uPlexa

Стимулирование вычислительных мощностей IoT-устройств объединятся для формирования анонимных блокчейн платежей на базе браузера.

Предупреждение:

Вы просматриваете версию документа от 26 ноября 2018. В будущем могут быть внесены изменения в бизнес, техническую и правовую модели. Проверьте веб-сайт uPlexa чтобы найти последнюю версию этого документа.

Содержание

Введение и концепция

uPlexa-это электронная система p2p платежей, ориентированная на использование возможностей интернета вещей и анонимности. Построенная на собственном блокчейне с использованием модифицированной версии алгоритма CryptoNight, uPlexa была разработана для того, чтобы объединить мощь устройств IoT (Интернет вещей) в целое, основываясь на поддержке анонимных платежей, для интернет провайдеров и поставщиков телекоммуникационных услуг, а также поддерживая анонимную электронную коммерцию. В 2018 году в мире насчитывается более 9 миллиардов устройств IoT, а к 2020 году ожидается более 20 миллиардов.

Как и Биткойн, uPlexa является одноранговой (p2p) электронной платежной системой. Однако uPlexa также поддерживает анонимные платежи и выгодный майнинг с помощью IoT. uPlexa не только ASIC устойчива, но и нацелена на то, чтобы быть самой выгодной монетой для пользователей с устройствами IoT, имеющих некоторое количество неиспользуемых ресурсов. Блокчейн uPlexa будет напрямую доступен через интернет, без необходимости загрузки каких-либо сторонних ресурсов. Тем не менее, загружаемые приложения также будут доступны.

В декабре 2017 года мы увидели крупнейшее продвижение криптовалюты Биткойн. В это время Биткойн не был готов к принятию таким большим количеством пользователей, что привело к перегрузке сети, к медленному времени проведения транзакций и большим комиссиям. uPlexa решает эти проблемы, используя нашу модель почти нулевой перегруженности (NZCM). NZCM состоит из объединения хешрейта устройств IoT, а также сокращения микроплатежей за счет увеличения платы за микроплатежи по мере увеличения сетевых транзакций. Любые платежи, не считающиеся микроплатежами, всегда будут иметь относительно низкие комиссии. NZCM также будет использовать uPlexa API в качестве использования вне-блокчейн транзакций, для опытных пользователей uPlexa. Это всего лишь несколько простых функций NZCM. Чтобы узнать больше, пожалуйста прочитайте о NZCM на странице 6.

Анонимность и конфиденциальность являются одними из крупнейших обсуждений в области криптовалют. uPlexa использует алгоритм CryptoNight для обеспечения не отслеживаемых анонимных транзакций. Наши с uPlexa цели - принести анонимность в интернет и электронные платежи, а также в электронную коммерцию. Это будет достигнуто путем заключения сделок с ИТ и телеком провайдерами, запуска нашей собственной платформы электронной коммерции, а также поддержки анонимных транзакций, анонимных владельцев магазинов и отказа от хранения и продажи личной информации для маркетинга и всех других целей.

Как это устроено – IoT модель (Основной функционал)

uPlexa использует модифицированную версию алгоритма CryptoNight для обеспечения бесспорной безопасности и анонимных платежей. После аудита стандартного алгоритма CryptoNight для наших целей, мы вскоре поняли, что добыча IoT устройств с помощью CryptoNight-стандарт не является непосредственно жизнеспособной и прибыльной. Изменения, внесенные в алгоритм, должны сделать майнинг IoT более прибыльным. В отличие от других платежных систем, наша сеть будет поддерживаться миллиардами IoT-устройств во всём мире.

Наша основная цель - создание выгодного количество uPlexa в качестве помощи оплаты за электричество при эксплуатации любого IoT устройства, майнинг дополнительных денежных средств с помощью любых IoT-устройств. Это может быть не так много в развитых странах. Тем не менее, в развивающихся странах, где большинство устройств IoT встроены, они также более доступны для покупки. Например, люди в Юго-Восточной Азии и других регионах имеют смарт-телевизоры, умные холодильники, умные автомобили и несколько мобильных устройств. Если бы они смогли получить достаточно прибыли, чтобы по крайней мере оплатить часть затрат их эксплуатации, они были бы в гораздо лучшей ситуации, поскольку ежемесячные расходы на электроэнергию могут достигать до 20% от их дохода.

