Loki

Конфиденциальные транзакции, децентрализованное общение.

Kee Jefferys, Simon Harman, Johnathan Ross, Paul McLean

Версия 3

13 июля 2018

Аннотация

Гибридная система proof of work / proof of service (доказательство выполнения работы / доказательство предоставления услуг) предлагает уникальный способ финансового стимулирования работы полных нод. Loki использует стимулированные ноды для создания вторичного приватного слоя маршрутизации. Минимально-необходимая работа нод второго уровня контролируется с помощью нового метода роевых меток. Loki основан на модифицированной версии Monero, что гарантирует высокий уровень конфиденциальности транзакций.
Этот документ описывает технологию, применяемую в Loki. Мы предполагаем, что по мере разработки в неё будут вноситься изменения. Для отражения этих изменений будут выпущены новые версии текущего документа.

1 Введение

Спрос на конфиденциальность цифрового общения и приватность транзакций постоянно растет. Существующие объемы сбора, обработки и продажи пользовательских данных являются беспрецедентными. Все данные пользователей, начиная от истории браузера и содержимого электронной почты, и заканчивая кредитным рейтингом и покупательскими предпочтениями, собираются, распространяются и продаются между крупнейшими корпорациями и государственными структурами. Loki планирует предоставить набор защищенных от цензуры инструментов, которые позволят совершать анонимные транзакции и общаться приватно.

Bitcoin пришел в наш мир, обещая повышение конфиденциальности, однако привел к еще большим возможностям отслеживания и контроля. Некоторые компании, такие как Chainalysis или BlockSeer используют прозрачность блокчейн-сети, чтобы отслеживать интересующие их транзакции [1]. Loki построен на основе Monero, криптовалюты, зарекомендовавшей себя в качестве самой безопасной и анонимной на сегодняшний день [2].

Мы, однако, признаем, что Monero имеет определенное количество недостатков. Транзакции в Monero гораздо объемнее транзакций в Bitcoin, с существенными требованиями к пропускной способности и дисковому пространству. По мере роста сети это приводит к большей нагрузке на ноды, однако владельцы не получают никаких стимулов или вознаграждений за свой вклад в общую сеть. Это превращает содержание ноды в дорогое и зачастую неблагодарное занятие. Внедрение схемы вознаграждения для нод (которые мы называем Сервисными Нодами) улучшит ситуацию, предлагая экономические стимулы для их владельцев.

Сервисные ноды могут быть использованы также для выполнения целого ряда других приватно-ориентированных функций, если будут должным образом стимулированы. В основном сеть Сервисных Нод позволит пользователям передавать и отправлять анонимные пакеты данных. Эта анонимная коммуникация основана на том, что каждая Сервисная Нода выступает в качестве ретранслятора в новой перемешивающей сети (mixnet), устойчивой к атакам Сивиллы (Sybil attack) [3][4]. Более того, эта новая коммуникационная сеть будет использована в качестве основы для децентрализованной службы отправки защищенных методом сквозного шифрования сообщений под названием Мессенджер Loki. Она позволит пользователям общаться напрямую, без участия доверяемых третьих лиц, и без необходимости обеим сторонам быть одновременно в сети онлайн.

Loki – это не только устойчивая среда конфиденциального обмена сообщениями, но и платформа для построения децентрализованных и анонимных интернет-сервисов.

2 Основные характеристики

Цель алгоритма регулирования сложности (время блока)	120 секунд
Алгоритм регулирования сложности	Zawy LWMA [5]
Алгоритм хеширования	CryptoNight Heavy
Эллиптическая кривая	Curve25519 [6]

3 Элементы протокола CryptoNote

Несмотря на то, что механизм стимулированных полных нод можно было бы реализовать на основе любой криптовалюты, Loki выбрал исходный код Monero из-за высокого уровня анонимности проводимых транзакций. Monero является эволюцией протокола CryptoNote, использует кольцевые подписи (ring signatures), скрытые адреса (stealth addresses), кольцевые конфиденциальные транзакции (RingCT), позволяет пользователям подписывать транзакции и обфусцировать их суммы, сохраняя при этом функцию правдоподобного отрицания (plausible deniability) [7].

Для того чтобы экосистема Loki сохраняла конфиденциальность, важно не только обеспечить средства обмена обеспечивающие внутреннюю экономику, но и минимизировать риск связанный с анализом времени (или *временной анализ*) взаимодействий между независимыми слоями Loki. Например, при использовании сервиса транзакций первого уровня, пользователи не должны потерять гарантии конфиденциальности полученные от сервисов второго уровня, и наоборот.

3.1 Кольцевые подписи (ring signatures)

Принцип работы кольцевых подписей заключается в том, что вместо одной подписи отправителя создается кольцо потенциальных создателей транзакции, в котором только один подписант является настоящим отправителем. Loki использует кольцевые подписи для того, чтобы обфусцировать реальную историю выходных параметров транзакции. Кольцевые подписи будут обязательными для всех транзакций внутри Loki (кроме транзакций вознаграждений за нахождение блока), при этом все кольца будут иметь обязательный фиксированный размер в 10 пользователей, что является уникальным отличием Loki от других систем. Это означает, что на каждый вход транзакции создается от одного до десяти потенциальный выходов, включая только один настоящий (см. раздел 6.3).

3.2 Скрытые адреса (stealth addresses)

Loki использует скрытые адреса для того, чтобы реальный публичный адрес получателя не мог быть привязан к транзакции. Каждый раз, когда в Loki отправляется транзакция, генерируется одноразовый скрытый адрес, и перевод отправляется на него. С помощью протокола Диффи-Хеллмана получатель (и никто другой) может рассчитать секретный ключ, позволяющий использовать полученные средства в будущих транзакциях, и таким образом получить доступ на владение средствами без необходимости раскрытия своего настоящего публичного адреса [8]. Скрытые адреса предоставляют защиту получателям транзакции и являются одной из основополагающих функций конфиденциальности в Loki.

3.3 Конфиденциальные транзакции (RingCT)

Конфиденциальные транзакции (RingCT) изначально были предложены Monero Research Lab как способ обфускации суммы транзакции [9]. Текущее решение RingCT основано на диапазонных доказательствах (range proofs), которые используют обязательства Педерсена (Pedersen commitments) для подтверждения, что отправленная сумма находится в диапазоне между 0 и 2^{64}. Такой диапазон позволяет убедиться в том, что отправлена неотрицательная сумма, без необходимости раскрытия реальной суммы транзакции. Недавно, ряд создателей криптовалют предложил реализацию «пуленепробиваемых доказательств» (bulletproofs) в качестве замены традиционных RingCT, поскольку они позволяют значительно уменьшить размеры транзакций [10]. Loki будет использовать bulletproofs, чтобы снизить объемы данных хранимые нодами, таким образом увеличив возможности масштабирования.

4 Сервисные ноды (Service Nodes)

Несмотря на внедрение нововведений поверх протокола CryptoNote (см. раздел 7), большая часть сетевой функциональности и возможностей масштабирования Loki основана на использовании стимулированных нод, которые называются Сервисными Нодами. Для управления Сервисной Нодой, оператор временно блокирует значительную сумму в Loki и предоставляет установленный минимальный уровень пропускной способности

и объемов дискового хранилища для сети Loki. Взамен за свои услуги операторы Сервисных Нод получают часть вознаграждения с каждого блока.

Полученная сеть обеспечивает основанную на рыночных отношениях устойчивость к атакам Сивиллы, устраняя ряд проблем в существующих перемешивающих сетях (mixnets) и других сервисах, ориентированных на конфиденциальность. Такая устойчивость основана на взаимодействии спроса и предложения, которое призвано помешать индивидуальным пользователям накопить сумму в Loki, достаточную для нанесения значительного урона конфиденциальности сервисов второго слоя. DASH первой предложила использование криптоэкономики для построения сетей, устойчивых к атакам Сивиллы [11]. Если злоумышленник начнет накапливать Loki для атаки, количество монет в обращении уменьшится, что приведет к повышению цены. По мере продолжения выкупа монет стоимость покупки будет становиться все более высокой, что сделает потенциальную атаку неоправданно дорогой.

Для достижения описанной экономической защиты, Loki поощряет активное подавление объема монет в обращении. В частности, кривая эмиссии и требования к Сервис Нодам должны быть спроектированы таким образом, чтобы достаточная часть оборота была заблокирована, а операторы получали достаточное вознаграждение для обеспечения защиты от атак Сивиллы.

4.1 Вознаграждение за нахождение блока (Block Reward)

Распределение вознаграждений за нахождение блока в Loki осуществляется через механизм доказательства проделанной работы (proof of work) – надежную и хорошо изученную систему создания блоков и упорядочивания транзакций. Майнеры собирают и записывают транзакции в блоки, получая за это комиссию. В качества правила консенсуса в Loki каждый блок содержит несколько исходящих вознаграждений, из которых только одно предназначено для майнера.

Вознаграждение майнера:
За создание нового блока майнер получает 45% от размера вознаграждения блока наряду с получением оплаты в виде комиссий от транзакций.

Вознаграждение Сервисной Ноды:
Вторым исходящим платежом каждого блока (50% от общей суммы вознаграждения) является платеж Сервисной Ноде или, если выбран режим ретранслятора, двум Сервисным Нодам (см. раздел 6.3). Сервисные Ноды вознаграждаются на основании времени, прошедшего с момента последнего получения вознаграждения (или времени, когда они были зарегистрированы в сети), отдавая предпочтение Нодам, которые ждали дольше остальных. Каждый раз, когда Сервисная Нода регистрируется в сети, она ставится на последнее место в очереди. Если Сервисная Нода предоставляет стабильный сервис и не была удалена из очереди роем (swarm) (см. раздел 8.3), она постепенно продвигается ближе к началу очереди. Когда Ноды из начала очереди получают вознаграждение, они отправляются в конец очереди, начиная продвижения заново.

Governance Reward:
Оставшиеся 5% вознаграждения блока распределяются для операционных нужд (см. раздел 9); 3.75% отправляются на адрес Фонда Loki, который детерминировано определяется каждым блоком, и 1.25% резервируется для выхода блока системы финансирования (см. раздел 9.2.3).

