 2: Сравнение между корневой цепью и субцепью

Свойства	**Корневая цепь**	**Субцепь**
Публичность/ Приватность	Публичная	Публичная или Приватная
Масштабируемость	Необходима	Варьируется
Надежность	Обязательна	Необходима
Конфиденциальность	Необходима	Варьируется
Расширяемость	Без полноты по Тьюрингу	Полнота-по-Тьюрингу
Мгновенное завершение блока	Необходима	Необходима

2. Контроль за субцепями, например, наказание связанных операторов из субцепей конфискацией обязательств;

3. Регулирование и привязка платежей и доверия в субцепях.

С этими определенными целями, корневая цепь специально фокусируется на

масштабируемости, надежности, сохранение конфиденциальности функций и способности организовывать субцепи.

С другой стороны, субцепь потенциально может быть как приватным блокчейном, так и опираться на корневую цепь как ретранслятор, для взаимодействия с другими субцепями. Субцепь требует гибкости и расширяемости для адаптации разнообразных требований различных IoT приложений. Субцепь, очень вероятно, управляется операторами, роль которых зависит от наличия достаточно высокой связи на корневой цепи. По желанию, система позволяет операторам назначать одного или нескольких операторов с или без дополнительной связи. Оператор действует как легкий клиент в корневой цепи и полный узел на субцепи, чтобы закрывать новые блоки.

В целом, свойства корневой цепи и субцепей приведены в Таблице 2.

4.3 Корневой блокчейн

Корневой блокчейн использует модель на основе UXTO как Bitcoin [21] и Monero [20] по следующим причинам:

- Упорядочение транзакций становится тривиальным без необходимости в текущих или порядковых номерах, что предъявляет минимальные требования к консенсусным схемам и позволяет параллельно обрабатывать транзакции;
- Возможность применения существующих методов сохранения конфиденциальности, таких как кольцевая подпись, и ZK-SNARK для скрытия отправителя, получателя и суммы транзакции становится возможной.

Корневой блокчейн состоит из хеш-связанных блоков, а блок состоит из заголовка, который содержит хэш-ссылки к предыдущему блоку и список транзакций. Корневой блокчейн разрешает главным образом выполнять два типа транзакций: (1) основные транзакции, включая P2PKH, P2SH, Multisig и т. д., и расширенные транзакции, которые позволяют выполнять операции с перекрестными цепочками, такие как BondedRegistration, Lock, ReLock, Reorg и т. д. Подтвержденные транзакции добавляются в блок, который имеет динамический размер, максимальный - 8 МБ. Блок создается каждые три секунды нашей консенсусной схемой, как описано в следующем разделе. Корневой блокчейн предназначен для не «полноты-по-Тьюрингу» с поддержкой скрипта на основе стека и богатого набора кодовых операций.

4.4 Субцепи

IoTeX имеет схему для разработки и создания специализированной субцепи для децентрализованных IoT приложений путем инкапсуляции примитивов низкого уровня, таких как, протокол сплетен и консенсусный механизм. Модель разрешения, спецификация, параметры и типы транзакций субцепи, могут быть настроены так, чтобы вписываться в ее приложение.

Субцепи IoTeX используют модель, основанную на учетной записи, которая лучше для контроля переходов состояния. Существует два типа аккаунтов, похожих на эфириум, регулярные аккаунты и контракты. В блок добавляются валидные транзакции, которые производятся по той же схеме консенсуса, что и корневой блокчейн, для достижения такой же степени завершенности, чтобы сделать межцепочную связь более эффективной. Субцепи либо используют токен корневого блокчейна, токен IoTeX, либо определяют свой собственный токен. Токен, определенный разработчиками на субцепях, может распространяться публично посредством продажи токенов или обмена на публично торгуемых биржах.

Смарт-контракт поддерживается субцепями и работает поверх легкой и эффективной виртуальной машины. В настоящее время мы оцениваем веб-сборку (WASM) [36] - новый веб-стандарт для создания высокопроизводительных веб-приложений. WASM эффективен и быстр, и его можно детерминировать и изолировать с помощью некоторых модификаций, как это было предпринято проектом EOS [9]. Другие варианты также изучаются. Благодаря смарт-контракту IoT устройства, подключенные к одной и той же субцепи, используют общее пространство двумя способами:

- Во-первых, устройства могут взаимодействовать с физической средой, основанной на состояниях их субцепей, например, лампочки включаются и выключаются сами по себе на основе «показания часов» на субцепи;
- С другой стороны, устройства могут изменять состояние на субцепях, когда изменяется физическая среда, например, температура термостата обновляется через смарт-контракт на основе данных его датчика.

4.5 Межблокчейновая коммуникация

Ожидается, что в IoT приложениях будет использоваться высокоскоростная связь с перекрестными цепями. Всегда необходимо, чтобы устройство IoT в субцепи координировалось с другим устройством в другой субцепи. Опять же, ограниченные низкими вычислениями и объемом памяти IoT устройств, мы стремимся к быстрому и экономичному построению межблочной связи.

Привязка (Pegging) и завершенность блока

Привязка (pegging) - это механизм масштабирования сети биткойна с помощью боковых цепей, первоначально предложенный в [1]. Он в значительной степени полагается на упрощенную проверку платежей (SPV) [21] и позволяет биткойн эффективно «перемещаться» из блокчейна биткойна к боковой цепи и обратно. Основная идея проста: токены отправляются на специальный адрес, который должен быть заблокирован в блокчейне биткойна; как только заблокированная транзакция подтверждена, посылается Reorg транзакция в боковую цепь, включая заблокированную транзакцию и доказательство включения в виде ветки Merkle. Боковая цепь использует SPV для проверки транзакции Reorg и, если она проверена, создает то же количество токенов и отправляет их на желаемый адрес боковой цепи. На сегодняшний день привязка служит

примитивом для почти всех протоколов связи между блокчейнами, например, Cosmos, Lisk, Rootstock. Два отдельных потока привязки могут быть легко связаны друг с другом, чтобы сделать так называемую двухстороннюю привязку (2WP) для передачи токенов назад и вперед.

Завершенность блока - это гарантия того, что новый блок генерируется окончательно и не может быть изменен. Завершенность блоков существенно влияет на конкретную реализацию привязки, поскольку нужно дождаться завершения финализации блока (по крайней мере с высокой податливостью) в отправляющем блокчейне, до запроса Reorg. Большинство публичных блокчейнов, таких как биткойн, не имеют мгновенной финализации. Принимающий блокчейн может получить только вероятностную гарантию, например, так как большее число PoW майнеров подтверждают транзакцию, более вероятно, что транзакция была принята. Использование консенсуса в реальном времени с мгновенным завершением решает эту проблему, поскольку принимающая цепочка имеет гарантию с одним подтверждением блока в отправляющей блочной цепочке. Ожидается, что для IoT приложений, межблокчейновая передача значений и данных будет быстрой и рентабельной, что требует консенсуса в реальном времени как для корневой цепи, так и для субцепей. Консенсус IoTeX обеспечивает мгновенную финализацию блока, подробно описанную в следующем разделе.

Протокол межблокчейновой коммуникации

Давайте рассмотрим протокол на высоком уровне, предположив, что адрес под названием Чарли в субцепи 1 хочет отправить транзакцию на адрес с именем Дэвид в субцепь 2, и все три блокчейна используют тот же тип токена без комиссии за транзакцию, для простоты. Обратите внимание, что, для применения привязки, необходимы четыре транзакции, чтобы сделать «удаленный вызов» из субцепи 1 в субцепь 2 с помощью корневой цепи, то есть, (1) Lock транзакцию в субцепи 1; (2) Reorg транзакцию от корневой цепи; (3) еще одну Lock транзакцию в корневой цепи; и (4) еще одну Reorg транзакцию от субцепи 2.