Мы планируем поддерживать большинство, если не все устройства IoT, разрабатывая программное обеспечение специально для каждого устройства, чтобы добывать uPlexa в процентом соотношении простоя процессора устройства. Величина использования может быть дополнительно настроена пользователем, и может иметь предел для того чтобы предотвратить чрезмерное использование IoT-устройства. Устройства, которые мы будем поддерживать:

- ПК и ноутбуки
- Мобильные телефоны и планшеты
- Смарт ТВ
- Умные приборы кухни (холодильники, печи, кофеварки и т.д.)
- Смарт автомобили
- Raspberry Pi
- Серверы (центры обработки данных и серверные фермы)
- Другие устройства по мере развития IoT

Как это устроено – Комиссии и модель почти нулевой перегрузки (Near-Zero Congestion Model - NZCM)

Чтобы свести к минимуму перегруженность сети и поддерживать чрезвычайно низкие тарифы, мы решили создать модель, известную как модель с почти нулевой перегруженностью (NZCM), которая имеет несколько уровней:

- Использование объединения мощностей внедрённых IoT
- Использование uPlexa API для NZCM вне-блокчейн цепочки транзакций
- Неодобрение весьма небольших микротранзакций
- Масштабирование комиссии для микротранзакций

С огромным количеством существующих устройств IoT и продолжающимся внедрением IoT, у нас нет абсолютно никаких сомнений в том, что мы получим значительную поддержку мощностью сети для нашего блокчейна. Однако, еще одним положительным является то, что для основных случаев использования uPlexa, при использовании API NZCM большая часть сделок пройдёт без использования актуального блокчейна.

NZCM API позволит веб-мастерам, разработчикам приложений и корпорациям кредитовать своих пользователей в uPlexa, в то время как пользователи выбирают майнинг для этой конкретной службы, приложения или бизнеса. Все это отправляется физическому лицу или бизнесу, в то время как uPlexa затем зачисляется этому отдельному пользователю на их платформе с помощью нашего API. Таким образом, когда пользователь тратит свои добытые uPlexa на их платформе, сделки не нужно проводить через блокчейн, всё обрабатывается на их платформе через базу данных.

Использоваться uPlexa в основном будет для анонимных платежей, для интернет провайдеров, а также для электронной коммерции. Таким образом, микротранзакции не являются основным приоритетом. В будущем мы хотим сосредоточиться на сети CryptoNight lightning для поддержки uPlexa и других микротранзакций CryptoNight. Однако, поскольку uPlexa напрямую не поддерживает микротранзакции, существует минимальное ограничение на то, сколько uPlexa может быть отправлено (не менее 1 uPlexa). Это количество может быть изменено в любой момент времени с помощью форка из-за стоимости uPlexa. Для микро-транзакций до 5 uPlexa будет взиматься изменяемая комиссия. Таким образом, если вы отправляете менее 5 uPlexa, когда сеть переполняется микроплатежами, плата за такие микротранзакции будет в 2 раза больше, чем любой стандартный платеж. Идея этого в том, чтобы отражать сетевые атаки и уменьшить использование микроплатежей с uPlexa. uPlexa, на данный момент, не является криптовалютой которая фокусируется на микро-транзакциях (<$0.15 USD)

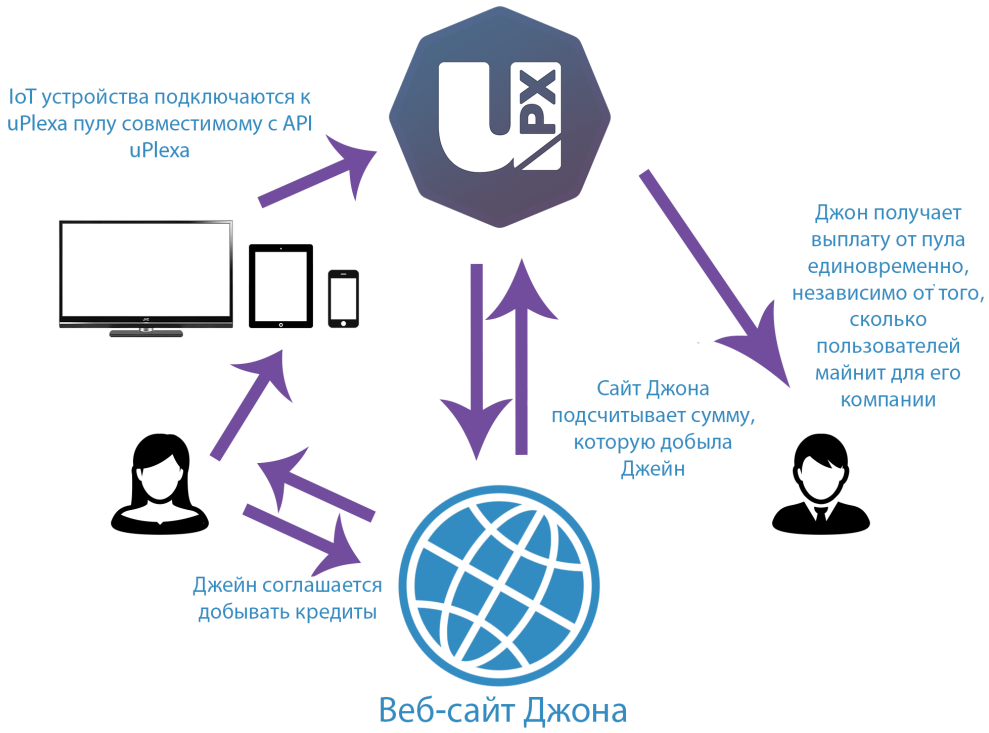
uPlexa NZCM API

API uPlexa может использоваться для того чтобы помочь обеспечить меньшую перегрузку сети, используя меньше транзакций в блокчейне, уменьшая комиссию для компаний и проектов.