4.2 Подтверждаемое Обеспечение

Сервисные Ноды должны быть способны доказать сети, что они удерживают требуемую сумму обеспечения. Встроенные в Loki Функции конфиденциальности, в особенности, невозможность просматривать балансы публичных адресов или использовать ключи просмотра (viewkeys) для анализа исходящих транзакций, делают такие доказательства сложными.

Loki использует новую функцию временного блокирования средств (выходов транзакций), что позволяет замораживать монеты Loki до достижения блокчейном определенной высоты блока. Пока заданное значение высоты блока не достигнуто, сеть будет аннулировать попытки потратить замороженные выходы. Loki использует этот процесс, чтобы убедиться, что соответствующая сумма удерживается определенной Сервисной Нодой, предотвращая перетасовку обеспечения.

Чтобы зарегистрировать Сервисную Ноду в сети, оператор создает замороженный по времени выход, который автоматически разморозится через минимум 21 600 блоков (примерно 30 дней). В дополнительных полях транзакции оператор Сервисной Ноды указывает адрес, на который он хочет получать вознаграждение. Этот адрес будет также использован в качестве публичного ключа для различных операций, осуществляемых Сервисными Нодами, таких как роевое голосование (swarm voting). Кошелькам имеет смысл не использовать эти регистрирующие транзакции для смешивания, поскольку они содержат реальные суммы и адреса назначения в открытом виде, и соответственно, такие транзакции не предоставляют дополнительную анонимность.

До того как Сервисная Нода подключится к сети, другие Ноды должны независимо подтвердить, что указанное обеспечение Ноды соответствует требуемой сумме согласно текущим требованиям к обеспечению. Несмотря на то, что обеспечивающие транзакции истекают через 30 дней, у кошелька будет возможность автоматизации повторного блокирования обеспечения.

5 Lokinet

Протоколы луковой маршрутизации позволяют создавать туннели или пути через распределенную сеть, используя несколько промежуточных нод для обфускации как получателя, так и инициатора пакетов данных. Сервисные Ноды в сети Loki будут работать на основе протокола луковой маршрутизации с низкой задержкой, образуя полностью децентрализованную оверлейную сеть, называемую Lokinet. Сеть не полагается на доверенные центры, и ее состояние полностью вычисляется из блокчейна. Пользователи могут подключаться к отдельным Сервисным Нодам и создавать двунаправленные пути для маршрутизации пакетов. Сеть может быть использована для доступа к внутренним сервисам, называемым SNApps (см. раздел 6.2). Пользователи также могут использовать функцию выходных Сервисных Нод для навигации во внешнем интернете без раскрытия своего реального IP адреса (см. раздел 6.3).

5.1 Протокол анонимной маршрутизации с низкой задержкой (LLARP)

В основе всех приложений для Сервисных Нод лежит анонимный протокол маршрутизации, который определяет, каким образом каждая Сервисная Нода будет общаться со своими пирами. Loki предлагает новый протокол маршрутизации, называемый LLARP [12], разработанный как гибрид между Tor и I2P для обеспечения дополнительных необходимых свойств, не предлагаемых ни одним из существующих протоколов. LLARP разработан специально для функционирования поверх сети Сервисных Нод Loki, и работа над оптимизацией LLARP велась с учетом этой архитектуры. Для понимания целей LLARP, необходимо произвести анализ существующих протоколов и рассмотреть, как LLARP улучшает их.

Луковый маршрутизатор (Tor)

В последние годы Tor является наиболее популярной анонимной смешивающей сетью. Tor сохраняет высокий уровень сопротивления цензуре и зарекомендовал себя как ценный инструмент для поддержания конфиденциальности в сети интернет. Однако Tor скорее иерархическая сеть, чем децентрализованная. Tor зависит от группы управляющих списками (directory authorities), являющихся централизованными серверами управляемыми добровольцами близкими к Фонду Tor [13]. Управляющие списками выполняют две основные функции. Во-первых, они достоверно сообщают о состоянии нод в сети. Когда пользователь Tor (или нода) подключается к сети впервые, он подключается к одному из 10 жестко заданных серверов управляющих списками. Эти сервера предоставляют пользователю или ноде файл, который называется «консенсус». Этот файл содержит список всех ретрансляторов (relays), сторожевых нод (guard nodes) и выходных нод (exit nodes), исключая мосты (bridges), которые в данный момент работают в сети Tor. Во-вторых, управляющие списками также замеряют пропускную способность предоставляемую отдельными нодами в сети. Эта информация используется для сортировки нод по категориям, и принятия решения, может ли конкретная нода использоваться как ретранслятор, сторожевая или выходная нода.

Такой высокий уровень централизации создает единую точку отказа, которая и делает Tor уязвимым. В 2014 году Tor получил достоверную информацию об угрозе отключения управляющих списками серверов [14]. Если отключить сервера управляющих списками в США, и в дополнение к этому в Германии либо Нидерландах, этого будет достаточно, чтобы отключить пять из десяти управляющих списками серверов. Такое действие приведет к нарушению стабильности сети Tor, при которой возможность новых ретрансляторов взаимодействовать с сетью пострадает значительно.

Методы коммуникации в сети Tor также ограничены, поскольку Tor позволяет взаимодействовать только по протоколу TCP. IP через Tor возможен, но ему не хватает поддержки протоколов на основе UDP (таких, как VoIP).

Проект «Невидимый интернет» (I2P)

I2P использует другой подход к архитектуре смешивающей сети, поддерживая высокий уровень доверия и гибкости с помощью Распределенной Хеш-Таблицы (DHT) для определения состояния сети, вместо доверенных управляющих списками [15]. I2P поддерживает как TCP, так и UDP трафик, что позволяет использовать широкие возможности различных протоколов. Однако у I2P отсутствует стабильный процесс разработки, и за долгое время проект накопил существенный технический долг, особенно в области криптографии. I2P использует 2048-битную схему Эль-Гамаля, шифрование и дешифрование в которой значительно медленнее этих же операций с использованием эллиптической кривой. Несмотря на то что в планах I2P заявлен переход от схемы Эль-Гамаля, прогресс в этом направлении крайне невысок.

В дополнение к этому в I2P отсутствует формальная поддержка выходных нод, то есть доминирующая часть трафика в сети используется для доступа к размещенным внутри неё вебсайтам – так называемым Eepsites. Это значительно снижает возможность получения анонимного доступа к ресурсам внешнего интернета для пользователей сети I2P.

Еще одной особенностью построения I2P является то, что большинство пользователей, подключенных к сети, также являются ретрансляторами. Это черевато дополнительными проблемами, так как в результирующей сети зачастую не хватает достаточной пропускной способности канала для построения быстрых путей маршрутизации. Скорость в смешивающих сетях определяется скоростью самого слабого звена в каждой цепочке. Как результат, если пользователи с низкой пропускной способностью становятся ретрансляторами, общая производительность сети заметно снижается.

Наконец, I2P отличается от Tor в том, что в нем реализована коммутация пакетов, а не коммутация каналов. Вместо того, чтобы организовать один долгоживущий туннель, через который протекает весь трафик, I2P создает множественные пути, через каждый из которых могут проходить пакеты, создавая разные маршруты внутри сети. Это дает возможность I2P прозрачно обходить перегрузки сети и сбои нод.

Ни I2P, ни Tor не исключают возможность атаки Сивиллы полностью. Достаточно мотивированный злоумышленник с запасом времени и финансовыми возможностями для покупки большого количества ретранслирующих нод, может произвести временной анализ, который приведет к нарушению конфиденциальности пользователей. Эффективность анализа повышается с количеством нод, ретрансляторов и сторожевых нод, находящихся под контролем злоумышленника [16]. Tor и I2P полностью управляются добровольцами, которые жертвуют своим временем и деньгами для поддержания жизнедеятельности нод. Мы предполагаем, что сеть, основанная на финансовых стимулах, а не на альтруизме, может достичь большей устойчивости к атакам и предоставлять более надежный сервис.

LLARP

LLARP работает без управляющих списками серверов, и вместо них использует DHT, построенную на транзакциях блокчейна, которая позволяет Сервисным Нодам исполнять роль ретрансляторов в сети. Пропускная способность не измеряется и не записывается в DHT. Вместо этого, измерение пропускной способности и сортировка производится роями (swarms) (см 6.1.1), которые оценивают каждую ноду и делают выводы о возможности предоставлять требуемую пропускную способность сети.

В Базовой Эталонной Модели Взаимодействия Открытых Систем (модель OSI), LLARP

предоставляет только анонимный сетевой слой. Это означает, что он поддерживает более широкий диапазон интернет-протоколов, и также минимизирует накладные расходы на хранение файловых дескрипторов, если выходные ноды проходят через UDP трафик [17]. Дополнительно, LLARP реализует маршрутизацию на основе коммутации пакетов, а не туннелей, что позволяет реализовать лучшее распределение нагрузки и доступность по всей сети.

Конечные пользователи сети Lokinet не должны (и не могут) маршрутизировать пакеты, что делает Lokinet более устойчивой к атакам Сивиллы, поскольку для запуска Сервисной Ноды требуется участие значительного капитала.

6 Сервисы Loki

Подобно инвестициям которые майнеры делают в оборудование, операторы Сервисных Нод должны заморозить монеты Loki для запуска ноды. Такая заморозка решает две задачи:

1. Каждый оператор вложил достаточное количество средств для того, чтобы быть заинтересованным в успехе сети. Если оператор Сервисной Ноды предоставляет низкую производительность сети или совершает нечестные действия, он рискует девальвацией своей доли в сети.
2. Это дает возможность более активного принуждения к соблюдению правил; если сеть имеет возможность ограничивать нечестные ноды в получении вознаграждения, ноды будут нести риски в упущенных вознаграждений в дополнение к уже замороженному залогу.

Допуская что ноды достаточно мотивированны соблюдать правила по описанным выше причинам, представляется возможным создание групп Сервисных Нод, к которым можно было бы обращаться для достижения консенсуса относительно состояния блокчейна или для предоставления дополнительного функционала вне блокчейна (см. пчелиные рои в разделе 6.1.1). В Loki эту функциональность можно разделить на две: сетевую и связанную с хранением данных. Вместе они смогут обеспечить back-end операции для пользовательских приложений – Loki сервисов.