Этот процесс показывает, что Дэвиду приходится ждать, по крайней мере, 4 блока, чтобы принять этот «удаленный вызов», а данные, которые этот «удаленный вызов» переносит, должны храниться на всех трех блокчейнах что делает его медленным и дорогостоящим. Мы стремимся оптимизировать этот процесс, комбинируя (2) и (3) на одну ReLock транзакцию, которая не только ускоряет весь процесс, но также позволяет избежать хранения данных в субцепи 1 и корневой цепи. Наш протокол изображен на Рисунке 2.

Рисунок 2: Межблокчейновые транзакции

Межблокчейновый протокол IoTeX включает следующие шаги:

1. Каждая субцепь, зарегистрированная в корневой цепи отправляет транзакцию BondedRegistration в корневую цепь, включая имя цепи, идентификатор сети, конфигурацию, исходный блок, и наименование операторов; Это одноразовый процесс;

2. Когда Чарли хочет отправить транзакцию Дэвиду, он инициирует Lock(X, $H(D)$, F/T) транзакцию, где X – количество токенов, $H(D)$ - хеш данных D которые должны быть присоединены, F/T показывают адреса (откуда и куда) включая идентификаторы для обеих цепей;

3. После того, как Lock транзакция была включена в субцепь 1 , Чарли инициирует ReLock(X, $H(D)$, F/T, S, P) транзакцию в корневую цепь, включая X, $H(D)$, F/T , некоторые текущие данные субцепи 1, обозначенные как S, а также доказательство включения P, которое включает Merkle ветви последних заголовков блока и Merkle ветви, подтверждающие Lock транзакцию;

4. Корневая цепь проверяет ReLock транзакцию и утверждает её, вставляет в последний блок, создаёт X токены и блокирует их по специальному адресу;

5. После того, как ReLock транзакция включена в корневую цепь, Чарли транслирует Reorg(X, D, F/T, P^j) транзакцию в корневую сеть с X, D, F/T и другим доказательством включения P^j, что доказывает включение ReLock транзакции;

6. Операторы из суб-цепи 2 узнают о Reorg транзакции, и они проверяют и создают такое же количество токенов в субцепи 2 и отправляют их по адресу Дэвида с соответствующей D.

Совместное использование пропускной способности корневого блокчейна

Одна из возможных проблем, связанных с межблокчейновой коммуникацией заключается в том, что вредоносная субцепь распространяет спам в корневую цепь или другую субцепь, отправляя огромное количество межблокчейновых транзакций, которые уменьшают пропускные способности других блокчейнов. Один из способов уменьшения

проблемы заключается в том, чтобы каждая субцепь запрашивала свою квоту и транзакции «предельного уровня» из субцепи, если ее квота исчерпана.

Рисунок 3. Модель пропускной способности для совместного использования производительности корневой цепи

Можно определить квоту на основе размера хранения в одном блоке. Предполагая, что размер блока максимально составляет 8 МБ, а 4 МБ зарезервировано для обычных транзакций, происходящих в корневой цепочке, и 4 МБ зарезервировано для всех межблокчейновых транзакций, которые далее

Таблица 3: Способы сохранения конфиденциальности в блокчейнах

Способ	Скрывает отправителя	Скрывает получателя	Скрывает количество
Скрытый адрес	нет	да	нет
Схема Pedersen	нет	нет	да
Кольцевые подписи	да	нет	нет
Zk0SNARKs	да	нет	да

делятся на, скажем, 4096 квот, при этом каждая часть квоты должна быть 1 КБ. Запросы субцепи для n частей квоты (с определенной верхней границей) в соответствии с предполагаемым использованием, путём размещения депозита, пропорционального n. В каждом раунде, только до nKB разрешено использовать в новом блоке для транзакций из этой субцепи, и каждая такая транзакция взимает плату за «пропускную способность» с депозита (чтобы вознаграждать майнеров, которые помогают обеспечить соблюдение этого правила); оставшиеся транзакции помещаются в очередь и в конечном итоге отбрасываются при тайм-ауте. Распределение квот может быть динамическим в том смысле, что оно изменяется, когда корневая цепь растет, как показано на Рисунке 3. Если одна субцепь распространяет спам на других, она быстро уменьшает свой депозит и в конечном итоге теряет квоту. С другой стороны, если одна субцепь помещает большой депозит просто для резервирования большой части полосы пропускания, фактически не используя ее, у корневой цепи будет механизм для возврата части

депозита на основе соотношения между средним количеством транзакций на блок и зарезервированной полосы пропускания, который помогает стабилизировать зарезервированную полосу пропускания около фактического использования.

5 Встроенная техника сохранения конфиденциальности транзакций

Конфиденциальность, предоставляемая изначально биткойн и эфириум, ограничена лишь псевдонимностью. Мы имеем в виду, что сведения о транзакции не являются конфиденциальными. Сумма транзакции, передаваемые активы, её метаданные и её отношение к другим транзакциям легко может узнать кто-угодно. Всего можно выделить три аспекта конфиденциальности: конфиденциальность отправителя, конфиденциальность получателя и конфиденциальность данных транзакции. Для их достижения могут применяться различные криптографические схемы показанные в Таблице 3.

IoTeX объединяет скрытый адрес для конфиденциальности получателя, кольцевую подпись для конфиденциальности отправителя и технологию Pedersen Commitments для скрытия суммы транзакции с несколькими нововведениями и улучшениями:

- Система легких скрытых адресов призвана освободить получателей от необходимости сканировать весь блокчейн если они хотят узнать данные о входящих транзакциях;
- Размер кольцевой подписи уменьшен и она также имеет децентрализованную надежную настройку.

5.1 Скрытие получателя с передаваемым платежным кодом

Скрытый адрес

Технология скрытого адреса возникла из протокола Cryptonote [28], который решает проблему получателя, используя «половинный раунд» протокола обмена ключами Диффи-Хеллмана. Предположим, что Боб хочет скрыть тот факт, что он получает токены от Алисы, вот как это работает:

1. Боб создает две пары приватных и публичных ключей, обозначенных как (a, A) и (b, B), где $A = a \cdot G$ и $B = b \cdot G$. G - базовая точка на эллиптической кривой.
2. Боб публикует открытые ключи (A, B) которые также являются его скрытым адресом;
3. Алиса вычисляет и отправляет токены на $P=(rA)\cdot G + B$ используя хеш-функцию H, случайное большое число r и секретный адрес Боба B. Эта транзакция передается вместе с $R = r \cdot G$;
4. Боб наблюдает за всеми транзакциями, вычисляет $P^j = (H(aR) + b)\cdot G$ (поскольку он знает a, b, R и G) надеясь, что P^j равно P. Если $P^j = P$, Боб может тратить токены P^j

используя приватный ключ $H(aR) + b$.

Очевидный недостаток скрытого адреса заключается в том, что получателю придется либо сканировать все транзакции в сети (что не подходит для мира IoT), либо полагаться на помощь доверенного полного узла (что в некоторой степени ущемляет конфиденциальность).

Код платежа

Код платежа был разработан для устранения вышеуказанного недостатка скрытого адреса немного жертвуя конфиденциальностью. Идея заключается в том, что Алиса конфиденциально уведомляет Боба о платежном коде, и Боб наблюдает только за транзакциями с тех адресов которые выводятся из этого кода. В этой системе существует два потока – уведомление, которое происходит один раз между двумя определенными сторонами, и отправление, которое может происходить несколько раз между этими сторонами.

