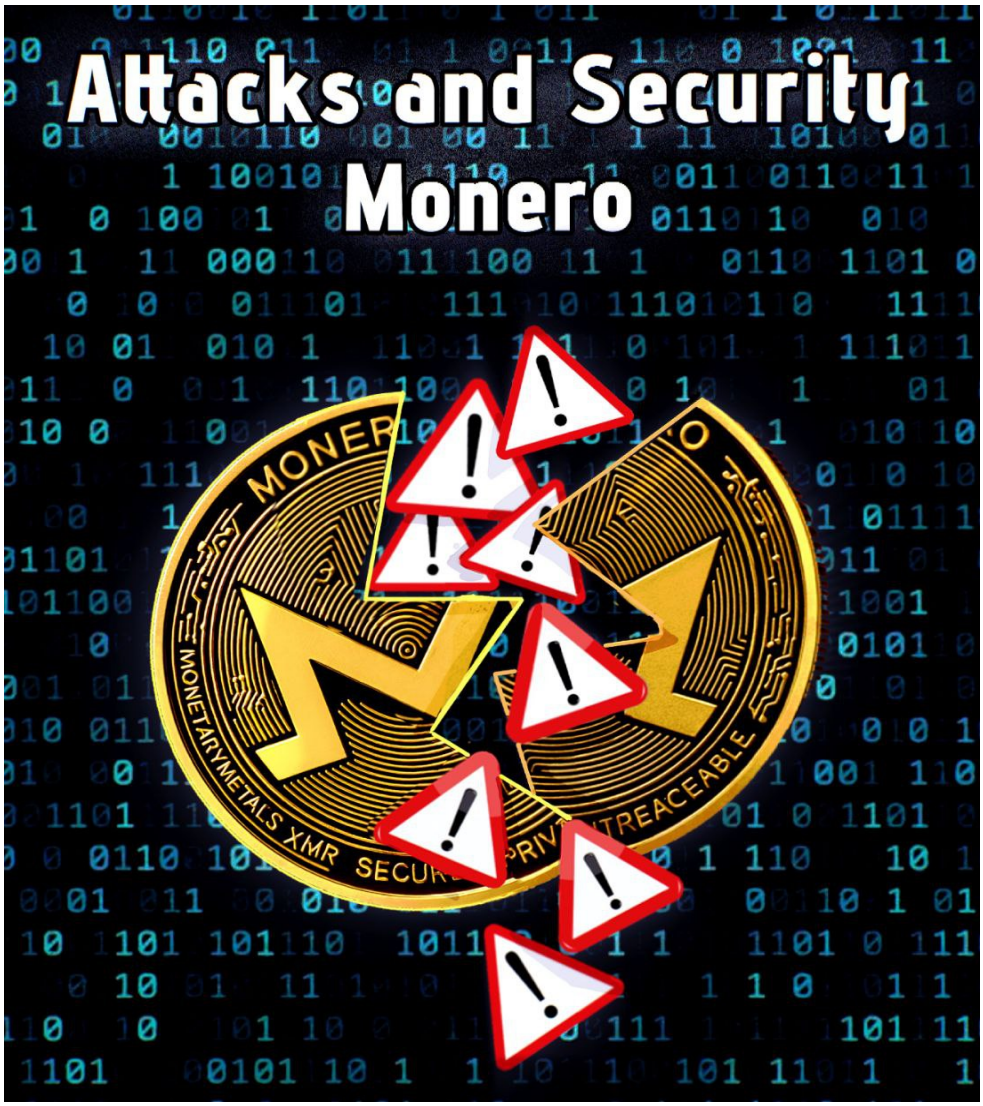
Атаки и защита Monero

1 августа 2025 г.



Содержание

1 Что такое Monero и как она работает? 3
- 1.1 Как Monero обеспечивает эту секретность? . . . 4
  - 1.1.1 Как Monero скрывает транзакции? . . . 4
  - 1.1.2 Как Monero скрывает суммы перевода? . . . 5
  - 1.1.3 Как Monero скрывает получателя? . . . 5
  - 1.1.4 Защита Monero на сетевом уровне . . . 7
  - 1.1.5 Кратко про майнинг в Monero . . . 7

2 Атаки на Monero 7
- 2.1 Виды атак . . . 8
  - 2.1.1 Black Marble Flooding . . . 8
  - 2.1.2 EAE . . . 9
  - 2.1.3 Атака на те же ключи в форках Monero . . . 9
  - 2.1.4 Сетевые атаки на Monero . . . 10
  - 2.1.5 Атака через каналы в сети P2P . . . 10
  - 2.1.6 Атака Eclipse Attack . . . 11
  - 2.1.7 Coinbase Output Heuristic . . . 12
  - 2.1.8 Ring Attack . . . 13
  - 2.1.9 OSPEAD . . . 13
  - 2.1.10 Leveraging Output Merging . . . 14
  - 2.1.11 Temporal Analysis . . . 14
  - 2.1.12 Burning Bug . . . 15
  - 2.1.13 10 Block Decoy Bug . . . 16
- 2.2 Примеры реальных атак на Monero . . . 17
  - 2.2.1 Атака Black Marble Flooding (март 2024) . . . 17
  - 2.2.2 Случай отслеживание Monero через биржу . . . 18
  - 2.2.3 Утечка видео Chainalysis . . . 19
  - 2.2.4 Отслеживание транзакций японской полицией . . . 20

3 Защита Monero 23
- 3.1 Защита которая уже есть в Monero . . . 24
  - 3.1.1 Кольцевые подписи . . . 24
  - 3.1.2 Скрытые адреса . . . 24
  - 3.1.3 RingCT . . . 25
  - 3.1.4 Защита на сетевом уровне . . . 25
  - 3.1.5 Защита майнинга . . . 25
  - 3.1.6 Динамический размер блока . . . 26
  - 3.1.7 Доступные меры защиты для юзера . . . 26
- 3.2 Преимущества Monero . . . 26
- 3.3 Меры защиты для пользователя . . . 27
  - 3.3.1 Сами меры защиты . . . 28
  - 3.3.2 Что вы не можете изменить в Monero? . . . 29
- 3.4 Практика защиты Monero . . . 29
  - 3.4.1 Установка Monero . . . 30

3.4.2 Запуск Monero через Tor 33
3.4.3 Настройка Monero с Kovri 35
3.4.4 Шифрование файла кошелка 36
3.4.5 Дополнительная защита 37

4 Вывод **38**
4.1 Мое мнение о безопасности Monero 39
4.2 Дополнительные ссылки 39

1 Что такое Monero и как она работает?

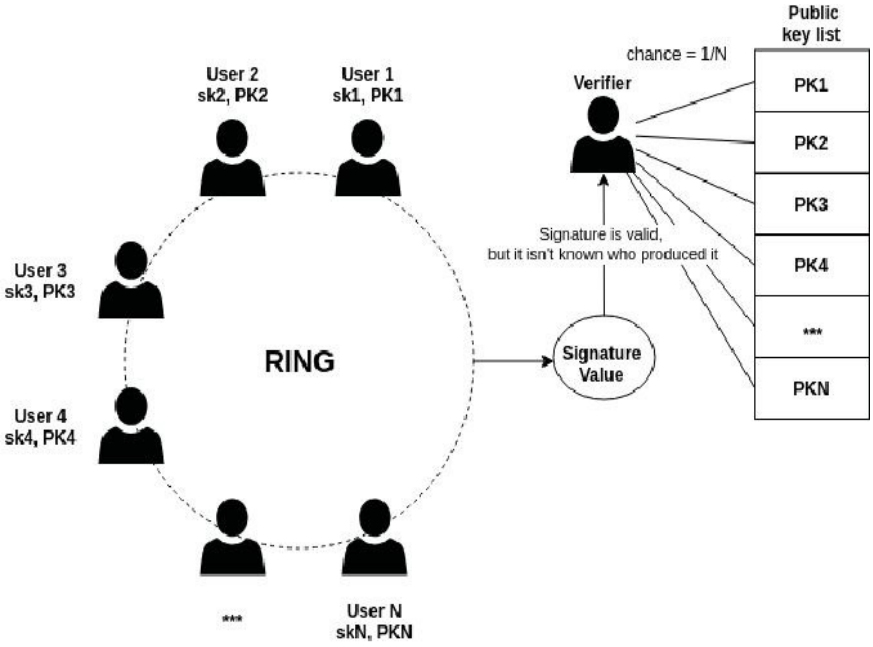
Monero это одна из лучших криптовалют для приватности. В отличие от Bitcoin, где блокчейн как открытая книга — кто, кому и сколько отправил, всё на виду, — Monero прячет всё: отправителя, получателя, сумму.

Эта монета появилась в 2014 году, когда от Bytecoin отпочковался форк Bitmonero из-за мутной истории с премайнингом, где 80% монет уже были распределены. Так родилась Monero, взяв за основу протокол CryptoNote, который стал его главным козырем.

XMR(монеты Monero) решает проблему отслеживания транзакций: в прозрачных блокчейнах, вроде Bitcoin или эфириум, можно отследить любые монеты, например "грязные" и отследить их путь, а в Monero все XMR одинаковы, и никто не вычислит, откуда они пришли.

1.1 Как Monero обеспечивает эту секретность?

1.1.1 Как Monero скрывает транзакции?



Представьте, что ваша транзакция - это письмо, которое вы отправляете в толпе курьеров. Чтобы никто не понял, от кого оно и кому, Monero использует кольцевые подписи. Когда вы отправляете транзакцию, она смешивается с другими, создавая группу из 16 участников, среди которых ваша транзакция — лишь одна. Эти 15 остальных участников — так называемые декои, которые добавляются для запутывания следов (можно сказать такой встроенный миксер). Никто, глядя на эту группу, не сможет точно определить, какая транзакция ваша и кто её отправитель или получатель.

В версии Monero 0.18 эта система стала ещё эффективнее благодаря технологии CLSAG. Это технология смешивает вашу транзакцию с 15 фальшивками (декоями), создавая группу из 16 участников, чтобы никто не мог вычислить, кто отправил деньги. По сравнению с предыдущей технологией MLSAG, CLSAG, внедрённая в версии 0.18 (октябрь 2022), делает подписи на 10-20% компактнее, уменьшая размер транзакций и снижая комиссии.

