По вопросу невозможности создания форков Monero

Димаз Анкаа Виджая (Dimaz Ankaa Wijaya)*
Университет Монаша
Мельбурн, Австралия
dimaz.wijaya@monash.edu

Джозеф К. Лю+
Университет Монаша
Мельбурн, Австралия
joseph.liu@monash.edu

Рон Штейнфельд
Университет Монаша
Мельбурн, Австралия
ron.steinfeld@monash.edu

Донси Лю
Data61, CSIRO
Сидней, Австралия
dongxi.liu@data61.csiro.au

Цзяншань Ю
Университет Монаша
Мельбурн, Австралия
jiangshan.yu@monash.edu

АННОТАЦИЯ

Monero, по рыночной капитализации являющаяся одной из лучших криптовалют, ориентированных на обеспечение приватности, реализовала регулярный полугодичный хардфорк в 2018 году. Несмотря на то, что хардфорк и не является таким уж редким событием в криптовалютной индустрии, два хардфорка, совершённые в 2018 году, представляли собой определённый риск для анонимности Monero, поскольку транзакции стали отслеживаемыми из-за возникновения возможности повторного использования ключей. Данная проблема была вызвана появлением нескольких копий одной и той же монеты в разных ветвях блокчейна Monero, в результате чего пользователи смогли тратить монеты несколько раз, не совершая каких-либо предварительных действий. Мы провели исследование хардфорков Monero, проанализировав данные транзакций из трёх различных ветвей блокчейна Monero. Несмотря на то, что нами было обнаружено лишь незначительное количество отслеживаемых входов, если сравнивать с общим количеством входов в доступном нам наборе данных, проведённый анализ показывает, что масштабируемость события зависит от внешних факторов, таких как рыночная цена и доступность рынка. Нами предлагается экономически доступная и простая в реализации стратегия предотвращения возможности повторного использования ключей, если в будущем на рынке будут реализованы более сильные форки Monero.

КОНЦЕПЦИИ CCS

Безопасность и приватность → Псевдонимность, анонимность и неотслеживаемость.

КЛЮЧЕВЫЕ СЛОВА

Monero, повторное использование ключей, хардфорк, отслеживаемость, анонимность, кольцевая подпись, криптовалюта

Формат ACM:

Димаз Анкаа Виджайя, Джозеф К. Лю+, Рон Штейнфельд, Донси Лю и Цзяншань Ю. 2019. По вопросу невозможности создания форков Monero Материалы Азиатской конференции ACM по компьютерной безопасности и защите коммуникаций (AsiaCCS '19), 9–12 июля 2019 года, Окленд, Новая Зеландия. ACM, Окленд, Новая Зеландия, 12 страниц. https://doi.org/10.1145/3321705.3329823

* Также сотрудничает с Data61, CSIRO, Мельбурн, Австралия. + Соответствующий автор.

AsiaCCS '19, 9–12 июля 2019 г., Окленд, Новая Зеландия
2019 Ассоциация вычислительной техники.
ACM ISBN 978-1-4503-6752-3/19/07. . . 15,00 USD
https://doi.org/10.1145/3321705.3329823

1 ВВЕДЕНИЕ

Криптовалюта стала глобальным феноменом. Первая в своём роде, Bitcoin, была создана Сатоши Накомото [22]. Проект Bitcoin стартовал 3 января 2009 года как одноранговая платёжная система, использующая общий реестр под названием блокчейн, в рамках которого метод консенсуса обеспечивал отсутствие контроля какой-либо централизованной стороной. В опубликованном документе Сатоши описывает Bitcoin как анонимную валюту, при использовании которой никакая информация не позволит связать публичные ключи с реальной личностью их владельцев [22]. Тем не менее анонимности публичных ключей недостаточно для защиты приватности пользователей. Исследователями были разработаны различные методы анализа, позволяющие раскрыть информацию, связанную с пользователями, на основе внешних источников [18]. Данные прозрачного блокчейна также использовались для построения шаблонов транзакций, позволяющих идентифицировать поведение пользователей [27].

В области приватности блокчейнов было проведено множество исследований, в рамках которых криптовалютные проекты, ориентированные на обеспечение приватности, такие как Monero, пытались решить проблему. Monero является одной из наиболее успешных криптовалют, обеспечивающих приватность пользователей, и, по данным Coinmarketcap.com, является одной из наиболее ценных монет. В основе Monero лежит протокол CryptoNote [34], гарантирующий неотслеживаемость отправителя и невозможность привязки отправителя с помощью криптографических методов, таких как связываемая кольцевая подпись (LRS) и одноразовый публичный ключ (OTPK), которые делают транзакции более анонимными, если сравнивать с другими криптовалютами, такими как Bitcoin [34]. Несмотря на реализацию функций обеспечения анонимности, результаты исследований показали, что транзакции Monero всё же можно отследить из-за наличия транзакций с нулевым количеством миксинов [14, 21].[1]

В рамках экосистемы блокчейна форк — это событие, при котором изменяется протокол [40]. Замятин и др. в работе [40] классифицировали возможные изменения следующим образом: расширение протокола, его сокращение, возникновение конфликта (двустороннее) и условное сокращение (бархатный форк). По сути, существует два типа форка блокчейна, а именно хардфорк и софтфорк. Хардфорк связан либо с расширением протокола, либо с двусторонним конфликтом, который приводит к разделению блокчейна или разделению цепочки. Софтфорк, включая сокращение протокола и бархатный форк, не приводит ни к какому разделению цепочки [40].

Форк блокчейна в случае с криптовалютами, как правило, приносит пользователям финансовую выгоду [26]. Например, до форка Bitcoin Cash у пользователя был один Bitcoin. После того как произойдёт форк, тот же пользователь удвоит свои деньги: один Bitcoin в оригинальном блокчейне и один Bitcoin Cash во вновь созданной ветви блокчейна. Цена Bitcoin составляла 2808 USD (свободная цена), в то время как Bitcoin Cash торговался по курсу 555,89 USD (свободная цена), поэтому пользователь получил монету стоимостью 555,89 USD за каждый Bitcoin, который у него имелся, ничего при этом не делая.[2][3]

В целях обновления своей системы Monero регулярно и интервалом один раз в полгода производит хардфорк. Хардфорки Monero в основном направлены на улучшение решений, связанных с обеспечением приватности. Однако Monero также стремится защитить криптовалюту от майнинга посредством ASIC. То есть разработчики программного обеспечения, по сути, препятствуют разработке машин на базе ASIC, которые могли бы участвовать в майнинге Monero, пользуясь существующим механизмом доказательства работы (PoW) [6, 34]. Именно с этой целью 6 апреля 2018 года проект Monero обновил алгоритм майнинга, сведя таким образом на нет эффективность уже существующих машин на базе ASIC. При обновлении протокола с версии 6 до версии 7 появился новый форк Monero.

Хардфорк произошёл из-за несовместимости двух версий протокола. Седьмая версия протокола вступила в силу начиная с блока номер 1 546 000, который был добавлен 6 апреля 2018 года. Но осталось несколько независимых сторон, которые заявили, что по-прежнему хотят использовать шестую версию протокола. Эти независимые стороны переименовали блокчейн-систему, работающую в соответствии с шестой версией протокола Monero, присвоив ей три разных названия:

1 На 26 октября 2018 года общая рыночная капитализация Monero составляла 1,7 миллиарда USD.

2 https://coinmarketcap.com/currencies/bitcoin/historicaldata/?start=20170723&end=20170723

3 https://coinmarketcap.com/currencies/bitcoin-cash/historicaldata/?start=20170723&end=20170723

Monero Original (XMO), Monero 0 (Monero Zero или ZMR) и Monero Classic (XMC) [19]. Несмотря на наличие трёх разных названий, на самом деле существует только один блокчейн [2]. После хардфорка Monero от седьмой версии Monero ответвился ещё один проект под названием MoneroV (XMV). Это случилось 3 мая 2018 года на высоте блока 1 564 966. MoneroV использует модифицированный вариант седьмой версии протокола. Одно из отличий протокола MoneroV от протокола Monero седьмой версии состоит в уменьшении количества десятичных знаков с 12 до 11. В результате номинал монет умножается на десять. История форка показана на рисунке 1.[4][5]

Рисунок 1. График хардфорка Monero, на котором показаны сразу два хардфорка, в результате которых к октябрю 2018 появилось сразу три новых блокчейна.

Подобно тому как это происходило в случае с другими форками, пользователи Monero удваивали количество своих монет Monero с каждым форком, получая ту же или даже большую сумму во вновь создаваемых криптовалютах. Тем не менее, если пользователи используют те же монеты, не приняв дополнительных мер предосторожности, уровень анонимности транзакций потенциально может снизиться. При реализации хардфорка Monero может возникнуть проблема, связанная с отслеживаемостью. При хардфорке создаются новые монеты, которые смогут потратить пользователи, существовавшие ещё до форка. И проблема возникает в том случае, если пользователи Monero тратят вновь созданные монеты таким образом, что появляется возможность отслеживания отправителя. Мы называем это проблемой повторного использования ключей. Повторное использование ключей снижает уровень анонимности транзакции из-за того, что пользователи повторно используют одни и те же ключи при трате одних и тех же монет. Данная проблема отслеживаемости известна разработчикам Monero [6], которые отмечали, что существующих стратегий недостаточно, чтобы полностью избежать этой проблемы.

