The Pirate Code

V1.0

By: Flexatron, FishyGuts, jl777c & KMD community

Аннотация

Полностью приватная и защищенная блокчейном криптовалюта, возникшая из экосистемы Комодо. Pirate coin решает проблему «взаимозаменяемости» Zcash посредством устранения функциональности транзакций для прозрачных адресов в своей цепочке, делая приватное использование «fool-proof». Эта функция приводит к полностью защищенной базе монеты пользователя в цепочке пиратов. Постоянно используя технологию zk-SNARK, Pirate coin не содержит пригодных для использования метаданных пользовательских транзакций на ее блокчейне. Все исходящие транзакции, кроме вознаграждений за добычу и нотариальные операции, отправляются в защищенные Sapling-адреса, увеличивая до максимума эффективность и скорость своей цепочки. Пират использует консенсусный алгоритм Equihash, подтверждающий работу, происходящий из Zcash, с добавленным уровнем безопасности отложенного доказательства работы от Komodo, который обеспечивает уровень безопасности BTC-уровня для Pchate blockchain. Будущее частных децентрализованных платежей здесь.

Оглавление

PIRATE Code

Заявление о миссии

Миссия Пиратов заключается в том, чтобы сохранить финансовую конфиденциальность людей в системе, в которой преобладают прозрачные транзакции.

Ценность предложения

- *По умолчанию все транзакции Pirate chain являются закрытыми*

Это облегчает проблемы взаимозаменяемости, такие как у многих криптовалют с необязательной конфиденциальностью, которые вносят их в свой протокол.
Это полный протокол конфиденциальности предоставляет пользователям больше уверенности в том, что нет возможности утверждать то, что средства пользователей «испорчены» из-за предыдущих транзакций, сейчас и в дальнейшем будущем.

- *Pirate coin полностью децентрализована*

В любое время ни одно третье лицо не отвечает за ваши средства.
Приватные транзакции подтверждены trustless manner blockchain и вам не нужна дополнительная сторона, чтобы проверить действительность ваших транзакций, пиратский код позаботится об этом.

- *Ценность Pirate в обеспечении безопасных и быстрых передач*

Пиратская цепь защищена механизмом, более сложным для взлома, чем биткойн, называемый задержанным Proof-of-Work (dPoW). Плата за использование очень недорога, как для клиента, так и для поставщика. Кроме того, там нет никаких шансов для мошеннических платежей, нет ошибочных периодов проверки фонда. Периоды проверки и транзакции подтверждены и защищены в течение нескольких минут. Только эти функции могут спасти продавцов и поставщиков по всему миру - миллиарды долларов, уменьшив плату за упрощение формальностей.

- *Pirate uспользует высокопрофессиональный протокол конфиденциальности*

Развитый и получивший высокие оценки протокол конфиденциальности zk-SNARKS не требует, чтобы данные из вашей транзакции были доступны для просмотра в эксплорере. Многие видные разработчики считают это одним из самых сильных методов скрытия ваших финансовых данных в блокчейне.

Внимание на приватность?

Crypto предлагает преимущества для пользователей и бизнеса, но это не должно исходить за счет финансовой конфиденциальности. Сегодняшние валюты FIAT уже совершают массовый исход в сторону цифровых систем (Japparova en Rupeika-Apoga 2017). Crypto показал и предлагает многочисленные преимущества для бизнеса, такие как экономия в сборах и скорость транзакций. По нашему мнению, пользователи заслуживают конфиденциальности в своих сделках.

Зачем показывать владельцу магазина размер вашего состояния или привычку расходов?

Поэтому финансовая конфиденциальность может потребоваться всем сторонам, которые хотят принимать криптовалюты, такие как: поставщики, дистрибьюторы, торговцы, покупатели, поставщики, поставщики услуг и клиенты. Бизнес может заверить своих клиентов и самих себя, что обе стороны транзакция получит наилучшую комбинацию конфиденциальности, скорости и экономию затрат за счет использования Pirate.

Команда

Будучи по-настоящему децентрализованной криптовалютой, Pirate приветствует разработчиков и специалистов различных навыков.

Уже более 30 участников предоставили услуги для роста и развития пиратской цепи с самого начала. Разработчики работают в согласованной командной моде, чтобы получить знания и опыт от всех частей криптосферы. С нашей разнообразной группой всегда есть человек, который знает, как выполнить нужную задачу, или кто-то знает кого-то, кто знает, как выполнить необходимую задачу.
Пират выполнил несколько пунктов в криптовалютной индустрии, в области защиты конфиденциальности (см. «Дорожная карта») и «Пират» будут продолжать работать с третьими лицами по инновационным методам упрощения конфиденциальности для всех.