Как это устроено

Например, Джон - владелец johnswebsite.com желает предоставить кредитную систему своим пользователям, чтобы они могли приобретать товары, услуги или делать пожертвования. Он может попросить своих пользователей подключать свои устройства к его интернет-сайту, чтобы добывать монеты uPlexa. За это, пользователи будут вознаграждены кредитами на сайте, с использованием API uPlexa. После того, как пользователи добудут достаточно кредитов Джона, они смогут сделать покупку, или использовать некоторые из кредитов для скидки на сайте Джона.

Добытые монеты во время этого процесса отправляется на один кошелек, кошелек Джона. Тем не менее, каждый отдельный пользователь и количество хэшей, которые они решили, отслеживается через API uPlexa. Таким образом, когда пользователь Джейн хочет совершить покупку, сумма списывается с баланса пользователя через API, но не делает отдельную транзакцию из своего кошелька на кошелек Джона.



Внедрение электронной коммерции

Индустрия электронной коммерции составляет более $ 2,3 трлн долларов мировых доходов, с оценками свыше $ 4,88 трлн долларов к 2021 году. Источник: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Команда uPlexa представит свою собственную платформу электронной коммерции, основанную на поддержке нескольких криптовалют, фиатных валют, а также с использованием uPlexa в качестве приватного, безопасного и анонимного шлюза как для веб-мастеров, так и для их клиентов. Для наших веб-мастеров не будет KYC, и они будут анонимно оплачены с помощью uPlexa. Другие вещи, такие как плагины и проекты, разработчики также будут доступны на рынке электронной коммерции для веб-мастеров, чтобы приобрести их с помощью uPlexa для своего собственного магазина.

Система электронной коммерции uPlexa не будет взимать плату с пользователей, пока указанный пользователь не запустит прибыльный магазин. Это означает, что магазин работает без оплаты, пока вы не начнете получать как минимум 3x месячную плату за магазин, которая составляет около $29 USD/месяц для стандартных магазинов. Выплаты будут производиться ежедневно, если вы превысили сумму > $ 29 USD. В противном случае выплаты будут производиться раз в две недели.

Наша команда ранее работала в индустрии электронной коммерции, от BigCommerce до Wordpress (WooCommerce) и Shopify. Мы сосредоточимся на настройке и анонимизации электронной коммерции, чтобы превзойти другие существующие системы электронной коммерции, прислушиваясь к предложениям и жалобам клиентов, которые эти компании всегда игнорировали. У нас лично было много хороших идей преобразования для этих систем, которые не могли быть внедрены без очень серьезных изменений. Некоторые из которых работают и сегодня для онлайн магазинов.

С учетом сказанного, приоритетным направлением uPlexa в отношении электронной коммерции будут как криптовалюты, так и увеличение улучшений для наших клиентов.

Сервис анонимных платежей

uPlexa окончательно преодолеет связь между анонимными платежами и поставщиков услуг. Это будет достигнуто путем создания нескольких партнерских отношений с развивающимися стартапами, которые позволят пользователям оплачивать свои услуги без KYC и использовать uPlexa в качестве дополнительного способа оплаты.

Почему оплата услуг должна быть анонимной?

- Анонимность обеспечивает защиту от шпионских программ, целью которых является кража Вашей личной информации
- Помогает защитить Вас от продажи Ваших данных в маркетинговых или других целях
- Оплачивайте услуги в других странах, путешествуя без оплаты "туристических" сборов, так как uPlexa является мировой валютой, и они не узнают, кто Вы
- Отсутствие того, что другие компании узнают, кому Вы платите или какую компанию Вы приобретаете
- Отсутствие правительственных репрессий и запретов на обслуживание
- Отсутствие шантажа со стороны интернет провайдеров или сотрудников, которые шпионят за Вашими данными
- Хакеры не смогут отследить Ваш номер телефона, или захватить ваш мобильный с доступом к Вашими личными данным, для дальнейшего получения доступа к онлайн-счетам

Анонимные функции uPlexa выходят далеко за рамки кодовой базы - в сферы крупных корпораций, а также политики в отношении KYC и анонимности. Наиболее трудными задачами будет поиск компаний и партнеров, готовых предоставить безопасную и анонимную опцию своим системам и сервисам. Таким образом, мы будем уделять большое внимание стратегическому партнерству, а также вознаграждать тех, кто помогает uPlexa реализовать свой истинный потенциал.