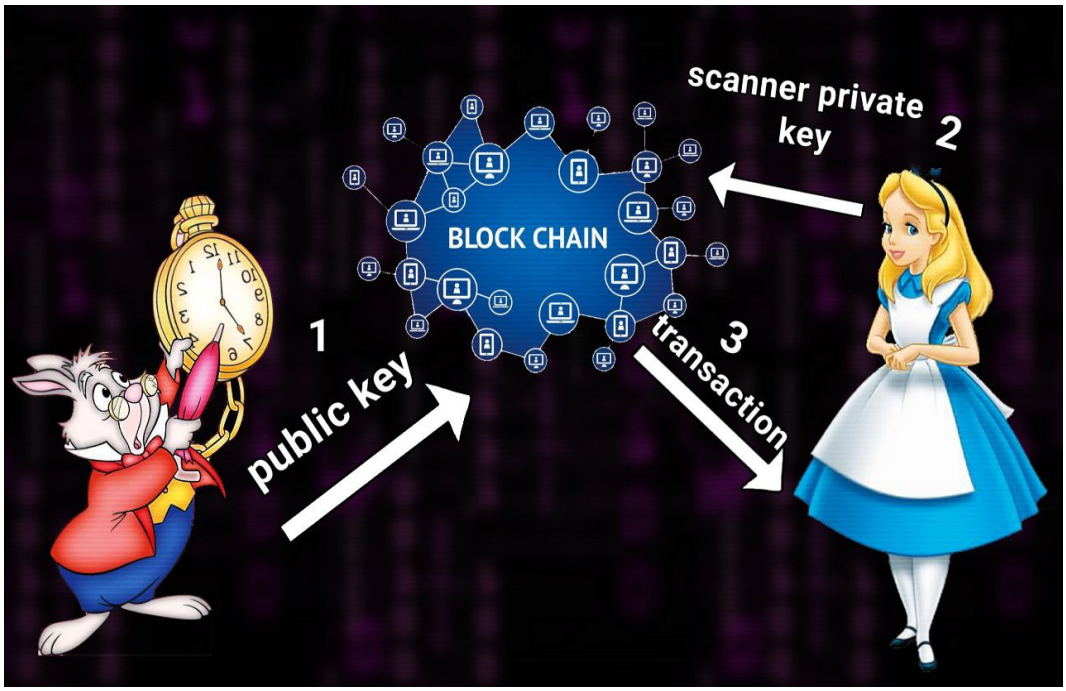
1.1.2 Как Monero скрывает суммы перевода?

Теперь о сумме перевода. Чтобы никто не мог узнать, сколько именно вы отправили, Monero использует технологию RingCT. Она шифрует сумму перевода с помощью сложных математических методов, таких как обязательства Педерсена. Эти обязательства позволяют доказать, что транзакция корректна, не раскрывая при этом конкретных цифр. А чтобы транзакции не раздувались в размере и не перегружали сеть, Monero применяет технологию Bulletproofs. Она значительно уменьшает объём данных: если раньше транзакция могла занимать около 13,2 КБ, то теперь её размер сократился примерно до 2,5 КБ.

1.1.3 Как Monero скрывает получателя?

А что с получателем? Monero генерирует одноразовые скрытые адреса для каждой транзакции. Даже если Алиса сто раз отправляет деньги Кролику, никто не догадается, что это один и тот же получатель. Monero создаёт для каждой транзакции уникальный одноразовый адрес. Этот адрес генерируется так, что он выглядит случайным для всех, кроме Кролика, который может распознать и использовать его для получения средств. Это работает с помощью эллиптической криптографии.

Как это происходит?



1. Когда Алиса хочет отправить деньги, она использует публичный адрес Кролика, который состоит из двух частей: view key и spend key.
2. На основе этих ключей и случайного числа, которое генерирует кошелёк Алисы, создаётся одноразовый публичный ключ -тот самый скрытый адрес, уникальный для транзакции.
3. Этот ключ записывается в блокчейн, но внешне он не связан с адресом Кролика.
4. Кролик, используя свой приватный ключ просмотра, сканирует блокчейн и определяет, что транзакция предназначена ему.
5. Затем, с помощью своего приватного ключа траты, он вычисляет одноразовый приватный ключ, который позволяет ему получить доступ к деньгам.

Для стороннего наблюдателя все эти адреса выглядят как случайные наборы данных, и связать их с Кроликом невозможно.

Эллиптическая криптография, на которой это основано, использует математические свойства эллиптических кривых для создания безопасных ключей. В Monero применяется кривая Curve25519.

1.1.4 Защита Monero на сетевом уровне

На сетевом уровне Monero тоже не спит. Есть штука под названием Dandelion++, которая маскирует, откуда пошла ваша транзакция, чтобы никто не вычислил вашы следы. А ещё есть Kovri — интеграция с I2P, которая прячет ваш IP-адрес. Если вы синхронизируете кошелёк через чужой узел, без Kovri владелец узла может подсмотреть ваш IP, но не сами транзакции — кольцевые подписи и шифрование всё ещё сохраняют относительную приватность.

1.1.5 Кратко про майнинг в Monero

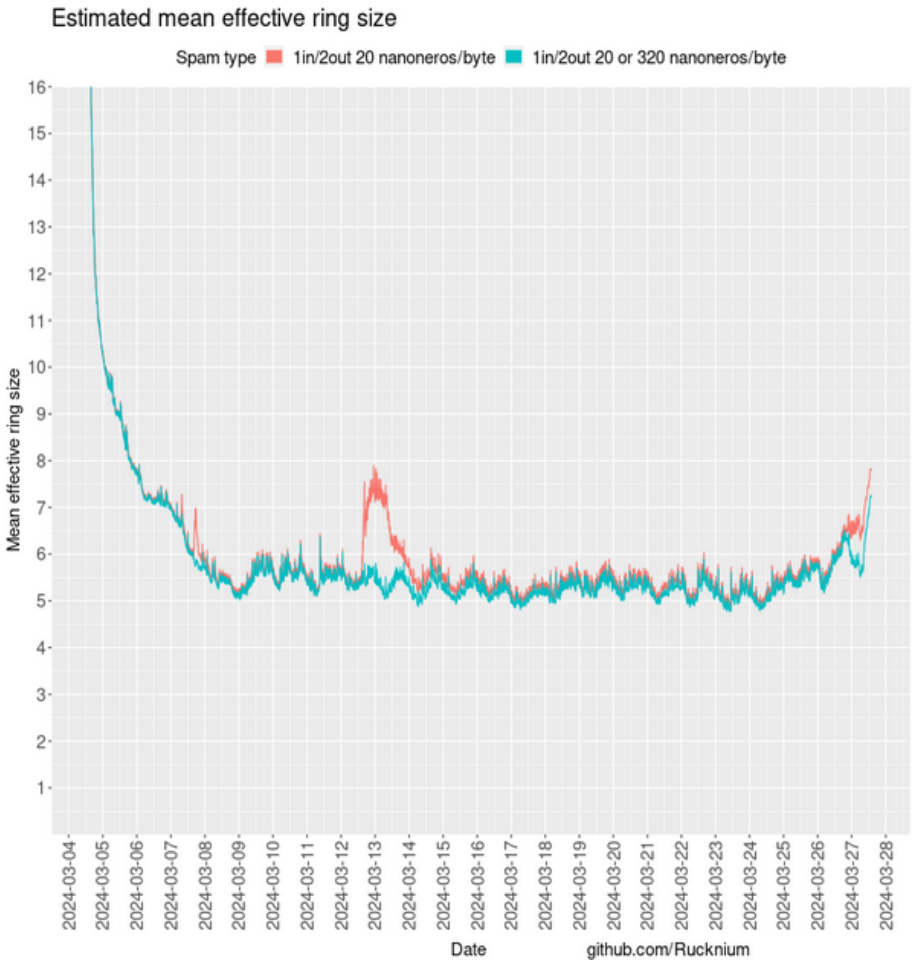
Майнинг в Monero - это отдельная песня. В отличие от Bitcoin, где майнеры с мощными ASIC-фермами правят балом, Monero использует алгоритм CryptoNight, который даёт шанс даже вашему старенькому ноутбуку. Это подход, чтобы никто не монополизировал сеть. CryptoNight требует много памяти, так что специализированное оборудование не получает большого преимущества. Плюс, Monero регулярно обновляет алгоритм, чтобы держать ASIC-майнеры на расстоянии.

2 Атаки на Monero

Атаки на Monero нацелены на подрыв её главного козыря — анонимности, используя уязвимости в криптографии, сетевом уровне или человеческом факторе. Некоторые думают, что Monero вообще не имеет уязвимостей, и атаковать её невозможно, но это совсем не так, да, атаки на неё бывают сложны в реализации. Но тем не менее они возможны, и это стоит учитывать, чтобы защитить себя.

2.1 Виды атак

2.1.1 Black Marble Flooding



Одна из интересных атак носит название Black Marble Flooding. Суть в том, что она спамит сеть кучей своих транзакций, чтобы заполнить кольцевые подписи своими данными. В Monero каждая транзакция скрывается среди 16 выходов — один настоящий, а остальные 15 — подставные (декои, как я писала ранее), чтобы никто не понял, кто отправил деньги. Злоумышленник создаёт множество транзакций, где, например, один вход превращается в два или даже 8–16 выходов, и все они под его контролем. Если эти выходы начинают попадать в кольца других пользователей, то большинство декоев в таком кольце оказываются фальшивыми и принадлежат атакующему. Это сильно снижает анонимность, потому что вероятность угадать настоящий выход становится выше. В худшем случае,

если почти все декои принадлежат злоумышленнику, анонимность пропадает полностью, и транзакция становится прозрачной, как, собственно, в обычном блокчейне от Bitcoin :)

Такая атака не только угрожает вашей приватности, но и создаёт проблемы для сети. Потому что в ней, злоумышленник использует минимальные комиссии, чтобы его транзакции были дешёвыми, и закидывает ими пул транзакций, где они ждут включения в блоки. Это может перегрузить сеть, вызывая задержки в подтверждении транзакций, которые иногда длятся часами, и раздувает размер блокчейна, нагружая компьютеры, поддерживающие сеть. Затраты на атаку невелики — несколько десятков XMR за пару недель, что делает её +- экономически доступной. Однако такие атаки не так уж часто встречаются, потому что их организация требует времени и каких не каких, но ресурсов, а эффект часто не точечный, ибо они вредят анонимности всей сети, а не конкретного человека, которого надо вычислить.

2.1.2 EAE

Другая атака, известная как EAE, бьёт по тем, кто работает с биржами. Главная проблема этой атаки в том, что кольцевые подписи не могут полностью защитить, если вы напрямую связываете свои действия через биржу. Они видят, какие монеты приходят и уходят, и могут связать их с вашим KYC-профилем. Допустим, вы выводите Monero с биржи на свой кошелёк, а потом отправляете их обратно на ту же или другую биржу. Кольцевые подписи, которые в Monero прячут отправителя, смешивая ваш перевод с 15 фальшивками, не всегда спасают. Биржа записывает, какие монеты (UTXO) вы забрали, и когда вы возвращаете их, она видит эти же монеты. Если они попадают в кольцо, биржа может с большой вероятностью понять, что отправитель — это вы, особенно если хранит данные о ваших действиях. Чтобы этого избежать, можно использовать инструменты вроде Kovri для маскировки IP или отправлять монеты через несколько кошельков, чтобы запутать следы, но про меры защиты мы поговорим позже.