Вступление

Криптовалюты

С момента выпуска знаменитого whitepaper, написанного Сатоши Накамото в 2008 году (Nakamoto 2008), капитализация биткоина как цифрового актива выросла до миллиардов долларов. Ряд альтернативных криптовалют возникли с тех пор, пытаясь заполнить пустоту множеством их сообществ. Криптотерминалы как средство платежа - это одним из самых популярных случаев, а также основная цель, о которой Сатоши написал whitepaper.

Цель Bitcoin - позволить каждому человеку передавать деньги в любой точке мира в любое время, мгновенно, используя интернет- соединение в одноранговой сети, trustless fashion. Биткойн использует распределенной регистр для облегчения и записи транзакций, из которых истинность определяется с помощью согласованного алгоритма Proof-ofWork (PoW).

Приватность

Одной большой проблемой, связанной с использованием этой технологии, является способность наблюдать и анализировать ваше поведение в расходах и состояние вашего счета (Мозер 2013). Это очень сильно ухудшает финансовую конфиденциальность пользователя. Было разработано несколько протоколов криптовалют, которые планировали улучшить аспекты конфиденциальности Bitcoin. Наиболее известные протоколы в настоящем времени были разработаны CryptoNote (Van Saberhagen 2013) и Zerocash (Sasson et al., 2014). В первом протоколе используется Ring Confidential Signatures, в то время как последний использует zero-knowledge proofs для запутывания транзакций и балансов на счетах, более подробно об этом позже. Оба протокола имеют свои преимущества и недостатки. Этот whitepaper показывает, как Pirate (ARRR) пытается улучшить аспекты конфиденциальности существующих децентрализованных платежных протоколов.

Основные недостатки, проиллюстрированные текущими децентрализованными платежными протоколами

Monero, форк Bytecoin на основе протокола CryptoNote, использует схему Ring Signature в их транзакциях в сочетании со сокрытием адреса, случайные разовые адреса для каждой транзакции от имени получателя. При схеме Ring Signature гораздо труднее отследить отправителя в зависимости от размера кольца. Однако эта схема оставляет способность сторон анализировать имеющиеся данные со сложными аналитическими инструментами прямо сейчас и в будущем.

Из-за использования Ring Signature анализ блокчейна Монеро достаточно сложен, как показано на рисунке 1.

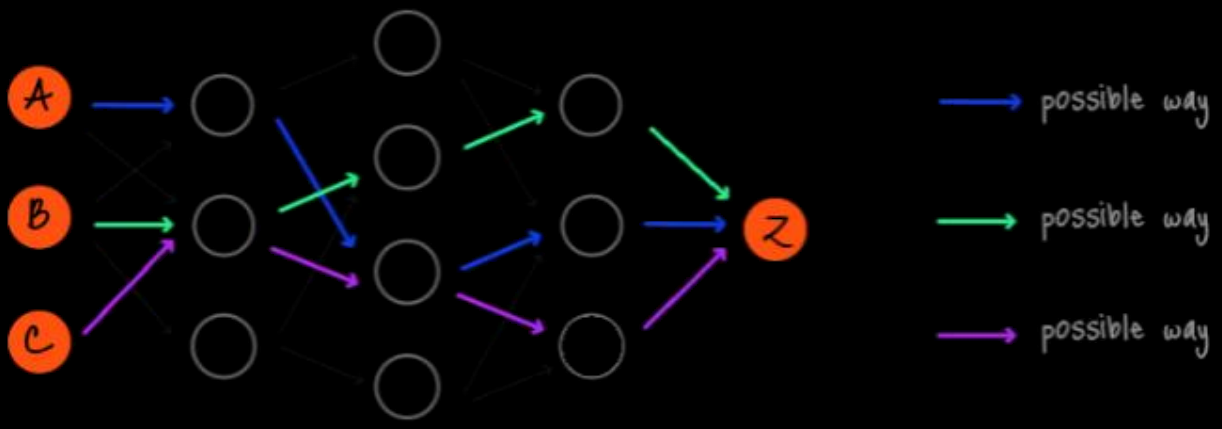

Рисунок 1 Кольцевой сигнатурный анализ блокчейна. Источник: https://cryptonote.org/inside#untraceable-payments

Трудность поиска правильного отправителя все труднее отследить при увеличении размера кольца. Размер кольца - общее количество возможных подписавших вас, что, в свою очередь, определяет сложность и трудно найти «реальный выход». Таким образом, более большой размер кольца обеспечивает более высокий уровень конфиденциальности, чем меньший.