Эффективность и рентабельность IoT

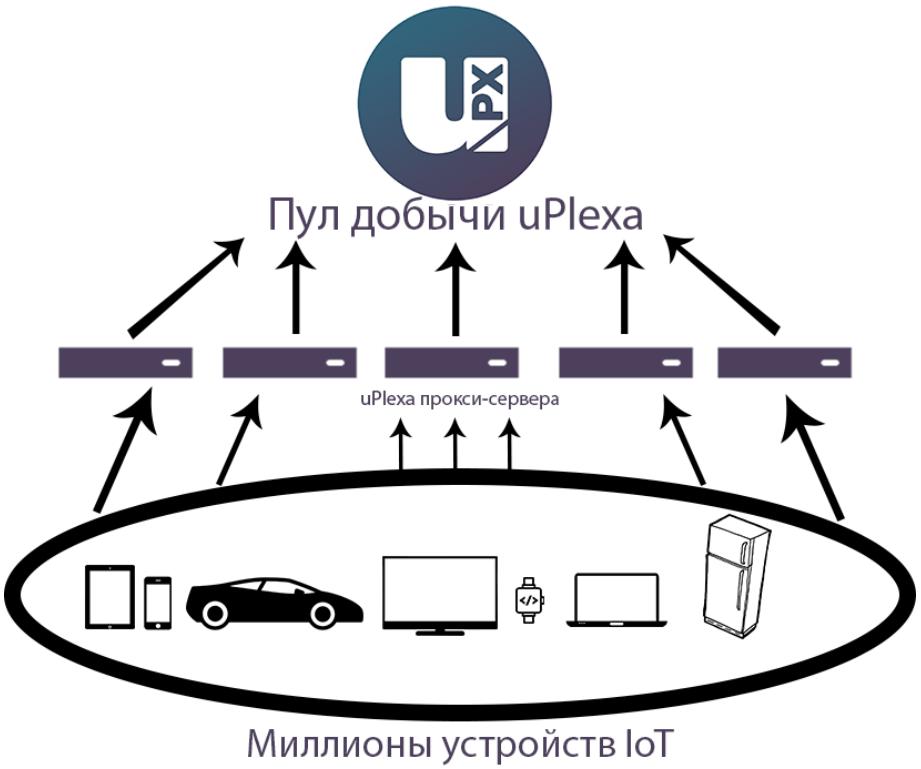
uPlexa будет предоставлять майнинг для множества устройств IoT, от смартфонов и планшетов до смарт-тв и даже смарт-авто. Это достигается путем запуска нашего программного обеспечения для майнинга. Программное обеспечение uPlexa для майнинга имеет набор установок отказоустойчивости, чтобы избежать перегрева устройств, подвисания, используя только определенную часть свободных ресурсов устройств. В наших тестах программное обеспечение для майнинга uPlexa требует меньше ресурсов процессора, чем обычно используемые приложения, такие как камера телефона, Facebook и Netflix.

Математика

Стандартный смартфон: 28H/s при полной нагрузке, или 10H/s при 35% загрузки процессора
Стандартный ноутбук: 45H/s при полной нагрузке, или 16H/s при 35% загрузки процессора

Использование 35% процессора обеспечивает среднюю мощность 13H/s. Если Алиса имеет 15 устройств, то она получит 13 * 15 = 195H/s.

Технология, делающая это возможным и легким - это форк CryptoNight пула в сочетании с расширенным прокси-протоколом для уменьшения количества подключений к пулу. С помощью нашего программного обеспечения мы можем принимать более двух миллионов одновременных подключений на пяти Amazon m5.2xlarge инстанса как прокси, и два Amazon m4.16xlarge инстанса (один для пула, второй для проверки общего доступа и балансировки рабочей нагрузки).



Рентабельность майнинга

Рентабельность заключается в нашей CryptoNight версии протокола, модифицированной для того чтобы обеспечить наиболее прибыльную, но анонимную форму добычи с помощью IoT. Протокол CryptoNight довольно устойчив к ASIC. Тем не менее, будущие обязательные хардфорки, которым будет следовать вся сеть, могут потребоваться, чтобы избежать майнинга с помощью ASIC на нашей платформе. Данные хардфорки не будут ни навязчивыми, ни рискованными.

Наша цель изменений в алгоритме состоит в том, чтобы достигнуть баланса между GPU и CPU так близко, как это возможно, с точки зрения стоимости за доллар для пользователей добывающего оборудования. Идея IoT добычи - это множество IoT устройств подключенных по всему миру поможет минимизировать централизацию майнинга, сохраняя устойчивый поток прибыли для наших шахтеров, постоянно помогающих обрабатывать транзакции в блокчейне uPlexa.

С помощью uPlexa люди могут использовать блокчейн который выгоден для добычи uPlexa, подключаясь непосредственно к одному из общественных пулов uPlexa. Они также могут выбрать подключение к компании или веб-сайту/игровому пулу для получения кредитов на указанной платформе.