Предположим, что у Алисы есть мастер-пара публичного и приватного ключей ($mpub_{Alice}$, $mpri_{Alice}$) где $mpub_{Alice} = mpri_{Alice} \cdot G$ и пара ключей от кошелька ($wpub_{Alice}$, $wpri_{Alice}$) где $wpub_{Alice} = wpri_{Alice} \cdot G$; У Боба тоже есть своя мастер-пара ключей ($mpub_{Bob}$, $mpri_{Bob}$) где $mpub_{Bob} = mpri_{Bob} \cdot G$, одноразовый поток-уведомление происходит следующим образом:

1. Боб получает $B_0 = b_0 \cdot G = (mpri_{Bob} + Hash(0, seed, metadata)) \cdot G$, преобразовывает его в адрес для уведомления addr (B0), публикует и следит за ним

2. Алиса выбирает случайный цепочный код; ($mpub_{Alice} \| cc$) её код платежа;

3. Алиса вычисляет совместный секрет $S = wpri_{Alice} \cdot B_0$ и отправляет зашифрованный код платежа $P^j = (mpub_{Alice} \| cc) \oplus HMAC512(xof\ S)$ на addr(B_0);

4. После полученияб Боб узнает $wpub_{Alice}$, восстанавливает $S = wpub_{Alice} \cdot b_0$, и расшифровывает P^j для получения ($mpub_{Alice} \| cc$).

Как только поток уведомления завершен, Алиса и Боб устанавливают один однонаправленный приватный канал для отправки токенов. Первая отправка будет работать следующим образом:

1. Алиса получает новый адрес из своего платежного кода (который уже передан Бобу) с помощью $A_0 = a_0 \cdot G = mpub_{Alice} + Hash(0, seed, metadata) \cdot G$;

2. Алиса выбирает следующий неиспользованный публичный ключ, полученный из B_0. Обратите внимание, что B_0 является неиспользуемым публичным ключом для первого раунда.

3. Алиса вычисляет новый совместный секрет $S_0 = a_0 \cdot B_0$, и вычисляет эфемерный публичный ключ, используемый для отправки транзакции, к которой относится $B_0^j = B_0 + \mathrm{SHA256}(S_0) \cdot G$

4. Боб может получить A_0 без посторонней помощи, так как он знает платежный код Алисы и следит только за адресами, полученными из $B_0^j = B_0 + \text{SHA256}(S_0) \cdot G$ and $S_0 = A_0 \cdot b_0$.

5. После получения, Боб может использовать токены с помощью приватного ключа $b_0 + \text{SHA256}(S_0)$.

Все последующие потоки отправления будут проходить аналогично.

Бобу не нужно сканировать блокчейн самому или полагаться на полный узел для сканирования всех транзакций. Транзакция уведомления сообщает о намерении Алисы отправить что-то Бобу, но фактическая «отправка чего-то» скрыта от всех остальных.

Передаваемый код платежа

Чтобы еще больше минимизировать утечку конфиденциальности, мы разработали передаваемый код платежа поверх исходного варианта кода. Хотя поток отправления остается таким же, мы улучшили поток уведомления, чтобы сделать возможным для Алисы тайно поделиться своим кодом с Чарли без использования транзакции уведомления, предполагая, что у Алисы и Боба есть однонаправленный приватный канал, также как и у Боба с Чарли. Для реализации мы используем Hashed Timelock Contracts (HTLC), которые требуют, чтобы получатель платежа подтвердил получение платежа до истечения предельного срока путем генерации криптографического доказательства платежа, в противном же случае платеж будет возвращен отправителю.

Предположим, что у Чарли есть мастер-пара публичного и приватного ключей ($mpub_{Charlie}$, $mpri_{Charlie}$) где $mpub_{Charlie} = mpri_{Charlie} \cdot G$. Улучшенный поток уведомления работает следующим образом:

1. Чарли получает $C_0 = c_0 \cdot G = (mpri_{Charlie} + Hash(0, seed, metadata)) \cdot G$, преобразовывает его в адрес уведомления $\text{addr}(C_0)$ и публикует его. Обратите внимание, что C_0 публикуется для Алисы, для вычисления совместного секрета, но не для получения каких-либо транзакций;

2. Алиса генерирует свой платежный код ($mpub_{Alice}||cc$) таким же образом;

3. Алиса вычисляет совместный секрет $S = wpri_{Alice} \cdot C_0$ и отправляет зашифрованный код платежа $P^j = (mpub_{Alice}\ cc)\ HM\ AC512(xof\ S)$ с токенами X в качестве стимула $HTLC(Hash^2(cc))$ используя их однонаправленные частный канал, где $HTLC$, как часть сценария блокировки или повторного использования, указывает, что токены можно потратить, если задан предварительный образ $Hash^2(v)$ то есть $Hash(cc)$;

4. Боб, стимулированный токенами которые отправила Алиса, отправляет Чарли P^j, Y, $Y < X$ токены и $HTLC(Hash^2(v))$ используя их однонаправленный приватный канал;

5. Чарли, получив транзакцию Боба, вычисляет $S = wpub_{Alice}\ c_0$ чтобы расшифровать

платежный код Алисы, и проводит транзакцию, раскрыв $Hash(cc)$, что делает транзакцию Алиса-Боб возможной и также награждает Боба.

Как только этот поток будет выполнен, Алиса и Чарли устанавливают один однонаправленный приватный канал для отправки токенов. Стоит отметить, что маршрутизация транзакции Алисы может быть многократной.

Наши передаваемые коды платежей обеспечивают лучшую конфиденциальность с точки зрения скрытия намерения «отправки чего-то» в блокчейне за счет использования существующих частных каналов, без добавления каких-либо вычислений или затрат на хранение для узлов, которые, хотя и предназначены для сценариев IoT, могут использоваться для большинства блокчейнов, таких как биткойн.

5.2 Возможности конфиденциальных транзакций

5.2.1 Постановка проблемы

Типичная транзакция в блокчейне биткойна показана на Рисунке 4. По сути, транзакции на блокчейне являются всего лишь кортежем $(\{pk_{in,i}\}, \{pk_{out,j}\}, \{v_{i,j}\})$, где $\{pk_{in,i}\}$ входящие адреса, $\{pk_{out,j}\}$ исходящие адреса, а $v_{i,j}$ это суммы транзакций среди этих адресов. Транзакции на блокчейне биткойна хранятся в открытом виде, что приводит к множественным проблемам с безопасностью и конфиденциальностью.

Рисунок 4. Транзакции на блокчейне биткойна

Цель конфиденциальных транзакций (см. Рисунок 5) заключается в том, чтобы позволить *только* отправителям и получателям транзакций выявлять значения $v_{i,j}$ и скрывать их от остального мира. Более того, конфиденциальные транзакции также позволяют другим сетевым организациям проверять достоверность данных транзакции, не видя фактических сумм. Для реализации конфиденциальных транзакций на блокчейне требуется применение ряда криптографических технологий.