Тем не менее, не рекомендуется повторно использовать нечетный узнаваемый размер кольца для предотвращения выявления из других транзакций [3]. Основная проблема методов смешивания монет заключается в том, что данные транзакций не скрываются посредством шифрования. RingCT - это система диссоциации, когда информация все еще видна в blockchain.

Учтите, что уязвимость может быть обнаружена в возможном будущем, что позволит отслеживать, так как Monero's blockchain обеспечивает запись каждой произошедшей транзакции.

Защищенные адреса Zcash направлены на реализацию и использование типов

Zcash, реализация схемы децентрализованного анонимного платежа Zerocash добавляет защищенную схему оплаты, обеспеченную zero-knowledge краткие не-интерактивные аргументы знания (zk-SNARKs) для существующей прозрачной платежной схемы, используемой Биткойном (Hopwood et al. 2016). Пользователь свободно может выбрать использование защищенных или незащищенных платежей. Процент защищенных транзакций предполагается, поскольку недавняя реализация Zcash «Sapling» делает обработку защищенных транзакций - всего лишь частью, использующую более интенсивно вычислительную мощность, в сравнение с незащищенными транзакциями (Bowe 2017). К сожалению, относительный высокий процент незащищенных транзакций и балансов на счете ухудшает качество монет, так как можно связать транзакции во время «приватной» платежной деятельности и, возможно, связывают их с смешиванием монет. Это особенно важно при проведении «транзакции «туда и обратно», что означает отправку точного количества монет от незащищенного (t-addr) до защищенного адреса (z-addr) и обратно на другой незащищенный адрес (Quesnelle 2017). Мы ссылаемся на это в whitepaper, называя это явление - как «проблему взаимозаменяемости».

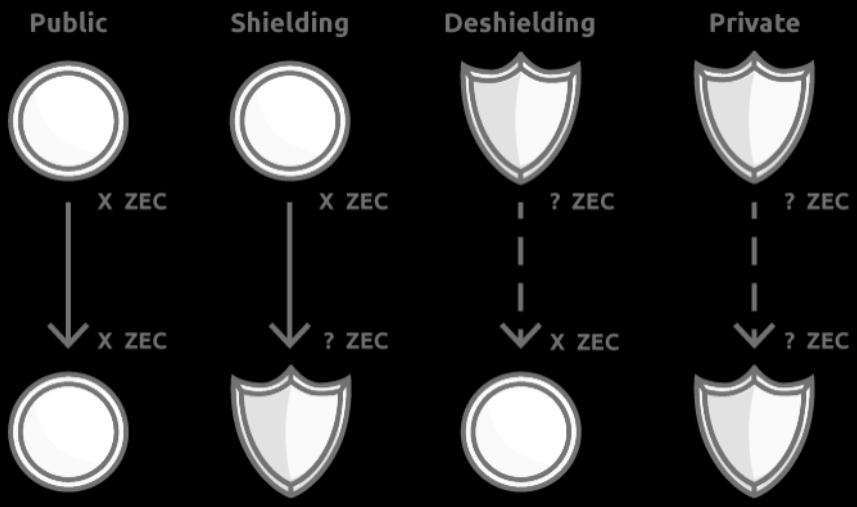

Рисунок 2 Пользователи Zcash имеют 4 разных варианта расходов Zcash. Источник: https://z.cash/blog/sapling-transaction-anatomy/

Как видно на рисунке 2, пользователям Zcash предоставляется возможность проводить 4 различных типов транзакций в текущем протоколе Zcash и быть способным отправлять средства от незащищенного в приватный адрес и наоборот, что ставит под угрозу совместимость монет. Можно идентифицировать шаблоны смешивания монет между различными типами транзакций, когда пользователи отправляют монеты обратно на незащищенные адреса, например, в

«Транзакции «туда и обратно», поскольку это поведение проявляет высокую связываемость (Quesnelle 2017). К сожалению, повышение производительности Sapling происходит в уединении поскольку транзакции Sapling показывают больше метаданных, чем «старое» наследие Операции JoinSplit. Операции Sapling показывают количество входов и используемые выходы. Эта функциональность увеличивает возможности для различения типов транзакций, анализировать данные транзакций и

возможно, определить поведение, связанное с перемешиванием. чтобы уменьшить или устранить этот риск, важно либо уменьшить использование незащищенных адресов или просто отключить его с самого начала в новом блокчейне, таком как Pirate.