2.1.3 Атака на те же ключи в форках Monero

Повторное использование ключей в форках — ещё одна угроза. Monero — это не только основная сеть, иногда появляются её форки, вроде MoneroB. Если вы используете один и тот же ключ в обеих сетях, аналитик может сравнить транзакции и вычислить реальные выходы. Допустим, вы создаёте транзакцию в Monero, где ваш реальный выход смешивается с пятью декоями. В форке вы делаете другую транзакцию, и тот же выход снова появляется в кольце с другими декоями. Аналитик видит, что этот выход присутствует в обоих кольцах, и делает вывод, что он ваш. Хуже того, если кто-то другой использует ваш выход как декой в своём кольце, аналитик может исключить его как фейковый, уменьшая анонимность других

транзакций. Механика атаки проста: форки создают параллельные цепи, где одни и те же ключи выдают совпадения, и злоумышленник, сравнивая блокчейны, может сузить круг подозреваемых.

2.1.4 Сетевые атаки на Monero

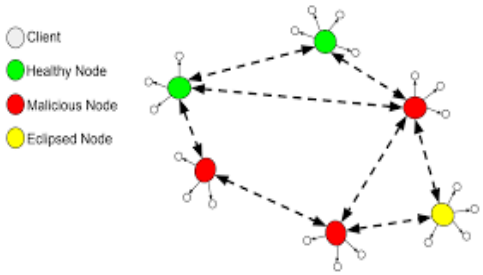
Сетевые атаки через Tor или I2P нацелены на метаданные. Хотя блокчейн Monero скрывает отправителя, получателя и сумму с помощью кольцевых подписей и других методов, он не маскирует сетевые следы. Если вы подключаетесь через Tor, I2P или чужой узел Monero, злоумышленник, контролирующий такой узел, может записать ваш IP и точное время отправки транзакции. Сопоставив эти данные с TXID, он может связать её с вами, даже если содержимое транзакции зашифровано. Атака становится опаснее, если злоумышленник управляет несколькими узлами в Tor, I2P или сети Monero. Чем больше узлов под его контролем, тем больше метаданных он собирает. Например, в Tor скомпрометированный выходной узел или в I2P ненадёжные узлы могут выдать ваш IP. Если вы используете удалённый узел Monero, он видит все ваши транзакции, и, если он вредоносный, ваши метаданные сразу попадают к атакующему. Эта атака корреляции времени работает, вычисляя совпадения между вашим IP, временем и TXID, что позволяет связать вашу активность с конкретными транзакциями.

2.1.5 Атака через каналы в сети P2P

Есть ещё исследование от Стэнфордского университета про Linking Anonymous Transactions. Они нашли, что через побочные каналы в сети P2P можно вычислить узел получателя транзакции. Как? Оказывается, кошелёк Monero по-разному обрабатывал транзакции в зависимости от того, получатель вы или просто сторонний наблюдатель. Когда твой кошелёк пытается расшифровать каждую транзакцию в блоке, он дольше возится, если ты получатель, потому что ему надо проверять, твои ли это деньги. Эти микросекундные задержки видны в сетевом трафике, и, если злоумышленник контролирует много узлов, он их замечает. Хуже того, он может построить целую карту транзакций, связав их с твоим узлом. Даже если ты используешь локальный узел, атака всё равно может сработать, хотя тут уже нужны серьёзные ресурсы и мозги, чтобы всё настроить. Если пользователь не использовал Tor или I2P, это значительно увелчивало возможность атаки.

Но сейчас эта уязвимость уже исправлена. После обнаружения уязвимостей исследователи из Стэнфорда ответственно сообщили о них разработчикам Monero, и в версии клиента v0.15.0 были внедрены исправления, устраняющие эти проблемы. А именно, поменяли алгоритмы обновления блоков и обработки транзакций, чтобы кошелёк не выдавал себя задержками.

2.1.6 Атака Eclipse Attack

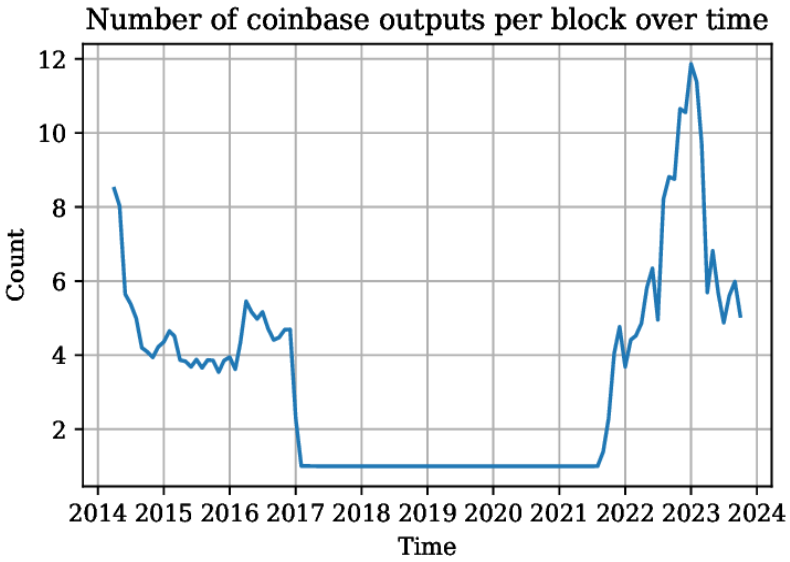


Атака Eclipse Attack идёт ещё дальше. Злоумышленник пытается изолировать ваш узел от обычных узлов сети, окружая его своими вредоносными узлами. Когда ваш узел отправляет транзакцию, она проходит через эти узлы, принадлежащие злоумышленнику, которые записывают ваш IP-адрес, время отправки и уникальный TXID. Так злоумышленник может связать вашу активность с конкретными транзакциями.

Механика атаки проста: Злоумышленник начинает с того, чтобы заполнить список контактов вашего узла своими серверами. Когда ваш узел подключается к сети Monero, он выбирает другие узлы из списка, чтобы отправлять и получать данные. Для этого, злоумышленник может запустить много своих узлов и сделать так, чтобы они выглядели как обычные участники сети. Он может, например, отправлять вашему узлу сообщения, предлагая подключиться к его серверам, или подменять ответы от сети, чтобы ваш узел видел только его узлы. Иногда он специально перегружает ваш узел ложными подключениями, чтобы вынудить его сбросить старые связи и выбрать новые — те, что контролирует он сам. Более настойчивый злоумышленник может манипулировать сетью вокруг вас. Например, он может использовать свои узлы, чтобы быстро отвечать на запросы вашего узла, делая их более привлекательными для подключения, чем честные узлы. Или он может блокировать ваши попытки связаться с другими участниками сети, создавая иллюзию, что его серверы — единственные доступные. Если у него много ресурсов, он может даже временно нарушить работу честных узлов, чтобы ваш узел чаще выбирал его поддельные серверы. Когда ваш узел полностью изолирован, злоумышленник получает контроль над тем, что вы видите и отправляете.

Даже с технологией Dandelion++, Eclipse Attack остаётся угрозой. Dandelion++ усложняет отслеживание, но если ваш узел полностью окружён вредоносными узлами, злоумышленник всё равно видит вашу активность в сети. Хотя такую атаку сложно провернуть, она очень опасна, потому что может полностью разрушить вашу анонимность и в отличие от Black Marble Flooding, нацелена на более конкретного человека.

2.1.7 Coinbase Output Heuristic



Coinbase Output Heuristic — это атака, использующая особенности майнинговых выходов. В кольцевых подписях реальный выход смешивается с декоями, но coinbase-выходы, которые майнеры получают как награду, редко бывают реальными, так как их тратят позже. Аналитик исключает такие выходы из анализа, уменьшая эффективный размер кольца. Например, если в кольце из 16 выходов несколько — coinbase, аналитик отбрасывает их, и вероятность вычислить реальный выход растёт. Механика атаки опирается на знание природы выходов: майнинговые транзакции легко отличить, что позволяет сузить круг подозреваемых и подорвать анонимность, особенно если кольца небольшие. Когда вы отправляете деньги, выход смешивается с декоями. Но среди этих декоев могут быть так называемые coinbase-выходы — это свежие монеты, которые майнеры получают как награду за добычу блока. Такие монеты обычно тратятся не сразу, а позже, поэтому они редко бывают настоящей частью вашей транзакции. Злоумышленник, зная это, может просто убрать coinbase-выходы из кольца, потому что они почти наверняка декои. Допустим, в кольце 16 выходов, и пять из них — coinbase. Если аналитик убирает их, остаётся меньше вариантов, среди которых спрятан ваш настоящий перевод. Чем больше coinbase-выходов в кольце, тем легче сузить круг и повысить шансы вычислить вашу транзакцию. Эта атака работает, потому что coinbase-выходы легко опознать в блокчейне, они помечены как награды майнерам. Да, такая атака не полностью деанонимизирует транзакции, но тем не менее она помогает в их вычислении.

2.1.8 Ring Attack

Стоит упомянуть и криптографические атаки на Monero. Первая в списке - Monero Ring Attack, которая была особенно актуальна до 2019 года. Тогда в Monero ещё использовались Payment ID.

Это такие метки, чтобы биржи или сервисы могли понять, кто и за что платит. Проблема в том, что эти ID давали злоумышленнику шанс вычислить реальный выход в кольцевой подписи. Представьте: вы отправляете транзакцию, она смешивается с 15 декоями, но Payment ID как бы намекал, куда идут деньги. Аналитик мог сопоставить ID с выходом и сказать: «Ага, вот настоящий перевод!» Это снижало анонимность до уровня, где можно было связать транзакцию с конкретным кошельком. К счастью, в 2019 году Monero отказалась от Payment ID, так что эта атака ушла в прошлое, но в своё время она доставила хлопот.

2.1.9 OSPEAD

Ещё одна атака - OSPEAD, он же Map Decoder Attack. Это метод, который, по словам исследователей, может снизить приватность Monero аж на 23%. И самое паршивое — он до сих пор актуален, и решения пока нет. Суть в том, что Monero строит кольца с декоями, полагаясь на гамма-распределение, чтобы замаскировать настоящие траты. Но вот засада: реальные транзакции по времени и структуре отличаются от фальшивых декоев, и OSPEAD этим пользуется. Атака разделяет данные блокчейна на два слоя: реальные траты и декойный шум. Для реализации используются статистические модели, которые ищут закономерности в транзакциях. А именно используется **параметрическое моделирование** и **непараметрическое моделирование**.

Параметрическое моделирование - использует заранее заданное распределение, например гамма или нормальное, и подбирает параметры, что-

бы выделить реальные траты.

А непараметрическое моделирование - в свою очередь анализирует данные напрямую через эмпирические распределения, это помогает справляться с нестандартными ситуациями, когда декои ведут себя необычно.