Наш вклад. Наш вклад в рамках данной работы заключается в следующем:

- Нами исследуются последствия двух хардфорков Monero, случившихся в 2018 году. Для выявления отслеживаемых входов нами были собраны данные каждой ветви блокчейна, а затем совместно проанализированы данные транзакций из этих ветвей блокчейна. Нами было обнаружено более 55 000 чётко отслеживаемых входов, при этом 90% из них принадлежали двум ветвям блокчейна, поддерживающим шестую и седьмую версии протокола. Примерно 19% всех входов из нашего набора данных, принадлежащих шестой версии протокола Monero, оказались отслеживаемыми. Однако в седьмой версии (или основной ветви) процент отслеживаемых входов относительно общего количества входов был незначительным. В отличие от существующих видов атаки [14, 21, 35, 37, 39] решение задачи повторного использования ключей позволяет идентифицировать отслеживаемые входы в рамках протокола RingCT Monero. Ни один из выявленных нами отслеживаемых входов нельзя обнаружить путём проведения существующих видов атаки.
- Нами была проанализирована взаимосвязь между выявленными отслеживаемыми входами и биржевым курсом. Для этого мы воспользовались методом статистического анализа, а именно определением коэффициентов корреляции и линейной регрессии. Результаты определения коэффициентов корреляции демонстрируют наличие в Monero6 сильной корреляции (от 0,553 до 0,761) между двумя факторами, в то время как в случае с MoneroV корреляция довольно слаба (от 0,242 до 0,32). Подобным образом результаты линейной регрессии демонстрируют среднее соотношение в Monero6, но слабое соотношение в MoneroV. Более значительная поддержка Monero6 со стороны криптовалютных бирж, если сравнивать с MoneroV, также объясняет огромную разницу между количеством отслеживаемых входов в обеих ветвях блокчейна. Полученные нами результаты подтверждают, что масштабируемость проблемы повторного использования ключей зависит от указанных внешних факторов.
- Нами предлагается стратегия решения проблемы повторного использования ключей, причиной которой являются хардфорки Monero. Масштабируемые фильтры Блума [1] являются недорогим механизмом проверки существующих образом ключей и миксинов. При добавлении механизма проверки до передачи новой транзакции в сеть транзакции, в

4 https://github.com/monero-project/monero

5 https://github.com/monerov/monerov

которых тратятся одни и те же монеты, будут поддерживать одинаковый уровень анонимности. Нами предлагается реализация нового сервисного узла, называемого объединённым узлом, обеспечивающего стратегию решения проблемы в рамках текущего протокола Monero без внесения каких-либо серьёзных изменений.

Структура документа. Оставшаяся часть статьи имеет следующую структуру. В Разделе 2 содержится описание технической основы связываемых кольцевых подписей (LRS) и протокола Monero. В Разделе 3 приводится информация о работе, проделанной в отношении известных атак на существующие механизмы обеспечения анонимности Monero, описана альтернативная стратегия реализации хардфорков, а также защита от повторной передачи перехваченных сообщений. Модель угрозы представлена в Разделе 4. В Разделе 5 описаны использованные нами методы анализа. Раздел 6 посвящён существующим на данный момент стратегиям решения указанных проблем, равно как и предлагаемой нами стратегии, которая также включена в данный раздел. В Разделе 7 рассматриваются вопросы, связанные с безопасностью и эффективностью предлагаемой стратегии, а в заключительном Разделе 8 — достигнутые результаты и будущая работа.

1 ОСНОВЫ

1.1 Связываемая кольцевая подпись

Связываемая кольцевая подпись (LRS) [15, 16] была разработана на основе технологии кольцевой подписи (RS). LRS обеспечивает пользователя всеми преимуществами RS. В случае с RS подписанта нельзя идентифицировать среди ряда потенциальных подписантов, даже если подписант создаёт множество подписей. Однако в случае с LRS создатель подписи может создать только одну подпись для каждого имеющегося у него приватного ключа, если хочет сохранить анонимность подписи. В LRS используется система тегов. Если один и тот же подписант для создания более чем одной подписи решит повторно использовать один и тот же приватный ключ, верификатор сможет связать такие подписи и определить, что они были созданы с помощью одного приватного ключа, поскольку во всех подписях будет присутствовать один и тот же тег. Поскольку такой тег будет известен исключительно подписанту, это будет подразумевать, что подписи созданы одним и тем же лицом. LRS ограничивает анонимность RS. Тем не менее данное ограничение оказывается полезным в ряде сценариев, таких как электронное голосование [5, 38] и криптовалютные системы [31], где возможность двойного голосования или двойной траты монеты должна быть исключена.

1.2 Структура и протокол транзакций Monero

Структура транзакций Monero показана на рисунке 2. Вход I содержит кольцевую подпись R с набором выходов O размера r. Набор выходов O содержит выход, который будет потрачен, и $r-1$ ложных выходов. Ложные выходы, как правило, выбираются случайным образом из публичного блокчейна B, и вероятность того, что реально расходуемый выход будет угадан, составляет не более $\frac{1}{r}$. При проведении транзакции Monero может быть создано от нуля до нескольких выходов, которые затем будут добавлены в базу данных выходов в блокчейне B. Эти новые выходы можно будет потратить, или же они будут выбраны в качестве ложных при создании последующих транзакций.

Рисунок 2. Конструкция транзакции Monero, состоящая из входов и выходов. При проведении транзакции ряд входов, содержащий множество существующих выходов, создаёт ряд новых выходов.

Каждый выход O в блокчейне B непосредственно связан с одним секретным ключом, называемым образом ключа. Чтобы потратить выход o_i требуется опубликовать образ ключа k_i. Тем не менее при использовании схемы кольцевой подписи, содержащей ряд из r выходов $\{o_1, o_2, \ldots, o_i, \ldots, o_r\}$, выход o_i невозможно отличить от ложных. Один и тот же выход нельзя потратить дважды в одном блокчейне. Чтобы данное правило работало, связанный с расходуемым выходом

образ ключа k_i сохраняется в блокчейне. Если в новой транзакции будет повторно использован тот же образ ключа k_i, система обнаружит попытку двойной траты и отклонит новую транзакцию.

2 СВЯЗАННЫЕ РАБОТЫ

2.1 Анализ отслеживаемости Monero

Monero использует технологии обеспечения анонимности, что выделяет эту криптовалюту среди прочих, таких как Bitcoin. Технология связываемой кольцевой подписи (LRS) не позволяет отследить отправителя. Технология кольцевой конфиденциальной транзакции (RingCT) [23] применяется для шифрования суммы монет, передаваемых плательщиком получателю. Одноразовые публичные ключи (OTPK) не позволяют привязать транзакцию к получателю, так как отправителю приходится создавать новый адрес назначения при проведении каждой новой транзакции за получателя [34].

Несмотря на то, что вышеуказанные механизмы были реализованы, исследователями были разработаны методы анализа, позволяющие выявить отслеживаемые входы. LRS использует в подписи ложные выходы (также называемые миксинами), что не даёт обнаружить реального подписанта. Результаты анализа свидетельствуют о том, что транзакции с нулевым количеством миксинов лишаю отправителя неотслеживаемости [14, 21]. Несмотря на то, что эта проблема была решена исправлением, в результате которого было запрещено создавать транзакции без мискинов, исследователями были выявлены новые способы отследить отправителя посредством специально создаваемых транзакций [35, 37] или идентификаторов платежа Monero [37]. Для выявления потраченных монет Monero был предложен вариант атаки с использованием закрытого набора выходов [39].

2.2 Бархатный форк

Бархатный форк — термин, придуманный Киаисом и др. [12]. В отличие от хардфорка, являющегося рискованным предприятием, бархатный форк предлагает новую стратегию, при реализации которой при смене протокола переменные заменяют постоянные параметры. Бархатный форк позволяет избежать хардфорка. Все прошлые случаи бархатного форка подробно исследовались [40].

Несмотря на то, что бархатный форк позволяет не производить хардфорк, меняющий параметры, он совершенно бесполезен при внесении изменений на уровне протокола. Если технологию бархатного форка применить к Monero, то увеличить размер кольца будет проще путём изменения подготовленной переменной, содержащей значение размера кольца. Тем не менее такие изменения на уровне протокола, как смена метода выбора ложных выходов, добавление новых свойств подписи [30] или изменение метода консенсуса [6], нельзя будет произвести при помощи бархатного форка.

2.3 Защита от повторного воспроизведения

Защита от повторного воспроизведения является механизмом, не позволяющим провести атаку повторного воспроизведения. В контексте криптовалют термин «атака повторного воспроизведения» подразумевает повторную передачу данных действительной криптовалютной транзакции в другие совместимые форки криптовалюты [17]. В результате проведения атаки повторного воспроизведения получатель принимает множество платежей в различных криптовалютах, а отправитель терпит убыток. В работе Маккори и др. [17] приводится несколько примеров защиты от повторного воспроизведения, реализованной различными криптовалютными проектами: использование идентификаторов блокчейна, версии транзакции, проверка высоты блока и метод Sighash Enum.

Идентификаторы блокчейна были реализованы Ethereum после хардфорка Spurious Dragon [4], в то время как проверка версии транзакции, высоты блока и метод Sighash Enum были предложены в качестве альтернативных решений защиты от повторного воспроизведения Bitcoin [17]. Также было предложено использовать новые методы: вход миграции и оракул хардфорка [17]. Вход миграции

предлагалось реализовать в рамках протокола Bitcoin, при этом размер хеша входа изменился бы с 32 до 41 байта, чтобы в него можно было включить дополнительную информацию. При использовании иной схемы хеша входа старый протокол не позволял производить валидацию транзакций, а следовательно, для этого требовался новый совместимый протокол [17]. Оракул хардфорка было предложено реализовать в качестве смарт-контракта Ethereum, который бы использовался для автоматического обнаружения транзакций из других форков.

В настоящее время протокол Monero не предусматривает защиты от повторного воспроизведения [25]. Одним из способов создания транзакции со встроенным механизмом защиты от повторного воспроизведения является включение в неё по крайней мере одного выхода, который можно найти только в определённом блокчейне в качестве ложного выхода, включаемого в кольцевую подпись [32].

2.4 **Атаки на обновляемые версии протокола Monero**

Асинхронное обновление протокола (то есть хардфорк) Monero также может стать причиной проведения атак [36]. Исследование показало, что узлы, не обновившие свои приложения до последней версии (что подразумевает использование последней версии протокола), уязвимы к проведению DoS-атаки (то есть отказу в обслуживании), когда для переполнения временного пула хранения транзакций создаётся огромное количество транзакций.