Наше решение

«Pirate» стремится существенно улучшить безопасность и конфиденциальность функции Monero и исправить «проблему взаимозаменяемости» Zcash. Пиратская цепь делает это с помощью принудительно принятых защищенных «Sapling» транзакций (z-tx), помимо вознаграждений за майнинг и нотариальных заверений, как объясняется в разделе dPoW. Кроме того, блокчейн пиратов обеспечен через механизм задержки с подтверждением работы, обеспечивающий конфиденциальность и функции безопасности, которые в настоящее время не имеют себе равных в индустрии блокчейна по сравнению с существующими приватными монетами.

29 августа 2018 года - призыв к полной анонимности

Pirate стартовал 29 августа в Discord как идея 100% - ной zk-SNARKS монеты. Разработка jl777c в Komodo Asset chain позволила задействовать использование защищенных транзакций при помощи корректировки параметров цепочки активов в новой цепочке активов (Grewal 2018). Цепочка активов - это вилка времени Komodo и актуальная независимая блочная цепь.

Первоначально пират начал эксперимент, чтобы наблюдать, будут ли принудительные ztransactions работать, но сообщество быстро осознало его потенциал после того, как jl777c успешно реализовал задержанную проверку работоспособности что делает Pirate по существу особенным.

Komodo – Zcash fork – zk-SNARKs

Pirate является частью asset chain экосистемы платформы Komodo. Проект «Комодо» фокусируется на расширении возможностей предпринимателей-блокчейн и возможностей обычных пользователей криптовалют со свободой и простотой использования через блокирующую технологию (Lee 2018). Комодо начинался как форк популярной приватной монеты, Zcash. Сам проект Zcash является форком Биткойна. Таким образом, все функции, разработанные Сатоши Накамото в биткойн-протоколе также доступны и в Комодо. Это означает, что Komodo сохраняет те же встроенные функции конфиденциальности, что и Zcash. Среди этих функций - параметры Zcash и технология zk-SNARK. Zk-SNARKS - одна из самых мощных форм конфиденциальности в блокчейне, поскольку предоставленная конфиденциальность фактически является постоянной.

Это заявление также подчеркивается главным представителем Monero, Riccardo "fluffypony" Spagni:

«ZkSNARKs ZCash по своим характеристикам обеспечивают гораздо более сильную неотслеживаемость, чем Monero (но гораздо меньше privacyset и намного больше системных рисков) ».

Komodo Asset chains

An Asset chain (официально Parallel Chain) - это независимо созданный blockchain, который наследует все функции Komodo, такие как BarterDEX- совместимость, конфиденциальность Zero Knowledge и delayed Proof-of-Work etc. но также имеет множество специальных спецификаций, таких как custom coin supply

и настраиваемый RPC-порт. Дополнительные пользовательские функции в настоящее время находятся в стадии разработки для добавления (PTY X 2018). Другие примеры Komodo asset chains включающие Bitcoin Hush (BTCH), ChainZilla (ZILLA), DEX, эквалайзер (EQL), KMDice, Monaize (MNZ), PUNGO, REVS, SuperNET, Utrum и ZEX.

Принудительные z-транзакции

Лучшее решение проблемы «взаимозаменяемости», на наш взгляд - это отключить возможность отправки незащищенных адресов, это исключит существование транзакций с защищенных балансов до открытых балансов, которые часто являются основной причиной снижения взаимозаменяемости. Как цитирует главный разработчик Zcash в ответ к статье под названием «О связывании транзакций Zcash» Джеффри Кеснеле:

«Но мой ответ заключается в том, что мы собираемся запретить незащищенные сделки. Это еще проще.

Delayed Proof-of-Work: максимальная безопасность и гибкость

Что задерживается Proof-of-Work?

Отсроченный Proof-of-Work связан с Комодо и обеспечивает уникальную и инновационную форму безопасности, которая так же сильна, как с присоединением сети, но не требует затрат на запуск этой сети. Отсроченный Proof-of-Work - это решение, которое объединяет несколько существующих методов в единую гибридную систему консенсуса, которая будет столь же энергоэффективной, как и Proof-of-Stake (PoS), будучи обеспеченным Proof-of-Work Биткойна. Пользователи, которые создают независимые blockchain (asset chains) в экосистеме Комодо могут выбрать block-hash, служащий в качестве «моментального снимка» их собственного блокчейна, который будет вставлен в основную цепь Комодо. Таким образом в записи о цепочке активов косвенно включаются в block-hash Комодо, который записывается в блокчейн самой сильной сети (в данный момент - биткойн).