Самое важное в этой атаке это алгоритм Bonhomme-Jochmans-Robin (BJR). Он ищет выбросы, будь то аномальные комиссии или настройки кошелька, и выдаёт точный результат. Всё это реализуется через пакет decoyanalysis на языке R, который прогоняет данные с блокчейна, строя вероятностные плотности и оценивая параметры распределений.

Если комбинировать эту атаку с другими, например, с Black Marble Flooding, о которой я писала раньше, то можно вообще деанонимизировать транзакции чуть ли не полностью, где то на 73%. Но так, средняя вероятность деанонимизации - около 23,5%, что делает кольцо размером 16, с эффективностью всего 4,2. Для рядового хакера это слишком замороченно и дорого, но для правительства такая атака вполне возможна.

2.1.10 Leveraging Output Merging

Дальше - Leveraging Output Merging, или атака на объединение выходов. Это когда вы отправляете деньги самому себе (так называемый churning, чтобы запутать следы), кошелёк разбивает твои средства на два выхода: основную сумму и «сдачу» на новый адрес. Если декоев в кольцевых подписях маловато, аналитик видит шаблон, где оба выхода кричат: «Это один и тот же человек!».

Проблема в том, что, если кольцо маленькое или в кошельке есть проблемы с настройками, след становится заметнее. Раньше, до 2016 года, Monero вообще допускала нулевые кольца, и транзакции очень просто было вычислить. Даже с нынешним минимумом в 15 декоев неправильный churn может выдать вас. Если вы отправляете монеты по цепочке, один выход остаётся в новых транзакциях, а другой пропадает, потому что Monero любит свежие выходы для декоев. Мёртвые выходы со временем выпадают из колец, и аналитик видит только «живой» след. Чтобы этого избежать, нужно быть осторожнее с настройками кошелька.

2.1.11 Temporal Analysis

Теперь о Temporal Analysis, или анализ времени транзакций. Это когда злоумышленник смотрит, в какое время транзакции появляются в блокчейне, и пытается угадать реальный выход в кольцевой подписи. Механизм Temporal Analysis основан на предположении, что реальные траты пользователей часто имеют характерные временные особенности. Например, если пользователь только что получил монеты (то есть выходы в блокчейне совсем "свежие") и сразу же их тратит, это создаёт шаблон, который

можно выявить. Как вы помните, Monero каждая транзакция включает кольцевую подпись, состоящую из одного реального выхода и нескольких декоев, выбранных из блокчейна. На момент 2025 года стандартный размер кольца в Monero составляет 16 выходов, из которых 15 — декои. Однако исследования, показывают, что, если злоумышленник имеет доступ к временным меткам блоков или даже точному времени трансляции транзакций (например, через перехват сетевого трафика), он может предположить, что самый "свежий" выход в кольце с большей вероятностью является реальным. Это связано с тем, что пользователи часто тратят недавно полученные монеты, а алгоритм выбора декоев, основанный на гамма-распределении, не всегда идеально маскирует эти временные корреляции.

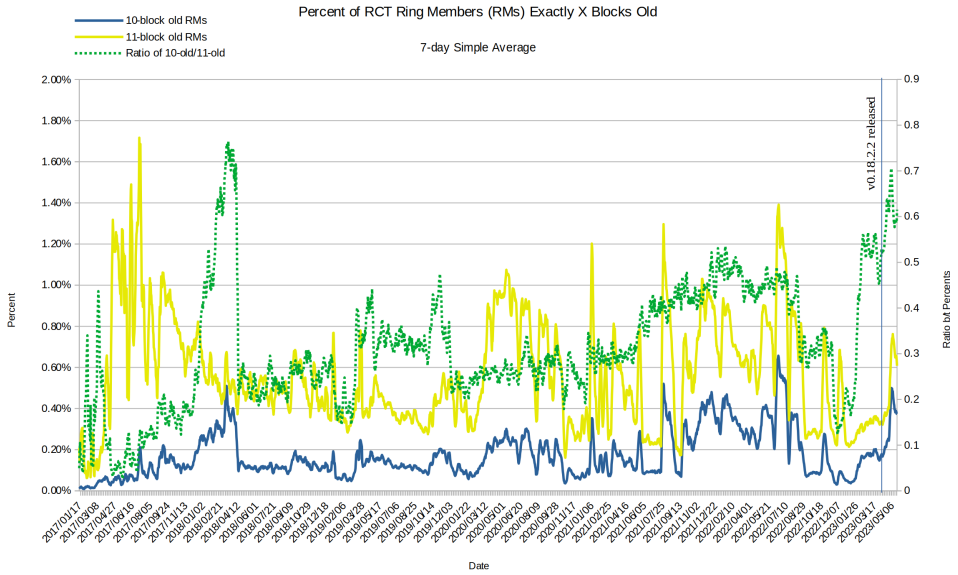
Эффективность Temporal Analysis зависит от нескольких факторов. Во-первых, размер кольца играет важную роль: чем меньше кольцо, тем проще злоумышленнику сузить круг возможных реальных выходов. Например, в ранних версиях Monero, когда размер кольца мог быть равен нулю или очень малым, такие атаки были особенно эффективны, позволяя с высокой точностью идентифицировать реальный выход. После введения обязательного минимального размера кольца и RingCT (Ring Confidential Transactions) в 2017 году уязвимость частично уменьшилась, но не исчезла полностью. Во-вторых, атака становится более точной, если злоумышленник может комбинировать временной анализ с другими данными, например, с информацией о транзакциях, полученной через уязвимости в выборе декоев (как в случае с "10 Block Decoy Bug", исправленной в 2023 году) или с атаками типа Black Marble Flooding, которые заполняют блокчейн контролируемыми транзакциями, чтобы упростить анализ. Временной анализ может угадывать реальный выход с точностью до 80% в транзакциях с одним или несколькими декоями, если используются старые данные или уязвимые настройки кошельков.

2.1.12 Burning Bug

Ещё есть немного устаревшая уязвимость, тем не менее я не могу её не упомянуть. Burning Bug - это старая уязвимость в Monero, которая позволяла злоумышленнику сделать деньги жертвы недоступными для использования, хотя они и отображались в кошельке. Представьте, что у вас есть кошелёк, где лежат ваши Monero, и кто-то отправляет вам несколько переводов на один и тот же адрес. На экране вы видите, что деньги пришли, но из-за ошибки в системе вы не можете их потратить — они как будто "сгорели". Суть атаки в том, что злоумышленник отправлял много транзакций на один и тот же адрес жертвы. В Monero для каждой транзакции создаётся уникальный одноразовый адрес, чтобы сохранить анонимность. Но из-за ошибки в RingCT (технологии, которая скрывает суммы транзакций) кошелёк жертвы неправильно обрабатывал эти повторные переводы на один адрес. В результате кошелёк показывал, что деньги есть, но часть из них становилась "замороженной" — вы не могли их отправить или использо-

вать. Это происходило из-за сбоя в том, как кошелёк проверял и учитывал входящие транзакции: он путался, когда несколько переводов шли на один адрес, и часть средств становилась недоступной. Эта уязвимость была исправлена разработчиками Monero в обновлениях протокола вскоре после её обнаружения (примерно в 2017 году). Атака не раскрывала, кто вы, но могла серьёзно навредить, потому что ваши деньги превращались в бесполезные цифры на экране.

2.1.13 10 Block Decoy Bug



Напоследок, ещё одна старая атака, а именно 10 Block Decoy Bug, была связана с ошибкой в выборе декоев. Как вы помните, Monero прячет транзакцию, смешивая её с подставными декоями. Но из-за этой ошибки система слишком часто выбирала одни и те же декои, созданные ровно 10 блоков назад, что делало их предсказуемыми. Это работало, потому что в ранних версиях Monero алгоритм, который подбирал декои, имел баг: он с большой вероятностью брал выходы, созданные ровно 10 блоков назад (примерно 20 минут назад, так как блоки в Monero появляются каждые 2 минуты). Это создавало шаблон, который аналитики могли заметить. Если в кольце был выход, созданный 10 блоков назад, он с высокой вероятностью был настоящим, а не декоем. Злоумышленник мог изучить блокчейн, отследить этот паттерн и сузить круг возможных настоящих выходов, что делало легче вычислить ваш перевод. Эта уязвимость не ломала Monero полностью, но сильно ослабляла анонимность. Разработчики Monero исправили этот баг ещё в 2017 году, обновив алгоритм выбора декоев. Теперь

декои выбираются более случайно, без привязки к конкретному количеству блоков, что убирает шаблон.

2.2 Примеры реальных атак на Monero

Monero гордится своей репутацией очень приватной криптовалюты, но на практике на нёё уже были успешные атаки, которые показали что даже её защита может дать трещины. Забегая вперед могу сказать, что многие из этих атак, связанны с техническими ограничениями или человеческим фактором. Но, давайте разберём, как эти атаки происходили, почему они сработали и какие уроки можно извлечь!

2.2.1 Атака Black Marble Flooding (март 2024)

Источники:

- **GitHub**, «Potential measures against a black marble attack»
- Defeating a Black Marble Flood Against Monero: Best Options for Ring Size and Transaction Fee

В начале марта 2024 года сеть Monero столкнулась с атакой, известной как Black Marble Flooding. С 4 по 27 марта число транзакций в сутки взлетело с привычных 15–25 тысяч до дикого уровня в 115–140 тысяч -явно ненормальный скачок. Злоумышленник закидал блокчейн спам-транзакциями, чтобы его подконтрольные выходы заполонили кольцевые подписи других пользователей. Кольцевая подпись в Monero смешивает реальный выход фейковыми декоями, чтобы скрыть, кто тратит средства. Однако, если большинство декоев принадлежат атакующему, он может вычислить реальный выход, снижая анонимность. Во время атаки эффективный размер кольца, то есть число неподконтрольных декоев, рухнул до 5,5, а местами вообще до 1, что делало некоторые транзакции почти прозрачными. Злоумышленник использовал два типа транзакций: с одним входом и двумя выходами (1-in/2-out) или с одним входом и 8–16 выходами (1-in/8-16-out), платя минимальные комиссии — от 20 до 320 нанонеро за байт. В итоге за 23 дня он потратил всего 1,3 XMR, что по тогдашнему курсу было где-то 6500–9000 евро. Атака вышла относительно дешёвой, для таких масштабов, особенно если это делало правительство.

Мехника атаки

Механика атаки была простой: злоумышленник создавал тысячи транзакций, которые попадали в пул и включались в блоки. Эти транзакции генерировали выходы, которые затем автоматически выбирались в кольцевые подписи других пользователей. Поскольку атакующий знал свои выходы, он мог исключить их как фейковые, увеличивая вероятность определения реального выхода. Самый большой удар понесли пользователи, которые,

использовали низкие комиссии, так как их транзакции дольше оставались в пуле, где атакующий мог манипулировать составом колец.