Кроме того, DoS-атака может использоваться для «сообщении» об отслеживаемости входов публике путём передачи двух разных транзакций, в которых будет потрачена одна и та же монета. Одна транзакция может быть отправлена старым узлам (использующим старую версию протокола), а другая — новым узлам (уже использующим новую версию протокола). При соблюдении обязательного условия в сети транзакции, переданные старым узлам, никогда не будут подтверждены сетью, а следовательно, двойной траты не произойдёт. Тем не менее, поскольку две монеты дважды появятся у различных узлов (использующих разные версии протокола), можно будет определить реальные входы соответствующих транзакций.

3 **МОДЕЛЬ УГРОЗЫ**

Обеспечение неотслеживаемости Monero требует, чтобы внешний наблюдатель не смог угадать реальный выход, который тратится в кольцевой конструкции R с вероятностью выше $\frac{1}{r}$, где r является количеством участников кольца. В этом случае анонимность реального входа будет зависеть от размера r.

Мы утверждаем, что вход I_j можно отследить по выходу 0_j в следующем случае. Выход 0_j является выходом из блокчейна B_1 с рядом выходов $\{i, o_a, i, \ldots, i, i, o_j, i, i, \ldots, i, i, o_t, i\}^{O_1}_{i}$, используемых в качестве участников кольца, и таким образом ключа k_j, что R_1, k_j и O_1 будут частями I_j. Тот же выход 0_j появляется в другом блокчейне B_2 и включается в другую связываемую кольцевую подпись R_2 с рядом выходов $\{i, o_m, i, i, \ldots, i, i, o_j, i, i, \ldots, i, i, o_z, i\}^{O_2}_{i}$ и образом ключа k_j. После этого можно прийти к заключению, что образ ключа k_j связан с выходом 0_j. Следовательно, вход I_j можно отследить по выходу 0_j, поскольку вероятность определения реального выхода составляет 1. Данная ситуация также соответствует условию связываемости, описанному в работе по связываемым кольцевым подписям [16], из-за возможности заключения, что кольцевые подписи R_1 и R_2 были созданы одним и тем же лицом, а значит, учитывая, что секретный образ ключа k_j известен только владельцу.

Снижение уровня анонимности происходит, если q участников кольца R можно проследить, так как они более не могут рассматриваться в качестве реального выхода, а следовательно, анонимный ряд r сокращается на q. Мы определяем вход со сниженным уровнем анонимности I_i как вход, принадлежащий блокчейну B_1 и используемый в связываемой кольцевой подписи R_3 с размером кольца r, рядом выходов $\{i, o_b, i, \ldots, i, i, o_a, i, i, \ldots, i, i, o_i, i, i, \ldots, i, i, o_m, i\}^{O_3}_{i}$ и образом ключа k_h. Тот же образ ключа k_h можно найти в кольцевой подписи R_4, записанной в другом блокчейне B_2 с набором выходов

, где по крайней мере два выхода (o_e, o_i) из R_4 будут соответствовать следующим критериям: $\{o_e, o_4\}$ и $\{o_e, o_3\}$. В рамках данного сценария нельзя прийти к заключению, что образ ключа k_h связан с o_e или o_i. Пример отслеживаемого выхода и снижения уровня анонимности приводится на рисунке 3.

Рисунок 3. Входы I_1 и I_3 имеют следующие общие особенности: образ ключа k_1 и выход o_4. Оба входа I_1 и I_3 можно отследить. Входы I_2 и I_4 содержат один и тот же образ ключа k_2, а также два идентичных выхода в кольце: o_7 им o_{10}. Уровень анонимности обоих входов I_2 и I_4 снижен на три.

В случае с Monero нами определяются пассивный и активный виды атаки. При проведении пассивной атаки злоумышленник собирает информацию из публичного блокчейна (блокчейнов) и проводит анализ отслеживаемости. При проведении активной атаки под контролем злоумышленника находятся вредоносные узлы, выдающие ложную информацию. Выдавая ложные ответы на запросы, связанные с образами ключей, вредоносные узлы пытаются снизить уровень анонимности клиента в результате повторного использования ключей, особенно если клиент тратит одни и те же монеты в разных блокчейнах.

Мы допускаем, что все те, кто имеет отношение к криптовалютам, включая разработчиков программного обеспечения, членов сообщества и рядовых пользователей, желают, чтобы их системы имели самые лучшие механизмы обеспечения приватности. Однако есть и такие пользователи, которые, сами того не зная, тратят идентичные монеты во множестве блокчейнов, делая соответствующие транзакции отслеживаемыми. Это вызывает «каскадный эффект», в результате которого и другие транзакции становятся отслеживаемыми или страдают от снижения уровня анонимности [21]. Также предполагается, что большинство узлов в системе являются честными и выдают правильные ответы на любые запросы.

Помимо прочего, предполагается, что в существующую систему можно внести лишь минимальные изменения, которые не окажут влияния на работу протокола в целом. Тем не менее также допускается, что в любой момент может быть реализован хардфорк, и не потраченные до форка монеты после него будут потрачены множество раз в разных блокчейнах. Хардфорки финансово мотивированы, так как вновь создаваемые монеты можно будет продать на рынке.

4 ПРОВЕДЁННЫЙ АНАЛИЗ

4.1 Анализ отслеживаемых входов

Нами были собраны данные всех транзакций из трёх разных блокчейнов, которые мы назвали, Monero6, Monero7 и MoneroV. Мы использовали термин Monero6 для тех криптовалют, что используют шестую версию протокола Monero: Monero Original, Monero 0 и Monero Classic. Monero7 мы обозначили основной блокчейн Monero, использующий седьмую версию протокола (по состоянию на октябрь 2018). Термин MoneroV говорит сам за себя и относится к блокчейну, использующему протокол MoneroV.

Алгоритм проверки выглядел следующим образом:

1 Создание множества K_{res} для хранения указанных образов ключей в качестве конечного результата.

2 Выполнение следующих шагов для каждого образа ключа k_i:

   a Вычисление общего количества появления во всех трёх блокчейнах и сохранение результата в переменной c_i.

   b Вычисление количества уникальных хешей транзакций (h_i) и сохранение результата в другой переменной u_i.

   c Построение условного утверждения: если $(c_i = 1)$ и $(u_i = 1)$, значит, $k_i \in K_{res}$. Условное утверждение необходимо, чтобы отфильтровать случаи повторного

воспроизведения ключей, так как они не помогут в идентификации реального расходуемого выхода.

1 Получение K_{res}.

С помощью приведённого выше алгоритма нами было изучено три блокчейна и создана база данных, что было сделано путём выделения не являющихся coinbase транзакций (транзакций, в которых не выплачивалось вознаграждение за добавление блока), подтверждённых на высоте блока от 1 546 000 до 1 675 606 в Monero6 (период, составляющий 181 день), на высоте блока от 1 546 000 до 1 675 303 в Monero7 (период, составляющий 181 день) и на высоте блока от 1 564 966 до 1 671 617 в MoneroV (период, составляющий 152 дня). Крайней датой выборки данных было задано 4 октября 2018. Также нами был проведён анализ каскадного эффекта, целью которого стало определение количества отслеживаемых входов в результате повторного использования ключей в рамках одного и того же набора данных. Результаты приводятся в таблице 1.

Блокчейн	Высота	Повторное использование ключей		Каскадный эффект		Набор данных	
		Кол-во отслеживаемых входов	Кол-во транзакций	Кол-во отслеживаемых входов	Кол-во транзакций	Кол-во входов	Кол-во транзакций
Monero6	1 675 606	52 646	3148	278	276	274 131	44 467
Monero7	1 675 303	53 162	5680	315	312	1 876 341	810 409
MoneroV	1 671 617	7542	888	0	0	269 335	84 053

Таблица 1. Количество отслеживаемых входов, появившихся в результате повторного использования ключей и каскадного эффекта.

С помощью разработанного нами алгоритма в Monero6 было обнаружено 52 924 отслеживаемых входа (включая те входы, которые были обнаружены методом каскадного эффекта), в Monero7 — 53 477 отслеживаемых входа и всего 7542 отслеживаемых входа в MoneroV. Несмотря на то, что разница между периодами MoneroV и двух других блокчейнов, Monero6 и Monero7, составляла всего 29 дней, количество отслеживаемых входов, выявленных в MoneroV, составило лишь 14% от количества отслеживаемых входов, обнаруженных в Monero6 и Monero7. Также наблюдалась большая разница между количеством не являющихся coinbase транзакций в блокчейне MoneroV и блокчейнах двух других криптовалют. В случае Monero7 оно составило 810 409 транзакций, в то время как в блокчейнах Monero6 и MoneroV процент составил всего 5% и 10% от количества таких транзакций в Monero7, соответственно.

Количество отслеживаемых входов в Monero6 составило 19% от общего количества входов Monero6 в нашем наборе данных, в то время как количество отслеживаемых входов Monero7 и MoneroV составило лишь 2% от их общего количества входов. Это свидетельствует о том, что проблема повторного использования ключей стоит более остро в случае с Monero6, чем с Monero7 и MoneroV. Также примерно 90% всех отслеживаемых входов приходится на блокчейны Monero6 и Monero7, в то время как всего 6% было обнаружено во всех трёх ветвях блокчейна. Это говорит о том, что Monero6 представляет собой более серьёзный источник проблемы повторного использования ключей для Monero7, чем MoneroV для Monero7.

1.1 **Анализ снижения уровня анонимности**

Нами также был изучен побочный эффект появления отслеживаемых входов и каскадного эффекта, заключающийся в снижении уровня анонимности. Вход с размером кольца r страдает от снижения уровня анонимности, если самое большее $\frac{r}{2}$ участников кольца были идентифицированы как потраченные в других транзакциях. Даже при сниженном уровне анонимности реальный выход по-прежнему будет нельзя отследить. Однако вероятность того, что реальный выход будет угадан, возрастает с $\frac{1}{r}$ до $\frac{1}{r-u}$, где $\frac{1}{r} \leq \frac{1}{r-u} \leq \frac{1}{\frac{r}{2}}$, а u является тем количеством выходов, которые были идентифицированы как потраченные в других транзакциях.

