MONERO RESEARCH LAB

ТЕХНИЧЕСКАЯ ЗАПИСКА MRL-0007

Множества потраченных выходов

Саранг Ноезер (Sarang Noether)*
Исследовательская лаборатория Monero (Monero Research Lab)
26 ноября 2018 г.

Аннотация

В данной технической записке содержится общее описание концепции потраченных выходов на основе теории базовых множеств. Определение охватывает результаты ранее проделанной работы, связанной с идентификацией таких выходов. Нами количественно определяется влияние такого анализа на блокчейн Monero и приводится краткий обзор способов избежать последствий.

1 Вступление

При проведении транзакций Monero генерируются *выходы* (иногда в других работах их ещё называют *расписками*), предназначенные для ряда получателей, использующих один или несколько существующих выходов под контролем получателя. Для каждого потраченного выхода в транзакции отправитель выбирает из блокчейна набор произвольных выходов, чтобы сформировать *кольцо*. Транзакция содержит доказательство, что для каждого кольца любой из выходов, составляющих это кольцо, будет являться равновероятным потраченным выходом. Также используется *образ ключа* (также называемый в других работах *тэгом*), который гарантирует, что ни один из потраченных выходов не был потрачен ранее при проведении предшествующих транзакций.

С точки зрения анонимности отправителя важно отсутствие какой-либо внешней информации, которая позволит узнать, что какой-либо из выходов, составляющих кольцо, уже был потрачен. Если будет известно, что выход был потрачен ранее, сторонний наблюдатель сможет сузить эффективный размер кольца, понизив тем самым уровень анонимности. Если процесс продолжится с достаточным количеством выходов, это позволит идентифицировать действительный потраченный выход. Нам хотелось бы подчеркнуть, что выходы Monero невозможно связать с адресом кошелька отправителя, что обеспечивает дополнительный уровень защиты.

В самом начале после появления Monero отправители могли выбирать размер кольца, в том числе кольцо могло содержать только один выход, и этот выход, очевидно, являлся действительным потраченным выходом. Обладая такой информацией, в небольших кольцах можно отследить другие потраченные выходы. В более поздних версиях протокола был введён основанный на консенсусе минимальный размер кольца, который увеличивался со временем. Такое увеличение в совокупности с переходом к конфиденциальности сумм в выходах устранило негативные последствия использования таких тривиальных колец на ранних этапах. Тем не менее остаётся возможность формирования более сложных множеств колец, которые в совокупности позволяют выявлять потраченные выходы, даже несмотря на то, что при этом невозможно определить, при проведении какой транзакции был потрачен такой выход.

*sarang.noether@protonmail.com

В данной технической записке нами даётся определение идеи выявления потраченных выходов в целом с применением теории базовых множеств. Нами показано, что определение охватывает несколько известных методов идентификации потраченных выходов. Используя инструмент, доступный всем пользователям Monero, мы количественно определяем наличие множества потраченных выходов в блокчейне Monero и показываем, что они не особо влияют на современные транзакции.

В независимых параллельных работах [1, 7] (появятся вскоре) даётся схожее определение и предлагается более общий алгоритм идентификации определённых потраченных выходов, а также способ проведения формального анализа.

2 Определение

Допустим, $\mathcal{N}$ - множество (ограниченное) всех выходов в блокчейне. Мы определяем *кольцо* как подмножество $\mathcal{N}$. Кольцо, включающее в себя n элементов, обозначаем как *n-кольцо*. Мы часто используем строчные буквы для обозначения типичных выходов.

Определение 1. *Допустим, $\{R_i\}_{i=1}^n$ является множеством колец. Мы говорим, что каждое R_i потрачено если*

$$\left|\bigcup_{i=1}^{n} R_i\right| = n.$$

Выход является потраченным, если он является элементом потраченного кольца.

Пример 1. *Допустим, $R = \{a\}$ является 1-кольцом. Значит, выход a (и само кольцо R) будет потраченным.*

Пример 2. *Допустим, $R = \{a, b\}$ и $S = \{b, c\}$ и $T = \{a, c\}$ являются кольцами. Значит, каждый выход (и кольцо) будет потраченным.*

3 Конкретные случаи

В предшествующих работах, таких как [5, 3, 2, 4, 6], было предложено несколько классов потраченных выходов. Нами вкратце рассматриваются некоторые из них, а также демонстрируется, как они соотносятся с нашим определением.