Техническое объяснение - обзор CryptoNight

CryptoNote алгоритм

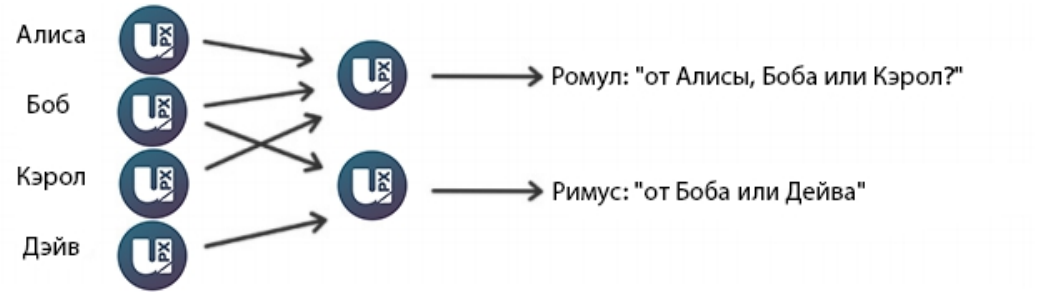
Алгоритм CryptoNote выпущен по лицензии с открытым исходным кодом и был принят и включен в uPlexa, поскольку он является основой для надежного, хорошо протестированного ядра криптовалюты. Это та же основная технология блокчейна, которая используется как Monero (топ-10 криптовалют), так и Bytecoin (топ-15 криптовалют).

Не отслеживаемые платежи

В обычной цифровой подписи (например, (EC) DSA, Schnorr и т.д.) процесс проверки включает открытый ключ подписывающего лица.
Это необходимое условие, поскольку подпись фактически доказывает, что автор обладает соответствующим секретным ключом. Но это не всегда достаточное условие.

Кольцевая подпись является более сложной схемой, которая требует несколько различных открытых ключей для проверки. В случае кольцевой подписи, у нас есть группа лиц, каждый с своим собственным секретным и открытым ключом. В заключении подтверждается кольцевыми подписями, что подписывающий данное сообщения является членом группы. Основное различие с обычными схемами цифровой подписи заключается в том, что подписывающее лицо нуждается в одном секретном ключе, но проверяющий не может установить точную личность подписывающего лица. Поэтому, если вы столкнулись с кольцевой подписью с открытыми ключами Алисы, Боба и Кэрол, вы можете только утверждать, что один из этих людей был подписавшим, но вы не сможете точно определить его или ее.

Эта концепция может быть использована для не отслеживаемых цифровых транзакций, отправленных в сеть с помощью открытых ключей других членов в кольцевой подписи, примененных в сделке. Этот подход доказывает, что создатель транзакции имеет право потратить сумму, указанную в транзакции, но его личность будет неотличима от пользователей, чьи открытые ключи он использовал в своей кольцевой подписи.

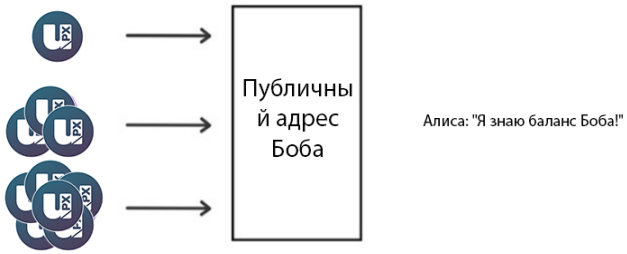


Не отслеживаемые транзакции

Следует отметить, что чужие транзакции не ограничивают вас в трате собственных средств. Ваш открытый ключ может появиться в десятках других кольцевых подписях, но только как запутывающий фактор (даже если вы уже использовали этот секретный ключ для подписания собственной транзакции). Кроме того, если два пользователя создают кольцевые подписи с одинаковым набором открытых ключей, подписи будут отличаться (если они не используют один и тот же закрытый ключ).

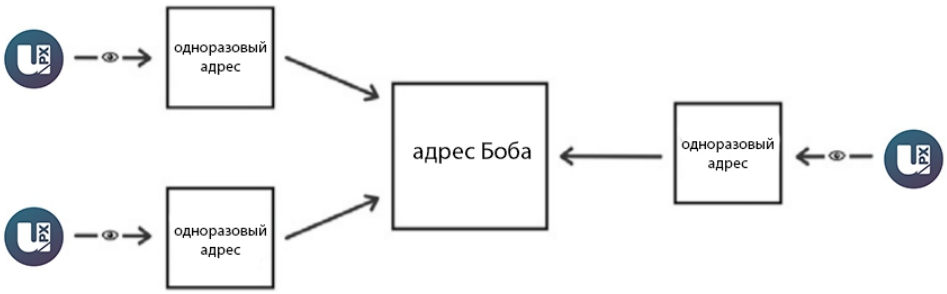
Не отслеживаемые транзакции

Обычно, когда вы публикуете свой публичный адрес, любой может проверить все ваши входящие транзакции, даже если они скрыты за кольцевой подписью. Чтобы избежать связывания, вы можете создать сотни ключей и отправить их своим плательщикам в частном порядке, но это лишает вас удобства иметь один общий адрес.



CryptoNote в uPlexa решает эту проблему путем автоматического создания нескольких одноразовых ключей, полученных из одного открытого ключа, для каждого p2p платежа. Решение заключается в хитрой модификации протокола обмена Диффи-Хеллмана. Изначально это позволяло двум сторонам производить общий секретный ключ, полученный из их открытых ключей. В нашей версии - отправитель использует публичный адрес получателя и собственные случайные данные для расчета одноразового ключа для оплаты.