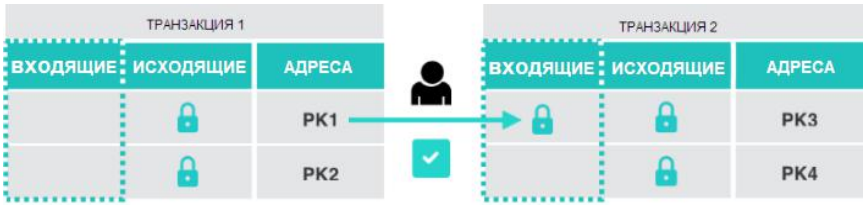

Рисунок 5. Конфиденциальная транзакция с общедоступной проверкой

5.2.2 Криптографическая постройка блоков

Доказательство знания

Доказательство знания (proof of knowledge), обозначаемое (*P, V*), является интерактивным доказательством между тем, кто доказывает *P* и верификатором *V* , в котором первый хочет продемонстрировать, что он знает некоторую информацию. Конкретнее, *P* имеет (*x, w*), которые принадлежат отношению *R*, где *x* это проблема и *w* это решение (также называемое свидетелем). *V* знает х он соглашается, что *P* знает информацию только если *P* сможет убедить *V* что знает *w*.

Доказательство с нулевым разглашением (Zero-Knowledge proof)

В протоколе с доказательством с нулевым разглашением, проверяющий доказывает утверждение верификатору, не разглашая ничего о заявлении, кроме того, что оно истинно, что защищает проверяющего от вредоносного верификатора, который пытается узнать больше чем ему положено. Протокол может быть как *интерактивным* так и *не интерактивным*. Основное отличие интерактивного протокола заключается в том, что все взаимодействия состоят из одного сообщения, отправленного верификатором. Мы используем обозначение **NIZKPoK**$(\alpha, \beta) : a = g^{\alpha}\ b = g^{\beta}$ чтобы обозначить не интерактивное доказательство знаний с нулевым разглашением о значениях α и β таких как $a = g^{\alpha}$ и $b = g^{\beta}$. Все значения, не заключенные в круглые скобки, считаются известными верификатору. Когда мы используем не интерактивное доказательство нулевого знания для аутентификации вспомогательных данных, полученная схема называется *подписью знания (signature of knowledge)* [8]. В принципе, схема подписи знаний означает, что тот, у кого есть решение *w* на проблему *x*, подписал сообщение *m*. Для вышеупомянутого **NIZKPoK**, мы используем уведомление SoK$[m](\alpha, \beta) : a = g^{\alpha} \wedge b = g^{\beta}$ для обозначения подписи знания в сообщении *m*.

Кольцевая подпись

Концепция кольцевой подписи была впервые введена Rivest et al. [27] в 2001 году как особый вид групповой подписи. В кольцевой подписи тот, кто подписывает сообщение выбирает набор участников кольца, включая себя в качестве возможных подписчиков сообщения. Верификатор может убедиться, что подпись действительно была создана

одним из участников кольца. Тем не менее, верификатор не может определить, какой именно участник сгенерировал подпись. В отличии от общей групповой подписи, схема кольцевой подписи не включает в себя назначение группового менеджера для управления набором членов кольца, тем самым устраняя возможность выявления личности подписавшего сообщения менеджером группы. Чтобы обеспечить анонимность в транзакциях токенов смарт-контрактов, применяется особый вид кольцевой подписи, так называемая связующая кольцевая подпись. Эта технология применена в Monero - криптовалюте, сфокусированной на конфиденциальности [20]. Связующая кольцевая подпись обладает дополнительным свойством – любые подписи, созданные одним и тем же подписывающим лицом, независимо от того, подписывают ли они одно и то же сообщение или разрозненные сообщения, имеют идентификатор (называемый тегом), связывающий подписи. Это свойство позволяет третьим сторонам эффективно проверять, что подписи были сгенерированы одним и тем же подписывающим лицом, не позволяя выявить его личность. Связующая кольцевая подпись, используемая в Monero, называется Multi-layered Linkable Spontaneous Anonymous Group Signature (MLSAG) [22] и является кольцевой подписью с набором ключевых векторов со сложностью связи $O(m(n + 1))$, где m количество пар приватного/публичного ключей, принадлежащих подписавшему, а n - размер кольца.

Криптографический Аккумулятор

Односторонними аккумуляторами, которые были впервые предложены Benaloh и de Mare в [2], называются односторонние хеш-функции с *квазикоммуникативными* свойствами. Квазикоммутативная функция f: $X \times Y \rightarrow X$ удовлетворяет условие, что для всех $x \in X$ и для всех $y_1, y_2\ Y$, мы имеем $f(f(x, y_1), y_2) = f(f(x, y_2), y_1)$. Односторонний аккумулятор позволяет объединить набор значений в безопасный дайджест который не зависит от порядка в котором эти значения были накоплены. Он также может использоваться для создания свидетеля, который позволяет доказать, что данное значение является частью аккумулятора.

Схема обязательств

Схема обязательств - это протокол, позволяющий пользователю фиксировать ценность по своему выбору, не раскрывая эту ценность получателю обязательства. На более позднем этапе, когда пользователю предлагается выявить зафиксированное значение, получатель будет иметь возможности для проверки того, что его выявленная ценность действительно безоговорочно связана с его обязательством. Схема обязательств должна отвечать двум требованиям. В то время как *скрытое* требование не позволяет получателю узнать содержание обязательства, требование о *выжидании* не позволяет пользователю обманывать при открытии этого обязательства. В схеме обязательств Pedersen [23] параметры домена являются циклической группой G простого порядка q, и генераторов $(g_0, \ldots, g_m)$. Для фиксации значений $(v_1, \ldots, v_m) \in Zm$, выбирается случайное число $r \in Z_q$ и устанавливается

обязательство $C = \mathsf{PedCom}(v_1, \ldots, v_m; r) = g_0^r \prod_{i=1}^{m} g_i^{v_i}$

5.2.3 Наши улучшения

В [31], Sun *et al*. представили RingCT 2.0, в которой использовался криптографический накопитель для дальнейшего снижения сложности связи до $O(n)$ за счет дополнительных вычислений. Отметим, что хотя RingCT 2.0 значительно уменьшал коммуникационную сложность по сравнению с MLSAG, для генерации параметров домена для аккумулятора требуется одноразовый процесс «надежной настройки», который применяет Zcash. В этом случае нужно доверять, что тот, кто генерирует секретные параметры, уничтожает их после использования, что повышает опасения по безопасности и конфиденциальности системы. Чтобы решить эту проблему, наше решение заключается в использовании безопасного протокола многопартийного вычисления (SMPC) среди группы самообеспечивающихся узлов блокчейна для создания секретных параметров домена в безопасном и распределенном виде. Кроме того, в настоящее время исследуются следующие направления для улучшения RingCT-подобных протоколов с точки зрения коммуникационных и вычислительных накладных расходов:

- Новая связующая кольцевая подпись со сложностью связи меньше, чем $O(n)$
- Новый подход для объединения множества связующих кольцевых подписей
- Сигма-протокол для не требующей доверия настройки секретных параметров домена

Мы стремимся предложить новое решение для конфиденциальных транзакций, которое может обеспечить хороший компромисс между связью и вычислительными расходами.

5.3 Доказательство диапазона сумм транзакций с использованием Bulletproofs

В качестве замены обязательств Педерсена, bulletproofs [5], был предложен новый, не интерактивный протокол доказательства с нулевым разглашением и без необходимости доверительной установки, что уменьшает размер диапазона доказательств с линейных до суб-линейных и сокращает вычесления без дополнительных затрат. Так как bulletproofs хорошо соответствуют дизайну IoTeX, мы собираемся интегрировать пуленепробиваемые модули в IoTeX.