В Monero6 нами было обнаружено 1848 входов со сниженным уровнем анонимности. Подобным образом в Monero7 было выявлено 2819 таких входов, а в MoneroV 264 кольцевые подписи страдали от снижения уровня анонимности, но всё же оставались неотслеживаемыми. На

рисунке 4 продемонстрирована тенденция снижения анонимности во всех трёх ветвях блокчейна. Приблизительно в 95% случаев снижения уровня анонимности размер $_{u}$ сокращался в пределах от 1 до 5.

Полученный результат свидетельствует о том, что транзакции, размер кольца которых равен 5 или меньше, являются более рискованными, чем те, размер кольца которых больше 5. Нами был вычислен средний размер кольца для трёх ветвей блокчейна, начиная с первого блока форка и заканчивая окончательной точкой выбранного периода, то есть 4 октября 2018 года. Средний размер кольца $_{r}$ Monero6, Monero7 и MoneroV составил 5,07, 7,56 и 7,75, соответственно. Больший размер кольца обеспечивает более высокий уровень защиты анонимности входа, даже несмотря на то, что создание транзакции с большим размером кольца может привести к росту размера комиссии, которую должен будет выплатить пользователь. Закрепление большего минимального размера кольца на уровне протокола также гарантирует достаточный уровень анонимности транзакций пользователей. Несмотря на то, что минимальный размер кольца в случае с Monero6 был равен пяти, а у Monero7 и MoneroV семи, на основе результатов можно рекомендовать устанавливать размер кольца ≥ 5 .

Рисунок 4. Снижение уровня анонимности в результате повторного использования ключей в Monero6, Monero7 и MoneroV.

1.2 Анализ корреляции повторного использования ключей и изменения цен на криптовалютном рынке

Мы взяли с Coinmarketcap.com исторические данные цены Monero Classic и Monero Original (за период с 20 апреля 2018 по 3 октября 2018), а данные цены MoneroV были взяты с Coingecko.com (за период с 4 июля 2018 по 3 октября 2018). Также мы вычислили статистические данные рыночной цены Monero Classic, Monero Original и MoneroV. Соответствующие цены приводятся в таблице 2. Мы выяснили, что несмотря на то, что цена Monero Classic и Monero Original в среднем составляла 4 USD (самая низкая составила 1 USD, а максимальная — 27 USD), средняя цена MoneroV была крайне низкой, то есть 0,06 USD (самая низкая составила 0,02 USD, а самая высокая — 0,26 USD). Если цену MoneroV умножить на десять, то в среднем она составит всего 0,06 USD, в то время как средняя цена Monero Classic и Monero Original будет в семь раз выше.

На основе информации о цене Monero Classic (высокой, низкой и при закрытии торгов), Monero Original (высокой, низкой и при закрытии торгов) и MoneroV (высокой, низкой и при закрытии торгов) мы изучили корреляцию между рыночными ценами и количеством отслеживаемых входов, а также количеством транзакций путём вычисления коэффициента корреляции Кендалла «тау-b» и коэффициента корреляции Спирмена «ро». Результаты приводятся в таблице 3.

Коэн, которого цитируют Сауро и Льюис в работе [28], предлагает три варианта интерпретации коэффициента корреляции $_{r}$: $_{r}$ является малым, если $0,1 \leq$, средним, если $0,3 \leq$, и высоким, если $\geq 0,5$. Полученные нами результаты демонстрируют, что все коэффициенты в случае с Monero Classic и Monero Original находятся в диапазоне 0,557 и 0,754, что указывает на сильную корреляцию между ценой и повторным использованием ключей в Monero Classic и Monero Original. С другой стороны, согласно результатам, можно отметить низкий уровень корреляции между ценой и повторным использованием ключей MoneroV, где соответствующие коэффициенты составляют 0,242 и 0,32. На основе такой информации мы приходим к выводу, что рыночная цена и количество отслеживаемых выходов коррелируют, несмотря на то, что причинную зависимость между этими двумя параметрами невозможно определить на основе проведённого статистического анализа.

Результаты линейного регрессионного анализа приводятся на рисунке 5. В случае с Monero Classic, Monero Original и MoneroV значения коэффициента детерминации составляют 0,180, 0,146 и 0,003, соответственно. Результат указывает на среднее отношение между количеством отслеживаемых входов и рыночной ценой Monero Classic и Monero Original, но слабым отношением двух переменных в случае MoneroV.

1.3 Анализ связи проблемы повторного использования ключей и доступности монеты

На момент написания данной работы на криптовалютном портале Coinmarketcap.com Monero Classic (XMC) и Monero Original (XMO) рассматривались как две разные монеты, несмотря на то что в реальности эти две криптовалюты находятся в одной ветви блокчейна. Каждая из этих криптовалют торговалась на различных криптовалютных рынках. Monero Classic[6] торговалась на следующих биржах:

- Gate.io (пара XMC/USDT и пара XMC/BTC)
- HitBTC (пара XMC/BTC, пара XMC/USDT и пара XMC/ETH)
- TradeOgre (пара XMC/BTC)

С другой стороны, торговля Monero Original была доступна только на HitBTC (пара XMO/BTC, пара XMO/ USDT и пара XMO/ETH). Торговля монетами из другого форка Monero, MoneroV (XMV), была доступна только на TradeOgre (пара XMV/BTC). По состоянию на 4 апреля 2018 года, за два дня до форка Monero6, шестью самыми востребованными криптовалютными биржами, поддерживающими торговлю Monero, были HitBTC, Binance, Bitfinex, Poloniex, Kraken и Livecoin. Они обеспечивали 84,8% от общего торгового оборота Monero [37]. Среди шести обменников у HitBTC была самая большая доля, составлявшая 37,68%, в то время как у Litecoin самая низкая — 3,82%. Несмотря на то, что информация о торгах на TradeOgre перед форком Monero недоступна, всё равно можно уверенно говорить о том, что большинство криптовалютных рынков не поддержали MoneroV, а следовательно, пользователи Monero так и не смогли приобрести MoneroV на криптовалютных биржах. В то же время, поскольку Monero6 поддерживалась такими большими биржами, как HitBTC, можно допустить, что то количество монет Monero6, которое получили пользователи, было больше, чем в случае с MoneroV.

Доступность криптовалюты на рынке, пожалуй, является одним из факторов, благодаря которым количество отслеживаемых входов MoneroV составило всего 14,3% от количества отслеживаемых входов Monero6. Тем не менее невозможно определить, сколько монет было потрачено в отслеживаемых входах, так как был реализован протокол RingCT, позволяющий скрыть сумму монет, переводимых в транзакциях.

	Monero Classic				Monero Original				MoneroV	
	Свободная	Высокая	Низкая	Окончат.	Свободная	Высокая	Низкая	Окончат.	Свободная	Окончат.
Макс. цена	21,99	27,42	18,02	21,55	21,81	24,36	14,88	20,75	0,26	0,26
Мин. цена	1,20	1,29	1,04	1,20	1,25	1,29	1,22	1,23	0,02	0,02
Сред. цена	4,38	4,84	4,04	4,34	4,24	4,64	3,92	4,21	0,06	0,06

Таблица 2. Рыночная цена Monero Classic, Monero Original и MoneroV.

Рисунок 5. Линейная регрессия количества отслеживаемых входов и рыночной цены Monero Classic (рис. a), Monero Original (рис. b) и MoneroV (рис. c).

	Корреляция	
	Коэффициента Кендалла «tau-b»	Коэффициент Спирмена «ро»
Monero Classic	0,561	0,755
Monero Original	0,557	0,754
MoneroV	0,242	0,32

Таблица 3. Корреляция количества отслеживаемых входов и рыночной цены (свободной) Monero Classic, Monero Original и MoneroV

Нами было сделано также несколько допусков:

1 После хардфорка пользователи получают бесплатные монеты, поскольку у них имеется некоторая сумма монет из оригинального блокчейна, которые были получены ими до хардфорка [9-11].

2 Пользователи предпочитают извлекать максимальную выгоду, продавая монеты по высокой цене.

3 Если пользователи предпочитают приватные кошельки (компьютерный кошелёк, кошелёк для смартфона, сетевой кошелёк или бумажный кошелёк), то для новых блокчейнов им

6 Информация по Monero Classic и Monero Original взята с сайта Coinmarketcap.com, а информация по MoneroV — с сайта Coingecko.com.

приходится создавать новые кошельки и импортировать информацию из старого кошелька, прежде чем они смогут совершать транзакции.

4 Если пользователи переводят свои монеты на кошельки криптовалютных бирж до реализации хардфорка, то сама биржа решает, будет ли она поддерживать новые монеты. Только после такого решения пользователи смогут получить от биржи новые монеты, которые будут записаны на её счёт [9-11].

Допуски 1 и 2 мотивируют пользователей к получению новых монет, а следовательно, потенциально возникает проблема повторного использования ключей. Тем не менее допуск 3 становится для пользователей определённым барьером, поскольку создание новых кошельков и импорт приватных ключей — задача не тривиальная и требует наличия технических знаний. В случае с допуском 4, если криптовалютная биржа не поддерживает монеты, появившиеся в результате форка, пользователи попросту не смогут получить новую криптовалюту.

1 СТРАТЕГИИ РЕШЕНИЯ ПРОБЛЕМЫ

В этом разделе говорится о существующих стратегиях решения проблемы повторного использования ключей. Также нами предлагается новая стратегия.

1.1 Существующие стратегии решения проблемы

1.1.1 *Не забирать монеты*. Пользователям Monero предлагается не получать бесплатно новые монеты [29]. Сумма монет, полученных пользователями, может меняться в зависимости от новых систем. Monero6 распределяет монеты в соотношении 1:1. Это означает, что каждый владелец Monero получает точно то же количество монет в новой ветке блокчейна. MoneroV распределяет новые монеты в соотношении 1:10, поэтому владельцы Monero получают в десять раз больше, чем у них было до форка.

