Анонимность транзакций: прошлое, настоящее и будущее

World Crypto Con, Лас-Вегас

Саранг Ноезер(Sarang Noether), кандидат наук

Хэллоуин 2019

Отказ от ответственности

Взгляды, представленные в данной презентации, принадлежат исключительно её автору и не обязательно отражают взгляды других людей, организаций или сообщества.

Материал, представленный в презентации, носит образовательный характер и не должен рассматриваться в качестве финансовых, юридических или каких-либо других рекомендаций или поддержки какого бы то ни было рода.

Автор является независимым исследователем, математиком, входящим в состав рабочей группы Исследовательской лаборатории Monero (Monero Research Lab) и получающим финансовую поддержку от сообщества Monero.

Цели

Вы должны понимать и ценить:

- **важность** взаимозаменяемости и анонимности в рамках протоколов транзакций;
- **развитие** используемых криптографических подходов;
- **отличия** моделей транзакций и систем доказательства;
- как **компромиссы** с точки зрения эффективности и доверия влияют на выбор технического решения.

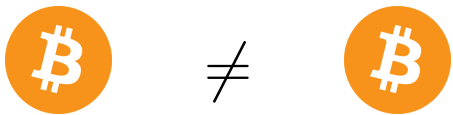
Математика может напугать, поэтому здесь её не будет.

Взаимозаменяемость?

Анонимность и взаимозаменяемость связаны. **Взаимозаменяемость** может означать неотличимость. Можно ли занести определённые средства в чёрный список?

Прозрачные реестры, такие как у Bitcoin, совершенно не обеспечивают взаимозаменяемости и анонимности.

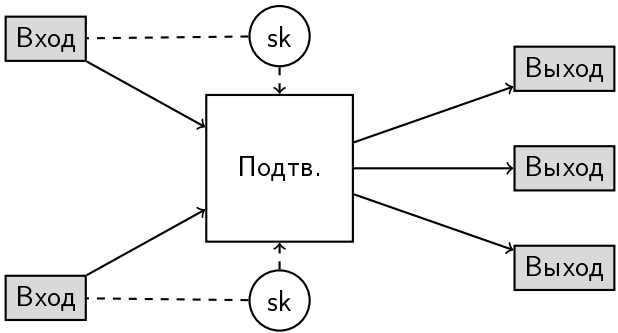
- Адреса отображаются в цепочке как часть транзакций
- Суммы указываются в открытую.
- Активы имеют отличную друг от друга историю и свойства.



Основные принципы построения транзакций

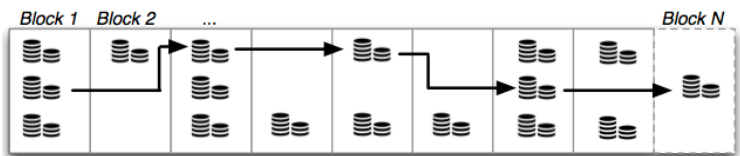
Транзакции (в первую очередь) включают в себя **входы**, **выходы**, и **подтверждения**.

Транзакция берёт входы, используя подтверждения, и генерирует новые выходы. Цифровая подпись является самым основным подтверждением.



Граф транзакции

Любой участник сети может проанализировать прозрачный реестр и изучить поток средств в транзакциях.



Темой очень многих исследований стали методы анализа блокчейна на основе его прозрачности.

Стоит ли беспокоиться?

Прозрачность и отсутствие взаимозаменяемости могут иметь последствия, которые вам могут как понравиться, так и не понравиться:

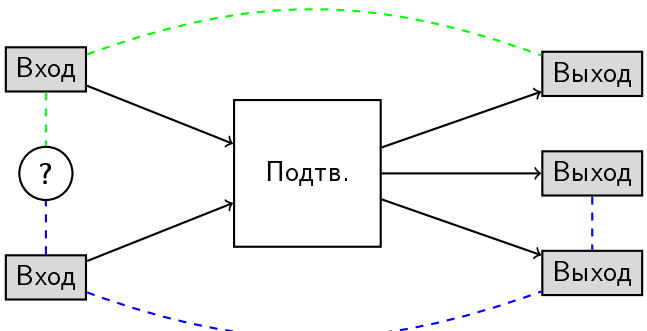
- **Цензурирование**: майнеры и другие лица могут цензурировать транзакции на основе информации адресов, суммы, местоположения и других данных/метаданных.
- **Рынки**: определённые типы или объёмы активов могут принести персональную надбавку в зависимости от истории или способов использования.
- **Связывание**: любая третья сторона, обладающая доступом к публичному блокчейну, может связать данные и суммы и попытаться привязать их к личности, что повышает персональный риск.
- **Конкуренция**: к онкурирующие бизнесмены банально могут получить информацию о транзакциях, а значит, информацию частного характера или деловую информацию.
- **Регулирование**: некоторые юрисдикции могут ввести правила, обязующие соблюдать анонимность финансовой информации при хранении и передаче.