Отправитель может создать только открытую часть ключа, в то время как получатель может вычислить приватную часть; следовательно, получатель является единственным, кто может освободить средства после совершения транзакции. Ему нужно выполнить проверку по единой формуле для каждой транзакции, чтобы установить, принадлежит ли она ему. Этот процесс включает его закрытый ключ, поэтому никакая третья сторона не может выполнить эту проверку и обнаружить связь между одноразовым ключом отправителя и уникальным открытым адресом получателя.



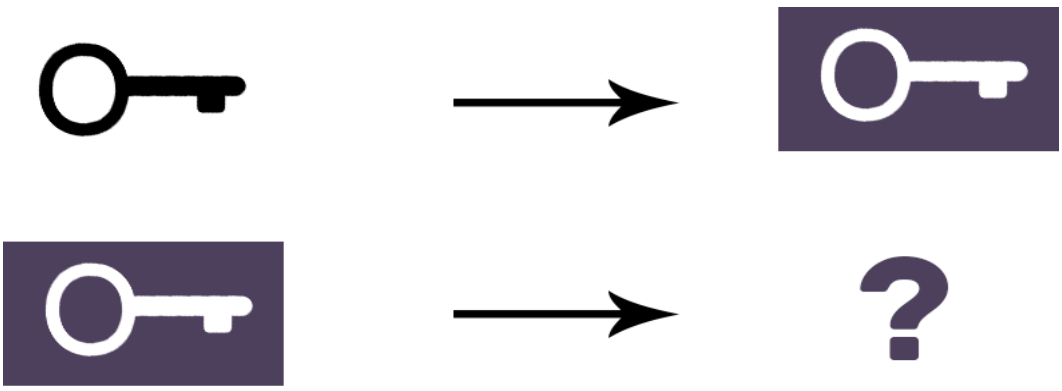
Важной частью нашего протокола является использование случайных данных отправителем. Это всегда приводит к другому одноразовому ключу, даже если отправитель и получатель остаются одинаковыми для всех транзакций (поэтому ключ называется “одноразовым”). Более того, даже если они оба являются одним и тем же человеком, все одноразовые ключи также будут абсолютно уникальными.

Доказательство двойной траты

Полностью анонимные подписи позволили бы тратить одни и те же средства многократно, что, конечно, несовместимо с принципами любой платежной системы. Проблему можно решить следующим образом.

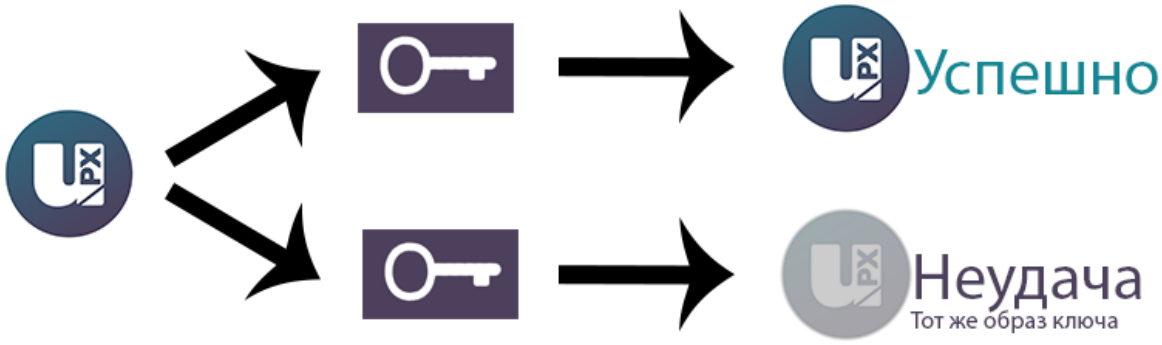
Кольцевая подпись является классом крипто-алгоритмов с различными функциями. CryptoNote в uPlexa является модифицированной версией “отслеживаемой кольцевой подписи”. Фактически мы превратили отслеживаемость в связываемость. Это ограничивает анонимность подписывающего лица следующим образом: если он создает более одной кольцевой подписи с использованием одного и того же закрытого ключа (набор внешних открытых ключей не имеет значения), эти подписи будут связаны вместе, что указывает на попытку двойной траты.

Для поддержки связываемости в uPlexa CryptoNote введён специальный маркер, генерируемый пользователем при подписывании, который мы назвали образом ключа. Это значение криптографической односторонней функции секретного ключа, поэтому в математических терминах это образ этого ключа. Односторонность означает, что при наличии только образа ключа невозможно восстановить закрытый ключ. С другой стороны, вычислительно невозможно найти коллизию (два разных закрытых ключа, которые имеют одинаковый образ). Использование любой формулы, кроме указанной, приведет к непроверяемой подписи. Учитывая все обстоятельства, образ ключа неоспоримый, однозначный и все же является анонимным маркером закрытого ключа.