6 Быстрый консенсус с мгновенным завершением

6.1 Концепция

6.1.1 Доказательство работы (PoW)

Доказательство работы (PoW) это основа достижения глобального консенсуса для большинства блокчейнов, включая биткойн и эфириум. PoW делает создание валидного блока и прикрепление его к блокчейну сложным в отношении вычислительной работы. Чем длиннее становится блокчейн, тем сложнее оказывается отмена/откат любой транзакции, ранее записанной данным блокчейном. Чтобы манипулировать блокчейном, атакующему необходимо владеть 51% всей вычислительной мощности блокчейн-сети, базирующейся на PoW.

Хотя PoW обеспечивает элегантное решение для достижения глобального консенсуса крупными распределенными блокчейнами, он имеет несколько характерных недостатков. Общая стоимость вычислений для поддержания глобального консенсуса такая же, как и стоимость атаки 51%. Это означает, что даже если большинство участников блокчейна честны, они все равно должны использовать огромное количество электроэнергии для поддержания блокчейна, что не подходит для среды IoT-сетей, которая обычно благоприятствует энергоэффективности. Вдобавок к этому, на уровне отдельных устройств, вычисления PoW обычно обходятся во множество циклов CPU и требуют значительного использования памяти, что усложняет требования к производству аппаратного обеспечения и повышает стоимость встроенных IoT-устройств. Последним, но не менее важным моментом является то, что PoW не обеспечивает мгновенного завершения, которое является критическим качеством, необходимым для формирования эффективной межблокчейновой коммуникации.

6.1.2 Доказательство доли

Доказательство доли (PoS) был предложен как альтернативный способ достижения консенсуса, нацеленный на избежание упомянутых выше проблем PoW. Основная идея PoS заключается в случайном выборе группы узлов, которые голосуют относительно следующего блока, при этом, вес их голосов основывается на размере их депозитов (т.е. ставок). Если определенные узлы нарушают правила, они могут потерять свои депозиты. Таким образом, блокчейн может работать намного эффективнее без вычислительно интенсивного PoW и достигать экономической стабильности: чем больше ставка у участника, тем большую мотивацию имеет данный узел для поддержания глобального консенсуса, и тем меньше вероятность неправильной работы узла. В качестве примера публичных PoS конструкций и реализаций можно назвать Tendermint [32], который был принят большим количеством приложений [33].

6.1.3 Делегированное доказательство доли (DPoS)

Делегированное доказательство доли (DPoS) улучшает идею PoS тем, что позволяет участникам выбирать определенных делегатов, которые представляют их доли ставок в сети. К примеру, Алиса может отправить в сеть сообщение о том, что она передает Бобу полномочия представлять ее ставку и голосовать от ее имени. DPoS предлагает ряд преимуществ для наших IoT-приложений:

- Некрупные участники могут объединять свои ставки, чтобы иметь совместно больше шансов на участие в предложении блока и голосовании, а затем разделять вознаграждения.
- Узлы с ограниченными вычислительными ресурсами могут выбирать своих делегатов, поэтому не всем узлам необходимо оставаться онлайн, чтобы участвовать в консенсусе.
- Делегатами могут быть узлы, имеющие мощные системы энергоснабжения и хорошие сетевые условия. Они могут выбираться динамически и в случайном порядке, поэтому у нас будет более высокая общая вероятность достижения консенсуса сетью.

К типичным криптовалютам, использующим DPoS, относятся EOS [9] и Lisk [18].

6.1.4 Практическая задача византийских генералов

Практическая задача византийских генералов (PBFT) была предложена Castro и Liskov [7] в 1999 году, как эффективный и устойчивый к атакам алгоритм, для достижения соглашений в распределенной асинхронной сети. Мы планируем использовать PBFT в качестве основополагающего алгоритма голосования для нашего DPoS-механизма консенсуса, поскольку он является понятным и хорошо изученным алгоритмом, обеспечивающий быстрое завершение, критически важное для создания эффективного и масштабируемого блокчейна. Как продемонстрировано в оригинальной статье Castro и Liskov, PBFT гарантирует доступность и безопасность, если неисправными или вредоносными являются не больше трети нод сети, при этом стоимость сети PBFT минимальна, около 3-х процентов по сравнению с нереплицированной сетевой системой. В число типичных криптовалют, основанных на PBFT, входят Stellar [30] и Zilliqa [38].

6.2 Рандомизированное делегированное доказательство доли (Roll-DPOS)

Чтобы иметь быстрый и эффективный механизм консенсуса с мгновенным завершением блоков в контексте IoT, мы объединяем концепции DPoS, PBFT и VRF (Verifiable Random Functions). VRF был впервые предложен Micali *et al.* [19] и представляет собой семейство функций, которые могут производить публично проверяемые доказательства правильности их случайным образом выдаваемых результатов вычислений. Если не

вдаваться в подробности, предлагаемый нами Roll-DPOS имеет четыре фазы: *выбор кандидатов, формирование комитета, предложение блока* и *завершение блока.*

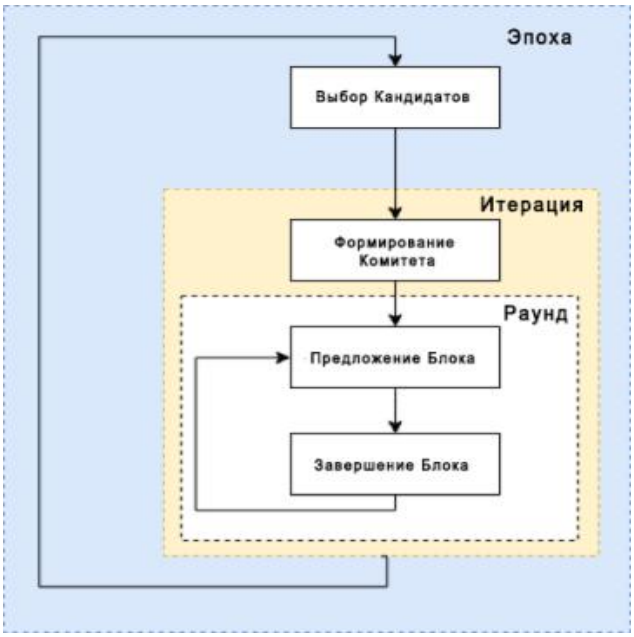

Рисунок 6: Рандомизированное делегированное доказательство доли (Roll-DPOS)

6.2.1 Набор кандидатов

В этой фазе могут участвовать — т.е. голосовать за кандидатов комитета —все узлы сети IoTeX. Чтобы мотивировать узлы на голосование, система удостоверяется, что делегаты разделяют полученные вознаграждения с голосующими. Кандидаты формируют группу минимум из 97 делегатов; в будущем это число будет увеличиваться, во избежание в дальнейшем централизации майнинг-мощностей. Выбранные кандидаты вносятся в одну эпоху, которая состоит из 47 итераций.

6.2.2 Формирование комитета

В каждой итерации посредством VRF из пула кандидатов случайным образом выбирается комитет из 11 кандидатов, для создания блоков в следующих 11 раундах. Идея заключается в том, чтобы использовать хэш блока из последней итерации и личный ключ узла в качестве входных данных для VRF и создания (Boolean output) логического вывода - если некто выбран как член комитета, преимущество, указывающего на его очередь в предложении блока, и доказательства, указывающего на его квалификацию для предложения блока в определенном раунде. Использование VRF имеет важное значение, поскольку обеспечивает не интерактивный способ сортировки всех делегатов для предложения блоков справедливым и безопасным образом. С этой целью мы

используем эффективный VRF, так, как он используется в Algorand [12].