Существует две проблемы, связанные с данным методом. Во-первых, этот метод не нравится пользователям, поскольку в этом случае они теряют потенциальную выгоду, так как не получают новых монет. Бесплатные монеты можно продать за другие криптовалюты или даже местные валюты. К тому же пользователи едва ли последуют этому совету, если выгода, которую они получат в случае траты новых монет, будет внушительной. Во-вторых, метод будет действенным только в том случае, если абсолютно все пользователи Monero не воспользуются возможностью получения новых монет. Если кто-то из пользователей Monero решит взять новые монеты, транзакции получения потенциально могут снизить или полностью лишить транзакции других пользователей анонимности, в результате чего такие транзакции можно будет отследить.

1.1.2 *Вспенивание*. Технология вспенивания позволяет расширить выбор выходов путём многократного направления монет пользователя по его собственным адресам [13]. При вспенивании монет количество участников кольца или ложных выходов увеличится, в результате чего злоумышленнику будет сложнее определить реальные выходы, которые использовались во множестве транзакций и были созданы в процессе вспенивания, чтобы отследить транзакции. Однако технология вспенивания всё же уязвима для известных видов атак, таких как атака по времени и сетевая атака, которые позволяют выделить реальные выходы на основе информации о происхождении транзакции [29]. Эффективность вспенивания в плане решения проблемы повторного использования ключей также сомнительна [29].

1.1.3 *Инструмент Blackball*. Разработчиками Monero был создан инструмент под названием Blackball (чёрный шар). Этот термин изначально появился в документе, в котором была описана первая выявленная в системе Monero проблема, которая состояла в том, что злоумышленник пытался добавить свои собственные выходы в блокчейн, создавая максимально возможное количество транзакций [24]. Выходы, контролируемые таким злоумышленником, и называются «чёрными шарами» (blackballs или black marbles), в то время как остальные выходы, создаваемые честными пользователями, называются «белыми шарами» (white balls или white marbles). Всякий раз, когда чёрные шары включаются в транзакцию $_t$ в качестве миксинов, злоумышленник может определить, что его чёрные шары являются ложными выходами, а белые - реально расходуемыми выходами. Таким образом, уровень анонимности повреждённой транзакции $_t$ снижается.

Приложение, созданное разработчиками Monero и предназначенное для выявления чёрных шаров, пытается составить список известных «плохих» выходов, и пользователям не рекомендуется использовать выходы из такого чёрного списка в качестве миксинов. Пользователи не обязаны задействовать приложение – оно было создано в качестве автономного приложения и не было включено ни в официальное приложение для запуска узлов Monero, ни официальный кошелёк Monero в рамках протокола.

Проблема с данным инструментом состоит в том, что у пользователя должна быть полная копия каждой ветви блокчейна, которую затем инструмент будет сравнивать и выделять информацию из ветвей блокчейна. Тем не менее учитывая, что одна ветвь блокчейна занимает 50 Гб дискового пространства, то хранение трёх ветвей потребует по крайней мере 150 Гб свободного места, чтобы уровень их анонимности никак не пострадал. Очевидно, что данный инструмент не будет работать на «лёгком» оборудовании, таком как смартфоны, память и вычислительная мощность которых ограничены. Следовательно, далеко не все пользователи смогут использовать такой инструмент, чтобы обезопасить свои транзакции. Помимо этого инструмента в используемом по умолчанию / официальном CLI-кошельке Monero имеются и другие функции, которые можно задействовать, чтобы снизить угрозу повторного использования ключей.

- Можно разрешить пользователям самостоятельно выбирать миксины / ложные выходы. Данная функция реализована в команде set_ring [33].
- Можно использовать только те миксины, которые существовали до форка. Эта функция была реализована в команде segregate-pre-fork-outputs [33].
- Можно комбинировать миксины, которые были созданы до и после форка. Данная функция была реализована в команде key-reuse-mitigation2 [33].

Наличие идентичных миксинов в транзакциях, опубликованных во множестве блокчейн-систем, не позволит пассивному злоумышленнику отследить транзакции, поскольку уровень анонимности не будет нарушен. Однако решение, которое позволило бы пользователям наилучшим образом обеспечить анонимность их транзакций, отсутствует.

1.1 **Предлагаемое нами решение**

Предлагаемое нами решение состоит из трёх частей: управления хардфорком, управления образами ключей и использования объединённого узла.

1.1.1 *Управление хардфорком*. Мы предлагаем добавить информацию Chain_ID (идентификатор блокчейна) в каждую транзакцию, что было бы полезно по нескольким причинам. Во-первых, Chain_ID можно использовать для повторного воспроизведения защиты от атаки, то есть это будет функция, которая пока не существует в Monero. Во-вторых, Chain_ID станет идентификатором того, когда пользователь будет получать информацию о выходах (когда он захочет создать новую транзакцию) или о существующих образах ключей (что будет описано далее в контексте нашего решения).

В дополнение к Chain_ID также требуется информация Fork_Point (точка форка). Fork_Point укажет на высоту первого блока в новом блокчейне, у которого будет другой хеш, отличный от родительского. Это схоже с реализацией FORK_BLKNUM в Ethereum [4]. В отличие от Chain_ID Fork_Point не нужно добавлять в данные транзакции. Fork_Point не добавляется в блок или в транзакцию, чтобы сэкономить место, избегая включения менее полезной информации. Для выполнения данного требования должна быть создана база данных Chain_Info. В новой базе данных будет храниться Chain_ID (в качестве основного ключа) и Fork_Point.

Chain_Info. Новые блокчейны, появившиеся в результате хардфорков, должны регистрироваться в базе данных в порядке появления (по принципу First-Come-First-Serve). Chain_ID может использоваться для запроса Fork_Point из новой базы данных Chain_Info. База данных Chain_Info должна быть сохранена в файле базы данных блокчейна узла. Этот подход отличается от метода, используемого Ethereum, когда информация Chain_ID хранится на странице GitHub [4]. В случае Monero информация о собственных хардфорках хранится в жёстко закодированной форме в виде исходного кода[7]. Тем не менее этот подход неосуществим в случае с внешними хардфорками, так как информация об их реализации может быть неизвестна разработчикам и сообществу Monero.

7 https://github.com/monero-project/monero/blob/master/src/cryptonote_core/blockchain.cpp#L120

1.1.2 *Управление образами ключей*. Нами были выделены несколько проблем, которые требуется решить в связи с управлением информацией образов ключей:

1 У многих ветвей блокчейна различное время блока.
2 В течение короткого периода у множества передаваемых в сеть транзакций будут идентичные образы ключей.
3 Обновляемость участников кольца в образах ключей (например, в случае добавления участника).
4 Наличие новых транзакций с участниками кольца, отсутствующими в «родительском» блокчейне, в котором изначально записываются образы ключей.
5 Новые блокчейны с меньшим обязательным размером кольца, чем в родительском блокчейне.

Масштабируемый фильтр Блума. Для решения обозначенных проблем предлагается использовать масштабируемые фильтры Блума [1]. Масштабируемые фильтры Блума (SBF) являются расширенной версией оригинального фильтра Блума [3], и их масштабирование обеспечивается использованием сразу множества фильтров Блума вместо одного, как в случае со стандартным фильтром Блума (BF). Следовательно, пропускная способность SBF может быть расширена после инициализации, в отличие от BF, который не может превысить предварительно заданной пропускной способности. Подобно BF, SBF может выдавать ложноположительные результаты, если обнаружит данные в том наборе, в котором их быть не должно. Однако SBF также унаследовал характеристики BF, благодаря которым получение ложноположительного результата очень маловероятно. Ложноположительным результатом будет выдача BF значения False (значит, что данные не находятся в наборе), хотя результатом при этом должно быть значение True (данные на самом деле будут находятся в наборе).

В рамках нашего предложения речь идёт о нескольких фильтрах SBF. Первый SBF, а именно SBF_k, должен использоваться для фильтрации образов ключей. Для вычисления SBF_k должны использоваться образы ключей из связанных блокчейнов (родительского, родственных или дочерних). Построение SBF_k позволяет идентифицировать новые образы ключей, если они будут существовать в каком-либо из блокчейнов, в результате чего, если результат алгоритма проверки будет действительным, протокол обозначит это во избежание проблемы повторного использования ключей. Второй фильтр SBF, SBF_m, используется для фильтрации значений хешей кортежей образов-миксинов ключей. Подобно SBF_k, SBF_m строится путём сбора кортежей образов-миксинов ключей из всех связанных блокчейнов. Задача SBF_m состоит в том, чтобы помочь системе определить, существовал входящий кортеж образов-миксинов ключей в одном или нескольких блокчейнах.

Несмотря на возможность масштабирования, фильтр SBF не поддерживает удаления данных. Следовательно, во избежание появления различного времени блоков и реорганизации блоков, при которой «незрелые» блоки могут быть заменены более сильными блоками, предлагается использовать временные SBF. Такие временные фильтры SBF, $tSBF_k$ и SBF_m^t, связаны с образами ключей и кортежами образов-миксинов ключей, соответственно. При использовании временных SBF новая информация в незрелых блоках и пулах памяти будет попадать не в основные SBF, а во временные . После того как информация будет подтверждена в «зрелых» блоках, данные можно будет сохранить в основных SBF. SBF_k и SBF_m могут дополнять друг друга, используя следующий механизм.

1 Система проверяет значение образа ключа в SBF_k. Если оно не существует, процесс проверки считается завершённым, и наоборот в противном случае. На этом этапе неизвестно, будет ли результат проверки ложноположительным или подлинным.
2 Задаём t как пороговое значение, которому должны будут соответствовать новые транзакции.
3 Для каждой кольцевой подписи R, имеющей размер кольца r, будет существовать r кортежей образов-миксинов ключей. Система проверяет каждый кортеж образов-миксинов ключей, если они имеются в SBF_m, и подсчитывает количество положительных результатов p. Если , то есть вероятность (из-за ложноположительной характеристики

SBF), что у входа будут те же самые участники кольца, что и у существующего входа. Тем не менее так бывает не всегда. Возможно, что p будет меньше r, но поскольку p может соответствовать пороговому значению t, при этом $\frac{p}{n} \geq t$, тогда всё должно соответствовать $\frac{r}{n} \geq t$. В противном случае:

a если $\frac{p}{n} \geq t$, транзакция, содержащая кольцевую подпись R, может быть принята, так как она была обозначена как ложноположительная SBF_k;

b если $\frac{r}{n} \geq t$, транзакция, содержащая кольцевую подпись R, может быть занесена в чёрный список, поскольку может содержать отслеживаемый выход.

