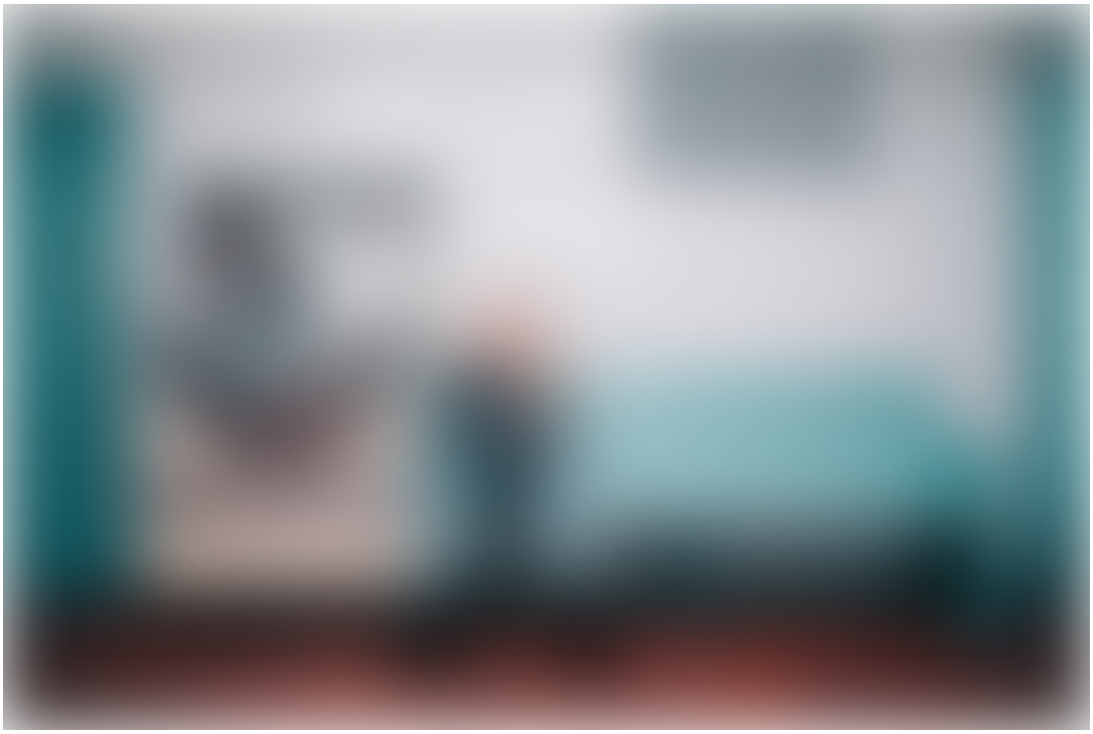
Миксеры и кольцевые подписи

16.11.2017 СТАТЬИ



Автор: Matt Luongo, основатель @fold_app

Существует несколько практических вариантов повышения уровня конфиденциальности: «миксеры» и «тумблеры», а также секретные криптовалюты, например, Monero и Zcash. Сегодня мы более подробно рассмотрим, как работают первые два варианта.

Миксеры

Основная идея, которая лежит в основе микширования почти так же стара, как и сам институт финансов.

Допустим, группа людей хочет скрыть свои транзакции от глаз посторонних. Для этого они объединяют свои средства в один пул на отдельный приватный реестр. Перемешанные средства расходуются, происхождение каждого платежа скрывается — наблюдатели видят оплаченную сумму и получателя, но не знают, какое лицо или лица в группе разрешили оплату. Возникает несколько вопросов: кто отвечает за реестр? Кому можно доверить общие средства?

Давайте посмотрим, как эти проблемы решаются в сети Биткоина.

Централизованные услуги

BitMixer – специальный сервис для микширования средств. Запущенный в 2014 году, он стал реализацией вышеуказанной схемы. Пользователи могут депонировать деньги непосредственно с помощью этой службы. BitMixer разбивает депозиты на

более мелкие части, смешивая их со средствами других пользователей, а также с собственными резервами. В итоге пользователи могут выводить только «новые» деньги, не связанные с их первоначальными депозитами. За свою работу сервис, конечно, взимает определенную плату.