Таким образом, dPoW позволяет даже самым слабым из блокчейнов извлекать выгоду из Биткойн hash-rate, а это, в свою очередь, увеличивает мощность Биткойна, этот способ более экологичный, поскольку он обеспечивает всю экосистему dPoW дополнительно (Jl777c 2016). Помимо Pirate, dPoW успешно реализованы в большом количестве цепочек активов, таких как Game Credits, Einsteinium (EMC2), Pungo и HUSH и некоторых других (Komodostats 2018)

Какова механика, отсроченного Proof-of-Work?

Служба безопасности Komodo выполняется нотариальными узлами, которым необходимо записывать block-hash в Bitcoin blockchain, как нотариальное заверение (рис. 3). Нотариальное заверение подразумевает создание групповой биткойн-транзакции, содержащей последний block-hashe Комодо, подписанный неизвестной комбинацией из 33 из 64 нотариальных узлов (Jl777c 2016). block-hashes пиратской цепи (среди других активов цепи) вставляются в блокчейн Комодо своевременно, также хорошо используя тот же метод. Таким образом, даже одна сохранившаяся копия главной цепи Комодо позволит всей экосистеме актива цепи перезаписать и отменить любую попытку атакующего сделать изменения. Нотариальные узлы опплачивают комиссию за транзакции в биткойнах нотариально заверяя блокчейн Komodo.

Расходы на транзакцию биткойнов для нотариальных узлов компенсируется блок-наградами и транзакцией сборов блокчейна Комодо, идущих к нотариальным узлам. Поэтому ожидается, что финансовые интересы заинтересованных сторон должны голосовать за нотариальные узлы, в которых они заинтересованы.64 широко распространенных нотариальных узла готовы к выборам и ак ожидается, будет оптимальным представлением децентрализованной экосистемы делая любой тип 51% атаки крайне маловероятным.

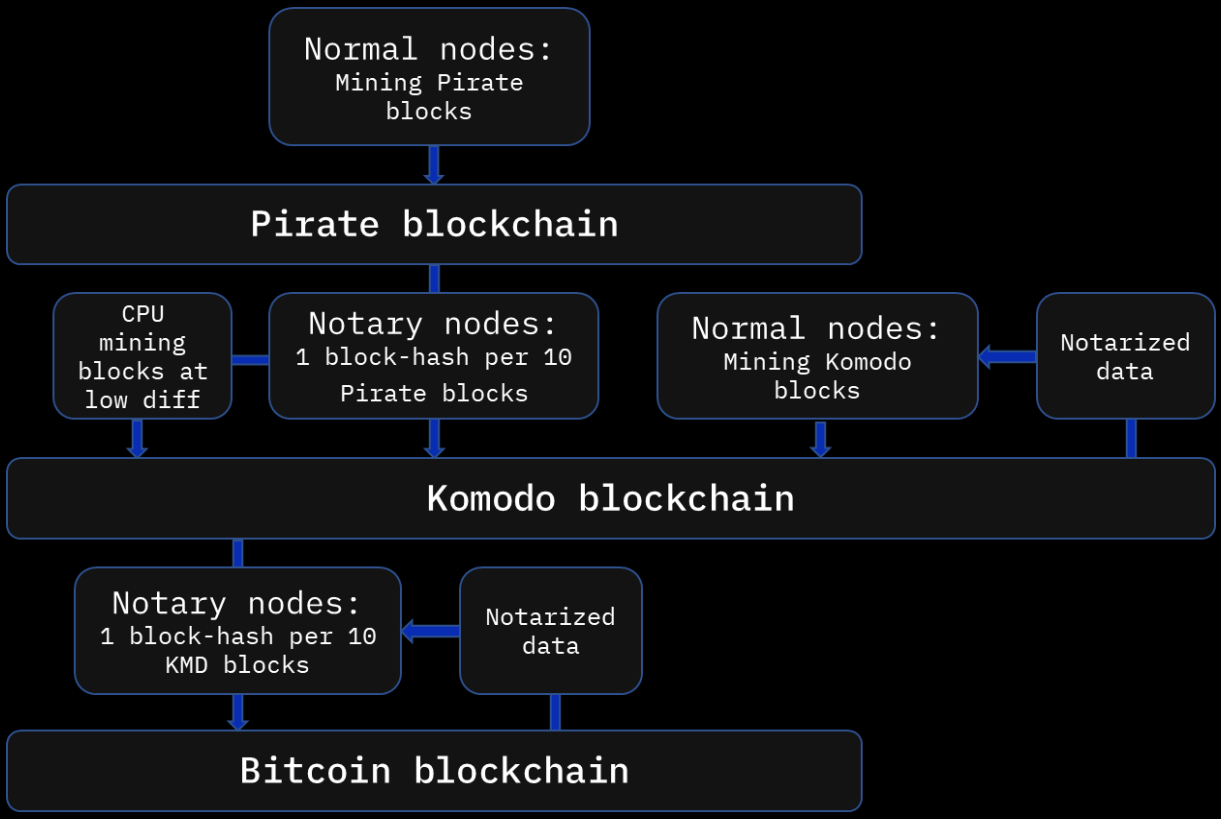

Рисунок 3 Схематическое представление отложенного Proof-of-Work.