Атака ещё и перегружала пул транзакций, из-за чего подтверждения задерживались до трёх часов, а размер блокчейна раздулся на 1,7 ГБ, добавив проблем узлам.

Правда ли это была атака?

Некоторые в сообществе Monero спорили, атака ли это или просто случайный всплеск активности, но анализ Rucknium, который проанализировал данные, подтвердил, что это была именно атака. После 27 марта объёмы транзакций немного устаканились, но до 29 мая ещё пару раз были небольшие всплески, хотя они, скорее всего, не связаны с этой атакой. Зато чуть позже заметили подозрительный рост транзакций типа 1-in/8-16-out - похоже, это был менее заметный способ продолжить атаку.

Но дело не только в том, атака это или случайность. Даже если это не было атакой (в чём я сомневаюсь), сам факт, что такое возможно сделать, причём относительно недорого, - это немного пугает. Ведь если государство или другие структуры захотят отследить Monero, они смогут сделать это без особого труда.

2.2.2 Случай отслеживание Monero через биржу

Источники:

- **BleepingComputer, 31 января 2024**: «Vastaamo hacker traced via 'untraceable' Monero transactions, police says»
- **itez.com, 31 января 2024:** «What's the catch with Finnish law enforcement Monero tracing»

В 2024 году Финская Национальная Бюро Криминальной Полиции, или просто KRP, сумела отследить транзакции Monero, которые вел Юлиус Александр Кивимяки, хакер, обвиняемый во взломе психотерапевтической клиники Vastaamo в 2020 году. Этот парень взломал базу данных клиники, и украл записи 33 000 пациентов, после этого он начал требовать выкуп в 40 BTC, что на тот момент тянуло примерно на 450 000 евро. Когда клиника отказалась платить, он переключился на шантаж отдельных клиентов, вымогая от 200 до 500 евро в Bitcoin. Чтобы замести следы, Кивимяки решил: конвертировал Bitcoin в Monero. Для этого он, перекидывал деньги на свой кошелёк через не-KYC биржу, а потом отправил на Binance, где снова обменял на Bitcoin. Но, как оказалось использовать Binance для обмена денег оказалось ошибкой. Потому что KRP, работая с Binance вычислила этот путь.

Как вычислили Кивимяки?

В октябре 2020 года полиция пошла на хитрость: отправила 0,1 BTC на адрес хакера, чтобы собрать метаданные, типа IP-адресов и времени транзакций. Этот «гениальный хакер» был настолько «аккуратен», что случайно слил данные со своего компа, включая папку с информацией о транзакциях, чем сильно облегчил жизнь следствию. В итоге в январе 2024 года прокуроры выкатили новые доказательства, основанные на анализе блокчейна Monero, которые прямо указывали на Кивимяки. В апреле того же года его приговорили к 6 годам и 3 месяцам тюрьмы.

Какая была механика атаки? Как вы понимайте механика в данной атаки была больше не в взломе протокола Monero, а в ошибках самого хакера. Конвертация Bitcoin в Monero и обратно через биржи, особенно через Binance с её KYC/AML, - это просто глупо. А ещё он умудрился спалить свой IP и слить личные данные.

Но вернёмся к делу: биржи, как я уже говорила, могут отслеживать входные и выходные UTXO, а кольцевые подписи не спасли Кивимяки, потому что он не использовал собственный узел и при этом не прятал IP через Tor или Kovri. Плюс KRP, похоже, применила атакуpoisoned outputs, подмешивая свои выходы в блокчейн, чтобы отследить их в кольцевых подписях. Это, скорее всего, помогло связать транзакции, хотя точные методы полиция держит в секрете.

Почему атака сработала?

Хакер оказался очень глупым, кхм... Использование KYC-биржи, вроде Binance, стало его главной ошибкой—- биржа просто слила властям данные о его личности. А утечка данных с его компа только добила ситуацию, дав следствию прямой доступ к истории транзакций. Ну и, конечно, небрежное хранение ключей тоже сыграло свою роль.

2.2.3 Утечка видео Chainalysis

Источники:

- **Cointelegraph**: Leaked Chainalysis video suggests Monero transactions may be traceable
- **Binance**: Leaked Chainalysis video suggests Monero transactions may be traceable
- Privacy of Monero in Question After Chainalysis Surveillance Leak
- **Тред на Reddit:** Tracing Monero via malicious nodes
- Monero Expert Fact Checks Chainalysis Video Claiming XMR Transactions Can Be Traced

В сентябре 2024 года произошла занятная история: утекло видео от Chainalysis, которое, похоже, по ошибке выложили 10–11 сентября. В этом видео компания хвасталась, что ещё с 2021 года умеет отслеживать транзакции Monero с помощью своих «вредоносных» узлов. Видео быстро стёрли, но копии уже разлетелись по сообществу, и начались жаркие споры. Chainalysis запустила кучу узлов Monero по всему миру, через разных интернет-провайдеров, чтобы собирать IP-адреса и временные метки транзакций. Эти узлы работали как фейковые прокси, выхватывая метаданные у пользователей, которые ленились запускать собственные узлы. Смешивая эти данные с анализом блокчейна и, возможно, подмешивая «отравленные» декои в кольцевые подписи, Chainalysis могла связать транзакции с IP-адресами, что било по анонимности. В видео уточнили, что они не взламывают кольцевые подписи или RingCT, а просто используют метаданные, вроде времени и IP, которые пользователи не защитили.

Как проходила атака?

Схема атаки была завязана на слабости сетевого уровня. Если юзер подключался к удалённому узлу вместо своего, он сам, не зная того, сливал метаданные. Chainalysis, управляя кучей таких узлов, собирала достаточно информации, чтобы привязать IP-адреса к TXID, то есть идентификаторам транзакций. Если не использовать Tor или Kovri, твой IP будет виден, а временные метки помогали связать транзакции с конкретным устройством.

Насколько опасна эта атака на деле?

Цилла Бример, одна из важных фигур в совете Monero, сразу вышла с опровержением, заявив, что атака работает только против тех, кто не заморачивается с собственным узлом или Tor/I2P. Она напомнила про партнёрство с Umbrel, которое позволяет легко поднять узел Monero на сервере или даже на Raspberry Pi, и посоветовала всем так делать. В сообществе эту утечку восприняли как попытку Chainalysis навести панику, ведь по факту, если следовать правильным практикам и использовать свои узлы, такие атаки не очень опасны.

Тем не менее, многие пользователи не утруждают себя запуском собственных узлов или использованием I2P/Tor, и это дало возможность собрать кучу данных. Monero защищает данные на уровне блокчейна, но сетевой уровень может подвести, если подключаться через чужие узлы. Chainalysis просто использовала эту дыру, настроив кучу узлов, которые собирали метаданные. Вывод, настраивайте свои узлы и защищайте их правильно.

2.2.4 Отслеживание транзакций японской полицией

Источники:

- **Binance:** Monero Decoded? Japanese Police Report Breakthrough in Stream Analysis Development
- **Оригнальная Японская новость:** Suspected credit card fraud, money laundering suspect arrested, 100 million yen loss

В октябре 2024 года японская полиция знатно вскрыла мошенническую схему, которая нанесла ущерб на 100 миллионов иен (примерно $663,000). Во главе аферы стоял 26-летний Юта Кобаяши, которого считают лидером банды из как минимум 18 человек. Эти ребята использовали Monero, чтобы отмывать деньги, добытые через кардерство. Но, как оказалось, даже Monero не спасла их от правосудия — полиция отследила около 900 транзакций в этой крипте, и это привело к аресту Кобаяши и его подельников.

Как действовала группировка?

Схема мошенничества была построена на классическом фишинге: группа Кобаяши получала данные кредитных карт через поддельные сайты и фишинговые письма. С этими данными они выводили деньги через торговую площадку Mercari, где выставляли фейковые товары и «покупали» их, используя украденные кредитки. Только за июнь-июль 2021 года они провернули 42 таких операции, украв 2,75 миллиона иен.

Как полицая выследила группировку?

Полиция начала копать под эту группировку ещё в августе 2024 года, когда к расследованию подключилась недавно созданная в апреле того же года киберспецгруппа Национального полицейского агентства NPA), они взялись за дело всерьёз. Кобаяши попал в их поле зрения благодаря перехваченным чатам в защищённых мессенджерах, где он общался со своими подельниками.

Но самое интересное - как полиция вышла на след Monero? Подробности, конечно, держат в секрете, но, судя по всему, японские киберкопы применили комбинацию методов. Один из них - запуск «вредоносных» узлов Monero, которые работали как ловушки для сбора метаданных: IP-адресов, временных меток транзакций и прочей инфы. Похоже на методы Chainalysis, не правда ли? Эти узлы могли притворяться обычными прокси, к которым подключались пользователи, не утруждавшие себя запуском собственных узлов. Скорее всего, полиция комбинировала эти данные с анализом блокчейна и, возможно, подмешивала «отравленные» декои, чтобы легче отслеживать транзакции.

Ведь если кто-то (например, полиция) контролирует кучу узлов или добавляет свои декои, они могут собрать достаточно метаданных, чтобы связать транзакции с конкретными IP или даже личностями. Судя по всему, банда Кобаяши не особо заморачивалась с безопасностью: они не использовали Tor или I2P, не запускали свои узлы, а, возможно, просто светили свои

IP, подключаясь к сторонним узлам. Ещё хуже, если они конвертировали Monero в другие валюты через биржи с KYC (верификацией личности) - это могло стать для полиции настоящим подарком. Плюс, если жертвы мошенников сообщали о переводах в XMR или даже BTC, которые потом конвертировались в Monero, у следствия появился целый кластер из 900 транзакций для анализа.

А правда ли отследили транзакции Monero?

По количеству данных об этой атаке в открытых источниках возможно, что японская полиция отследила злоумышленников как-то иначе. Например, через Японскую отечественную площадку ***Mercari***, где злоумышленники отмывали средства, или мессенджеры, в которых те общались. Не исключено, что про Monero полиция упомянула просто чтобы запугать людей. Впрочем, вариант с реальной атакой в принципе тоже возможен, ведь в Азии не особенно любят вдаваться в детали расследований, и, возможно, поэтому не рассказали подробнее о методах отслеживания Monero.

3 Защита Monero

Monero выстроило мощную систему защиты, которая делает его одной из самых конфиденциальных криптовалют на рынке. Его архитектура, основанная на протоколе CryptoNote, сочетает криптографические и сетевые механизмы, чтобы скрыть отправителя, получателя и сумму каждой транзакции. Эти решения, вместе с децентрализованным управлением и активным сообществом, обеспечивают Monero устойчивость к атакам и дают преимущества перед другими блокчейнами, такими как Bitcoin или Zcash. Да-

вайте разберём, как Monero защищается и почему он остаётся впереди.