Образ ключа через одностороннюю

Все пользователи хранят список использованных образов ключей (для сравнения с историей всех действительных транзакций, это незначительный объем памяти) в целях немедленного отклонения любой новой кольцевой подписи с дубликатом образа ключа. Это не будет идентифицировать пользователя нарушителя, но это предотвращает любые попытки двойной траты, вызванные плохими намерениями или программными ошибками.

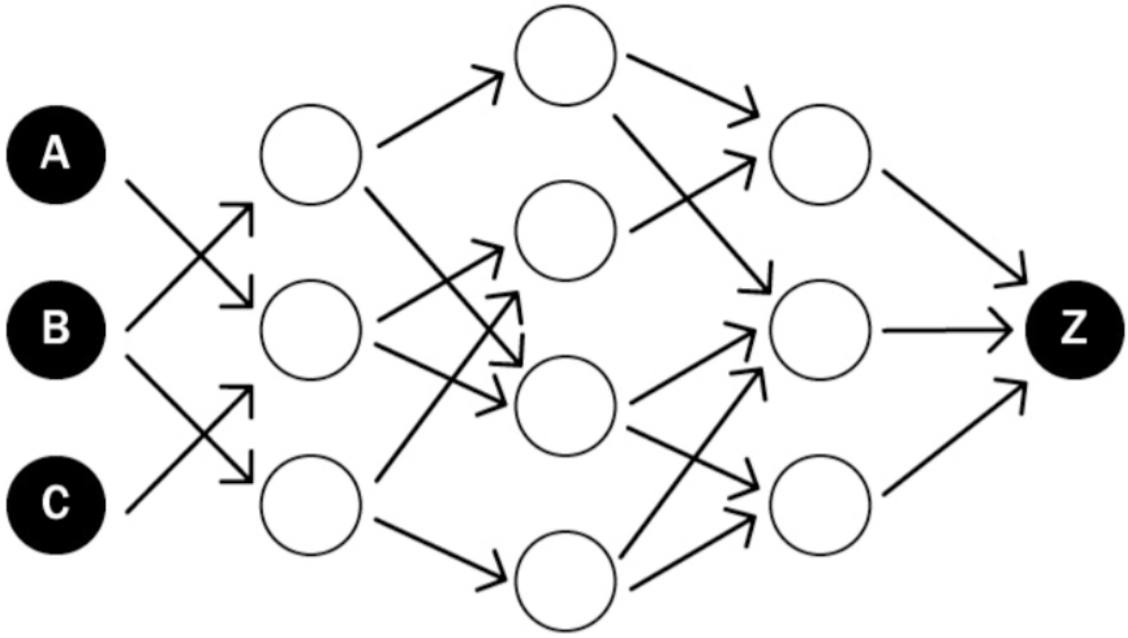


Анализ устойчивости блокчейна

Существует множество научных работ, посвященных анализу блокчейна биткоина. Их авторы отслеживают денежный поток, идентифицируют владельцев монет, определяют балансы кошельков и так далее. Возможность сделать такой анализ обусловлена тем, что все переводы между адресами прозрачны: каждый вход в транзакции относится к уникальному выходу. Более того, пользователи часто повторно используют свои старые адреса, получая и отправляя с них монеты многократно, что упрощает работу аналитика. Это происходит непреднамеренно: если у вас есть публичный адрес (например, для пожертвований), вы обязательно будете использовать этот адрес во многих вводах и транзакциях.

CryptoNote в uPlexa предназначен для снижения рисков, связанных с повторным использованием ключа и отслеживания один вход - один выход. Каждый адрес для платежа - это уникальный одноразовый ключ, полученный как из данных отправителя, так и из данных получателя. Его можно выявить с двойной вероятностью для коллизии 256-разрядного хэша. Как только вы используете кольцевую подпись во входных данных, это влечет за собой неопределенность: какие выходные данные только что были потрачены?

Пытаясь нарисовать схему с адресами на концах и транзакциями между ними, мы получим схему без циклов (потому что ни один ключ/адрес не использовался дважды). Кроме того, существуют миллиарды возможных схем, так как каждая кольцевая подпись создает неопределённость. Таким образом, вы не можете быть уверены, от какого отправителя приходит транзакция на адрес. В зависимости от размера кольца вы будете угадывать от “Один из двух” до “Одного из тысячи”. Каждая следующая транзакция увеличивает энтропию и создает дополнительные препятствия для анализа.



Стандартная транзакция CryptoNote

Стандартная транзакция в uPlexa CryptoNote создается по следующей последовательности, рассматриваемой в данном документе.