Спектр общих подходов

Mimblewimble

Пример: прозрачные миксеры

Прозрачные миксеры берут прозрачные средства, возможно, принадлежащие различным владельцам, и включают их в одну транзакцию. Подтверждения могут быть изменены соответствующим образом, но, как правило, это не требует каких-либо новых математических решений.



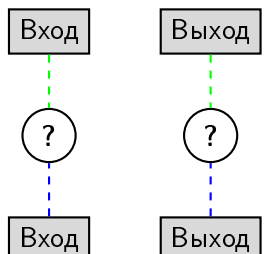
Пример: прозрачные миксеры

Плюсы:

- исключают возможность предположения принадлежности одному владельцу.

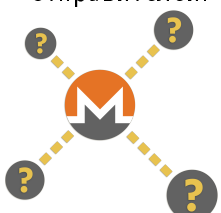
Минусы:

- анонимность отправителей и получателей находится либо на очень низком уровне, либо отсутствует;
- интерактивный процесс с возможностью выбора;
- не обеспечивает взаимозаменяемости активов, только неопределённость;
- возможность применения многих обычных методов анализа.



Пример: RingCT

RingCT является протоколом, использующим набор конструкции, используемых Monero и в других местах. Протокол использует одноразовые адреса, чтобы избежать связывания (но не совершенно устранить его). Неопределённые подписи создаются от лица выбранной отправителем группы таких же возможных отправителей. Суммы скрываются при помощи обязательств Педерсена.



Всё вместе это обеспечивает ограниченную неопределённость отправителя, анонимность получателя, а также сокрытие суммы, что ведёт к взаимозаменяемости.

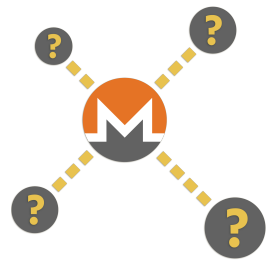
Пример: RingCT

Плюсы:

- заменяет явные подписи неопределёнными подписями;
- скрывает суммы;
- маскирует граф транзакции.

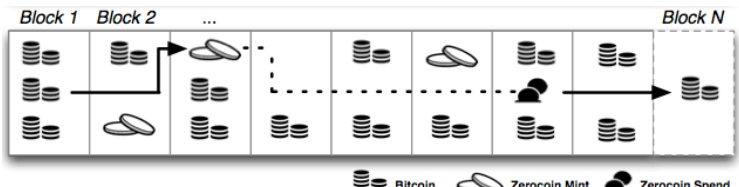
Минусы:

- метаданные могут снизить уровень фактической анонимности;
- масштабирование неэффективно;
- не до конца устраняет возможность эвристического анализа принадлежности одному владельцу.



Пример: Zerocoin

Zerocoin является / был первым серьёзным накопительным подходом к взаимозаменяемости как к расширению прозрачных реестров. Он использовался такими активами, как Zcoin (уже не используется!), но сейчас считается слабым.



Монета Zerocoin **чеканится** путём сжигания известной монеты Bitcoin и добавления в накопитель монет. Zerocoin **тратится** путём доказательства владения неизвестной монетой в накопителе, которая переводится в Bitcoin.

Пример: Zerocoin

Плюсы:

- накопители гарантируют максимальную неопределённость траты;
- прекрасно работает с прозрачными активами.

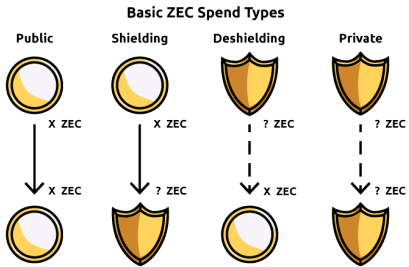
Минусы:

- возможность того, что будут сожжены активы честных пользователей;
- взломанное с целью повышения инфляции доказательство создания («чеканки») монеты;
- ограничение до фиксированной суммы при отсутствии прямой передачи;
- большие и неэффективные доказательства;
- данные времени и связывания переносятся в основной блокчейн.