3.1 Защита которая уже есть в Monero

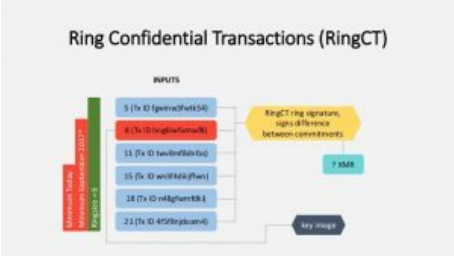
3.1.1 Кольцевые подписи

Кольцевые подписи это фундамент анонимности Monero: Когда вы отправляете транзакцию, ваш реальный выход UTXO смешивается с 15 фейковыми выходами, или декоями, формируя кольцо из 16 элементов. Это создаёт неразбериху для аналитиков, которые не могут точно определить, какой выход принадлежит отправителю. С версии 0.18 Monero использует схему CLSAG (Compact Linkable Spontaneous Anonymous Group), которая улучшает эффективность по сравнению с предыдущей MLSAG, сокращая размер подписи примерно на 20%. Это уменьшает вычислительную нагрузку и комиссии, сохраняя анонимность. CLSAG защищает отправителя, делая практически невозможным связать его с транзакцией без внешних данных, таких как метаданные с бирж или сетевых узлов. Даже если злоумышленник анализирует блокчейн, он сталкивается с множеством возможных отправителей, что делает деанонимизацию крайне сложной. Этот механизм эффективно противостоит атакам, таким как Coinbase Output Heuristic, где аналитики пытаются исключить майнинговые выходы, но увеличение размера кольца (до 25–40 в краткосрочных планах) ещё больше усложняет их задачу.

3.1.2 Скрытые адреса

Скрытые адреса защищают получателя: Monero не использует постоянный публичный адрес, а создаёт для каждой транзакции уникальный скрытый адрес. Отправитель формирует этот адрес, смешивая публичный адрес получателя со случайными данными. Получатель может восстановить закрытую часть ключа и получить деньги, но для всех остальных адрес выглядит как случайный набор символов. Это мешает связать несколько транзакций с одним человеком, даже если вы отправляете ему деньги много раз. Скрытые адреса защищают от атак типа EAE (хотя у бирж всё же есть методы отслеживания), где биржи с KYC/AML пытаются связать входы и выходы, так как одноразовые адреса не дают возможности коррелировать транзакции. Эта система делает невозможным определение получателя без доступа к его приватному ключу.

3.1.3 RingCT



RingCT: Monero прячет суммы транзакций с помощью обязательств Педерсена и доказательств диапазона через Bulletproofs. Обязательства Педерсена шифруют сумму, но показывают, что входы равны выходам, сохраняя блокчейн честным. Bulletproofs, введённые в 2018 году, проверяют, что суммы положительные и в допустимом диапазоне, не раскрывая их. Они уменьшили размер транзакций с 13,2 КБ до примерно 2,5 КБ, снизив комиссии и улучшив работу сети. RingCT защищает от анализа транзакций, который в блокчейнах вроде Bitcoin может выдать, как и зачем вы тратите деньги.

3.1.4 Защита на сетевом уровне

На сетевом уровне Monero использует Dandelion++ для маскировки транзакций: Когда вы отправляете транзакцию в Monero, она сначала проходит «стеблевую» фазу, где передаётся случайным узлам, а потом «фазу пуха», где распространяется по всей сети. Это запутывает путь транзакции, так что исходный IP-адрес не вычислить, если только злоумышленник не контролирует много узлов. Dandelion++ защищает от атак затмения и сетевых атак, вроде тех, что Chainalysis пыталась использовать в 2024 году для связи IP с транзакциями. Ещё есть Kovri — проект на основе I2P, который скрывает IP, направляя трафик через анонимную сеть. Kovri пока в разработке, но после внедрения он защитит от атак, таких как использовала Финская полиция, где IP-метаданные помогли вычислить пользователя. С Kovri сеть станет ещё устойчивее к сбору данных, даже если вы подключаетесь через удалённые узлы.

3.1.5 Защита майнинга

Эгалитарный майнинг это ещё одна линия обороны: Monero использует алгоритм CryptoNight, который подходит для обычных процессоров и видеокарт, а не для ASIC, как в Bitcoin. Он требует много памяти, из-за чего ASIC становятся невыгодными. Monero регулярно меняет алгоритм через хардфорки, чтобы майнинг не сосредотачивался в одних руках. После добычи 18,132 млн XMR сеть перешла на хвостовую эмиссию — 0,6

XMR каждые две минуты, чтобы майнеры продолжали поддерживать безопасность. Это защищает сеть от крупных пулов, которые могли бы контролировать транзакции или блокировать их, сохраняя децентрализацию и устойчивость к атакам на консенсус.

3.1.6 Динамический размер блока

Динамический размер блока позволяет Monero адаптироваться к нагрузке: Блоки могут достигать 300 КБ без штрафа, а при превышении майнеры платят штраф, рассчитываемый по формуле: Штраф = BaseReward * ((BlockSize / MN) — 1)², где MN — медиана размера блока за последние 100 блоков. Это защищает сеть от спама, как в атаке Black Marble Flooding в марте 2024 года, когда злоумышленник пытался перегрузить пул транзакций. Динамическая система позволяет обрабатывать всплески активности, минимизируя задержки, которые могут достигать трёх часов при атаках. Регулярные хардфорки, проводимые сообществом, внедряют улучшения, такие как CLSAG, RingCT и Bulletproofs, а в будущем — FCMP++ (через 12–18 месяцев) для устранения уязвимостей кольцевых подписей и Seraphis (через 5+ лет) для нового протокола транзакций.

3.1.7 Доступные меры защиты для юзера

Пользовательские меры усиливают защиту: Monero позволяет пользователю самому себя защитить. Например, запуск собственного узла снижает риски, связанные с внешними узлами, которые могут собирать данные, как делала Chainalysis. Использование Kovri или Tor прячет IP-адрес, защищая от сетевых атак, вроде тех, что помогли Финской полиции в 2024 году. Если избегать бирж с KYC/AML, можно предотвратить атаки EAE, где биржи связывают транзакции с личностью. При грамотном подходе Monero становится очень безопасным.

3.2 Преимущества Monero

Теперь поговорим о преимуществах Monero.

Первое, обязательная приватность. В отличие от Zcash, где анонимность опциональна (только 1–2% транзакций используют zkSNARKs, Monero применяет кольцевые подписи, скрытые адреса и RingCT ко всем транзакциям. Это создаёт единый анонимный пул, где все XMR взаимозаменяемы. В Bitcoin «грязные» монеты можно отследить и пометить, что создаёт риски для пользователей и продавцов. В Monero такого риска нет — все монеты равны, и их история не поддаётся анализу.

Второе, преимущество децентрализованное управление и финансирование. Monero не имеет центральной команды, а разработки финансируются через Forum Funding System (FFS). Хотя это создаёт риск «без-

билетника», когда пользователи пользуются результатами без вклада, FFS профинансировала ключевые улучшения, такие как Bulletproofs и Kovri. Monero Research Lab активно работает над устранением уязвимостей, таких как атака Black Marble Flooding, предлагая краткосрочные меры (увеличение размера кольца до 25–40, повышение минимальной комиссии до 80 нанонеро/байт) и долгосрочные решения (FCMP++, Seraphis). Эти пратики делают Monero устойчивым к внешнему давлению.

Третье, устойчивость к атакам. Случаи 2024 года, такие как Black Marble Flooding, работа Финской полиции и утечка Chainalysis, показали, что в основном уязвимости Monero связаны не с протоколом, а с пользовательскими ошибками или сетевыми слабыми местами. Запуск собственного узла и использование Kovri/Tor защитит вас от атак, основанные на метаданных, как в случае с Chainalysis. Увеличение размера кольца и оптимизация выбора декоев защищают от спама, как в Black Marble Flooding. Активное сообщество и регулярные хардфорки позволяют Monero быстро адаптироваться к угрозам.

Наконец, философия Monero. Его обязательная приватность, децентрализованный майнинг и гибкость сети создают систему, устойчивую к цензуре и регуляторам. В мире, где прозрачные блокчейны всё чаще отслеживаются, Monero остаётся убежищем для тех, кто ценит анонимность. Несмотря на проблемы масштабируемости (транзакции в 30 раз больше, чем у Bitcoin, с комиссиями около 0,013 XMR) и перегрузки пула при атаках, Monero продолжает совершенствоваться, предлагая пользователям инструменты для полной защиты их данных.

3.3 Меры защиты для пользователя

Несмотря на угрозы безопасности, Monero остаётся одной из самых защищённых криптовалют. Сейчас я объясню, почему это так, и какие меры вы можете использовать, чтобы сохранить свою анонимность и безопасность. Вы уже знаете из начала статьи, что Monero построена на протоколе CryptoNote. Она использует мощные инструменты: кольцевые подписи CLSAG, скрытые адреса и RingCT с Bulletproofs. Эти механизмы скрывают, кто отправил деньги, кому и сколько, делая блокчейн сложным для анализа. Также есть сетевые инструменты, такие как Dandelion++, который мешает отследить ваш IP, и Kovri, который сделает это ещё надёжнее. Активное сообщество Monero- ещё один плюс: разработчики и пользователи быстро реагируют на проблемы, предлагают улучшения и финансируют их через Forum Funding System

Большинство атак на Monero случаются из-за того, что пользователи что-то не так настроили или вообще забили на безопасность. Атаки, которые затрагивают сам протокол, устраняются разработчиками довольно быстро. Например, то же случай с Black Marble Flooding, она снизила эф-

фективность кольцевых подписей до 5,5 или даже 1, но разработчики быстро подсуетились: увеличили размер кольца до 25–40 и задрали минимальную комиссию до 80 нанонеро за байт. А в будущем вообще планируются улучшения вроде FCMP++ и Seraphis. FCMP++ ожидается через 12–18 месяцев, и он значительно повысит анонимность и масштабируемость сети. Seraphis — это долгосрочный проект, запланированный примерно через пять лет. Он полностью переработает структуру транзакций Monero, вводя новые типы адресов и схемы подписи, которые сделают протокол устойчивее к атакам, включая добавления постквантовых алгоритмов в криптографии. Seraphis также улучшит производительность, уменьшив размер транзакций, что снизит комиссии и нагрузку на сеть.

3.3.1 Сами меры защиты

Теперь я расскажу о мерах защиты, чтобы избежать фальшивых узлов и других угроз.

Для начала самое важное: запускайте свой собственный узел Monero. Это очень важно, чтобы не зависеть от внешних узлов, которые могут быть вредными, как в случае с Chainalysis, где фальшивые узлы собирали IP и временные метки. Настройка узла не требует особых знаний: используйте официальный кошелёк Monero GUI или CLI на компьютере. Для настройки узла выделите около 170 ГБ для полного блокчейна (по состоянию на 2024 год) и стабильный интернет. Регулярно обновляйте узел, чтобы он оставался свежим.