1 Чтобы повысить вероятность нахождения новых транзакций с идентичным набором существующих участников кольца, пороговое значение t может быть задано как $\frac{p}{n}$, чтобы $\frac{r}{n} < t$.

Включение в чёрный список может использоваться как опция, альтернативная непринятию транзакции, как описано выше в пункте 3b, поскольку непринятие транзакции может мотивировать пользователя к повторному созданию транзакции, что сделает новую транзакцию отслеживаемой [20].

Ложноположительные результаты. Определение относительного количества ложноположительных результатов является компромиссом, связанным с тем, что в нашем решении не используются реальные данные транзакций, а вместо этого в качестве эффективного решения задействованы SBF. Частота ошибок в оригинальном решении SBF составляет от 0,0001% до 0,1% [1]. Использование двух различных SBF, то есть SBF_k и SBF_m, как ожидается, значительно сократит относительное количество ложноположительных результатов в случае с новым образом ключа, который никогда не использовался ранее, что произошло бы в противном случае.

Мы используем простое уравнение для определения вероятности двух независимых событий: $p_1 \cdot p_2$, где p_1 и p_2 обозначают вероятность первого и второго событий, соответственно. Согласно уравнению и самому большому значению частоты ошибок SBF, вероятность того, что результат обнаружения образа ключа, который никогда не был потрачен, будет ложноположительным в случае с обеими проверками, составляет 0,0001%.

Фильтр SBF для множества ветвей блокчейна. Фильтр SBF состоит из множества фильтров Блума (BF) [1], где $\{SBF_1 \| SBF_2 \| \ldots\}$, где, в свою очередь символ, || является операцией конкатенации. SBF также можно построить путём конкатенации множества SBF так, чтобы $SBF_{result} = \{SBF_a \| SBF_b \| \ldots\}$. Мы определяем локальные SBF (LBSF) как набор SBF, которые создавались с использованием информации из одной ветви блокчейна. Мы также определяем глобальные SBF (GSBF) как набор SBF, которые создавались путём конкатенации всех локальных SBF. Фильтры GSBF используются, чтобы проверить наличие связанной информации, независимо от того, в каком блокчейне находится такая информация, в то время как LSBF используются для проверки информации в определённом блокчейне.

SBFChain. В целях учёта создаваемых GSBF нами предлагается использовать SBFChain. SBFChain — это подобная блокчейну структура данных, содержащая метаданные, связанные с GSBF, и позволяющая отследить изменения в фильтрах GSBF. Все записи данных в SBFChain нумеруются. Запись e_n в SBFChain связывается с записью e_{n-1} путём добавления значения хеша $h_{e_{n-1}} = \{e_{n-1}\}$ к записи e_n. Запись создаётся через определённый период времени, то есть каждые 4 минуты, чтобы продемонстрировать последовательный процесс создания фильтров GSBF. Структура SBFChain показана на рисунке 6.

Запись e_n содержит следующую информацию:

- значение хеша $h_{e_{n-1}}$;
- номер блока n;
- временную метку ts_n;
- значения хешей самых последних GSBF:

– $h_{GSBF_1}^{height}$;
– $h_{GSBF_m}^{height}$;

- метаданные всех ветвей блокчейна, в которые добавляется информация в соответствии с самыми последними SBF:
  – Chain_ID;
  – высота блока;
  – содержимое регистра данных.

Обратившись к самой последней записи $_{\ell}$, можно определить, какая информация была добавлена в самые последние GSBF. Запись $_{\ell}$ также поможет в любой момент восстановить GSBF по информации, сохранённой в ближайшей записи $_{\ell}$.

1.1.1 *Объединённый узел*. Термин «объединённый узел» был придуман нами для обозначения нового типа узла, который будет хранить и управлять фильтрами GSBF и SBFChain. Объединённый узел будет совместно управляться мейнтейнерами множества ветвей блокчейна. Идея объединённого узла изначально возникла благодаря базам данных чёрных шаров, где информация собирается множеством сторон [7]. В то же время объединённый узел работает подобно оракулу хардфорка [17], где информация о множестве форков блокчейна может управляться из одного места. Объединённый узел собирает всю связанную информацию из различных ветвей блокчейна и строит фильтры SBF и SBFChain.

Рисунок 6. Структура SBFChain.

SBFChain может использоваться для синхронизации фильтров SBF, поддерживаемых различными объединёнными узлами. Предполагается, что среди объединённых узлов существует простой метод консенсуса, позволяющий добавлять новые записи в SBFChain, при этом все объединённые узлы следят за каждым новым обновлением информации в SBFChain как участники системы.

Введение объединённых узлов не вызовет каких-либо проблем с масштабируемостью в работе каждого блокчейна, особенно связанной с необходимым местом для хранения данных и требуемой вычислительной мощностью, чтобы обрабатывать запросы и ответы. Объединённые узлы сформируют новую подсистему Monero, которая будет отделена от основной системы, состоящей из обычных узлов, следующих протоколам Monero. Несмотря на то, что объединённые и обычные узлы будут находиться в различных системах, предполагается, что будет реализован механизм, позволяющий им обмениваться информацией.

В качестве схемы обмена данными между объединёнными и обычными узлами может использоваться RPC, равно как и для обмена данными между объединёнными узлами и SPV-кошельками с клиентской стороны. Чтобы объединённые узлы смогли обновлять информацию, поступающую из сети множества блокчейнов, требуется P2P-схема обмена данными. Отношение между объединёнными узлами, обычными узлами и SVP-кошельками продемонстрировано на рисунке 7.

Кошельки пользователей также могут активно сообщаться с объединёнными узлами в отношении необработанных транзакций, создаваемых кошельком, чтобы предотвратить проблему повторного использования ключей на ранней стадии. Однако обычные узлы могут использовать фильтры SBF, поддерживаемые объединёнными узлами, для выполнения простого алгоритма проверки перед обработкой транзакции.

Несмотря на то, что объединённые узлы хранят GSBF, они не имеют полномочий, чтобы расширить блокчейн или изменить информацию, сохранённую в блокчейне. Все обновления блокчейнов и пулов памяти связаны с фильтрами LSBF и GSBF. Для обозначения сети объединённых узлов нами используется термин «сервисная подсистема».

2 ОБСУЖДЕНИЕ

В данном разделе рассматривается анализ безопасности и эффективности предлагаемого нами решения.

2.1 **Анализ безопасности**

2.1.1 *Активная атака*. Предполагается, что в сервисной системе существуют недобросовестные объединённые узлы, в которых большинство участников не следуют протоколу надлежащим образом. Когда недобросовестные объединённые узлы получают запросы от клиента (кошелька или обычного узла) для верификации того, присутствуют ли образы ключей или кортежи образов-миксинов ключей в текущих SBF, недобросовестные объединённые узлы дают неправильные ответы. Чтобы избежать этой проблемы, клиент может отправлять запросы множеству объединённых узлов подсистемы, выбранных произвольным образом. Учитывая, что большинство объединённых узлов в подсистемах демонстрируют честное поведение, клиент обнаружит несоответствие ответов. После этого клиент рассматривает ответы как голоса, чтобы отличить правильные ответы от неправильных, так как правильные ответы наиболее вероятно поступят от большинства честных объединённых узлов, поскольку они всегда дают честные ответы.

Рисунок 7. Объединённые узлы могут помочь SPV-кошелькам, а также обычным узлам, принадлежащим различным блокчейнам

Недобросовестный объединённый узел также может быть обнаружен своими одноранговыми узлами. Объединённые узлы проверяют файлы SBF друг друга, подтверждая значения хешей SBF и значений хешей, которые хранятся в SBFChain. Если информация не будет совпадать, любые узлы, выдающие неверную информацию, будут занесены в чёрный список. Информация из чёрного списка будет опубликована для всех клиентов. В качестве механизма проверки для выявления недобросовестных объединённых узлов также могут использоваться случайные запросы.

Обычные узлы, принадлежащие различным ветвям блокчейна, также могут совместно верифицировать правильность SBF, поддерживаемых объединёнными узлами. Тем не менее в случае с обычными узлами это требует дополнительных вычислительных ресурсов. Верификация правильности GSBF может быть выполнена в форме реконструкции в два этапа:

1 **Этап первый: реконструкция внутри блокчейна**. На данном этапе обычные узлы из каждой ветви блокчейна вычисляют локальные SBF (LSBF), используя данные собственного блокчейна в соответствии с согласованной записью в SBFChain. Реконструкция локальных SBF может начаться с Fork Point (точки реализации форка) этой ветви блокчейна, а не с генезис-блока (нулевого блока). Правильность локальных SBF (LSBF) зависит от честности обычных узлов, принадлежащих блокчейну. Учитывая, что большинство узлов демонстрирует честное поведение, всегда имеется возможность сгенерировать правильные LSBF.

2 **Этап второй: реконструкция между блокчейнами**. Узлы из различных ветвей блокчейна совместно генерируют ряд глобальных SBF (GSBF). Эти GSBF создаются путём конкатенации всех LSBF. При условии, что все LSBF будут правильными, и GSBF также будут правильными.

Недобросовестный обычный узел также может попытаться подтвердить транзакции, у которых есть проблемы с повторным использованием ключей, для включения в новые блоки, которые он производит в сотрудничестве с майнерами, обладающими достаточной вычислительной мощностью. В этом случае другие обычные узлы могут произвести повторную валидацию этих транзакций с помощью объединённых узлов. После того как неправильность этих транзакций будет подтверждена, блоки, содержащие их, можно будет игнорировать. Учитывая, что большинство узлов демонстрирует честное поведение, согласно текущему протоколу Monero произойдёт временный форк, который чрез несколько блоков исчезнет. Так как майнеры в случае удаления вычисленных блоков понесут финансовые потери, они наименее заинтересованы в бесчестном поведении.