Итак, кто хранит деньги и контролирует работу реестра? Все это подвластно одним и тем же людям– это самое слабое место в этой системе. Различные виды мошенничества довольно распространены в сети биткоин, особенно богата ими история бирж и других операторов услуг. Даже если оператор честен, он все равно зачастую не может обеспечить защиту вашей конфиденциальности от правительства, хакеров и внутренних угроз.

Однако, владелец BitMixer закрыл сервис. В сообщении на BitcoinTalk он (она? они?) объяснил, что служба закрыта, поскольку конфиденциальность в блокчейне биткоина – недостижимая цель. Учитывая, что этот человек управлял услугами микширования в течение 3 лет, это довольно странное заявление. Тем не менее, стало понятно, что полной конфиденциальности в блокчейне биткоинов достичь гораздо сложнее, чем кажется.

CoinJoin

Грегори Максвелл в 2013 году предложил децентрализованный подход к микшированию, реализовав его в приложении CoinJoin.

Представим схему работы. Допустим, пользователю A необходимо перевести пользователю B 10 BTC, пользователь C также хочет отправить пользователю D 10 BTC. Все четыре участника могу объединить свои транзакции одной общей подписью. Каждый пользователь может опубликовать часть транзакции, но ни один биткоин не может быть потрачен до тех пор, пока обе части не будут объединены в единое целое. После объединения, пользователи B и D получат по 10 BTC каждый, однако, информация о том, кто для кого был отправителем будет недоступна.

Использование CoinJoin не требует наличия центрального органа для объединения средств. И поскольку микширование происходит с каждой транзакцией, нет необходимости в отдельном реестре.

Как это работает? Войдите в JoinMarket, децентрализованный сервис микширования биткоинов, используя CoinJoin. JoinMarket хранит книгу заказов точно так же, как и криптобиржи. «Производители» - участники рынка, которые добавляют ликвидность на биржу - предлагают выступать в качестве участников CoinJoin за определенную плату. «Покупатели», желая замикшировать свои монеты, объединяются с «производителем», который обменивает биткоины.

JoinMarket – это огромное шаг вперед в сравнении с централизованными микшерами, но на практике существует ряд проблем.

Фото: Ришаб Варшни

Деанонимизация

MIT Technology недавно выпустили отчет, который обобщил результаты исследователей Принстона по деанонимизации транзакции биткоинов. Они обнаружили, что, если пользователь использует 3 раунда CoinJoin, микшируя кошелек и делая два платежа онлайн, личность пользователя все равно может быть раскрыта с «точностью до 98%».

Современное наблюдение: как работает деанонимизация?

С появлением рекламы в интернете отсутствие устойчивой модели доходов стало затруднять процесс создания уникального контента: создателям нужен способ финансирования своей работы. И хотя были попытки предоставить альтернативные источники дохода, проверенным и работающим вариантом все же стал доход от сторонней рекламы.

Поскольку сегодня реклама есть на каждой сайте, невероятное количество специалистов посвятили себя развитию так называемых «технологий рекламы», улучшая ее доставку, отслеживание и настройку. Каждый шаг в этом направлении был обоснован, но в стремлении к созданию хорошего продукта, современная сеть превратилась в глобальный аппарат наблюдения.

Каким образом связаны реклама в интернете и исследование команы Принстонского университета? Ученые применили существующий метод анализа блокчейнов для идентификации транзакций CoinJoin, а также метод «атаки пересечения кластеров» (как они сами его и называют). Они объединили пропущенные данные платежа с рекламными трекерами с информацией на блокчейне, таким образом отслеживая пути микшированных средств. Так был запущен процесс деанонимизации пользователей.

Возможно ли обеспечить приватность?

Есть несколько вещей, которые мы можем извлечь из попыток деанонимизации пользователей.

Во-первых, в результате исследования, были обнаружены пользователи, которые еще ни разу не микшировали свои средства. Немногие пользователи в реальном

мире знают о рисках деанонимизации и предпринимают шаги для смягчения угрозы. Однако микшеры в качестве решения этой проблемы не пригодны, потому что они не работают по умолчанию.

Во-вторых, причина, по которой предпринять какие-то усилия по деанонимизации стало в принципе возможным, заключается в том, что в пуле микшера задействовано мало людей. Если в транзакции CoinJoin участвуют три человека, конкретный результат можно получить даже от одного из трех. А это уже кое-какие данные для блокчейн–аналитика.