3.1 Цепная реакция

Так называемый метод *цепной реакции* использует тривиальные кольца, чтобы итеративно идентифицировать потраченные выходы. При использовании этого метода все 1-кольца помечаются как потраченные, а соответствующие выходы удаляются из всех остальных колец. Этот процесс повторяется до тех пор, пока не останется ни одного 1-кольца. Изначально этот метод был представлен в контексте активной атаки, в ходе которой злоумышленник тратит множество выходов в 1-кольцах, чтобы идентифицировать потраченные выходы честных пользователей.

В конце процесса итерации каждое потраченное кольцо даёт один уникальный потраченный выход, который был последним идентифицированным выходом в кольце. Это означает, что сбор всех таких потраченных колец соответствует нашему определению.

3.2 Повтор кольца

Так называемы метод *повтора кольца* ля идентификации потраченных выходов использует множество образов одного и того же кольца. Применение данного метода подразумевает просто идентификацию набора n, состоящего из отдельных n-колец , содержащих одни и те же выходы, благодаря чему можно прийти к выводу, что кольцо было потрачено. Этот анализ был изначально представлен как «полукооперативная» атака, при проведении которой злоумышленник генерирует повторяющиеся кольца с контролируемыми выходами, чтобы указать другим злоумышленникам, что кольцо потрачено.

Этот метод, очевидно, подходит под наше определение.

3.3 Анализ подмножеств

Стандартный набор инструментов Monero включает в себя специальный инструмент маркировки (blackball tool), который сканирует блокчейн и помечает определённые классы потраченных выходов. Помимо того что позволяют сделать методы цепной реакции и повтора кольца, этот механизм также даёт возможность производить *анализ подмножеств*. При использовании этого метода итеративно проверяется каждое кольцо. Для каждого из $2^n - 1$ (непустых) подмножеств n-кольца Rподсчитывается количество появлений подмножества в качестве отдельного кольца где-либо ещё. Если сумма таких обнаруженных подмножеств точно будет составлять n, то кольцо R будет помечено как потраченное.

Этот метод, очевидно, подходит под наше определение.

3.4 Другие методы анализа

При отсутствии другой информации наше определение полностью соответствует методам выявления потраченных выходов в блокчейне. Тем не менее на практике существуют и другие способы, позволяющие пометить выходы как потраченные либо злоумышленниками, либо пользователями, желающими избежать выбора таких выходов при создании новых колец.

- **Форки блокчейна**. В случае реализации форка блокчейна пользователь может по собственному желанию потратить один и тот же выход во множестве форков. Структура образов ключей Monero подразумевает, что в результате каждой траты одного и того же выхода появится один и тот же образ ключа. Наблюдатель, который видит во множестве форков кольца с одним и тем же образом ключа, может прийти к выводу, что потраченный выход может быть найден на пересечении всех таких колец, что статистически равноценно обнаружению потраченного выхода. Следует отметить, что такой метод анализа не попадает под наше определение.

- **Распределение по возрасту выходов**. Существуют самые разнообразные эвристические способы, обеспечивающие злоумышленнику статистическое преимущество при выявлении потраченных выходов в кольце. Например, анализ потраченных выходов в прозрачных блокчейнах показывает, что недавно сгенерированные выходы будут потрачены более вероятно, чем старые. Нами было отмечено, что на практике выбор непотраченных элементов кольца в соответствии с распределением, при котором сопоставляются ожидаемые модели траты, позволяет с лёгкостью снизить эффективность такого эвристического подхода. Существуют и другие эвристические методы, которые не рассматриваются нами в этом документе. Они не позволяют наверняка доказать, что определённый выход был потрачен, и не подходят под наше определение.

4 Предупреждение последствий

Теоретически каждый пользователь может просканировать свою копию блокчейна, идентифицировать все потраченные выходы, используя любые доступные источники информации, и убедиться в том, что для создания кольца для проведения транзакций в будущем им не были выбраны уже потраченные выходы. Тем не менее полный теоретико-множественный подход, используемый с нашим определением, не является практичным. Даже использование интегрированного инструмента маркировки, проводящего только частичный анализ, может занять несколько часов, когда речь заходит о последней версии блокчейна Monero, и для обеспечения максимальной анонимности потребуется регулярное обновление.

К счастью, пользователи подвергаются ничтожному риску в связи с идентификацией выходов. Метод цепной реакции, связанной с использованием малых колец, перестал использоваться ещё на ранних этапах истории Monero. По мере обязательного наращивания размера колец подобие случайных совокупностей колец, позволявшее вычислить множества потраченных выходов, стало исчезающе малым. Несмотря на то, что злоумышленник мог бы сгенерировать наборы колец специально для того, чтобы получить потраченные выходы, не сотрудничающему ни с кем злоумышленнику, вероятно, придётся произвести сложные вычисления, чтобы обнаружить их; кроме того, генерирующий кольца злоумышленник всегда может идентифицировать контролируемые им выходы, независимо от их связи с другими кольцами, что едва ли делает такую атаку выгодной, так как это стоит комиссий, выплачиваемых самим злоумышленником.