1.1.1 *Пассивная атака*. В случае пассивной атаки предполагается, что у злоумышленника имеется доступ к публичным блокчейнам. Чтобы выделить отслеживаемые транзакции, злоумышленнику необходимо разработать аналитические инструменты. Успешность атаки определяется количеством отслеживаемых транзакций и соотношением этого количества с общим количеством транзакций в системе.

Поскольку активную атаку можно предотвратить с помощью предлагаемого нами решения, то же самое можно сделать и с пассивной атакой. При проведении пассивных атак анализируются

существующие действительные транзакции, подтверждённые и включённые в блоки. При отсутствии неправильных транзакций в блоках пассивная атака не даст ожидаемых результатов при условии отсутствия у злоумышленника какой-либо дополнительной информации.

1.2 **Анализ эффективности**

1.2.1 *Управление хардфорком*. Чтобы вычислить дополнительную вычислительную мощность, необходимую для управления дополнительной информацией при управлении хардфорком, нами был проведён ряд экспериментов. При этом использовалась виртуальная машина Ubuntu 18.04 LTS с 8 Гб RAM и максимум 2 ядрами CPU. Новая таблица под названием Chain_Info была создана с помощью системы базы данных LMDB, являющейся той базой данных, которая используется для хранения и управления данными блокчейна в текущей версии Monero.

В базу данных было записано и считано из неё два миллиона кортежей Chain_ID - Fork_Point. Процессы были повторены 10 000 раз. Для хранения двух миллионов записей понадобилось примерно 1,2 Мб памяти, среднее время записи составило 28,37 миллисекунд, а среднее время считывания — 28,19 миллисекунд. Результаты подробно представлены на рисунке 8. Эксперимент демонстрирует, что вычислительные ресурсы, необходимые для выполнения соответствующих операций, настолько малы, что доступны для существующих на сегодняшний день обычных компьютеров.

1.2.2 *Доступность объединённого узла*. В соответствии с нашим предложением GSBF будет поддерживаться специальным типом узла под названием объединённый узел. Объединённый узел поддерживает ряд GSBF, соответствующих всем существующим или будущим ветвям блокчейна Monero.

Чтобы вычислить время и необходимый для создания SBF объём памяти, был проведён эксперимент. При этом использовалась библиотека Scalable Bloom Filter Python Джея Бейрда, pybloom[8]. С учётом возможного большого роста набора данных при проведении эксперимента использовалась настройка LARGE_SET_GROWTH. При этой настройке всякий раз, когда система достигает максимальной производительности, происходит резкий рост объёма памяти. Результаты, показанные на рисунке 9, свидетельствуют о том, что время, необходимое для создания SBF, линейно соотносится с количеством данных, включаемых в SBF, при среднем объёме 17,308 данных в секунду. Размер файла, однако, согласно алгоритму LARGE_SET_GROWTH, значительно увеличивался всякий раз, когда достигался максимум производительности. Наш эксперимент также показал, что в результате создания SBF с 100 миллионами данных примерно чрез 96 минут появляется файл SBF размером 372,1 Мб. Из-за небольшого объёма необходимых для создания SBF ресурсов повторное вычисление SBF не является проблемой.

Рисунок 8. Время обработки при считывании/записи в базу данных Chain_Info с помощью LMDB

1.3 **Ограничения**

Позволяя избежать проблемы повторного использования ключей, наше решение также позволяет избежать пассивной атаки, при которой применяется анализ публичных блокчейнов. Тем не менее наше предложение не позволяет предотвратить проведение пассивной атаки на сетевом уровне, что пока считается одной из самых больших проблем с точки зрения обеспечения приватности криптовалюты [8]. Наше решение также уязвимо к пассивной атаке, проводимой «честным, но подозрительным» объединённым узлом, который потенциально может отследить транзакцию пользователя при наличии достаточного количества информации. Эта проблема, однако, характерна не только для предлагаемой нами системы, но и для всех узлов Monero.

2 **ЗАКЛЮЧЕНИЕ И БУДУЩАЯ РАБОТА**

Нами исследуется проблема повторного использования ключей как нежелательное последствие хардфорков Monero. Нами был создан набор данных, взятых из трёх различных ветвей блокчейна, и идентифицированы отслеживаемые входы, появившиеся в результате повторного использования

8 https://github.com/jaybaird/python-bloomfilter

ключей. Также в качестве побочных последствий основной проблемы нами были выделены каскадный эффект и снижение уровня анонимности. Проведённый анализ позволил определить, что масштабируемость проблемы повторного использования ключей коррелирует с рыночной ценой уважаемых монет и поддержкой новых криптовалют со стороны криптовалютных рынков. Нами также была предложена стратегия решения проблемы в форме управления хардфорками и управления образами ключей, где важную роль играют объединённые узлы.

Рисунок 9. (a) Время создания SBF положительно линейно размеру данных. (b) Размер получаемого файла повышается при достижении максимальной производительности SBF

В рамках будущей работы нами будет исследовано, как наше решение может быть реализовано в случае с различными типами криптовалюты. Также нами будут исследованы различные варианты работы с изменениями на уровне протокола, позволяющие избежать хардфорка. Новый метод должен поддерживать фундаментальные изменения в системе без создания новой ветви в блокчейне. Этот тип решения также можно было бы выгодно реализовать в активно развивающихся системах, таких как Monero. Также было бы интересно более глубоко исследовать корреляцию между ценой на криптовалютных рынках и количеством транзакций, сохранённых в блокчейне Monero, что позволило бы раскрыть фактическое поведение пользователей Monero, а также то, как Monero используется в реальном мире.

БЛАГОДАРНОСТЬ

Работа Рона Штейнфельда и Джозефа К. Лю была частично поддержана в рамках гранта ARC Discovery Project (DP180102199).

СПИСОК ЛИТЕРАТУРЫ

1 Пауло Серхио Алмейда (*Paulo Sérgio Almeida*), Карлос Бакеро (*Carlos Baquero*), Нуно Прегица (*Nuno Preguiça*) и Дэвид Хатчисон (*David Hutchison*). 2007. Масштабируемые фильтры Блума (*Scalable bloom filters*). Inform. Process. Lett. 101, 6 (2007), 255–261.

2 BatmanLovesCrypto. 2018. Monero Classic и Monero Original в одном блокчейне? Помогите понять. (*Monero Classic and Monero Original on the same blockchain? Help me understand*). https://www.reddit.com/r/Monero/comments/8eovv5/monero_classic_and_monero_original_on_the_same/

3 Бёртон Х. Блум (*Burton H Bloom*). 1970. Компромисс между пространством и временем в хеш-кодировании с допустимыми ошибками (*Space/time trade-offs in hash coding with allowable errors*). Commun. ACM 13, 7 (1970), 422–426.

4 Виталик Бутерин (*Vitalik Buterin*). 2016. Простая защита от атаки повторного воспроизведения (*Simple Replay Attack Protection*). https://github.com/ethereum/EIPs/blob/master/EIPS/eip-155.md

5 Шерман С. М. Чоу (*Sherman S. M. Chow*), Джозеф К. Лю (*Joseph K. Liu*) и Дункан С. Вонг (*Duncan S. Wong*). 2008. Устойчивая система выборов без бюллетеней с сохранением тайны голосования и возможностью верификации (*Robust Receipt-Free Election System with Ballot Secrecy and Verifiability*). NDSS.

6 dEBRYUNE. 2018. Изменение алгоритма доказательства работы и повторное использование ключей (*PoW change and key reuse*). https://ww.getmonero.org/2018/02/11/PoW-change-and-key-reuse.html

7 Джастин Эхренхофер (*Justin Ehrenhofer*). 2018. Сайт чёрных шаров Monero (*Monero Blackball Site*). https://monero-blackball.github.io/monero-blackball-site/

8 Райан Генри (*Ryan Henry*), Амир Херцберг (*Amir Herzberg*) и Аникет Кейт (*Aniket Kate*). 2018. Приватность доступа к блокчейну: проблемы и направления их решения (*Blockchain access privacy: challenges and directions*). IEEE Security & Privacy 16, 4 (2018), 38–45.

9 HitBTC. 2018. Форк Monero Original состоялся (*The Monero Original Fork has happened*). https://blog.hitbtc.com/the-monero-original-fork-had-happened/

10 HitBTC. 2018. Заявление по форку MoneroV (*Statement on MoneroV fork*). https://blog.hitbtc.com/statement-on-monerov-fork/

11 HitBTC. 2018. Заявление по форку XMO Monero (*Statement on XMO Monero fork*). https://blog.hitbtc.com/statement-on-xmo-monero-fork/

12 Ангелос Кияис (*Aggelos Kiayias*), Эндрю Миллер (*Andrew Miller*) и Дионис Циндрос (*Dionysis Zindros*). 2017. Неинтерактивные доказательства для доказательства работы (*Non-interactive proofs of proof-of-work*). Технический отчёт. Архив электронных документов по криптологии (*Cryptology ePrint Archive*), Отчёт 2017/963, 2017. Доступ открыт 10.03.2017.

13 knaccc. 2017. Описание потенциальной возможности снижения уровня приватности и рекомендации по решению проблемы (*Description of a potential privacy leak and recommendation to mitigate*). https://github.com/monero-project/monero/issues/1673#issuecomment-278509986

14 Амрит Кумар (*Amrit Kumar*), Клемент Фишер (*Clément Fischer*), Шрути Топль (*Shruti Tople*) и Пратик Саксина (*Prateek Saxena*). 2017. Анализ отслеживаемости в блокчейне Monero (*A traceability analysis of Monero's blockchain*). Материалы Европейского симпозиума по исследованиям в области компьютерной безопасности (*European Symposium on Research in Computer Security*). Springer, 153–173.