6.1 Мессенджер Loki

Первым сервисом Loki, который будет разработан и запущен в сети, станет децентрализованное приложение для сквозной передачи зашифрованных конфиденциальных сообщений под названием Мессенджер Loki.

Приложения, которые позволяют пользователям отправлять сквозным методом сообщения в шифрованном виде, уже существуют, однако они основываются на централизованных серверах, которые могут быть обнаружены, заблокированы и отключены [18, 19]. Централизованная модель обладает высоким риском для анонимности общающихся сторон, поскольку зачастую требует от пользователя регистрации с помощью номера мобильного телефона или раскрытия другой информации, которая может быть напрямую привязана к IP пользователя. Эта информация может быть извлечена из серверов через утечки данных или на основе юридических действий, предпринимаемых против пользователя. Применяя архитектуру Сервисных Нод в сети Loki, мы можем создать

сервис, схожий с тем, что предлагают популярные централизованные приложения с шифрованием, такие, как Signal, но с более высоким уровнем конфиденциальности и устойчивости к цензуре.

6.1.1 Маршрутизация в Мессенджере

Маршрутизация сообщений в сети Loki зависит от того, находится получатель сообщения онлайн или офлайн. Когда оба пользователя находятся онлайн, сообщения могут обходить процесс хранения на Сервисных Нодах, давая возможность общения с более высокой пропускной способностью.

В Loki публичный ключ является и долговременным ключом шифрования, и адресом маршрутизации. В простейшем случае им следует обмениваться через другие каналы коммуникации, чтобы защититься от атаки “человек посредине”. Такой обмен должен происходить или лично, или через сторонний защищенный метод обмена (см. раздел 6.1.2).

Передача сообщений Онлайн

Предположим, что Алиса получила публичный ключ Боба. Она предполагает, что Боб сейчас находится онлайн и старается проложить к нему путь через сеть. Алиса запрашивает DHT у любой Сервисной Ноды и получает набор Знакомящих Серверов, относящихся к публичному ключу Боба. В LLARP такой набор содержит список Знакомящих Серверов, которые хранит и поддерживает каждый пользователь. Именно через эти сервера сеть может прокладывать пути между пользователями. Зная Знакомящий Сервер Боба, Алиса может выбрать три другие случайные Сервисные Ноды, которые будут служить посредниками между ней и получателем (Знакомящим Сервером Боба). После того как этот путь установлен, Алиса и Боб могут начать обмениваться сообщениями. Если аутентификация прошла удачно и с использованием OTR (см. раздел 6.1.2), Алиса и Боб могут общаться, поддерживая высокий уровень конфиденциальности.

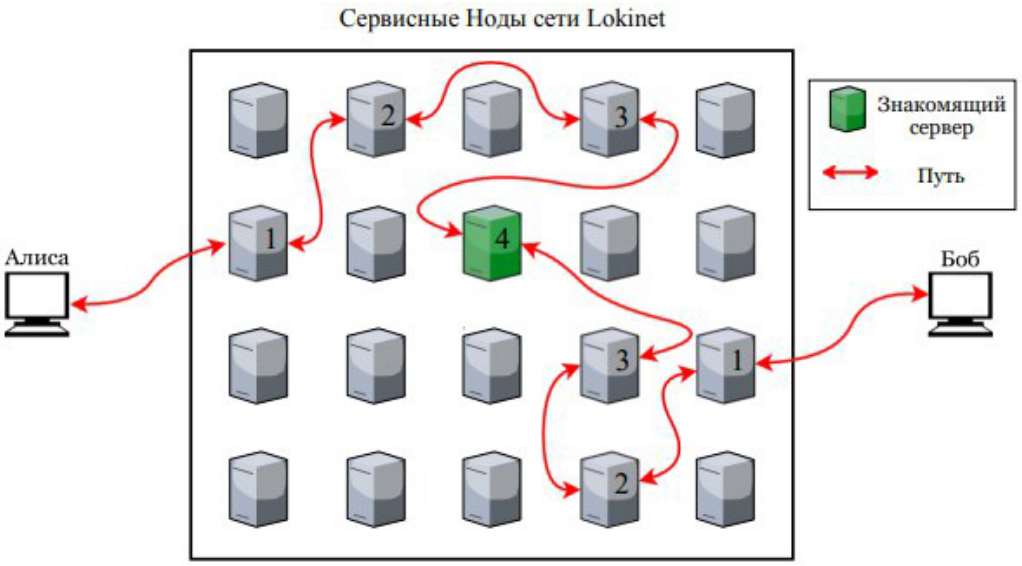

Рис. 1: *Упрощенная версия онлайн-маршрутизации, в которой Алиса общается с Бобом, используя случайную Сервисную Ноду для прокладывания пути через сеть.*

Передача сообщений Офлайн

В случае, если Алисе не удается получить ответ от Боба, она может инициировать процесс офлайн передачи сообщения. Офлайн-маршрутизация использует модифицированную версию Почтовых Серверов поверх Роев (Postal Services over Swarm – PSS) [20]. Рои – это Сервисные Ноды, логически сгруппированные на основе данных об их публичном ключе и хэш-суммы блока, в котором произошла регистрирующая транзакция Сервисной Ноды. Каждый рой имеет идентификатор swarmId и состоит из девяти нод. Чтобы отправить сообщение Бобу, Алисе необходимо определить к какому из роев принадлежит Боб, используя его публичный ключ. Обладая этой информацией, Алиса может анонимно простроить путь для сообщения через сеть к случайной Сервисной Ноде из этого роя. Когда Сервисная Нода получает уникальное сообщение, предназначенное для своего роя, она должна распространить это сообщение оставшимся восьми нодам роя. Все ноды хранят это сообщение в течение определенного времени жизни (Time-to-live – TTL), (см. раздел 8.3). Когда Боб выйдет онлайн, он может опросить любые две ноды в рое на наличие сообщений, которые он способен расшифровать. Офлайн сообщения защищены от спама с помощью небольшого доказательства выполнения работы, прикрепленного к каждому сообщению (см. раздел 8.2)

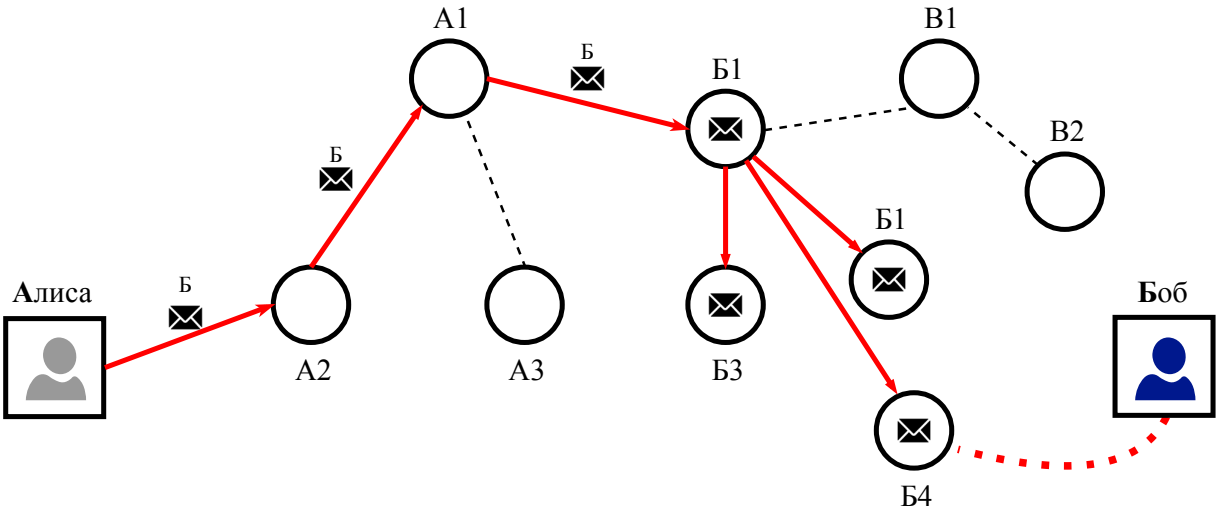

Рис. 2: *Алиса отправляет сообщение Бобу, рой Боба – Б. Когда Боб выходит онлайн, он опрашивает случайную ноду из роя, и получает сообщение от Алисы.*

6.1.2 Шифрование и аутентификация в Мессенджере

После того как цепочка сообщений установлена, Мессенджер Loki обеспечивает соблюдение протоколов Совершенной Прямой Секретности (Perfect forward secrecy – PFS) и Отрицаемой Аутентификации (Deniable Authentication – DA). PFS и DA являются ключевыми понятиями протокола систем мгновенного обмена сообщениями Off The Record (OTR) [21]. Централизованные сервисы, такие как Signal и WhatsApp, используют функции шифрования, поддерживающие защиту OTR. Loki базирует свою реализацию на основе существующего протокола Tox – распределенного, однорангового протокола обмена сообщениями, который основан на хорошо проверенной библиотеке NaCl [22].

PFS позволяет защититься от атак в случае компрометации долговременного ключа.

Для каждой сессии создается новый ключ общего доступа, и, если один сессионный ключ окажется скомпрометированным, цепочка сообщений целиком не будет подвержена риску. Если третье лицо захочет нарушить шифрование цепочки сообщений, оно должно завладеть ключами каждой отдельной сессии. PFS гарантирует, что мессенджер Loki будет чрезвычайно сложно скомпрометировать по сравнению с мессенджерами, основанными на других существующих методах, таких как шифрование Pretty Good Privacy (PGP), в котором одного долговременного ключа достаточно, чтобы вскрыть всю цепочку сообщений.

Отрицаемая Аутентификация (DA) относится к возможности двум сторонам доказать, что именно они являются отправителями каждого следующего сообщения. Однако третья сторона не сможет определить настоящего отправителя сообщения достоверно. При использовании DA, Коды Аутентификации Сообщений (Message Authentication Codes – MACs) публикуются после каждой сессии, позволяя третьим сторонам правдоподобно создавать сообщения, выглядящие так, будто они исходят из публичного адреса отправителя. При правильной реализации третья сторона не сможет доказать, что отправителем конкретного сообщения является именно настоящий отправитель.