Количество потраченных выходов, полученных из форка блокчейна, сильно зависит от количества существующих выходов, потраченных во множестве блокчейнов, и требует участия большой части существующей сети. Более того, современные алгоритмы выбора членов кольца сильно тяготеют к выбору новых выходов, что означает возможность быстрого рассеивания форка со временем. На практике комбинация этих действий делает их в целом непрактичными.

Чтобы количественно оценить эти эффекты, в октябре 2018 нами был произведён анализ блокчейна Monero. При этом использовался инструмент маркировки (blackball tool). Нами были проверены несколько классов потраченных выходов:

- выходы, входившие в состав 1-колец;
- выходы, входившие в состав повторяющихся колец (обсуждались выше);
- выходы, идентифицированные методом анализа подмножеств (обсуждались выше);
- выходы, идентифицированные методом цепной реакции (обсуждались выше).

Затем мы классифицировали эти выходы в зависимости от того, обеспечивали они конфиденциальность сумм или нет. В случае с современными транзакциями выбираются только те ложные выходы, суммы в которых скрываются. В Таблице 1 представлены результаты анализа.

Несмотря на то, что анализ показал, что 86% всех не конфиденциальных выходов идентифицируются как потраченные, 0% конфиденциальных выходов были идентифицированы как таковые. Так как современные транзакции используют только второй тип ложных выходов, эффект анализа потраченных выходов на анонимность является совершенно ничтожным.

5 Заключение

Нами было представлено простое определение, основанное на теории базовых множеств, позволяющее отличить потраченные выходы в блокчейне Monero при наличии только информации о самих элементах

	Унаследованные выходы	Конфиденциальные выходы
1-кольцо	12147067	0
Повторяющиеся кольца	40	5
Анализ подмножеств	5916927	0
Метод цепной реакции	749688	0
Общее количество потраченных выходов	18813722	5
Общее количество выходов в блокчейне	21850122	7445622

Таблица 1: Анализ потраченных выходов в блокчейне Monero с применением инструмента маркировки по состоянию на октябрь 2018

колец. Определение охватывает и обобщает другие существующие подходы к анализу. Несмотря на то, что это определение не учитывает внешней информации, которую можно получить из таких источников, как блокчейн, возникший после форка, или же в результате временного анализа, оно обеспечивает понимание процесса выбора выходов, необходимое для оптимальной анонимности трат. Несмотря на то, что полный анализ всех потраченных выходов в блокчейне Monero неосуществим с точки зрения необходимых для этого вычислений, нами были количественно проанализированы несколько классов потраченных выходов, и было определено, что они никак не влияют на анонимность современных транзакций.

Список литературы

[1] Under anonymous submission. Rethinking untraceability in the CryptoNote-style blockchain (Под видом анонимности. Пересмотр свойств неотслеживаемости в cryptonote блокчейне), 2018.

[2] Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A traceability analysis of Monero's blockchain (Анализ отслеживаемости блокчейна monero). Cryptology ePrint Archive, Report 2017/338, 2017. `https://eprint.iacr.org/2017/338`.

[3] Adam Mackenzie and Surae Noether. Improving obfuscation in the CryptoNote protocol (Совершенствование методов маскировки в рамках протокола cryptonote). Monero Research Lab, MRL-0004, 2015. `https://lab.getmonero.org`.

[4] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin. An Empirical Analysis of Traceability in the Monero Blockchain (Эмпирический анализ отслеживаемости в блокчейне Monero). *ArXiv e-prints*, April 2017.

[5] Surae Noether, Sarang Noether, and Adam Mackenzie. A note on chain reactions in traceability in CryptoNote 2.0 (Техническая записка по цепной реакции и её влиянию на отслеживаемость в рамках протокола cryptonote 2.0). Monero Research Lab, MRL-0001, 2014. `https://lab.getmonero.org`.

[6] Dimaz Ankaa Wijaya, Joseph Liu, Ron Steinfeld, and Dongxi Liu. Monero ring attack: Recreating zero mixin transaction effect. Cryptology ePrint Archive, Report 2018/348, 2018. `https://eprint.iacr.org/2018/348`.

[7] Zuoxia Yu, Man Ho Au, Jiangshan Yu, Rupeng Yang, Qiuliang Xu, and Wang Fat Lau. New empirical traceability analysis of CryptoNote-style blockchains (Атака на кольца monero: воссоздания эффекта транзакций с нулевыми миксинами). FC 2019, to appear.