Zerocash/Zcash

Zerocash был протоколом транзакций, повлиявшим на протоколы **Zcash**. Текущие протоколы используют накопители на основе дерева Меркла, но гораздо более гибко, чем Zerocoin, благодаря более устойчивым системам доказательства.

Транзакции поддерживают прямую передачу скрытых сумм, скрывая траты внутри накопителей. Анонимность обеспечивается опционально.



Пример: Zerocash/Zcash

Плюсы:

- накопители гарантируют максимальную неопределённость траты;
- прекрасно работает с прозрачными активами;
- поддерживает прямые передачи;
- малый размер доказательства и эффективная верификация.

Минусы:

- целостность системы доказательства требует отсутствия конфликтов и правильности MPC;
- сложность структуры из-за более общего характера системы доказательства;
- опциональный характер анонимности;
- транзакции допускают анализ связывания и времени.

Зачем так много подходов?

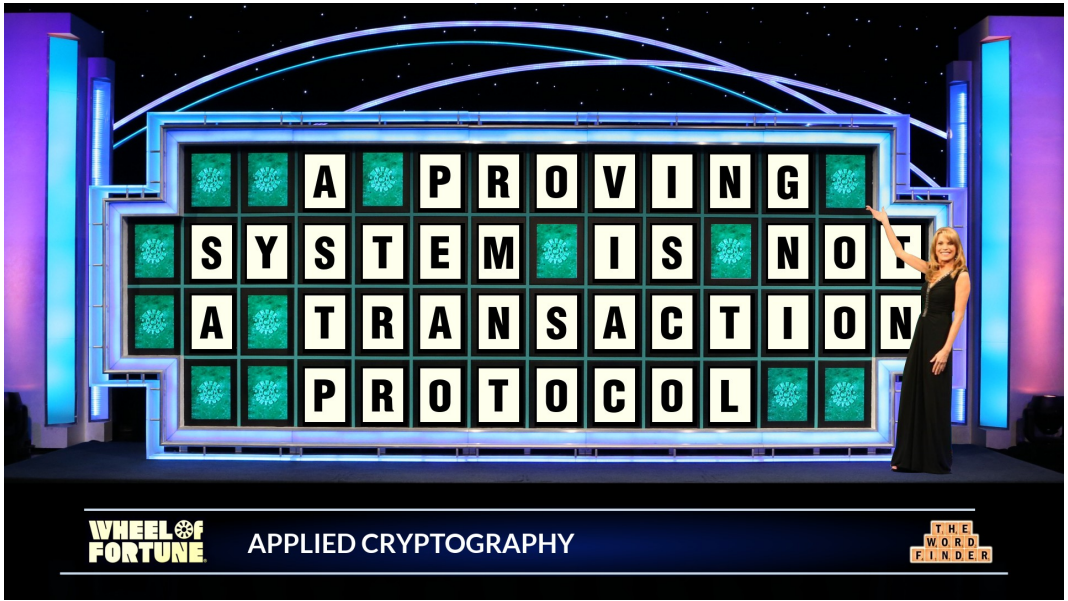
- **Прозрачное смешивание**, по сути, не обеспечивает *никакой* анонимности и даёт очень низкий уровень взаимозаменяемости, но позволяет сохранить совместимость с открытыми реестрами за счёт использования интерактивных процессов.
- Подходы, предполагающие **сокрытие / неопределённость** могут обеспечить разумный уровень анонимности и взаимозаменяемости, но за счёт эффективности и возможности применения некоторых методов анализа графов.
- **Общие системы доказательства** могут использоваться для построения небольших и быстрых транзакций в рамках моделей транзакций, основанных на использовании накопителей, с хорошим уровнем анонимности, но практически за счёт гарантий целостности.

Модель транзакции и система доказательства

Модель транзакции является набором криптографических конструкций (подписей, доказательств), используемых для демонстрации таких вещей, как право владения активом, отсутствие двойной траты, баланс, место назначения и так далее. Нами были рассмотрены несколько.

Система доказательства является криптографической конструкцией, используемой для доказательства и верификации математически определяемых утверждений, включающих приватные и публичные данные, в идеале — с нулевым разглашением.