Аутентификация Пользователя

Аутентификация пользователей важна, чтобы защититься от атаки «человек посредине» (man-in-the-middle). Например, если Боб ожидает сообщение от Алисы, но пока не знает ее публичного ключа, то третья сторона (Ева) может обмануть Боба и отправить ему сообщение со своим публичным ключом, притворившись Алисой. По этой причине пользователи должны аутентифицировать друг друга до того, как начнут обмениваться личной информацией.

Подобно Pidgin и другим сервисам обмена сообщениями, основанным на OTR, Мессенджер Loki использует аутентификацию заранее переданного ключа (Pre-Shared Key – PSK). У пользователей есть множество возможностей организовать передачу ключа для PSK. Они могут сделать это, используя сторонние каналы связи, или договориться организовать PSK с помощью Мессенджера Loki, задавая вопросы, на которые стороннее лицо не сможет ответить. Loki реализует PSK аутентификацию на основе модифицированного плагина аутентификации Pidgin [23].

6.2 SNApps (Приложения Сервисных Нод)

Функционирование приложений SNApp похоже на работу так называемых «скрытых сервисов» в Tor, которые завоевали популярность. Они дают пользователям возможность общаться внутри окружения смешивающей сети, предоставляя еще больший уровень анонимности, чем тот, что может быть достигнут доступом к внешнему контенту. Приложения SNApp позволяют организовывать и размещать торговые площадки, форумы, информационные вебсайты, социальные сети и другие интернет-приложения на компьютерах и серверах, сохраняя анонимность как на стороне сервера, так и на стороне пользователя. Это значительно расширяет возможности сети и позволяет пользователям строить значимые сообщества внутри сети Lokinet.

Операторы приложений SNApp используют традиционную модель клиент-сервер с тем важным различием, что Сервисные Ноды становятся посредниками в подключении пользователей через сеть Lokinet. Когда приложение SNApp хочет зарегистрироваться в сети, оно должно обновить DHT со своим дескриптором. Этот дескриптор содержит

набор Знакомящих Серверов, являющихся определенными Сервисными Нодами, через которые пользователь может проложить путь к SNApp. Когда эти пути проложены, пользователи могут подключиться к SNApp не раскрывая его расположения внутри сети.

6.3 Выходные Ноды (Exit Nodes)

Выходные ноды позволяют пользователям делать запросы во внешний интернет и возвращать результаты этих запросов через смешивающую сеть. При правильном использовании, выходные ноды позволяют пользователям просматривать интернет без раскрытия своего реального IP-адреса конечному серверу.

Несмотря на то что работа выходных узлов является важным для расширения возможностей Loki, попытка заставить всех операторов Сервисных Нод играть роль выходных нод может оказаться неуспешной. У оператора выходных нод могут возникнуть потенциальные юридические риски, так как некоторые сети пользователи могут совершать вредоносные действия при использовании ноды в качестве прокси. Поскольку выходные ноды ретранслируют трафик от интернета до конечного пользователя, они часто получают запросы о нарушении «Закона об Авторском Праве в Цифровую Эпоху» (Digital Millennium Copyright Act – DMCA) или считаются источниками попыток взлома. Хотя в большинстве юрисдикций законы могут защищать операторов выходных нод, провайдеры интернет-услуг, предоставляющие трафик, могут опасаться юридических рисков и зачастую прекращают обслуживание таких серверов.

При регистрации Сервисной Ноде ставится метка ретранслятора, что ограничивает ее активность маршрутизацией пакетов только внутри сети Lokinet, не позволяя делать запросы во внешний интернет. Оператор должен самостоятельно высказать желание управлять выходной нодой, таким образом демонстрируя, что он понимает все дополнительные риски. Он также подвергается дополнительным роевым (swarm) тестам (см. раздел 8.3).

Выбрав запуск выходной ноды, оператор удваивает свое вознаграждение по сравнению с ретранслирующей нодой во время выбора и начисления вознаграждения за блок. Такая стимуляция предоставляется для того, чтобы у операторов выходных нод были финансовые причины их создавать. Это также помогает в защите от атак Сивиллы, специально предназначенных для захвата сети выходных нод. Такой уязвимостью страдает Tor, поскольку соотношение выходных к ретранслирующим нодам в нем достаточно низко.

6.4 Внешние Ноды (Remote Nodes)

В любой криптовалютной сети хранение полной копии блокчейна если и возможно, то как минимум не практично для большинства пользователей. В Bitcoin и Ethereum у пользователя есть возможность подключиться к публичной полной ноде, которая содержит копию блокчейна и может запрашивать и отправлять транзакции в сеть. Такой подход работает, поскольку полные ноды сети Bitcoin и Ethereum могут осуществлять эффективный поиск по транзакциям в блокчейне, используя публичный ключ пользователя в качестве цели поиска.

Из-за специфики внутреннего устройства валют на основе CryptoNote, реализация публичных полных нод (называемых внешними нодами), становится более сложной. Когда пользователь подключается к внешней ноде, он должен временно скачать каждый блок (во время создания кошелька или начиная с последнего проверенного блока) на локальное устройство для проверки каждой транзакции на наличие публичного транзакционного ключа, соответсвующего приватному просмотровому ключу пользователя. Этот процесс может значительно сказаться на нагрузке внешних нод. Учитывая, что вознаграждение за предоставление внешних нод обычно отсутствует, операторы Сервисных Нод могут отказаться от предоставления сервиса синхронизации для «тонких» клиентов. Мобильные кошельки валют на основе CryptoNote часто ненадежны и вынуждены переключаться между разными внешними нодами по нескольку раз до установки надежного соединения, которое позволяло бы просканировать блокчейн или отправить транзакцию.

Кроме этого, злоумышленные операторы внешних нод могут записывать IP адреса пользователей по мере трансляции определенных транзакций. Несмотря на то, что во время такой атаки реальную информацию о транзакции получить невозможно, определенные транзакции можно привязать к IP адресам, по которым в свою очередь можно выяснить личность пользователя в реальном мире, что нарушит конфиденциальность.

Loki решает эти проблемы, требуя чтобы каждая Сервисная Нода одновременно исполняла и функции внешней ноды, которой могут пользоваться обычные пользователи. Эта задача является естественной для Сервисных Нод, поскольку они уже содержат полную копию блокчейна и формируют собой распределенную сеть с высокой пропускной способностью. При использовании Сервисных Нод в качестве внешних, количество таких нод для каждого пользователя ограничено финансовыми причинами, и таким образом, ограничено количество данных, которыми нечестный оператор может завладеть.

6.5 Blink-транзакции

В типичной системе блокчейна время подтверждения любой транзакции – это время включения транзакции в блок. Из-за конкуренции майнеров, наличия скрытых блоков и атак Финни (Finney attacks), обычно требуется некоторое количество дополнительных блоков, созданных поверх транзакции, до того, как она будет считаться завершенной [24]. В зависимости от множества факторов, характерных для конкретного блокчейна, этот процесс может занять от 10 до 60 минут, что очевидно неудобно для продавцов и покупателей, которые вынуждены ждать определенное количество подтверждений до того как купленный товар или услуга станут доступны покупателю.

Из-за наличия архитектуры Сервисных Нод, в Loki возможно проведение транзакций, называемых Blink, которые близки по скорости к мгновенным. Blink позволяет подтвердить транзакцию до того, как она будет включена в блок, гарантируя её действительность как отправителю, так и получателю, и защищая получателя от двойной траты.

Blink работает по тому же принципу, что и механизм InstantSend в DASH. При создании каждого блока один из роев (swarm) Сервисных Нод детерминировано выбирается в качестве группы свидетелей, которые могут подтвердить действительность транзакции и заблокировать ее от двойного использования. Вместо блокировки непотраченых выходов в транзакции (как это делается в DASH), в Loki блокируется ключевой образ (key image). Ключевым образом является уникальный ключ, который присоединяется к каждому непотраченному выходу в кольцевой подписи. Для проведения мгновенных

подтверждений, Blink разрешает выбранному рою сигнализировать, что определенный ключевой образ ассоциированный с конкретным выходом, должен быть заблокирован до момента включения транзакции в блок. При попытке двойного использования, созданный ключевой образ окажется идентичным первому. Этот образ будет отклонен роем, а значит и всей сетью в целом.

Для возможности проведения Blink-транзакций, подтверждаемых в течение нескольких секунд, а не минут, пользователи должны будут заплатить повышенную комиссию. Эта возможность открывает целый набор новых применений Loki, позволяя существенно улучшить практическое использование личных переводов и облегчить интеграцию онлайн-платежей. Все свойства конфиденциальности, встроенные в Loki, остаются действенными в течение всего процесса.

7 Изменения в CryptoNote

Как криптовалюта, Loki функционально похожа на своих собратьев, построенных на основе CryptoNote. Однако между ними существует ряд ключевых отличий, помимо описанных выше Сервисных Нод и связанного с ними функционала.

7.1 Защита от ASIC

Интегральная Схема Специального Назначения (Application-Specific Integrated Circuit – ASIC) – это компьютерный чип, созданный для выполнения конкретной задачи. В контексте майнинга, ASIC-и используются для вычисления конкретных хеш-алгоритмов. Они создают риск децентрализации, поскольку: опережают другие способы майнинга по производительности; созданы ограниченным кругом конкретных компаний; ограничены в каналах дистрибуции из-за специализированного характера оборудования; требуют значительных капиталовложений в разработку и прибыльную эксплуатацию. Существуют также потенциальные выгоды от использования ASIC-ов, например, разработка оборудования под конкретный алгоритм требует существенных инвестиций, что снижает вероятность нечестного поведения разработчиков оборудования заинтересованных в прибыльности собственных инвестиций. Однако разработка и дистрибуция ASIC чипов с использованием зрелых хеш-алгоритмов все еще централизована вокруг нескольких крупных компаний. Эти компании могут отказывать в доставке целым географическим регионам, решать, какие из них получат доступ к более производительным ASIC-ам, выпускать ограниченные тиражи и манипулировать ценами.