Поэтому, чтобы реорганизовать и атаковать Пирата, нападающему понадобится разрушить:

- все существующие копии пиратской цепи;
- все копии основной цепи Комодо;
- сеть безопасности PoW (биткойн), в которую вставлены нотариально заверенные данные Komodo.

Кроме того, нотариальные узлы имеют право переключать процесс нотариального заверения в другую сеть PoW, если сдвиг в хэш-частотах между большими блокировками произойдет в будущем. Delayed Proof-of-Work предоставляет пирату более высокий уровень, чем безопасность биткойна. В то же время, избегая чрезмерных финансовых и эко-недружественных расходов. Благодаря гибкости dPoW он предлагает более гибкий и адаптивный характер, чем сам биткойн.

Примеры атак на блокчейны

Существует ряд примеров, в которых подчеркивается необходимость создания механизма как отложенный Proof-of-Work:

В апреле 2018 года ошибка в механизме перенацеливания алгоритмов в криптовалюте Verge (XVG) была использована для атаки 51%. С помощью поддельных временных меток, потребность в другом алгоритме каждого блока была обойдена. Хакеры смогли отправить блоки в цепочку при скорости добычи 1 блок в секунду, фактически отрицая 99% законных блоков пулов и заставляя их терять деньги (Ocminer 2018a). В мае 2018 года произошла такая же атака, но с другим подходом: хакеры отправили один блок с алгоритмом Scrypt, содержащим поддельную временную метку, за которой следовал блок с алгоритмом Lyra2re содержащий поддельную временную метку и повторяя этот процесс, таким образом, снижая сложность, хакеры смогли добыть несколько блоков в минуту (Ocminer 2018b).
16 мая 2018 года Биткойн Голд подвергся нападению неизвестного актера, которому удалось украсть более 388 000 БТГ с биржи криптовалют, монеты стоили 17,5 миллионов долларов во время атаки (Roberts 2018). В настоящее время NiceHash предлагает более чем достаточно хеш-мощности в аренду, чтобы атаковать несколько криптовалют с малой и средней крышкой. Семестр«Nicehashable» был придуман за способность арендовать хеш для атаки монет и сайты уже появились, чтобы продемонстрировать взлом возможности (EXAKING 2018).

Интеграция и активация Sapling

Саженец (Sapling) интеграция

Интеграция саженцев в пиратскую цепочку была успешной благодаря сотрудничеству между членами экосистемы Komodo, с особой благодарностью Mike Toutonghi из проекта Veruscoin.

Pirate означает быстрые, дешевые и 100% частные транзакции, и Sapling - лучшая версия технологии zk-SNARKS, которая предлагает это. По этой причине использование Sapling с 15 февраля 2019 года и далее необходимо для обеспечения эффективной и частной работы сети. Пользователи, владеющие Pirate, должны перенести свои монеты со своих адресов Sprout на адреса Sapling до этой даты.

Выбор времени для хард-форка для активации Sapling основывался на отметке времени блока 15 декабря, 1:00 UTC. Крайний срок для перехода из Ростка (Sprout) в Саженец был установлен 15 февраля 2019 года, чтобы создать стабильность, срочность и привлечь всех, кто владеет Pirate.
Чем раньше будет выполнен переход, тем лучше ситуация для централизованных обменов и других сторонних приложений.
Jl777c разработал децентрализованное приложение (dApp) под названием «zMigrate», которое автоматически преобразует средства пользователя в адресах Sprout в адрес Sapling, чтобы упростить процесс перехода на Sapling. Все узлы были необходимы для завершения этого процесса к 15 февраля 2019 года, и пулы также перешли на адреса Sapling после хард-форка.

Миграция в Sapling

DApp zMigrate - это отдельная программа, которая взаимодействует с daemon «Komodod». Приложение dApp отправит пиратский адрес (-ы) пользователя Sprout на одноразовый случайный прозрачный адрес с максимальной скоростью 10 тыс. Pirate транзакций. Создается столько одноразовых t-адресов, сколько необходимо для перемещения всех средств, причем последняя транзакция, вероятнее, содержит менее 10 КБ (если средства не делятся на 10 КБ). Следовательно, средства от каждого t-addr отправляются на указанный экранированный адрес Sapling.