Используйте Kovri или Tor для скрытия IP-адреса. Kovri, основанный на I2P, перенаправляет ваш трафик через анонимную сеть. Еще можно настроить Monero CLI для работы через Tor, используя параметр --tx-proxy или прокси-сервер, чтобы отправлять транзакции через onion-адреса. Ну и во время настройки Tor, убедитесь, он настроен без утечек DNS (ниже я напишу, как настроить Tor для работы с Monero)

Избегайте бирж с KYC/AML для обмена или хранения XMR. Атака EAE, описанная в случае с Финской полицией (впрочем, это, наверное, и так было понятно), показала, как биржи, такие как Binance, могут связать входные и выходные UTXO с вашей личностью, если вы проходили проверку. Используйте децентрализованные обменники, или платформы без KYC. Если биржа неизбежна, можете отправить XMR на свой кошелёк, и подождать несколько блоков (например, 10–20), чтобы ложные входы смешались, и только потом переводите дальше. Это снижает шанс связи транзакций. Никогда не возвращайте XMR на ту же биржу, с которой выводили, чтобы избежать анализа EAE.

Не используйте одни и те же ключи в форках Monero. Атака на повторное использование ключей показала, что аналитики могут сравнить транзакции в разных цепях и вычислить реальные выходы. Создавайте новые ключи для каждой сети, особенно если участвуете в раздачах или тестируете форки. Проверьте свой кошелёк на наличие копий ключей и храните их в зашифрованном виде на устройстве без интернета, чтобы избежать утечек.

Используйте высокие комиссии во время возможных атак, таких как Black Marble Flooding. В марте 2024 года спам-транзакции перегружали пул, задерживая подтверждения до трёх часов для транзакций с низкими комиссиями (20–320 нанонеро/байт). Устанавливайте комиссии выше среднего (например, 80 нанонеро/байт), чтобы ваши транзакции быстро попадали в блоки, уменьшая риск проблем с ложными входами (да, это дороже, но думаю безопасность средств важнее низкой комиссии). Для проверки возможных атак на сеть, проверяйте состояние сети через сайты вроде xmrchain.net, чтобы оценить текущую нагрузку и выбрать подходящую комиссию.

Обновляйте кошелёк и следите за хардфорками. Monero регулярно добавляет улучшения, такие как CLSAG или Bulletproofs, через хардфорки, которые закрывают слабые места, вроде 10 Block Decoy Bug или Burning Bug. Используйте последнюю версию официального кошелька (GUI или CLI) и проверяйте объявления на getmonero.org или в сообществе Reddit (r/Monero).

Ну и при желании отслеживайте новости в сообществе Monero. Следите за обсуждениями на GitHub (monero-project/research-lab) или форумах, чтобы знать о угрозах, таких как Black Marble, и новых способах защиты.

3.3.2 Что вы не можете изменить в Monero?

Эти меры помогают сделать вашу анонимность в Monero почти полной и решают многие недостатки. У Monero есть проблемы, например, транзакции в 30 раз больше, чем у Bitcoin, и комиссии около 0,013 XMR, но разработчики работают над их улучшением. Иногда сеть перегружается из-за атак, но это не вредит приватности, если вы всё делаете правильно.

3.4 Практика защиты Monero

Пришло время практике, в этом разделе я расскажу, как запустить свою ноду. Вам понадобится Debian, минимум 170 ГБ на диске (блокчейн растёт на 1–2 ГБ в месяц), стабильный интернет и комп с 4 ГБ оперативки и SSD для скорости. Если у вас старый ноут или Raspberry Pi, тоже сойдёт, но синхронизация будет дольше.

3.4.1 Установка Monero

Сначала подготовьте систему.

Сборка monerod из исходников

Откройте терминал и обновите Debian, чтобы все пакеты были актуальными:

```
sudo apt update && sudo apt upgrade -y
```

Установите зависимости, необходимые для сборки Monero - это пакеты для компиляции кода, работы с сетью и криптографией:

```
sudo apt install build-essential libboost-all-dev
cmake pkg-config libssl-dev libzmq3-dev libunbound-dev
libsodium-dev libexpat1-dev libgpg-error-dev
libgcrypt20-dev libboost-all-dev git -y
```

Скачайте исходный код Monero. Перейдите в домашнюю папку:

```
cd ~
```

Склонируйте официальный репозиторий Monero, чтобы получить все необходимые файлы для сборки:

```
git clone --recursive https://github.com/monero-project/monero.git
```

Перейдите в папку Monero:

```
cd monero
```

Переключитесь на стабильную версию:

```
git checkout release-v0.18
```

Проверьте на getmonero.org актуальную версию на 2024 год это v0.18, но может быть новее.

Создайте папку для сборки, чтобы не засорять исходный код:

```
mkdir build
```

Перейдите в неё:

```
cd build
```

Настройте проект с помощью CMake, которая генерирует файлы для компиляции:

```
cmake ..
```

Соберите и установите Monero, используя все доступные ядра процессора для ускорения процесса:

```
make -j$(nproc)
sudo make install
```

Это установит Monero в /usr/local/bin.

Скачивание monerod с офицального сайта

Если не хотите собирать monerod из исходников, можно просто скачать его с офицального сайта:

```
wget https://downloads.getmonero.org/cli/monero-linux-x64-v0.18.3.4.tar.bz2
tar -xvjf monero-linux-x64-v0.18.3.4.tar.bz2
cd monero-linux-x64-v0.18.3.4
```

Настройка блокчейна

Создайте папку для блокчейна и дайте себе права на неё, чтобы избежать проблем с доступом:

```
mkdir -p ~/.bitmonero
sudo chown $USER:$USER ~/.bitmonero
```

Запустите ноду для синхронизации блокчейна:

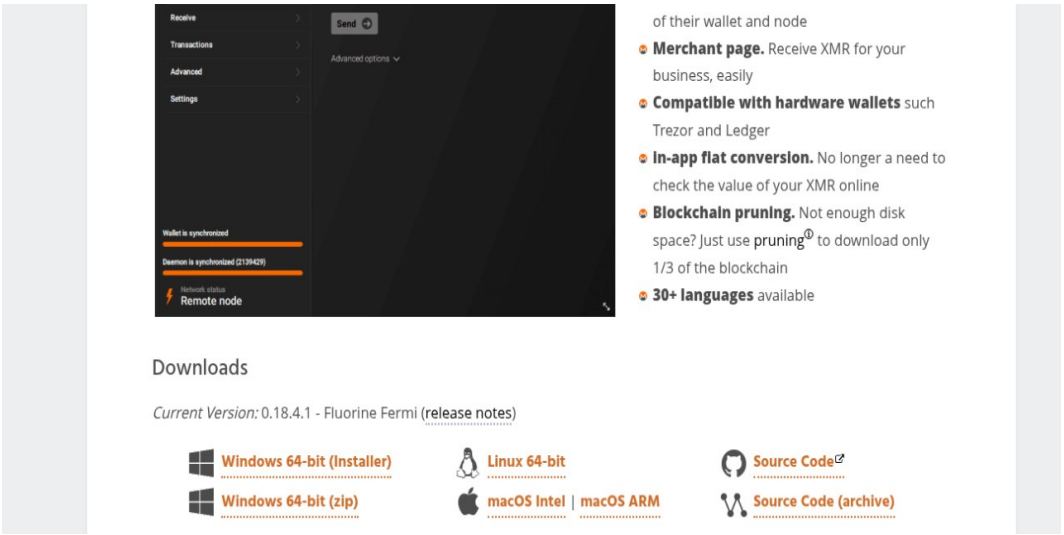
```
monerod --data-dir ~/.bitmonero --log-file ~/.bitmonero/monero.log
--log-level 0
```

Это может занять от нескольких часов до пары дней, в зависимости от оборудования и интернета

Проверяйте прогресс синхронизации с помощью этой команды, которая покажет текущий статус и высоту блока:

```
monerod status
```

Установка Monero GUI



Скачайте Monero GUI с http://getmonero.org/downloads/ (версия для Linux 64-бит).

Распакуйте архив, например, в ~/monero-gui:

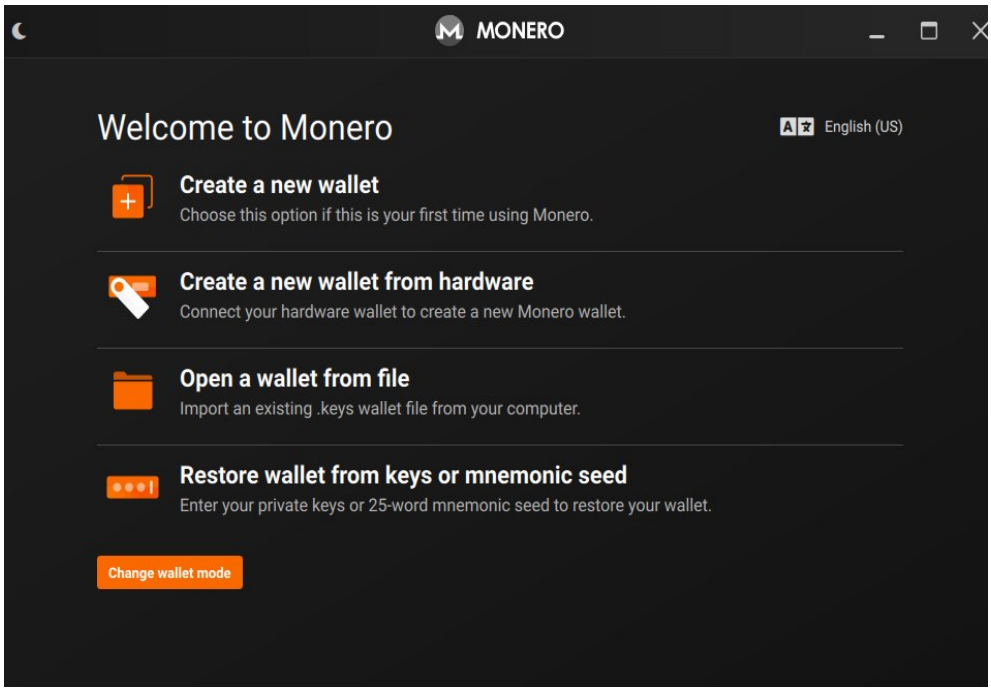
Перейдите в папку с GUI:

```
cd ~/monero-gui-v0.18.4.1
```

Запустите кошелёк:

```
./monero-wallet-gui
```

При первом запуске выберите "Create a new wallet" Или восстановите кошелёк, если у вас есть сид-фраза:



3.4.2 Запуск Monero через Tor

Для защиты IP настройте Tor, чтобы никто не мог отследить ваши транзакции, как это было в случае с Финской полицией.