Для предотвращения монополизации хешрейта ASIC оборудованием, многие криптовалюты разработали ASIC-устойчивые алгоритмы, например, Scrypt и Ethash [25][26]. До последнего времени Monero использовал алгоритм CryptoNight, для которого требуется большое количество L3 кеша. В теории, большие требования к памяти должны усложнить производство ASIC. Однако в 2018 году компания Bitmain выпустила модель X3, содержащая специфичный для CryptoNight ASIC чип, который может майнить со скоростью в 10 раз больше, чем стандартная графическая карта (GPU) [27]. Другие алгоритмы постигла та же судьба, и сейчас Scrypt, Ethash и Equihash майнятся с помощью ASIC.

Для борьбы с ASIC-ами, разработчики Monero предложили использовать стратегию хард-форков (hard fork), в которых алгоритм CrytpoNight немого изменяется каждые

3-6 месяцев (первым форком был переход на алгоритм CryptoNightV7 [28]). Для производства ASIC-ов требуются значительные расходы и время, а поскольку аппаратная конструкция оборудования крайне специфична, небольшие изменения в алгоритме хеширования делают чип неработоспособным, что приводит к потерям инвестиций производителей ASIC. Однако, у такого подхода есть свои сложности. Если сделанные изменения в алгоритме окажутся недостаточными для предотвращения перепрограммирования ASIC-ов, то сеть может стать уязвимой к централизации до тех пор, пока новый хард форк не станет доступен. Программируемые Пользователем Вентильные Матрицы (Field Programmable Gate Arrays – FPGAs) также необходимо учитывать в стратегиях защиты от ASIC, поскольку нечастые и небольшие изменения в алгоритмах хеширования легко могут быть перепрограммированы на FPGA. Еще одна проблема заключается в том, что постоянные изменения в ядре механизма консенсуса могут привести к случайному появлению багов. Такой подход также централизует разработку вокруг основной команды программистов.

Был предложен целый ряд альтернатив алгоритму доказательства работы, которые исключали бы необходимость регулярных хард форков, в частности, существуют алгоритмы с высокой скоростью заполнения памяти, такие как Argon2, Balloon hashing и полиморфические алгоритмы хеширования, например ProgPoW и RandProg [29][30][31][32]. Команда Loki опубликует дополнительные исследования по вышеупомянутым алгоритмам для разработки долгосрочного решения по устойчивости к ASIC.

Пока эта работа ведется, Loki будет использовать модификацию CryptoNight под названием CryptoNight Heavy, который поддерживает устойчивость к существующим ASIC майнерам для CryptoNight. CryptoNight Heavy отличается от CryptoNight V7 в следующем: в нем увеличены требования к внутренней сверхоперативной памяти (SPM – scratch pad memory) до 4 Мб, а также изменен способ работы с некоторыми строковыми операциями (implode и explode) [33]. Эти изменения отличают его от основной цели ASIC майнеров – CryptoNight V7, используемый в Monero, а также предоставляют более надежную защиту от разработки новых ASIC-ов, пока более устойчивое решение не будет найдено.

7.2 Динамический размер блока

Как и в других монетах на основе CryptoNote, размер блока в Loki не является фиксированным. Размер блока изменяется со временем, вырастая по мере достижения сетью большего объема транзакций. Размер блока в Loki масштабируется путем вычисления медианы за последние 100 блоков, и соответственно, максимальный размер новых блоков постепенно пересчитывается.

Давней озабоченностью в криптовалютной среде является то, что большие блоки перегружают ноды, которые должны хранить и проверять транзакции. По мере роста размера блока, ноды, работающие на менее производительном оборудовании, становятся неспособными обрабатывать и распространять новые блоки, что приводит к централизации нод среди владельцев, коммерчески заинтересованных в их обслуживании. Это может настораживать, поскольку распределение блокчейна среди большого количества нод позволяет подтверждать его состояние множеством различных сторон, повышая таким образом достоверность и устойчивость к цензуре.

В Loki часть вознаграждения блока отдается Сервисным Нодам, которые обрабатывают и распространяют блоки в качестве полных нод. Поскольку Сервисные Ноды, не обеспе-

чивающие необходимую пропускную способность и производительность, исключаются из сети (см 7.3), вознаграждающий пул обеспечивает минимально необходимые требования к производительности. Такая стимулирующая структура позволяет убедиться не только в том, что количество нод всегда будет достаточно высоким, но и в том, что ноды будут обладать необходимым уровнем производительности, чтобы распределять данные блокчейна по сети независимо от того, насколько сильно вырастет блокчейн или насколько большими будут требования к пропускной способности. Однако и в этом случае требуется принимать меры по оптимизации размеров транзакции, чтобы сеть масштабировалась эффективно, а расходы на содержание Сервисных Нод были достаточно низкими и их количество оставалось большим в долгосрочной перспективе.

7.3 Размер Кольцевой Подписи

Кольцевые подписи используются, чтобы скрыть реальный выход среди множества других в каждой транзакции. Размер кольцевой подписи характеризуется количеством смешений, на основе которых строится кольцо. В Monero на данный момент кольцо состоит из минимум семи выходов, из которых шесть используется для прикрытия одного настоящего выхода транзакции.

Влияние больших размеров кольца изучено достаточно слабо, однако в работе 0001 (опубликованной исследовательской лабораторией Monero Research Lab) было проанализировано влияние различных размеров кольца на эффективность атаки, в которой атакующему принадлежит большое количество выходов в блокчейне [34]. Было обнаружено, что чем больше размер кольца, тем меньше времени, в течение которого у атакующего, владеющего большим количеством непотраченных выходов, будет возможность произвести эффективный анализ транзакций. Принудительное увеличение размера кольца также позволяет защититься от теоретической атаки под названием EABE (Биржа обмена → Алиса → Боб → Биржа обмена), описанной пользователем Knacc [35], где сторонний участник (например, биржа обмена) может осуществлять ограниченный временной анализ транзакций между двумя пользователями.

Кроме этого, у Monero нет ограничений по максимальному размеру кольца, установленного консенсусными правилами сети. Многие кошельки, например, Monero GUI wallet, ограничивают размер кольца в 26. Однако любой пользователь имеет возможность вручную создать транзакцию с любым размером кольца больше шести. Это может стать проблемой, поскольку размер кольца по умолчанию для большинства кошельков равен минимально допустимому значению – семи. Увеличение размера кольца для транзакции делает ее более заметной (рис. 3). К тому же, если какой-то пользователь всегда задает один и тот же нестандартный размер кольца в Monero (например, десять), третья сторона может использовать это знание для анализа блокчейна и обнаружения паттернов, используя временной анализ.

Хеш транзакции	Размер кольца	Размер транзакции [kB]
3feaff3f48de0bc4c92ec027236165337b64df404aca098e212c1215e9456697	7	13.47
39d484f7c0a2e8f3823a514056d7cb0bf269171cb4582e05955d4c5ee995cad0	7	13.47
e08f5a937e725011bedd44075334ae98dcca32749da231c56da1278d49c0a231	7	13.50
ab35e69d9cca39219c90df8b2b7aab4a54c82127fb1fbaae65d76357f8f76387	7	13.50
6d8ccd56dc2d3eb7de03ba767f0dbf4d5f42ae91e67f4c28f16d6f8b0229c272	10	13.87

Рис. 3: *Иллюстрация того, как нестандартный размер кольца делает транзакцию заметной, на примере xmrchain.net (сайт со списком блоков и транзакций Monero)*

Loki улучшает обе описанные ситуации, делая размер транзакции статическим, и задавая его равным десяти. Ограничение размеров кольца статическим значением позволяет защитить пользователей, смешивающих выход с более чем девятью выходами в кольце, помимо собственного, а увеличение размера до десяти позволит более эффективно защититься от возможности определения настоящего выхода кольцевой подписи атакующим, владеющим большим количеством выходов. Больший размер кольца также нелинейно увеличивает эффективность «взбивания» (churning – отправка самому себе средств множество раз для защиты источника транзакции), и оно становится более эффективным по мере роста размера кольца. В текущей транзакционной схеме увеличение размера кольца до 10 привело бы к росту размера транзакции на 2.6%. Однако внедрение «пуленепробиваемых доказательств» (bulletproofs) изменит это соотношение до 8 – 13%. Это происходит из-за общего уменьшения размера транзакций с Bulletproofs. Накладные расходы связанные с увеличением минимума размеров кольца могут создать проблемы для сети, не обладающей архитектурой, достаточной для поддержания транзакций большого размера. Однако в Loki эту нагрузку возьмут на себя Сервисные Ноды, стимулированные к работе и обладающие достаточной пропускной способностью.

8 Предотвращение атак

8.1 Блокировка IP и Пакетов

Несмотря на то, что у сети Сервисных Нод нет единой точки отказа, существуют две серьезные угрозы цензурирования сети, а именно: харвест-атака с целью сбора действующих адресов (harvesting attack) [36] и глубокий анализ пакетов (deep packet inspection – DPI) [37]. При харвест-атаке атакующий пытается собрать IP-адреса всех работающих Сервисных Нод сети, и использует брандмауэр интернет-провайдера для блокировки соединений к этим адресам. Такой вид цензуры постоянно применяется к сети Tor в Китае [38]. При глубоком анализе пакетов (DPI) происходит изучение структуры всех пакетов, проходящих через брандмауэр, и те из них, которые похожи на принадлежащие запрещенному сервису, блокируются. DPI–атаки также используются в основном на государственном уровне [39].

Чтобы создать сеть, неуязвимую к DPI, был проведен большой объем работы. Пользователи могут использовать типы подключаемых транспортов, изменяющих подпись пакета таким образом, чтобы он выглядел как обычный неблокированный трафик. Блокировка по IP обычно обходится с использованием создания мостов прикрытия доменом (domain fronting), при которых трафик шифруется в виде HTTPS запросов к неблокированным сервисам, например, Azure или Cloudflare. Когда запрос достигает небло-

кированного сервиса, мост перенаправляет его в требуемое место. При использовании метода прикрытия доменом, правительствам становится сложнее блокировать поток трафика к популярным мостам, не вызывая значительного нарушения общего пользования интернетом.