Наконец, транзакции CoinJoin можно легко обнаружить на блокчейне.

Спрятавшись в толпе

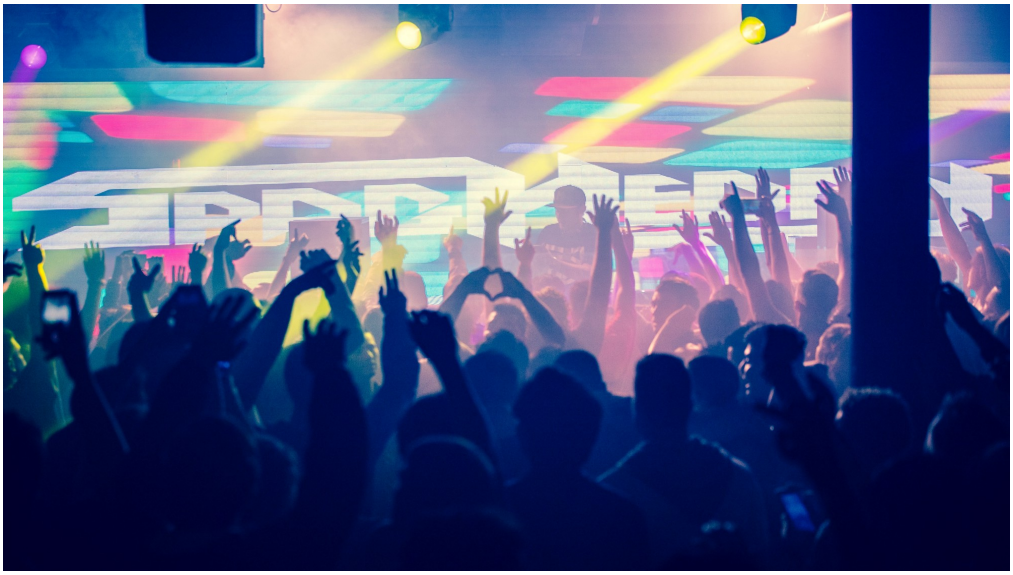


Фото: Мэди Адам

В период с середины 2015 года по 2017 год в сети Биткоин было совершено 164 млн транзакций. Из них 78 697 транзакций были сделаны при помощи CoinJoin.

Основная мысль, которую я хочу донести сегодня: конфиденциальность работает лучше всего, когда все в этом заинтересованы.

Идеальная приватная транзакция не выглядит таковой на самом деле. По иронии судьбы, объявляя о своем стремлении к конфиденциальности, скорее всего, вы только привлечете к себе дополнительное внимание. Лучший способ гарантировать, что никакие транзакции не получают дополнительного внимания, — убедиться, что все они являются приватными – это своего рода коллективный иммунитет. Чем больше приватных транзакций, тем меньше появляется нестандартных частных транзакций.

Анонимные сеты

Мы говорили о двух основных недостатках микширования средств: непонятно, кому доверяются средства и кто отвечает за дополнительный реестр. CoinJoin и другие децентрализованные методы решают первый вопрос, а такие сервисы, как JoinMarket, направлены на решение второго.

К сожалению, в этом уравнении есть еще одна переменная - размер пула. Если пул средств состоит из двух вкладчиков, нет смысла и говорит о конфиденциальности.

«Пул» также иногда называют инструментом конфиденциальности, или анонимности. И если он слишком мал, то транзакции можно легко разоблачить с

помощью обычного статистического анализа. Это важный вопрос, который будет возникать снова и снова в любом последующем обсуждении темы анонимности. Данный пробел во многих схемах сохранения приватности, в том числе построенных на основе сети Биткоин, должен быть заполнен.

Источник

Теги: **АНОНИМНОСТЬ**, **МИКСЕРЫ**, **CRYPTO**

Поделиться в соц сетях:

Похожие материалы

16.11.2017 **СТАТЬИ**

Надвигается эра зомби-токекнов?

28.10.2017 **НОВИЧКАМ**

FAQ - Bitcoin

11.11.2017 **НОВОСТИ**

Королевский монетный дв
Великобритании собирае
использовать блокчейн д
золотым запасом

О ПРОЕКТЕ

Информационный ресурс о криптовалютах, блокчейне и децентрализованных технологиях. Мы работаем для вас.

КОНТАКТЫ