Таким образом, пользователь все время контролирует средства, и движение прозрачных средств будет выглядеть как можно более однородным, чтобы снизить ущерб, наносимый цепочке. Результатом этого процесса является то, что все средства пользователя переводятся со старого адреса Sprout на их выбранный адрес Sapling.

Технические улучшения Sapling позволяют разрабатывать следующие функции:

- Интеграция в точках продаж
- Аппаратные кошельки
- Плагины интернет-магазина (быстро)
- Мобильные кошельки с помощью простой проверки платежей (zSPV) (в разработке)

Схема распространеия и технические характеристики

Pirate цепь содержит следующие технические характеристики и особенности после 15 декабря:

- Майнинг algorithm: Equihash Proof-of-Work
- Задержка Proof-of-Work
- Время блокировки: 60 seconds
- Комиссия за транзакцию: 0.0001 ARRR
- Подпись транзакций за секунды
- Транзакций в секунду: 50–80 TPS
- Отправка до 100 адресов за одну транзакцию
- Размер Tx +- 2000 bytes with с макс. 200 kB
- Использование памяти всего 40 МБ (Raspberry Pi)
- Максимальный размер блока 4 мБ
- Просмотр ключей, которые позволяют просматривать все отправленные транзакции по назначенному адресу
- Возможность генерировать «бесконечное» количество «Lite» кошельков

График распространения

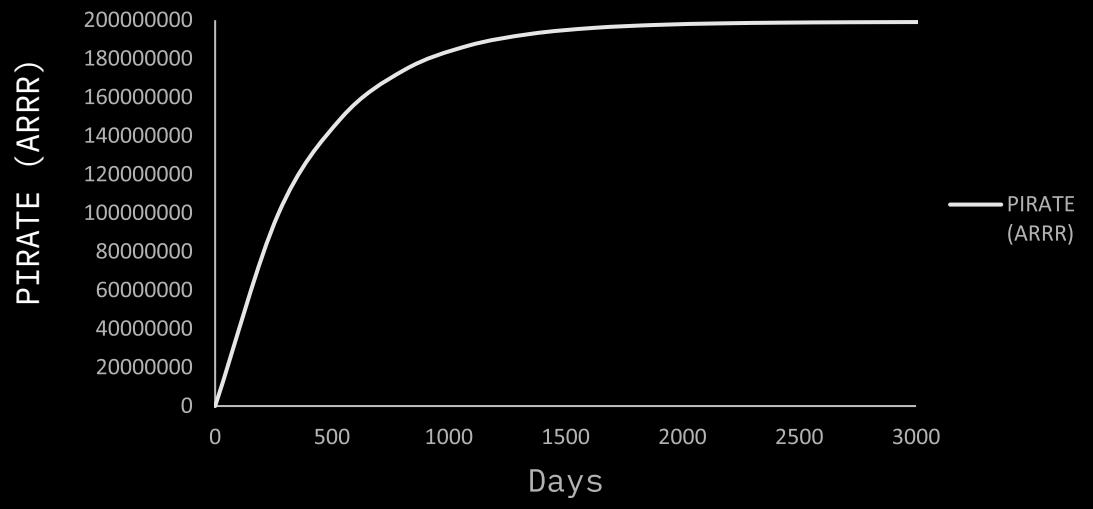

Рисунок 4 График распространения Pirate (ARRR)

Каждые 388885 блоков получают награду за блок в два раза, что соответствует примерно 270 дням за период вознаграждения. Максимальное предложение составляет около 200 миллионов пиратских (ARRR).

Поддержка TOR

Можно запустить сеть Pirate по сети TOR и скрыть ваш IP-адрес, номер которого связан с вашим географическим местоположением. Как пользователь, вам нужен браузер TOR и двоичные файлы Komodo, чтобы иметь возможность запускать цепочку пиратов. Пошаговое руководство доступно на pirate.black. Запрос поддержки TOR передан разработчикам Agama Wallet. После этого настроить Tor для монеты или цепочки активов очень просто.

Поддержка централизованных бирж

Сообщество не было уверено, смогут ли централизованные биржи сначала принять Pirate из-за отсутствия прозрачных адресов. Вскоре после создания Pirate, Pirate работал с разработчиками и кодировщиками бирж, чтобы упростить использование депозитов и выводов по Z-адресу как первого в мире. Эта биржа является DigitalPrice на которой успешно началась торговля в конце октября 2018 года.

Roadmap

Даты следующих функций Pirate и сторонних разработок (таких как Tortuga) являются оценками, основанными на квартальной годовой основе, и перечислены в порядке ожидания.