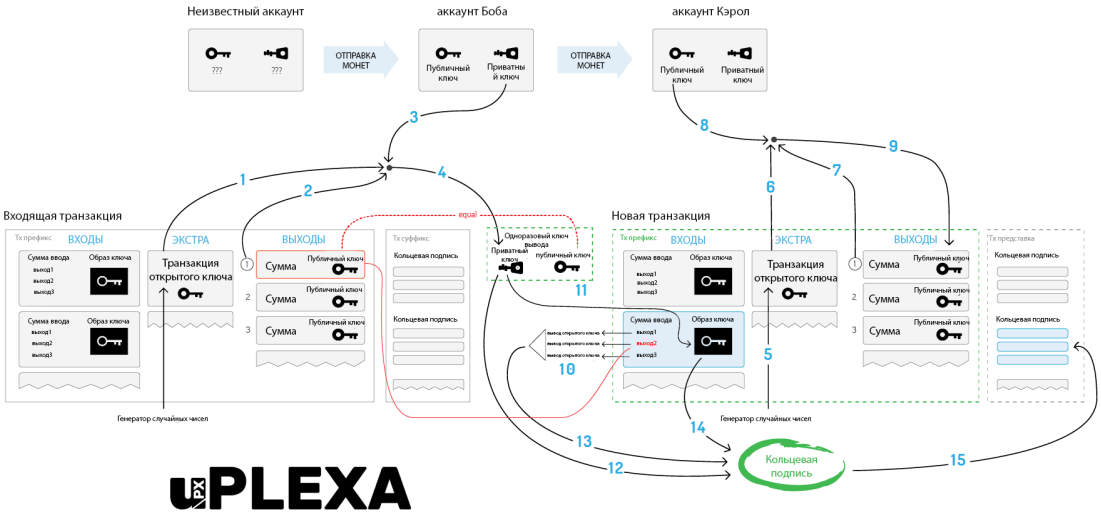
Боб решает совершить вывод монет, которые были отправлены на его одноразовый открытый ключ. Он нуждается в дополнительных данных (1), TxOutNumber (2), и его же закрытый ключ (3) для восстановления его одноразового секретного ключа (4).

При отправке транзакции Кэрол, Боб генерирует значение её суммы случайным образом (5). Он использует дополнительные данные (6), TxOutNumber (7) и открытый ключ учетной записи Кэрол (8), чтобы получить открытый ключ её вывода (9).

На входе Боб скрывает связь своего выхода среди чужих ключей (10).

Для предотвращения двойной траты он также закладывает образ ключа, полученный из его одноразового закрытого ключа (11).

В заключении, Боб подписывает транзакцию, используя свой одноразовый закрытый ключ (12), все открытые ключи (13) и образ ключа (14). Далее он добавляет результат в кольцевую подпись.
Итоговая подпись транзакции (15).



Адаптивные ограничения

Децентрализованная платежная система не должна зависеть от решения одного человека, даже если этот человек является основным разработчиком. Жесткие постоянные и магические числа в коде сдерживают эволюцию системы и поэтому должны быть устранены (или хотя бы сведены до минимума). Каждое важное ограничение (например, максимальный размер блока или минимальная сумма комиссии) должно быть пересчитано на основе предыдущего состояния системы. Поэтому ограничения всегда меняется адаптивно и независимо, позволяя сети развиваться самостоятельно.

CryptoNote в uPlexa имеет следующие параметры, которые автоматически подстраиваются для каждого нового блока:

1. Сложность. Главная идея нашего алгоритма состоит в том, чтобы суммировать всю работу, проделанную нодами за последние 720 блоков и разделить сумму на время, потраченное на выполнение работы. Показателем работы является соответствующее значение сложности для каждого из блоков. Время рассчитывается следующим образом: отсортируем все 720 отметок времени создания блоков и отсечём 20% резко отличающихся значений. Диапазон остальных 600 значений - это время, затраченное на 80% соответствующих блоков.

2. Максимальный размер блока. Пусть MN - медиана размеров последних N блоков. Тогда "жесткое ограничение" для размера допускаемых блоков равно 2 x MN. Это предотвращает раздувание блокчейна, но все же позволяет пределу медленно расти со временем, если это необходимо. Размер транзакции не обязательно должен быть чётко ограничен. Её размер связан с размером блока.

Плавная эмиссия

Верхняя граница общего количества всех цифровых монет также является цифровой:

Макс. количество = 264 − 1 атомная единица

Это естественное ограничение, основанное только на пределах реализации, а не на интуиции, такой как " N количества монет должно хватить на всех". Чтобы сделать в CryptoNote плавный процесс эмиссии uPlexa используются следующая формула вознаграждения за блок:

Базовая награда = (Макс. количество - A) > > 18

Где A - сумма ранее созданных монет. Это дает прогнозируемый рост денежной массы без каких-либо резких изменений.

Заключение

uPlexa фокусируется на предоставлении анонимной монеты с бесплатными утилитами для электронной коммерции и сферы услуг платежей. Эти утилиты будут находиться поверх основных уровней, таких как объединение хеш-мощностей IoT и вне-блокчейн транзакций.

Используемая литература

Cryptonote вайт папер:
https://cryptonote.org/whitepaper.pdf

Как устроен Cryptonote:
https://cryptonote.org/inside

Bitcoin вайт папер:
https://bitcoin.org/bitcoin.pdf

Статистика: IoT подключенных устройств 2015-2025:
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

PRISM (Программа наблюдения):
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)