6.2.3 Предложение блока

В каждом раунде (это примерно каждые 3 секунды), каждый узел в комитете предлагает новый блок и передает его всей сети, вместе с приоритетом и доказательством. Только блок, предложенный узлом с самым высоким приоритетом, еще не выносившей предложений в той же итерации, рассматривается другими узлами и получает статус блока-кандидата.

6.2.4 Завершение блока

В том же раунде все остальные узлы голосуют за/против блока-кандидата посредством PBFT. Если более 2/3 узлов комитета соглашаются о валидности блока-кандидата, он завершается и добавляется каждым в сети к блокчейну. После этого, процессы *предложения* и *завершения* блока осуществляются в следующем раунде; если текущая итерация заканчивается, перед осуществлением процессов *предложения* и *завершения* блока формируется другой случайный комитет.

6.3 Создание периодических контрольных точек для легковесных клиентов

В IoT-сетях, мы ожидаем множество устройств, которые являются *легковесными клиентами*, они представляют собой участников блокчейна, не записывающих всю историю транзакций локально. Учитывая потребление ресурсов при хранении полного блокчейна (к примеру, для биткойн [4] это более 100 ГБ), многие встроенные бюджетные IoT-устройства не обладают производительностью, достаточной для загрузки всего блокчейна. Однако, эти легковесные клиенты, по-прежнему обладают способностью проверять правильность блокчейна и взаимодействовать с ним — такой дизайн включен в оригинальную белую бумагу биткойн, написанную Satoshi [21].

Тем не менее, использование PoS вместо PoW имеет один недостаток для легковесных клиентов. При проверке правильности блокчейнов на базе PoS, клиентам необходимо загружать список публичных ключей и сигнатур для тех, кто предлагает блоки и голосует, а состав тех, кто предлагает блоки и голосует, может меняться для каждого блока. Таким образом, когда легковесные клиенты снова переходят в онлайн-режим после пребывания в офлайн-режиме в течение определенного времени, им приходится загружать большое количество публичных ключей и сигнатур, а затем проверять их все. Чтобы смягчить подобную проблему производительности, Виталик Бутерин, создатель Ethereum, предложил создать периодические контрольные точки на блокчейне, называемые *эпохами* [6], например, каждые 50 блоков. Каждая контрольная точка может быть проверена на основании предыдущей контрольной точки, благодаря чему легкие клиенты могут быстрее догонять весь блокчейн.

7 Токен в сети IoTeX

Нативный, цифровой, криптографически безопасный токен сети IoTeX (IOTX) — это основной компонент экосистемы сети IoTeX, который предназначен исключительно для использования в сети. До запуска основной сети IoTeX он будет существовать как токен стандарта ERC20 на блокчейне Ethereum, а после будет преобразован в токен на основной сети IoTeX.

IOTX необходим в качестве виртуального крипто “топлива” для использования определенных функций сети IoTeX (таких как осуществление транзакций и запуск распределенных приложений в сети IoTeX), которое обеспечивает экономическое поощрение, необходимое для стимулирования участников к внесению их вклада в поддержание экосистемы сети IoTeX. Для работы различных приложений и осуществления транзакций в сети IoTeX, а также валидации и верификации дополнительных блоков/информации на блокчейне требуются вычислительные ресурсы, и провайдеры этих ресурсов/сервисов будут получать вознаграждения за предоставление последних (т.е. майнинг в сети IoTeX) для поддержания целостности сети. IOTX будет использоваться как единица обмена для количественной оценки и оплаты расходов на затраченные вычислительные ресурсы. IOTX будет доступен для майнинга в течение 50 лет, при этом вознаграждения за майнинг будут со временем уменьшаться в соответствии с линейной моделью сокращения.

IOTX — это неотъемлемая часть сети IoTeX, поскольку в случае отсутствия IOTX не было бы единой единицы обмена для оплаты необходимых расходов, что делало бы экосистему сети IoTeX нежизнеспособной.

IOTX — это невозмещаемый функциональный утилити токен, который будет использоваться как единица обмена между участниками сети IoTeX. Цель внедрения IOTX — обеспечить удобное и безопасное средство оплаты и расчета между участниками, взаимодействующими в рамках экосистемы сети IoTeX. IOTX никоим образом не обеспечивает владение долей, участие, права, получение должности или процентов в IoTeX Foundation Ltd. (**Фонд**), его дочерних или ассоциированных предприятиях (аффилиатах), или в любых других компаниях. Также, токен IOTX не дает держателям токена никаких прав на комиссии, доходы, поступления или прибыль от инвестиций и не может использоваться как ценная бумага в Сингапуре, равно как и в любой другой юрисдикции. IOTX подлежит использованию только в сети IoTeX и владение IOTX не предполагает никаких прав, явных и подразумеваемых, помимо права использовать IOTX в качестве средства, позволяющего пользоваться сетью IoTeX и взаимодействовать с ней.

В частности, IOTX:

I. является невозмещаемым и не подлежит обмену на наличные средства (или эквивалент в любой другой виртуальной валюте) или любые платежные обязательства Фондом или аффилиатами;

II. не предоставляет держателю токена никаких прав в отношении Фонда (или любых его аффилиатов), а также его доходов или активов, в том числе никаких прав на получение будущих доходов, акции, владение долей, ценных бумаг, участие в голосовании и распределении, прав на погашение, ликвидацию, владение собственностью (включая все формы интеллектуальной собственности) или любых других финансовых или юридических прав, эквивалентных прав, прав на интеллектуальную собственность или любую другую форму участия в работе сети IoTeX, Фонда, Дистрибьютора и/или их провайдеров услуг;
III. не предназначен для того, чтобы представлять деньги (включая электронные деньги), ценные бумаги, товары, облигации, долговые обязательства или любой другой вид финансовых инструментов или инвестиций;
IV. не является кредитом для Фонда или любых его аффилиатов, и не предназначен для того, чтобы представлять долг, принадлежащий Фонду или любым его аффилиатам;
V. не обеспечивает держателям токена никакой собственности или других прав в Фонде или в любых его аффилиатах.

8 Экосистемы на базе IoTeX

Блокчейн IoTeX поддерживает целый ряд экосистем Интернета Вещей (IoT): экономика совместного использования, умный дом, автономные транспортные средства, цепочки поставок и т.д. Разработчики самых разных профилей используют IoTeX различными способами. В число разработчиков, поддерживаемых IoTeX, входят производители аппаратного обеспечения для IoT, разработчики систем контроля IoT-устройств, разработчики приложений для умного дома, производители устройств для экономик совместного использования, интеграторы данных цепочек поставок, поставщики данных для краудсорсинга, разработчики автономных автомобилей и т.д. В данном разделе описывается несколько экосистем, работающих на основе IoTeX.

8.1 Экономики совместного использования

За последние несколько лет, многие компании сфокусировались на экономиках совместного использования, начиная с совместных поездок (Uber/Lyft/Didi), совместной аренды домов (Airbnb), велосипедов (Mobike/ofo), и заканчивая совместным использованием совсем небольших предметов, таких как зарядные устройства, зонты и пр. Все они обеспечивают людям лучшую жизнь, хотя некоторые из них страдают от своих бизнес-моделей. Однако бизнес-модели таких экономик— это отдельная тема для обсуждения; здесь речь в основном пойдет об их технологической архитектуре. Среди всех экономик совместного использования, есть одна, которая не может обходиться без управления людьми, а именно водителя - это совместные поездки. Она не относится к экономикам, работающим на основе IoT. Тем не менее, в будущем, когда технология автономных автомобилей станет зрелой и популярной, совместные поездки будут

опираться на технологии IoT.