- TOR browser поддержка 100% Z-адресов — Q3 2018 (Complete)
- Выплаты майнинг пулов для Z-адресов — Q3 2018 (Complete)
- Первый Discord Tip bot — Q3 2018 (Complete)
- Содействие Z-адресам на CEX — Q3 2018 (Complete)
- Paper Wallet — Q4 2018
- Website Rebrand — Q4 2018
- Бортовые рефералы — Q4 2018
- Pirate Lottery Bot — Q4 2018
- Sapling — Q1 2019
- Pirate Фонд — Q1 2019
- Tortuga (CEX) — Q1 2019
- Z Простое Подтверждение оплаты(zSPV) — Q2 2019
- Интеграция аппаратного кошелька — Q3 2019

Гид PIRATE

На борт к Pirate

Купить легко и безопасно небольшое количество ARRR:

https://dexstats.info/onboarding.php

Как майнить- Рассчитайте ваш предполагаемый доход:

https://dexstats.info/piratecalc.php

Начните знакомство :

https://medium.com/piratechain/how-to-mine-pirate-step-by-step-with-gpu-s-4c98f3dbcf5e

Выберите пул, чтобы присоединиться :

https://miningpoolstats.stream/pirate

Следите за хэшрейтом PIRATE:

https://dexstats.info/piratehash.php

Купить и обменять PIRATE

Зарегистрируйтесь в DigitalPrice и обменяйте ARRR на BTC, ETH или KMD:

https://digitalprice.io/?inviter=4fdaf7 (official PIRATE ref. link)

Социальные media

Pirate активен на Bitcointalk, Discord, Medium, Reddit, SteemIt, Telegram, Twitter и включен в статистический веб-сайт CoinPaprika.

https://coinpaprika.com/coin/arrr-pirate/

https://discord.gg/mBZhZgz

https://medium.com/@piratechain

https://www.reddit.com/user/piratechain

https://steemit.com/@piratechain

https://twitter.com/PirateChain

https://t.me/piratechain

https://bitcointalk.org/index.php?topic=4979549.0

Исходный код и кошельки

Github: https://github.com/PirateNetwork

Agama Wallet: https://github.com/KomodoPlatform/Agama/releases

PIRATE GUI wallet: https://github.com/leto/TreasureChest

Рекомендации

Bowe, S. 2017. “Cultivating Sapling: Faster zk-SNARKs--Zcash Blog”. *Zcash Blog*.

EXAKING. 2018. “PoW 51% Attack Cost”. 2018. https://www.exaking.com/51.

Grewal, Satinder. 2018. “Satinder’s notes on the PIRATE chain”. 2018. https://blog.komodoplatform.com/pirates-of-komodo-platform-cdc991b424df.

Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. “Zcash protocol specification”.

Japparova, Irina, en Ramona Rupeika-Apoga. 2017. “Banking Business Models of the Digital Future: The Case of Latvia”. *European Research Studies* 20 (3A). Professor El Thalassinos: 846.

Jl777c. 2016. “Delayed Proof of Work (dPoW) Whitepaper”. Github. 2016. https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper.

Kappos, George, Haaroon Yousaf, Mary Maller, en Sarah Meiklejohn. 2018. “An Empirical Analysis of Anonymity in Zcash”. *arXiv preprint arXiv:1805.03180*.

Komodostats. 2018. “Asset Chains Notarizations Summary”. 2018. https://komodostats.com/acs.php.

Lee, James. 2018. “Komodo: An Advanced Blockchain Technology, Focused on Freedom.” Komodo. 2018.

Moser, Malte. 2013. “Anonymity of bitcoin transactions”.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system”. Working Paper.

Ocminer. 2018a. “Network Attack on XVG / VERGE”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.0.

———. 2018b. “Network Attack on XVG / VERGE (Page 57)”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.msg38135174#msg38135174.

PTY X. 2018. “What is a Parallel Chain (Asset Chain)?” Komodo Platform. 2018. https://komodoplatform.atlassian.net/wiki/spaces/KPSD/pages/71729160/What+is+a+Parallel+Chain+Asset+Chain.

Quesnelle, Jeffrey. 2017. “On the linkability of Zcash transactions”. *arXiv preprint arXiv:1712.01210*.

Roberts, Jeff John. 2018. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’”. FORTUNE. 2018. http://fortune.com/2018/05/29/bitcoin-gold-hack/.

Saberhagen, Nicolas Van. 2013. “CryptoNote v 2.0”.

Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, en Madars Virza. 2014. “Zerocash: Decentralized anonymous payments from bitcoin”. In *2014 IEEE Symposium on Security and Privacy (SP)*, 459–74.