15 Джозеф К. Лю (*Joseph K. Liu*), Мэн Хо О (*Man Ho Au*), Вилли Сусило (*Willy Susilo*) и Цзяньин Жоу (*Jianying Zhou*). 2014. Связываемая кольцевая подпись с безусловной анонимностью (*Linkable Ring Signature with Unconditional Anonymity*). IEEE Trans. Knowl. Data Eng. 26, 1 (2014), 157–165.

16 Джозеф К. Лю (*Joseph K Liu*), Виктор К. Вей (*Victor K Wei*) и Дункан С. Вонг (*Duncan S Wong*). 2004. Связываемая подпись спонтанной анонимной группы для специально созданных групп (*Linkable spontaneous anonymous group signature for ad hoc groups*). Материалы Австралийской конференции по информационной безопасности и приватности данных (*Australasian Conference on Information Security and Privacy*). Springer, 325–335.

17 Патрик Маккори (*Patrick McCorry*), Итан Хейлдман (*Ethan Heilman*) и Эндрю Миллер (*Andrew Miller*). 2017. Автоматический трейдинг с согласия: спекуляции на успешном хардфорке (*Atomically trading with roger: Gambling on the success of a hardfork*). Управление приватностью данных, криптовалюты и блокчейн-технология (*Data Privacy Management, Cryptocurrencies and Blockchain Technology*). Springer, 334–353.

18 Сара Микльджон (*Sarah Meiklejohn*), Марьори Помароле (*Marjori Pomarole*), Грант Джордан (*Grant Jordan*), Кирилл Левченко (*Kirill Levchenko*), Деймон Маккой (*Damon McCoy*), Джеффри М. Вёлькер (*Geoffrey M. Voelker*) и Стефан Севедж (*Stefan Savage*). 2013. Куча Bitcoin: как отличить платежи людей, не имеющих имени (*A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*). USENIX ;login: (2013).

19 Monero. [n. d.]. Форки и хардфорки Monero XMR (*Monero XMR Forks & Hard Forks*). https://monero.org/forks/

20 monero hax123. 2018. Повреждённые ответы RPC от удалённых демонов могут стать причиной отслеживания транзакций (*Corrupt RPC responses from remote daemon nodes can lead to transaction tracing*). https://hackerone.com/reports/304770

21 Мальти Мёзер (*Malte Möser*), Кайл Соска (*Kyle Soska*), Этан Хейлман (*Ethan Heilman*), Кевин Ли (*Kevin Lee*), Генри Хеффан (*Henry Heffan*), Шашват Шриваштава (*Shashvat Srivastava*), Кайл Хоган (*Kyle Hogan*), Джейсон Хеннеси (*Jason Hennessey*), Эндрю Миллер (*Andrew Miller*), Арвинд Нараянан (*Arvind Narayanan*) и др. 2018. Эмпирический анализ отслеживаемости данных в блокчейне Monero (*An Empirical Analysis of Traceability in the Monero Blockchain*). Материалы по технологиям повышения уровня приватности 2018 (*Proceedings on Privacy Enhancing Technologies 2018*), 3 (2018), 143–163.

22 Сатоши Накомото (*Satoshi Nakamoto*). 2008. Bitcoin: одноранговая электронная денежная система (*Bitcoin: A peer-to-peer electronic cash system*). Отчёт. http://bitcoin.org/bitcoin.pdf

23 Шен Ноезер (*Shen Noether*), Адам Маккензи (*Adam Mackenzie*) и др. 2016. Кольцевые конфиденциальные транзакции (*Ring confidential transactions*). Ledger 1 (2016), 1–18.

24 Шурэ Ноезер (*Surae Noether*), Саранг Ноезер (*Sarang Noether*) и Адам Маккензи (*Adam Mackenzie*). 2014. MRL-0001: техническая заметка по возможности цепной реакции с

точки зрения отслеживаемости в рамках протокола CryptoNote 2.0 (*MRL-0001: A note on chain reactions in traceability in CryptoNote 2.0*). Технический отчёт 2014 (2014).

25 propercoil. 2018. Защита от атаки повторного воспроизведения? (*Replay protection?*) https://www.reddit.com/r/Monero/comments/8agjfd/replay_protection/dx0lun4/

26 Бейли Ревцель (*Bailey Reutzel*). 2017. Логично это или нет? Грядущий форк Bitcoin приведёт к росту его цены (*Logical or Not, Bitcoin's Coming Fork Is Boosting Its Price*). https://www.coindesk.com/logical-not-bitcoins-coming-fork-boosting-price/

27 Дорит Рон (*Dorit Ron*) и Ади Шамир (*Adi Shamir*). 2013. Количественный анализ полного графа транзакций Bitcoin (*Quantitative analysis of the full bitcoin transaction graph*). Финансовая криптография и безопасность данных (*Financial Cryptography and Data Security*). Springer, 6–24.

28 Джеф Сауро (*Jeff Sauro*) и Джеймс Р. Льюис (*James R Lewis*). 2016. Количественная оценка пользовательского опыта взаимодействия: прикладная статистика при исследовании пользователей (*Quantifying the user experience: Practical statistics for user research*). Morgan Kaufmann.

29 sgp. 2018. Как отдельным пользователям обезопасить себя и сообщество от повторного использования ключей в результате форка? (*How can individuals safeguard themselves and the community against a key reusing fork?*) https://monero.stackexchange.com/a/7847

30 Риккардо Спаньи (*Riccardo Spagni*). 2018. Версия Monero 0.13.0 Beryllium Bullet (*Monero 0.13.0 "Beryllium Bullet" Release*). https://www.getmonero.org/2018/10/11/monero-0.13.0-released.html

31 Шифенг Сан (*Shifeng Sun*), Мэн Хо О (*Man Ho Au*), Джорзеф К. Лю (*Joseph K. Liu*) и Ц Хон Йен (*Tsz Hon Yuen*). 2017. RingCT 2.0: Протокол компактной связываемой кольцевой подписи на базе аккумуляторов для блокчейн-криптовалюты Monero (*RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero*). ESORICS II (LNCS), том 10493. Springer, 456–474.

32 user36303. 2017. Атака повторного воспроизведения в контексте протоколов Cryptonote (*Replay attack and Cryptonotes*). https://monero.stackexchange.com/a/5718

33 user36303. 2018. Как отдельным пользователям обезопасить себя и сообщество от повторного использования ключей в результате форка? (*How can individuals safeguard themselves and the community against a key reusing fork?*) https://monero.stackexchange.com/a/7844

34 Николас Ван Саберхаген (*Nicolas van Saberhagen*). 2018. Cryptonote v2.0, 2013. URL: https://cryptonote.org/whitepaper.pdf. White Paper. Accessed (2018), 04–13.

35 Димаз А. Виджая (*Dimaz A. Wijaya*), Джозеф Лю (*Joseph Liu*), Рон Штейнфельд (*Ron Steinfeld*) и Донси Лю (*Dongxi Liu*). 2018. Атака на кольца Monero: последствия воссоздания транзакций с нулевым количеством миксинов (*Monero Ring Attack: Recreating Zero Mixin Transaction Effect*). TrustCom. IEEE, 1196–1201.

36 Димаз Анкаа Виджая (*Dimaz Ankaa Wijaya*), Джозеф Лю (*Joseph Liu*), Рон Штейнфельд (*Ron Steinfeld*) и Донси Лю (*Dongxi Liu*). 2019. Риск, связанный с асинхронным обновлением протокола: атаки на протоколы Monero (*Risk of Asynchronous Protocol Update: Attacks to Monero Protocols*). (2019). Готовится к публикации.

37 Димаз Анкаа Виджая (*Dimaz Ankaa Wijaya*), Джозеф Лю (*Joseph Liu*), Рон Штейнфельд (*Ron Steinfeld*), Донси Лю (*Dongxi Liu*) и Ц Хон Йен (*Tsz Hon Yuen*). 2018. Атаки с целью снижения уровня анонимности Monero (*Anonymity Reduction Attacks To Monero*). Материалы 14-й международной конференции по защите информации и криптологии (*14th International Conference on Information Security and Cryptology*). Springer.

38 Бин Ю (*Bin Yu*), Джозеф К. Лю (*Joseph K. Liu*), Амин Сакзад (*Amin Sakzad*), Шурья Непал (*Surya Nepal*), Рон Штейнфельд (*Ron Steinfeld*), Пол Римба (*Paul Rimba*) и Мэн Хо О (*Man Ho Au*). 2018. Не зависящая от используемой платформы, безопасная система голосования на базе блокчейна (*Platform-Independent Secure Blockchain-Based Voting System*). ISC (LNCS), том 11060. Springer, 369–386.

39 Цзося Ю (*Zuoxia Yu*), Мэн Хо О (*Man Ho Au*), Джаньшань Ю (*Jiangshan Yu*), Рупенг Янг (*Rupeng Yang*), Кюлянг Ксю (*Qiuliang Xu*) и Вонг Фэт Лау (*Wang Fat Lau*). 2019. Новый эмпирический анализ отслеживаемости в блокчейнах на базе протокола Cryptonote (*New*

Empirical Traceability Analysis of CryptoNote-Style Blockchains). Финансовая криптография и безопасность данных (*Financial Cryptography and Data Security*).

40 Алексей Замятин (*Alexei Zamyatin*), Николас Штифтер (*Nicholas Stifter*), Алёша Юдмаер (*Aljosha Judmayer*), Филипп Шиндлер (*Philipp Schindler*), Эдгар Вейпль (*Edgar Weippl*) и В. Дж. Кноттебельт (*WJ Knottebelt*). 2018. Новый дикий бархатный форк! Изменение инклюзивного блокчейн-протокола на практике (*A wild velvet fork appears! Inclusive blockchain protocol changes in practice*). Материалы 5-го семинара по Bitcoin и исследованиям в области блокчейн-технологии (*5th Workshop on Bitcoin and Blockchain Research*), Финансовая криптография и безопасность данных (*Financial Cryptography and Data Security*), том 18.