Все экономики совместного использования на основе IoT имеют нечто общее: они требуют “замок”, который может быть снят депозитом или арендной платой. Обеспечивать весь процесс совместного использования и возврата средств, используя IoT-устройства, не просто возможно — это эффективно. В централизованном мире такие экономики работают посредством централизованного облака. Однако они имеют ряд недостатков:

1. Крупный депозит удерживается компанией, которая может быть ненадежной. За последнее время, произошло много случаев, когда компания, предоставляющая услуги по совместному использованию велосипедов в Китае, оказалась неспособной вернуть депозиты своим пользователям;

2. Экономики за счет совместного использования опираются на сообщество не полностью. Многие совместно используемые вещи принадлежат компании. Это вызывает трату общественных ресурсов. Взять, к примеру, велосипеды. Когда компании, предлагающие велосипеды для совместного пользования, прекращают свой бизнес, велосипеды просто списываются.

3. В условиях централизации пользовательские данные сохраняются и контролируются одной компанией. Существует риск взлома либо облака, либо клиентской стороны с целью получения пользовательских данных.

IoTeX, как инфраструктура, могла бы применяться для обеспечения работы подобных приложений без упомянутых выше проблем и делать экономики совместного использования децентрализованными и более эффективными. Если точнее, экономики совместного использования на основе IoTeX были бы способны обеспечивать следующие преимущества:

1. Депозит полностью регулируется смарт-контрактом. Так как деньги никто не удерживает, возвращение депозита гарантировано всегда. Пользователям не нужно доверять компании, чтобы использовать сервис.
2. Каждая совместно используемая вещь реализует свою ценность и назначение автономным образом. В рамках экосистемы не имеет значения, кто владеет совместно используемой вещью. Владельцем может быть каждый, внося свой вклад в экосистему. Управлять экономикой может сообщество. В результате, компании могут выполнять функцию обслуживания замка IoT и управлять сообществом. Такая бизнес-модель намного легче, компании могут быстро расширять ее и обслуживать больше людей.
3. Опять же, пользователям не нужно доверять компании, чтобы сохранять свои данные. Их данные сохраняются на блокчейне с защитой конфиденциальности.

На Рисунке 7 изображено, как экономика совместного использования работает на базе блокчейна IoTeX.

Рисунок 7: Экономика совместного использования на базе IoTeX

8.2 Умный дом

На существующем рынке умных домов многие производители IoT-устройств по-прежнему используют для разработки своих продуктов устаревшие технологии. Им приходится выполнять объемные работы по разработке на своем облаке. Из-за необходимого для облака полного цикла приема и обработки запросов от клиентов, стоимость разработки и обслуживания оказывается высокой, а производительность — низкой. Развертывание продуктов на блокчейне IoTeX в значительной степени сократило бы операционные расходы на проектирование и облачные вычисления, и в то же время существенно повысило бы производительность их устройств. Если взять в качестве примера простую умную лампочку, то при использовании облачной технологии для изменения состояния лампочки требуется два цикла перехода от пользовательской инструкции. Производители не являются специалистами в области облака, поэтому их сервис зачастую оказывается не оптимальным. На полный цикл может уходить от одной до трех секунд. Это заставляет производителей прибегать к помощи облачных сервисов, предлагаемых крупными IT-компаниями. Использование таких сервисов имеет два недостатка:

1. Производители не могут полностью контролировать доступность облачных сервисов.
2. Им необходимо постоянно платить за облачный сервис, тогда как при продаже своих IoT-устройств они взимают единовременную плату.
3. Существует риск взлома их облака, клиентской стороны или интрасети, влекущего за собой кражу пользовательских данных или проблемы с безопасностью дома.

Для сравнения, блокчейн IoTeX, управляет устройствами локально и взаимодействует с

публичной цепочкой в интернете по мере необходимости. Публичная цепочка обслуживается сообществом. Для производителей IoT, никаких расходов на обслуживание нет. Блокчейн IoTeX обеспечивает защиту конфиденциальности, которая предотвращает утечку данных или взлом системы контроля, даже в условиях небезопасности интранета.

Рисунок 8: Умный дом на базе IoTeX

Помимо предоставления производителям IoT возможности разворачивать их IoT-устройства на блокчейне, IoTeX планирует сотрудничество с создателями IoT-чипов в целях разработки чипов на основе блокчейна IoTeX для ускорения цикла проектирования и производства IoT-устройств. Производителям IoT нужно будет просто интегрировать чип, чтобы их устройства поддерживались блокчейном IoTeX.

8.3 Управление идентификацией

Развивающийся мир IoT оказал влияние на функционирования менеджмента идентификации и доступа (Identity and Access Management, IAM). Применительно к идентификации вещей, IAM должен быть способен управлять системами пользователь-устройство, устройство-устройство и/или стройство-сервис/система. Одним из простых решений для осуществления менеджмента идентификации, является рассмотрение блокчейна IoTeX в качестве децентрализованной ИОК-системы (благодаря его неизменяемости), на котором каждому объекту выдается криптографическая идентичность в форме сертификата TLS и обеспечивается соответствующая конфиденциальность. Такой сертификат, обычно имеющий непродолжительный срок существования, подписывается встроенным долгосрочным сертификатом устройства и публикуется на блокчейне IoTeX (на корневой цепи, либо на субцепи). Одноранговые узлы и другие объекты могут получать доступ к привязанному к блокчейну краткосрочному сертификату и доверять ему, а предметы могут проходить аутентификацию при подключении к сети, обеспечивая безопасное сообщение между другими устройствами, сервисами и пользователями, и гарантировать их целостность.

В дополнение к этому, встроенные долгосрочные сертификаты для устройств могут располагаться в иерархическом порядке, как обычные ИОК, при котором родительские устройства могут подписывать дочерние сертификаты. Благодаря иерархии, становится возможным аннулирование и ротация сертификатов. Например, если одно устройство оказывается скомпрометированным, его родительское или даже прародительское устройство может подписывать команду аннулирования и отправлять ее на блокчейн, который деактивирует сертификат устройства.

9 Будущие исследовательские работы

В число некоторых существующих и будущих направлений исследований, нацеленных на усовершенствование IoTeX, входят следующие.

Вычисления с сохранением конфиденциальности

В этом направлении существует несколько сфер, которые мы активно исследуем:

- Как удержать состояние конфиденциальности на блокчейне, во время проведения вычислений определенной группой узлов;
- Сохраняющий конфиденциальность смарт-контракт, при котором оценка смарт-контракта возможна при защите его бизнес-логики шифрованием. Тогда как в теории заветной целью являются полностью гомофобное шифрование и схемы неразличимой обфускации (11), в ближайшем будущем перспективными представляются такие практические предложения, как Hawk (17);
- Будущее сокращение требований по ресурсам для вычислений и хранения техник сохранения конфиденциальности, которые IoTeX использует в настоящее время;
- Квантово-безопасные версии техник сохранения конфиденциальности, которые IoTeX использует в настоящее время, такие как квантово-безопасная кольцевая подпись.

Усечение и перенос состояний

Мы оцениваем различные способы безопасного усечения состояний, хранящихся на субцепях в целях сокращения требований по ресурсам для хранения, поскольку многие IoT-устройства имеют ограниченные хранилища. Самое очевидное решение — это, определенно, сжатие блоков и транзакций. Помимо этого, интересной темой для изучения также является эффективное перемещение состояний с субцепей на корневую цепь (так как последняя мощнее в отношении хранения) с сохранением конфиденциальности.