- Наличие системы доказательства не даёт нам модели транзакции. Наличие языка бесполезно, если вам нечего сказать.
- Конструкции в некоторых моделях транзакций могут быть построены с использованием систем доказательства для создания и верификации транзакций, но тут мы сталкиваемся с рядом препятствий, связанных с эффективностью и специфичностью. Природа контрольной последовательности играет важную роль (например, в случае с ZCash и связанными с ней активами).


A PROVING
SYSTEM IS NOT
A TRANSACTION
PROTOCOL
WHEEL of FORTUNE
APPLIED CRYPTOGRAPHY
THE WORD FINDER

Метаданные имеют значение

Сетевые данные / данные местоположения

Ретрансляция транзакций

Структура ввода-вывода

Временные данные / периодичность

Связывание адресов

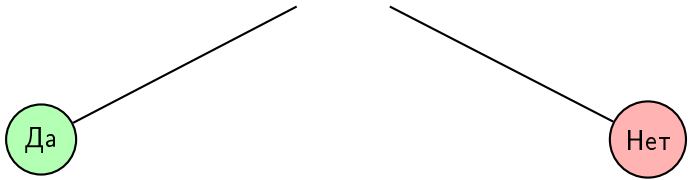
Перемещения / переводы

Атаки по сторонним каналам

Лучшие модели транзакции в мире не обеспечивают удаления всех метаданных!

Направления исследований

Готовы ли вы доверить обеспечение целостности третьим сторонам?



Существуют хорошие системы доказательства, на основе которых можно построить быстрые и эффективные протоколы транзакций, которые будут обеспечивать анонимность и конфиденциальность на основе использования накопителей.

Опции по большей части имеют узкоспециальный характер и страдают от проблем с масштабированием подписей и размера доказательства. Процесс верификации обычно масштабируется так же плохо, как и размер.

Пример: MMORPG (Zcash Sapling)

MMORPG вариант системы доказательства, предложенный Боуи *и др.* от Groth. Он доказывает утверждения относительно соответствия схемы с нулевым разглашением.

Требуются структурированные/доверенные настройки, но они являются распределёнными. Размер доказательства составляет менее 200 байт для схемы любой сложности. Доказательство является линейным для сложности схемы, но верификация будет линейной только для сложности свидетельства.

В случае со схемой ZCash Sapling время доказательства составляет $O(1)$ секунд, а время верификации - $O(1)$ миллисекунд. (Здесь время доказательства зависит от не общей оптимизации схем!)

Используется:

Пример: Bulletproofs

Bulletproofs является расширением, предложенным Бюнцем *и др.* для основной системы доказательств, авторами которой являются Бутль *и др.* Расширение доказывает утверждения относительно соответствия схемы с нулевым разглашением.

Структурированные или доверенные настройки отсутствуют; контрольные последовательности генерируются публично. Размер является логарифмическим (сублинейным) для сложности схемы, но доказательство и верификация происходят линейно.

Для оценки схемы ZCash Sapling: время доказательства составляет $O(10)$ секунд, а время верификации - $O(1)$ секунд (и вплоть до $O(100)$ миллисекунд) при размере доказательства $O(1)$ Кбайт.

Используется (только при оптимизированном доказательстве диапазона):

Дикое упрощение

	Боуи[1]	Бюнц[2]	Бен-Сассон[3]
Отсутствие доверенных настроек	✗	✓	✓
Размер доказательства	✓	✓	✗
Скорость доказательства*	✗	✗	✗
Скорость верификации	✓	✗	✓

* крайне зависит от варианта реализации и схемы

[1] IACR 2017/1050
[2] IACR 2017/1066
[3] IACR 2018/046

Цель

Целью современных исследований является выработка **общих систем доказательства, не требующих доверенных настроек** для обеспечения целостности и практической эффективности.

В одной интересной работе было предложено использовать универсальную и/или обновляемую контрольную последовательность, но и тут есть некоторая возможность использования доверенной модели.

Всё гораздо замысловатее, чем звучит, даже если это уже звучит замысловато.

Спасибо

Рад ответить на ваши вопросы.

Анонимность транзакций и взаимозаменяемость активов - сложная и нерешённая проблема, поэтому, пожалуйста, задавайте вопросы.

sarang.noether@protonmail.com