Сначала установите Tor:

```
sudo apt install tor -y
```

Включите и запустите службу:

```
sudo systemctl enable tor
sudo systemctl start tor
```

Откройте конфигурационный файл Tor:

```
sudo nano /etc/tor/torrc
```

Добавьте в конец файла строки:

```
HiddenServiceDir /var/lib/tor/monero/
HiddenServicePort 18083 127.0.0.1:18083
HiddenServicePort 18084 127.0.0.1:18084
```

Сохраните файл (Ctrl+O, Enter, Ctrl+X) и перезапустите Tor:

```
sudo systemctl restart tor
```

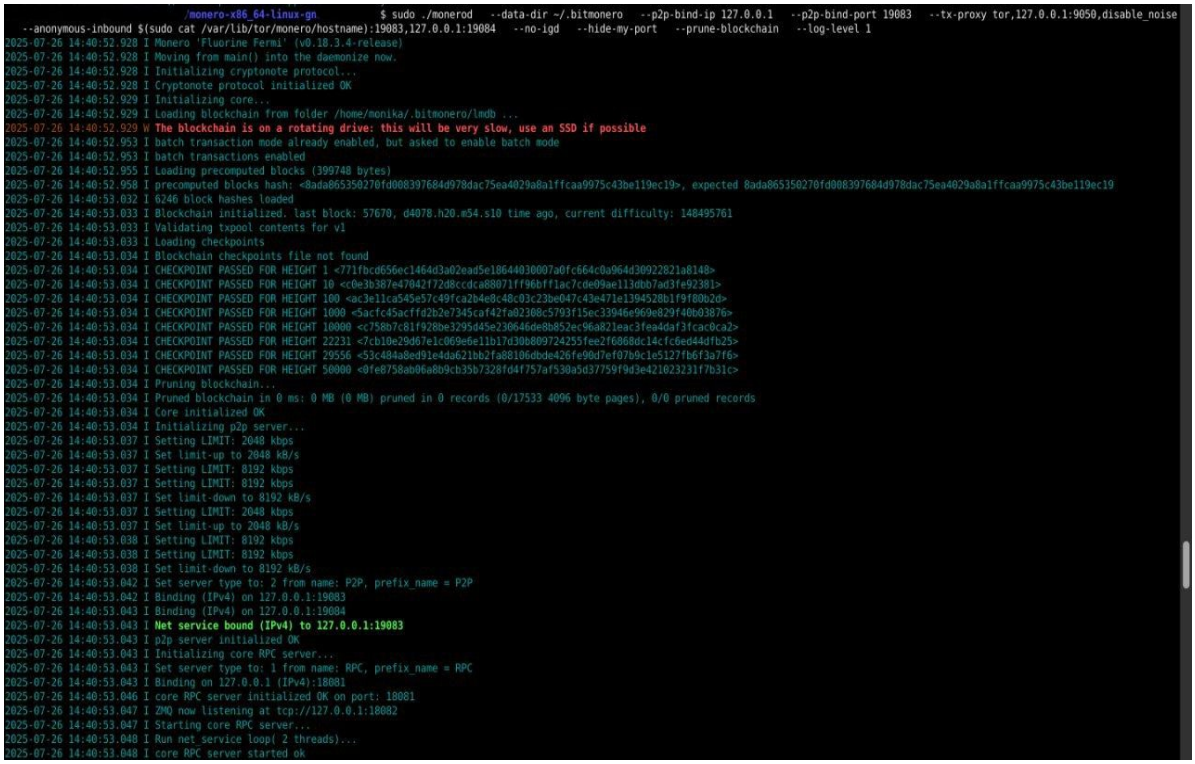
Узнайте ваш onion-адрес для ноды:

```
sudo cat /var/lib/tor/monero/hostname
```

Запустите ноду с использованием Tor, чтобы скрыть IP:

```
sudo ./monerod --data-dir ~/.bitmonero --p2p-bind-ip 127.0.0.1
--p2p-bind-port 19083 --tx-proxy tor,127.0.0.1:9050,disable_noise
--anonymous-inbound $(sudo cat /var/lib/tor/monero/hostname):19083,127.0.0.1:19084
--no-igd --hide-my-port --prune-blockchain
--log-level 1
```

Результат:



Эти параметры спрячут ваш IP и ограничат доступ к ноде через onion-адрес.

Настройка Firewall

Для дополнительной защиты можно настроить firewall:

```
sudo apt install ufw -y
sudo ufw allow 9050/tcp comment 'Tor'
sudo ufw allow 18083/tcp comment 'Monero P2P'
sudo ufw allow 18084/tcp comment 'Monero RPC'
sudo ufw enable
```

Правильная настройка DNS через Tor

```
Откройте: /etc/tor/torrc.
sudo nano /etc/tor/torrc
```

Добавьте строки:

```
DNSPort 9053
AutomapHostsOnResolve 1
```

Перезапустите Tor:

```
sudo systemctl restart tor
```

3.4.3 Настройка Monero с Kovri

Если хотите попробовать Kovri (I2P для Monero), учтите, что он пока в альфа-версии и менее надёжен.

Установка Kovri

Установите зависимости:

```
sudo apt install libcrypto++-dev libcrypto++-doc libcrypto++-utils
libboost-all-dev libssl-dev cmake git -y
```

Скачайте Kovri:

```
git clone --recursive https://gitlab.com/kovri-project/kovri
```

Перейдите в папку Kovri:

```
cd kovri
```

Настройте и соберите Kovri:

```
make release
make install
```

Создайте папку для данных Kovri:

```
mkdir -p ~/.kovri
sudo chown $USER:$USER ~/.kovri
```

Настройте туннель

Откройте конфигурационный файл:

```
nano ~/.kovri/tunnels.conf
```

Добавьте строки:

```
[XMR_P2P_Server]
type = server
address = 127.0.0.1
port = 18080
in_port = 18080
keys = xmr-p2p-keys.dat
```

Сохраните файл и запустите Kovri:

```
kovri --data-dir ~/.kovri
```

Проверьте ваш I2P-адрес:

```
cat ~/.kovri/client/keys/xmr-p2p-keys.dat.b32.txt
```

Запустите ноду с I2P:

```
monerod --data-dir ~/.bitmonero --rpc-bind-ip 127.0.0.1
--rpc-bind-port 18081 --p2p-bind-ip 127.0.0.1
--p2p-bind-port 18080 --tx-proxy i2p,127.0.0.1:4447
--anonymous-inbound <ваш_i2p_адрес>:18080,127.0.0.1:18080
--no-igd --hide-my-port
```

Kovri пока нестабилен, так что лучше используйте Tor до выхода стабильной версии (ориентировочно 2026 год с FCMP++).

3.4.4 Шифрование файла кошелка

Еще можно зашифровать файлы кошелька:

```
gpg - populate ~/.bitmonero/wallet-file.keys
```

Сохраните зашифрованный файл на флешке или запишите сид-фразу на бумагу и храните в безопасном месте.

3.4.5 Дополнительная защита

Для защиты от атак, таких как Black Marble Flooding 2024 года, когда сеть забивали спамом, используйте высокие комиссии. В Monero GUI в разделе “Send” перед отправкой транзакции выберите приоритет “High” (около 80 нанонеро за байт). Если пул транзакций перегружен (больше 10 МБ, проверьте на xmrchain.net), выберите “Very High” (около 100 нанонеро за байт). Это ускорит подтверждение.

Избегайте бирж с KYC,таких как Binance, чтобы не попасть под анализ. Используйте Bisq или платформы без верификации. Если выводите XMR с биржи, отправьте их на свой кошелёк через GUI, подождите 10–20 блоков (20–40 минут) для смешивания декоев, и только потом переводите дальше. Не возвращайте XMR на ту же биржу.

Создавайте новый кошелёк для форков, чтобы избежать анализа транзакций. В Monero GUI выберите “Create a new wallet” и сохраните сид-фразу.

4 Вывод

Как вывод могу сказать, что, хотя Monero и остаётся одной из самых крутых и безопасных криптовалют на рынке, существует множество атак — от Black Marble Flooding до сетевых, таких как Eclipse, или даже банальных ошибок пользователей, которые могут подорвать анонимность. Вспомните случаи 2024 года: финские полицейские отследили хакера через биржи и метаданные. Это показывает, что протокол Monero хорош, но без тщательной настройки не стоит уповать на судьбу или думать, что "всё само как-нибудь". Атаки эволюционируют, и такие угрозы, как OSPEAD или Temporal Analysis, могут снизить вашу приватность на 75% и более, если

не принимать мер.

4.1 Мое мнение о безопасности Monero

Но хорошая новость: Monero предоставляет все инструменты для защиты. Запускайте собственную ноду, шифруйте трафик через Tor или I2P, избегайте бирж с верификацией, используйте высокие комиссии во время всплесков активности и следите за обновлениями.

Плюс, разработчики не сидят сложа руки: впереди FCMP++ и Seraphis, которые устранят текущие уязвимости и сделают сеть ещё безопаснее.

Напоследок скажу: чтобы безопасность Monero вас не подвела, держите руку на пульсе. Читайте материалы по Monero и не забывайте про базовую сетевую гигиену. Если всё делать с умом, даже Chainalysis или подобные организации не смогут отследить ваши транзакции. Так что защищайте себя сами и не надейтесь на авось!

4.2 Дополнительные ссылки

OSPEAD - Репозиторий OSPEAD, где вы можете посмотреть его реализацию.

github_issues - Обсуждение атаки Black Marble Flooding. Там проанализировали всплески в 2024 году и предлагают меры защиты вроде повышения комиссий и увеличения ring-size, но многие требуют хардфорка.

monero-xmr-analysis - Подробная статья с разбором Monero, там разобраны ring-подписи, stealth-адреса и RingCT для приватности, плюс майнинг на CryptoNight.

monero-xmr-privacy-potential-and-challenges - Тоже неплохая статья с разбором Monero с точки зрения приватности. Автор разбирает методы обеспечения приватности Monero и сравнивает её с Zcash.

RingCT_Attack - Статья об атаке на RingCT Monero. Помимо описания атаки, предлагаются меры защиты, такие как blacklisting и улучшения протокола.

Traceable_Monero_Anonymous - Ещё одна статья о слежении за Monero с разбором различных моделей угроз и атак.

eclipse-attack - Хорошее исследование eclipse-атаки на P2P Monero.

Zero-to-Monero - Интерсная официальная книга о криптографии Monero. Объясняет ring signatures, stealth addresses, multisig и TxTangle.

Monero_secrety - Сатьтя с анализом RingCT Monero на безопасность, где нашли баги вроде "burning".

misc-research - Репозиторий с кучей интерсных исследований Rucknium по Monero, вроде его криптографии и анализа ring-подписей.

И помните:

Когда Червонная Королева хотела срубить Чеширскому Коту голову, оказалось, что у него есть только голова. Поэтому вы тоже, чтобы избежать вреда, действуйте наперёд!