Встроенные в Loki управляющие механизмы (см. раздел 9) могут быть использованы для работы мостов прикрытия доменов, чтобы пользователи получали доступ к Loki в тех странах, в которых производятся широкомасштабные акты цензуры. Кроме того, в Сервисные Ноды будет встроен подключаемый транспорт OBFS4, что поможет в дополнительной защите против DPI [40].

8.2 Атаки отказа в обслуживании (Denial of Service)

Пользователи децентрализированных блокчейнов не обязаны идентифицировать себя цифровым или физическим способом. Это может быть полезно пользователям без идентификатора личности, либо тем, кто преследуется на основании личных данных. Однако системы, не требующие идентификации пользователей, становятся уязвимыми к атакам Сивиллы, в которых злоумышленник создает множество ложных личностей (для Loki – множество пар публично-приватных ключей), и использует их для спама сети запросами.

Многие криптовалюты столкнулись с этой проблемой, и вынужденно внедряют модели оплаты за услугу или доказательства работы. В модели оплаты за услугу, которая используется, например, в Siacoin, пользователи платят за используемую услугу. В Siacoin стоимость определена ценой за терабайт хранения в месяц [41]. Модели с оплатой за услугу эффективно снижают риски атак Сивиллы, однако, могут отпугивать пользователей, особенно когда аналогичный сервис предоставляется бесплатно (например, Google Drive и Onedrive в случае с Siacoin). Системы с доказательством работы, используемые, например, в Hashcash или Nano, требуют от пользователей произвести небольшие расчеты для отправки сообщения или транзакции [42][43]. Такие мелкие доказательства работы вероятно лучше уравнивают пользователей, чем модель оплаты за услугу, но могут пасть жертвой злоумышленников, обладающих большими объемами вычислительной мощности.

Loki предлагает измененную схему доказательства работы для решения двух основных объектов атаки Сивиллы в системе Loki: офлайн-сообщений и создания путей. Офлайн сообщения являются потенциальной целью, поскольку каждое из них должно храниться в рое из девяти нод. Потенциальное злоупотребление может возникнуть, когда злоумышленник перегружает определенный рой большим количеством сообщений, которые необходимо хранить. В атаках создания путей атакующий пытается поучаствовать в процессе создания путей как можно большего количества нод, забирая ресурсы пропускной способности и отбирая их у пользователей, создающих пути с легитимными целями.

Чтобы защититься от обеих атак, сеть Loki требует, чтобы к каждому сообщению и созданию пути было присоединено небольшое доказательство работы. Для сообщений таким доказательством работы является расчет Blake2b хеша сообщения. Для создания пути доказательство работы отправляется вместе с запросом к ноде на включение в процесс строительства пути. Чтобы обеспечить масштабируемость и доступность для мобильных пользователей, требования к сложности выполнения работы задаются на

основе желаемого времени жизни (time-to-live — TTL) сообщения в сети, а не на основе общей активности сети.

8.3 Роевые Метки

В ситуации, когда ноды оперируют в не требующим доверия (trustless) окружении без централизованного лидера, отслеживание их правильного поведения в сети становится затруднительным. Несмотря на то, что Сервисные Ноды в Loki должны заморозить определенную сумму обеспечения для работы, они могут принять решение не перенаправлять трафик или не хранить необходимые данные в памяти. Поскольку такой выбор представляется финансово выгодным (использование меньших объемов пропускной способности сети / процессорной мощности / хранилища), необходимо разработать систему распределенного маркирования для отключения неэффективных нод. Для Loki реализация такого маркирования сталкивается с серьезными сложностями. По сути, каждая Сервисная Нода финансово заинтересована помечать другую ноду как плохую, поскольку, когда Сервисная Нода помечена для удаления из пула, шансы на выигрыш у того, кто поставил метку, вырастают. Одним из потенциальных решений распределенного проставления меток является такой, в котором во время проставления метки предоставляется доказательство нарушения, однако такой подход уязвим перед нодами, фабрикующими доказательства в свою пользу. И наоборот, проставление меток без ограничения позволяет отдельным нодам или группам взаимодействующих нод специально помечать честные ноды как плохие для повышения собственного шанса на выигрыш. Для предотвращения этих проблем Loki предлагает использовать роевые метки.

Проставление роевых меток работает с использованием текущих роев (см 6.1.1) для выбора участников каждого раунда тестирования. Все Сервисные Ноды содержат копию блокчейна, и созданный майнером блок детерминистически определит несколько тестовых роев. 1% роев выбирается для участия в тестовом рое для каждого блока. Для их вычисления используется хеш-сумма пяти предыдущих блоков, на основе которой с помощью функции Вихря Мерсенна (Mersenne Twister) выбираются рои по порядку их нахождения в детерминированном списке.

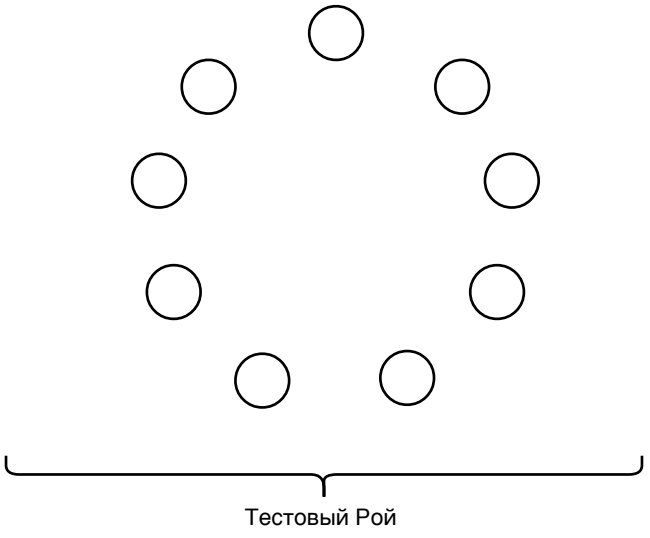

Рис. 4: *Тестовым роем является набор из 9 нод*

Когда рой выбран для участия в тестировании, каждая нода в этом рое проводит набор тестов для всех остальных нод в рое. Эти тесты не являются активными, каждая нода хранит историю взаимодействии со всеми другими нодами роя. Информация о пропускной способности, хранении сообщений, запросах блокчейна и выходных нодах собирается и хранится в течение времени. Новые участники, которые еще не собрали эту информацию, могут опросить Сервисные Ноды за пределами текущего роя, и собрать необходимые данные по тестируемым нодам.

Каждая Сервисная Нода принимает решение на основе вышеупомянутых тестов и голосует по каждому из других членов роя, сообщая ему о своем решении. Каждая нода в рое может проверить голоса всех участников. Если какая-либо нода получила более 50% голосов против нее, любой участник роя обладает всей необходимой информацией, чтобы создать дерегистрирующую транзакцию. Как только транзакция проверена и включена в блок, все Сервисные Ноды обновляют свои DHT, удаляя ноды, отклоненные на основании голосования.

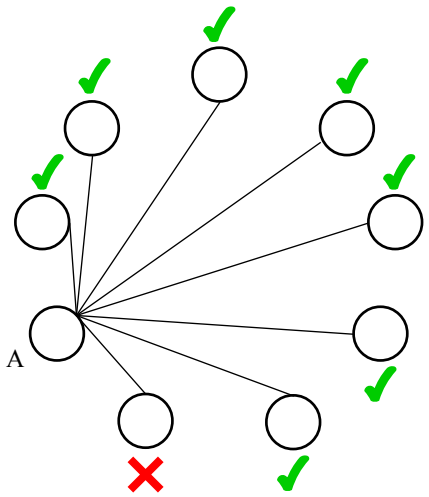

Рис. 5: *Нечестная нода тестируется нодой A и проваливает тест. Нода A приходит к локальному пониманию, какие ноды проходят тесты, а какие нет.*

8.3.1 Набор тестов

Чтобы сеть могла обеспечить требуемые стандарты производительности, Сервисные Ноды должны обладать необходимыми инструментами для тестирования других нод. Эти тесты должны охватывать всю требуемую функциональность Сервисных Нод, что поможет предотвратить атаку «ленивых мастернод» [44]. В первоначальном решении предлагается четыре фундаментальных теста. По мере расширения функциональности Сервисных Нод в набор могут быть добавлены новые тесты.

Когда оператор запускает программное обеспечение Сервисной Ноды впервые, на ней создается пустой файл заданного размера, необходимый, чтобы обеспечить требуемое дисковое пространство для хранения данных. После этого производится простое тестирование пропускной способности между Сервисной Нодой и географически распределенным набором серверов, принадлежащих Фонду Loki. Эти тесты не являются обязательными, Сервисные Ноды могут пропустить, проигнорировать или провалить их. Однако прохождение этих тестов может быть хорошим индикатором для потенциального оператора в принятии решения – рисковать блокированием залогового обеспечения

для ноды, не соответствующей минимальным требованиям, или нет. Когда Сервисная Нода подключается к пулу непроверенных нод, ее сумма обеспечения замораживается, и она тестируется выбранным тестирующим роем. Решения в роевых тестах принимаются на основе консенсуса, новые участники сети Сервисных Нод не могут избежать этих тестов. Если нода проходит все роевые тесты, ей проставляется доверительная метка, и она может начать маршрутизировать пакеты. Если нода проваливает тесты, она удаляется из сети, а обеспечение остается замороженным на 30 дней.

Тест Пропускной Способности

Тест пропускной способности является основным в наборе тестов Loki. Если нода проходит тест успешно, то предполагается, что она честно маршрутизирует пакеты со скоростью выше минимально требуемого порога.

Каждый раз, когда одна Сервисная Нода общается с другой, она делает запись о предоставленной входящей пропускной способности. Со временем ноды будут включены в тысячи путей и смаршрутизируют миллионы сообщений. Эти взаимодействия сформируют основу таблицы пропускной способности каждой ноды. Используя эту таблицу, нода сможет отвечать на запросы тестов пропускной способности внутри роя.