Управление и самосовершенствование

Хотя блокчейны IoTeX предлагают поощрения за поддержание консенсуса в своих

реестрах, на данный момент IoTeX не имеет встроенного механизма, который бы точно вносил поправки и изменения в правила, регулирующие его протокол, и вознаграждал разработку протокола. В целях решения этого вопроса мы планируем провести исследование, посвященное управлению и самостоятельного внесения изменений.

Древовидные блокчейны

Существующий IoTeX представляет собой двухуровневый блокчейн, который, естественно, должен быть расширен до дерева блокчейнов путем использования таких техник как Plasma и Cosmos. Мы планируем оценить эти предложения и улучшить существующий дизайн IoTeX, чтобы в конечном счете поддерживать более сложные иерархические структуры.

10 Заключение

В данной белой бумаге мы представили IoTeX, масштабируемый, конфиденциальный и расширяемый блокчейн для Интернета Вещей, архитектура и ключевые технологии которого включают:

1. блокчейны в блокчейне для максимизации масштабируемости и конфиденциальности,
2. настоящую конфиденциальность на блокчейне, основанную на ретранслируемом платежном коде, кольцевой подписи с постоянным размером без доверенной настройки и первой имплементации версий, устойчивых к ошибкам,
3. быстрый консенсус с мгновенным завершением на основе VRF и PoS для высокой пропускной способности и мгновенного завершения, и
4. гибкие и легковесные системные архитектуры на базе IoTeX.

11 Благодарность

Мы хотели бы выразить благодарность нашим наставникам и консультантам, а также участникам различных сообществ в сфере IoT, криптографии и криптовалют за их ранние отзывы и конструктивные предложения.

12 Сноски

[1] Adam Back et al. “Enabling blockchain innovations with pegged sidechains”. In: *URL: http://www. opensciencereview. com/papers/123/enablingblockchain- innovations-with-pegged-sidechains* (2014).

[2] Josh Benaloh and Michael de Mare. “One-Way Accumulators: A Decentral- ized Alternative to Digital Signatures”. In: *Advances in Cryptology — EURO- CRYPT ’93: Workshop on the Theory and Application of Cryptographic Tech- niques Lofthus, Norway, May 23–27, 1993 Proceedings*. Ed. by Tor Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 274–285. isbn: 978-3- 540-48285-7. doi: 10.1007/3-540-48285-7_24. url: https://doi.org/10.
1007/3-540-48285-7_24.

[3] *Bitcoin Improvement Proposals.* https://github.com/bitcoin/bips.

[4] Blockchain Size. https://blockchain.info/charts/blocks-size. [5]Benedikt Bu¨nz et al. *Bulletproofs: Efficient Range Proofs for Confidential Trans-actions*. Cryptology ePrint Archive, Report 2017/1066. https://eprint.iacr. org/2017/1066. 2017.

[6] Vitalik Buterin. *Light Clients and Proof of Stake*. https://blog.ethereum. org/2015/01/10/light-clients-proof-stake/.

[7] Miguel Castro, Barbara Liskov, et al. “Practical Byzantine fault tolerance”. In: *OSDI*. Vol. 99. 1999, pp. 173–186.

[8] Melissa Chase and Anna Lysyanskaya. “On Signatures of Knowledge”. In: *Ad- vances in Cryptology - CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006. Proceedings*. Ed. by Cynthia Dwork. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 78–96. isbn: 978-3-540-37433-6. doi: 10.1007/11818175_5. url: https:
//doi.org/10.1007/11818175_5.

[9] *EOS*. https://eos.io/.

[10] AB Ericsson. “Ericsson mobility report: On the pulse of the Networked Society”. In: *Ericsson, Sweden, Tech. Rep. EAB-14* 61078 (2015).

[11] Sanjam Garg et al. “Candidate indistinguishability obfuscation and functional encryption for all circuits”. In: *SIAM Journal on Computing* 45.3 (2016), pp. 882– 929.

[12] Yossi Gilad et al. “Algorand: Scaling byzantine agreements for cryptocurrencies”. In: *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM. 2017, pp. 51–68.

[13] *HDAC Blockchain for IoT*. https://hdac.io/.

[14] *Hyperledger Fabric*. https://www.ibm.com/blockchain/hyperledger.html.

[15] Internet of Things (IoT) Market by Software Solution (Real-Time Streaming Analytics, Security Solution, Data Management, Remote Monitoring, and Net- work Bandwidth Management), Service, Platform, Application Area, and Region

- *Global Forecast to 2022*. https://www.jasper.com/sites/default/files/ cisco-jasper-hidden-costs-of-delivering-iiot-services-en_2.pdf. 2016.

[16] *ITC Blockchain for IoT*. https://iotchain.io/.

[17] Ahmed Kosba et al. “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”. In: *Security and Privacy (SP), 2016 IEEE Sym- posium on*. IEEE. 2016, pp. 839–858.

[18] *Lisk*. https://lisk.io/.

[19] Silvio Micali, Michael Rabin, and Salil Vadhan. “Verifiable random functions”. In: *Foundations of Computer Science, 1999. 40th Annual Symposium on*. IEEE. 1999, pp. 120–130.

[20] *Monero – Private Digital Currency*. https://getmonero.org/. [21]Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[22] Shen Noether and Adam Mackenzie. “Ring Confidential Transactions”. In: *Ledger* Vol. 1 (2016), pp. 1–18. doi: https://doi.org /10 .5195 /ledger. 2016.34.

[23] Torben Pryds Pedersen. “Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing”. In: *Advances in Cryptology — CRYPTO ’91: Pro- ceedings*. Ed. by Joan Feigenbaum. Berlin, Heidelberg: Springer Berlin Heidel- berg, 1992, pp. 129–140. isbn: 978-3-540-46766-3. doi: 10.1007/3-540-46766-1_9. url: https://doi.org/10.1007/3-540-46766-1_9. [24]Serguei Popov. “The tangle”. In: *IOTA* (2016).

[25] *Raiden Network*. https://raiden.network/.

[26] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. “On data banks and privacy homomorphisms”. In: *Foundations of secure computation* 4.11 (1978), pp. 169–180.

[27] Ronald Rivest, Adi Shamir, and Yael Tauman. “How to leak a secret”. In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 552–565.

[28] Nicolas van Saberhagen. *Cryptonote v 2. 0*. 2013.

[29] Samsung. *Samsung ARTIK and Successful Strategies for Industrial IoT Deploy- ment*. Samsung, 2016.

[30] *Stellar*. https://www.stellar.org/.

[31] Shi-Feng Sun et al. “RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero”. In: *Com- puter Security – ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*. Ed. by Simon N. Foley, Dieter Gollmann, and Einar Snekkenes. Cham: Springer International Publishing, 2017, pp. 456–474. isbn: 978-3-319-66399- 9. doi: 10.1007/978-3-

319-66399-9_25. url: https://doi.org/10.1007/ 978-3-319-66399-9_25.

[32] *Tendermint*. https://tendermint.com/.

[33] *Tendermint Ecosystem*. https://tendermint.readthedocs.io/en/master/ ecosystem.html.

[34] *Tezos: A new digital commonwealth.* https://www.tezos.com/.

[35] *The hidden costs of delivering IIoT services*. https : / / www . jasper . com / sites / default / files / cisco - jasper - hidden - costs - of - delivering - iiot-services-en_2.pdf. 2017.

[36] *WebAssembly*. http://webassembly.org/.

[37] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges". In: *Security and Communication Networks* 7.12 (2014), pp. 2728–2742.

[38] *Zilliqa*. https://www.zilliqa.com/.