Ожидается, что все ноды также будут отвечать на запросы об их собственной таблице пропускной способности от других нод. Это означает, что даже те ноды, которые недавно присоединились к сети, могут запрашивать информацию о любой конкретной ноде в рое.

Тест Хранения Сообщений

Хранение сообщений — важнейшая составляющая функциональности офлайн-сообщений для пользователей Мессенджера Loki. Севисные Ноды необходимо тестировать на их способность кешировать сообщения и доставлять их пользователям в течение времени жизни (Time-to-live – TTL) сообщения.

Пользователи, отправляющие офлайн сообщения, выбирают случайную Сервисную Ноду из роя получателя. Эта нода должна распространить копию сообщения среди оставшихся нод роя. В зависимости от прикрепленного доказательства работы, Сервисные Ноды, получающие копии сообщения, будут хранить его в течение определенного времени жизни (TTL). Как только время жизни достигнет окончания, распределяющая нода отправит определённый одноразовый код (nonce) остальным участникам роя. Рой добавляет этот код к сообщению, хеширует результат и отправляет его обратно распределяющей ноде. Тест гарантирует, что Сервисная Нода сохранит сообщение до конца времени жизни и будет исключена, если не сможет создать правильный дайджест сообщения. Поскольку выборка распределяющей ноды является случайной, со временем каждая Сервисная Нода сможет собирать данные о производительности других участников роя.

Тест Хранения Блокчейна

Ожидается, что Сервисные Ноды будут хранить полную копию блокчейна Loki. Храня эти данные, Сервисные Ноды могут выполнять ряд задач, необходимых для пользователей сети, включая работу в качестве внешних нод, подтверждение транзакции и блокировку транзакций для Blink.

В то время как честные ноды хранят копию блокчейна, нечестные могут попытаться не делать этого, а запрашивать копию блока у честной ноды во время тестирования. Чтобы избежать этого, тест хранения блокчейна построен таким образом, что честные ноды, хранящие копию блокчейна, пройдут этот тест, а нечестные – провалят.

Для достижения этого, нода, проводящая тест, просит тестируемую ноду сделать выбор из K случайных транзакций в истории блокчейна, которые необходимо объединить и захешировать. Этот хеш отправляется ноде, проводящей тест. Измеряя задержку запроса, тестирующая нода может сравнить эту задержку с ожидаемым временем возврата ответа T. Точное значение T будет установлено, чтобы с достаточной достоверностью определить разницу между задержкой, связанной с загрузкой данных с диска, и

задержкой, связанной с загрузкой блоков из сети. Для атакующего скачивание и хеширование K блоков в течение времени T должно быть трудноосуществимо, что позволит затруднить приспособительные атаки.

Тест Выходных Нод

Сервисные Ноды, решившие выступать в качестве Выходных Нод, получают повышенное вознаграждение. Чтобы убедиться, что ноды не злоупотребляют получением этого вознаграждения, необходимы дополнительные тесты.

Для проведения функционального тестирования выходных нод требуется имитация естественного поискового поведения человека. Если Сервисная Нода сможет определить, что ее тестируют, она будет иметь возможность отвечать только на тесты, и игнорировать реальные пользовательские запросы. Имитация естественного поведения пользователя при запросе страниц является сложной задачей, однако выходные ноды могут быть спроектированы таким образом, что накладные расходы на определение обычных и тестовых запросов были настолько большими, что разница в стоимости объема трафика между обычной и нечестной нодой была незначительной.

Сервисные Ноды используют локально хранимый список поисковых систем, а также словарь псеводслучайных естественных поисковых запросов. Поисковый запрос отправляется в поисковую систему, и из результатов поиска случайным образом выбирается несколько веб страниц. Сервисная Нода теперь может проложить путь со случайными нодами, играя роль маршрутизатора, и соответствующая нода может быть протестирована в качестве выходной. Используя её, тестирующая нода запрашивает страницу на основе результатов своего псевдослучайного поиска. Если полученный результат совпадает со сгенерированным тестирующей нодой, выходная нода считается прошедшей тест.

9 Управление, Финансирование и Голосование

Управление является важнейшей частью конструкции криптовалюты и должно поддерживаться на уровне протокола. Риски слабого, формально не утвержденного управления были хорошо изучены за историю блокчейна. Bitcoin и Ethereum переживают постоянные хард-форки, распыляющие внимание и усилия своих сообществ. Несмотря на то, что хард-форки могут быть использованы в качестве стратегии управления, они должны рассматриваться в крайних случаях, а не для решения каждого спорного вопроса. Система управления Loki создана для решения потенциальных проблем путем создания структурированной среды для общения и представительства, а также для функционирования в качестве источника финансирования разработки Loki без зависимостей от внешнего влияния или степени альтруизма участников.

Помимо предотвращения хард-форков, структуры управления должны создавать средства для финансирования новых проектов, улучшающих экосистему Loki. Внутреннее финансирование проектов должно препятствовать созданию групп со специальными интересами, которые не обязательно совпадают с интересами пользователей, майнеров или операторов Сервисных Нод. Мы наблюдали такую ситуацию в Bitcoin и его различных форках. Коммерческие компании, такие как Blockstream, Bitcoin ABC и Bitcoin Unlimited, обвинялись в найме разработчиков для изменений протоколов Bitcoin и Bitcoin Cash, нацеленных на достижение собственных бизнес-целей или определенной идеологии этих компаний.

По этой причине в каждом блоке Loki 5% вознаграждения резервируется для целей сетевого управления. Это обеспечивает постоянный поток финансовых средств в виде монет Loki, которые распределяются между проектами сообщества, разработчиками программного обеспечения и командами интеграции. Из этих 5% вознаграждения, 3.75% контролируется Фондом Loki, и 1.25% контролируются Сервисными Нодами через Систему Финансирования Loki. Такой подход поощряет справедливое представительство интересов Сервисных Нод и позволяет сообществу финансировать предложения, возникающие за пределами прямого контроля Фонда Loki.

9.1 Фонд Loki

Фонд Loki (Loki Foundation) является зарегистрированной некоммерческой организацией, основанной в Австралии. Существование центрального юридического лица позволит проекту Loki действовать в рамках хорошо определенной правовой базы, предоставлять работникам юридическую защиту и гарантировать обязательства. Фонд Loki был зарегистрирован в Австралии в 2018 и использует конституцию, предоставленную Австралийской Комиссией Благотворительных Фондов и Некоммерческих Организаций (Australian Charities and Not-for-profits Commission – ACNC) [45]. Конституция формирует такую же структуру управления Фондом, какая существует для многих некоммерческих организаций. В этой структуре у компании нет акционеров или бенефициаров, члены правления ограничены определенными временными сроками, а действия предпринимаются путем голосования по предложениям, выдвинутым другими членами правления. Фонд Loki структурирован таким образом, чтобы получить статус благотворительной организации в Австралии.

Организация конституционно обязана тратить любой доход (включая свою часть вознаграждения за нахождение блока) на продвижение проекта и согласованные инициативы. Для компании, подвергающейся внешнему аудиту, очень важно поддерживать прозрачность как для сохранения зарегистрированного статуса благотворительной организации, так и для того, чтобы показать общественности, что Фонд Loki остается прозрачной организацией и производит траты в разумных пределах. Фон Loki подотчетен как сообществу, так и аудиторам. Для ситуаций, в которых такая система окажется неспособной обслуживать Loki и смежные проекты, создан механизм жесткой защиты. При достаточном сетевом консенсусе возможно создание хард-форка, который удалит или заменит Фонд Loki в качестве получателя вознаграждения.

9.2 Система Финансирования Loki

Хотя Фонд Loki состоит из разнообразной группы лиц, представляющих проект Loki, фонд подчиняется как собственной конституции, так и законам Австралии. Это может оказаться ограничивающим фактором в решениях, которые фонд способен принимать. Система финансирования Loki позволяет Сервисным Нодам полностью управлять частью вознаграждения за блок. Сервисные Ноды представляют лиц из различных стран и не обязаны принимать во внимание информацию, исходящую от команды проекта Loki или фонда, что позволяет им достичь определенного уровня автономности в принимаемых решениях. Сервисные ноды являются наиболее заинтересованными участниками сети и стимулированы финансово в принятии решений, повышающих ценность Loki.

9.2.1 Предложения

Каждое предложение, для которого требуется решение Сервисных Нод, публикуется в блокчейне. Если какая-то сторона хочет выдвинуть предложение, она должна опубликовать специальную транзакцию. Поскольку содержимое предложения должно быть читаемым, а выходы уничтожены, такие транзакции отказываются от функций конфиденциальности, стандартных для транзакций Loki.

Блоки распределения финансирования создаются через каждые 43 000 блоков (примерно 60 дней). Создатели предложения могут выдвинуть их в любое время в течение этого периода. Однако они должны принять во внимание, что чем ближе к началу этапа голосования предложение будет опубликовано, тем больше времени у него будет для получения голосов от Сервисных Нод.

К каждой транзакции присоединяется дополнительное поле, содержащее информацию, которую все Сервисные Ноды должны получить, чтобы проголосовать по данному предложению. Эта информация включает: заголовок предложения, URL со ссылкой на детальное объяснение, сумму в Loki, необходимую для реализации этого предложения, адрес для платежа, и информацию об агенте условного депонирования (escrow agent), если такой назначен.

В ожидании соглашения от Фонда Loki, пользователи, делающие предложение, могут выбрать Фонд Loki или третью сторону в качестве агента условного депонирования, которые будут выделять средства по мере достижения заданных этапов. Дополнительно к этому, чтобы поощрить высокий стандарт предложений и защититься от спама, каждая транзакция с предложением должна сопровождаться уничтожением значительной суммы в Loki.

9.2.2 Голосование

Каждая Сервисная Нода хранит специальный ключ для голосования. Этот ключ может быть экспортирован и использован для голосования от имени конкретной ноды без необходимости входить на сервер, где она расположена.

Голосование происходит вне блокчейна, каждая Сервисная Нода сообщает о своей поддержке, несогласии или воздержании по каждому предложению в блокчейне. Сервисные Ноды могут голосовать по предложению, если они участвовали в блокчейне в период до следующего двухмесячного блока финансирования. Непосредственно перед созданием следующего блока финансирования выбирается рой, который будет собирать и подсчитывать все поданные голоса. Этот подсчет затем отправляется в память узлов в пуле (mempool) и находится там, пока майнер не дойдет до блока финансирования. После чего информация используется для создания блока, выделяющего вознаграждение победившему предложению. Проходят только те предложения, в которых количество голосов «За» минус количество голосов «Против» больше или равно 15% от общего количества зарегистрированных Сервисных Нод в сети.

9.2.3 Распределение средств

Вся вырученная сумма от системы финансирования Loki оплачивается через блоки финансирования. Работа блоков финансирования схожа с работой традиционных блоков вознаграждения, в которой приватные ключи хранятся только у пользователя (non-custodial). Каждые 43,000 блоков (примерно 60 дней) майнеры создают блок финансирования. Блок содержит 1.25% всех вознаграждений за прошедший с прошлого создания блока период.

Чтобы создать валидный блок финансирования, майнеры должны иметь возможность оценивать предложения, получившие необходимый процент голосов. Это делается с использованием информации, которую ноды сообщают блокчейну, содержащую адрес для оплаты и статусы всех голосов. Все Сервисные Ноды должны проверить блок финансирования от майнера и отклонить блоки с платежами на неверные адреса.

Зачастую требуемая для предложения сумма будет либо меньше, либо выше суммы, созданной за 60-дневный период. Если общая сумма одобренных предложений превысит сумму, доступную в блоке, майнер создаст блок финансирования, приоритезируя те предложения, которые были выдвинуты раньше. Оставшиеся предложения останутся в блокчейне до создания следующего блока финансирования.

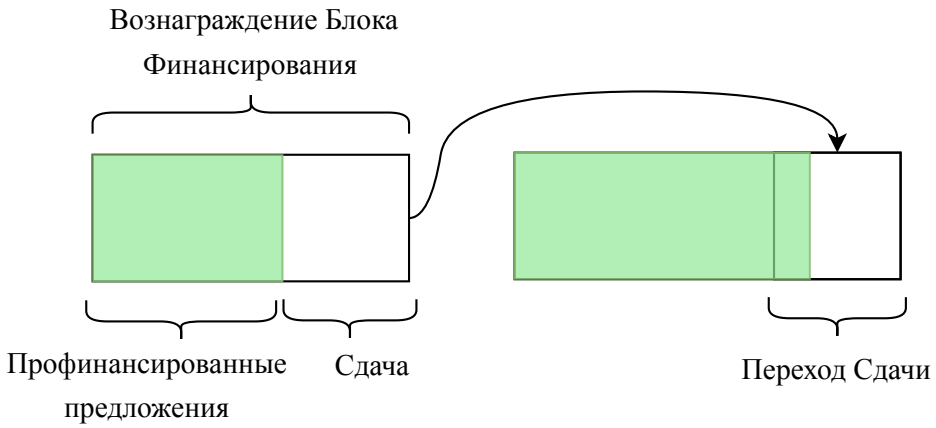

Рис. 6: *Неиспользованные средства создают сдачу, которая повышает вознаграждение следующего блока*

10 Заключение

Loki предлагает модель анонимных транзакций и децентрализованного общения, построенную на сети экономически стимулированных нод. Loki базируется на протоколе CryptoNote для обеспечения конфиденциальности и использует систему сервисных нод для повышения устойчивости и функциональности сети.

В дополнение к этому Loki предлагает улучшения, основанные на предыдущих исследованиях и проектах с открытым кодом, и представляет новый анонимный протокол маршрутизации, обладающий значительными преимуществами перед существующими протоколами. Комбинация уникальной архитектуры и конфигурации протокола позволяет создать сеть с основанной на рыночных законах устойчивостью к атакам Сивиллы, уменьшенной эффективностью временного анализа, и предоставляемой пользователям высокой степенью цифровой конфиденциальности.

Список литературы

[1] Mike Orcutt, *Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong* (September 11, 2017), https://www.technologyreview.com/s/608763/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong.

[2] *Monero*, https://getmonero.org.

[3] *Tor Project*, https://www.torproject.org.

[4] *I2P Anonymous Network*, https://geti2p.net/en.

[5] *LWMA Difficulty Algorithm*, https://github.com/zawy12/difficulty-algorithms/issues/3.

[6] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards Curves* (2008), https://eprint.iacr.org/2008/013.pdf.

[7] Nicolas van Saberhagen, *CryptoNote v 2.0* (2013), https://cryptonote.org/whitepaper.pdf.

[8] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR0437208

[9] Shen Noether, Adam Mackenzie, and Monero Core Team, *Ring Confidential Transactions* (2016), https://lab.getmonero.org/pubs/MRL-0005.pdf.

[10] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More* (2017), https://eprint.iacr.org/2017/1066.pdf.

[11] Evan Duffield and Daniel Diaz, *Dash: A Privacy-Centric Crypto-Currency*, https://github.com/dashpay/dash/wiki/Whitepaper.

[12] *GitHub - loki-project/loki-network*, https://github.com/loki-project/loki-network.

[13] *Tor Project: Docs*, https://www.torproject.org/docs/faq#KeyManagement.

[14] *Possible upcoming attempts to disable the Tor network | Tor Blog.* (December 19, 2014), https://blog.torproject.org/possible-upcoming-attempts-disable-tor-network.

[15] Petar Maymounkov and David Mazières, *Kademlia: A Peer-to-peer Information System Based on the XOR Metric*, https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf.

[16] Philipp Winter, Roya Ensafi, Karsten Loesing, and Nick Feamster, *Identifying and characterizing Sybils in the Tor network* (February 25, 2016), https://arxiv.org/abs/1602.07787.

[17] *OSI model - Wikipedia*, https://en.wikipedia.org/wiki/OSI_model.

[18] Farid Farid, *No Signal: Egypt blocks the encrypted messaging app as it continues its cyber crackdown* (December 26, 2016), https://techcrunch.com/2016/12/26/1431709.

[19] Matt Burgess, *Russia's Telegram block tests Putin's ability to control the web* (April 24, 2018), http://www.wired.co.uk/article/russia-google-telegram-ban-blocks-ip-address.

[20] *Go Ethereum - Postal Services over Swarm*, https://github.com/ethersphere/go-ethereum/blob/ddfc0a2a02ce574f4c252068ce81f0f5ada1c1ff/swarm/pss/README.md.

[21] Nikita Borisov, Ian Goldberg, and Eric Brewer, *Off-the-record Communication, or, Why Not to Use PGP*, Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, 2004, pp. 77–84, DOI 10.1145/1029179.1029200.

[22] *NaCl: Networking and Cryptography library*, https://nacl.cr.yp.to.

[23] *Pidgin-Encryption - SourceForge*, http://pidgin-encrypt.sourceforge.net.

[24] *Irreversible Transactions - Bitcoin Wiki* (March 15, 2018), https://en.bitcoin.it/wiki/Irreversible_Transactions.

[25] *Scrypt - Litecoin Wiki - Litecoin.info* (February 12, 2018), https://litecoin.info/index.php/Scrypt.

[26] *Ethash · ethereum/wiki Wiki - GitHub*, https://github.com/ethereum/wiki/wiki/Ethash.

[27] *BITMAIN*, https://shop.bitmain.com/product/detail?pid=00020180314213415366s4au3Xw306A4.

[28] *Monero Cryptonight V7 - GitHub*, https://github.com/monero-project/monero/pull/3253/files/e136bc6b8a480426f7565b721ca2ccf75547af62.

[29] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, *Argon2: the memory-hard function for password hashing and other applications* (December 26, 2015), https://password-hashing.net/argon2-specs.pdf.

[30] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter, *Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks* (2017), https://eprint.iacr.org/2016/027.pdf.

[31] *GitHub - A Programmatic Proof-of-Work for Ethash*, https://github.com/ifdefelse/ProgPOW.

[32] *GitHub - hyc/randprog: Randomly generate a C (or javascript) program*, https://github.com/hyc/randprog.

[33] *GitHub - curie-kief/cryptonote-heavy-design: Cryptonote Heavy deign essay*, https://github.com/curie-kief/cryptonote-heavy-design.

[34] Surae Noether, Sarang Noether, and Adam Mackenzie, *A Note on Chain Reactions in Traceability in CryptoNote 2.0* (2014), https://lab.getmonero.org/pubs/MRL-0001.pdf.

[35] *Github Comment - EABE/Knacc Attack*, https://github.com/monero-project/monero/issues/1673#issuecomment-312968452.

[36] *I2P's Threat Model - I2P*, https://geti2p.net/en/docs/how/threat-model#harvesting.

[37] *Deep packet inspection - Tec Gov*, http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf.

[38] Philipp Winter and Stefan Lindskog, *How China Is Blocking Tor* (2012), https://arxiv.org/abs/1204.0447.

[39] *Egypt Quietly Blocks VOIP Services Skype, Whatsapp - TorGuard* (October 26, 2015), https://torguard.net/blog/egypt-quietly-blocks-voip-services-skype-whatsapp.

[40] *GitHub - Yawning/obfs4: The obfourscator (Development mirror)*, https://github.com/Yawning/obfs4.

[41] David Vorick and Luke Champine, *Sia: Simple Decentralized Storage* (2014), https://sia.tech/whitepaper.pdf.

[42] Adam Back, *Hashcash - A Denial of Service Counter-Measure* (2002), http://www.hashcash.org/papers/hashcash.pdf.

[43] Colin LeMahieu, *RaiBlocks: A Feeless Distributed Cryptocurrency Network*, https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf.

[44] *Lazy Masternodes: do you actually have to do any work to get paid/vote?*, https://www.reddit.com/r/dashpay/comments/5t6kvc/lazy_masternodes_do_you_actually_have_to_do_any/.

[45] *ACNC template constitution for a charitable company*, https://acnc.gov.au/CMDownload.aspx?ContentKey=2efea0fa-af4f-4231-88af-5cffc11df8b7&ContentItemKey=6046cbc5-d7fd-4b6b-93ba-c8e3114b07ba.