Исследование методов деанонимизации биткоин-кошельков

Антонов Илья Михайлович

Научный руководитель: Подлесных Дмитрий Артурович, каф. ИВМ МФТИ

Московский физико-технический институт

20 мая 2025 г.

Модель UTXO в Bitcoin

- **UTXO (Unspent Transaction Output)** — непотраченный выход транзакции.
  - **TXO** — базовая единица: пара «сумма + скрипт блокировки».
  - Любая транзакция — это набор *входных* и *выходных* TXO. Входы «погашают» ранее созданные UTXO, выходы создают новые.
  - Все биткоины существуют только в виде совокупности актуальных (непотраченных) UTXO.

Структура UTXO и транзакций

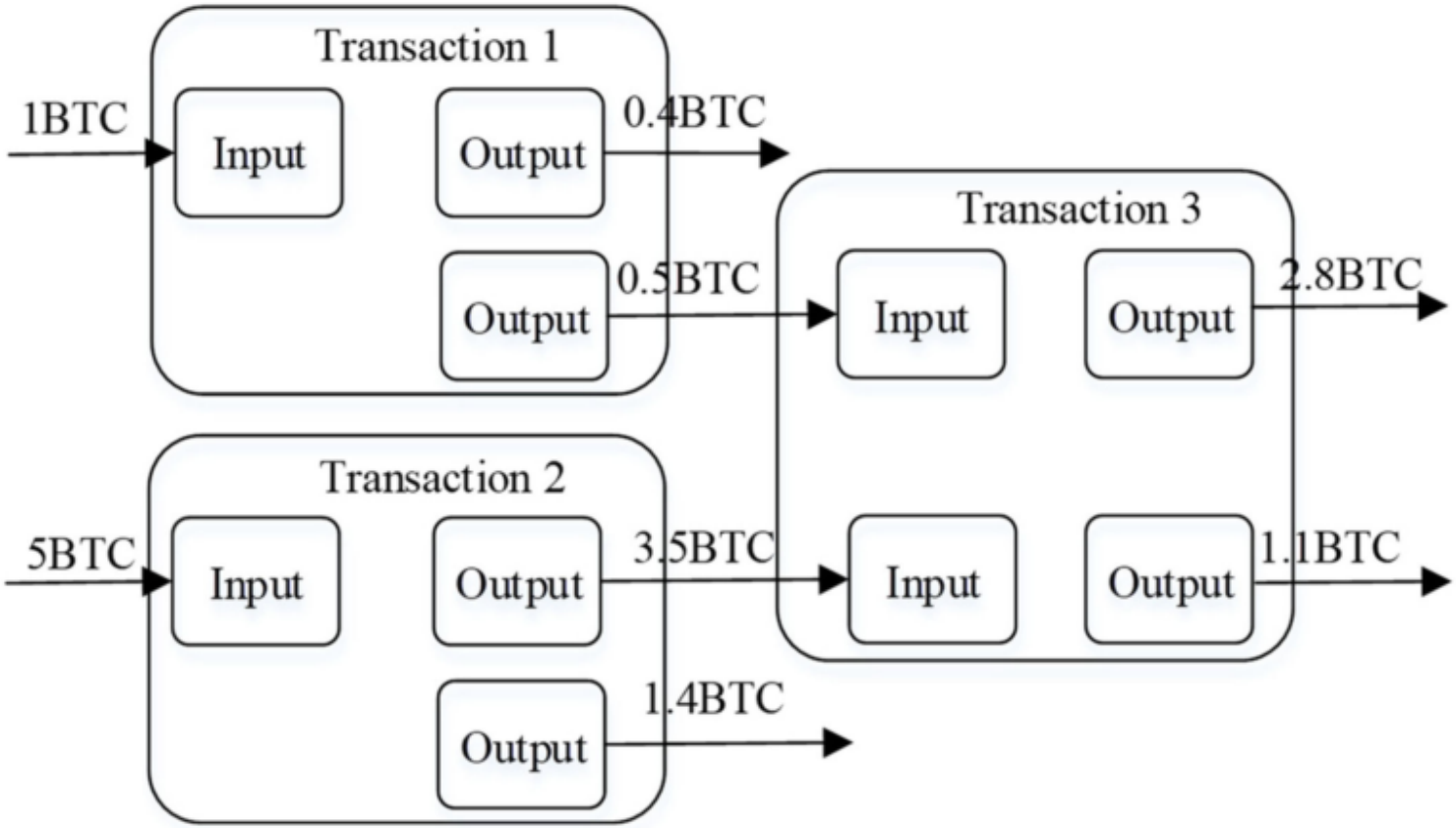


Рис.: Схема модели UTXO: входы ссылаются на предыдущие UTXO, создаются новые выходы

Мотивация и постановка задачи

- **Цель**: выявить совокупности скриптов, принадлежащие одной экономической сущности.
- **Постановка задачи**: сгруппировать скрипты так, чтобы каждый кластер представлял отдельную конечную сущность.
- **Метод**:
  - применяем эвристики к наборам данным
  - измеряем эффективность и качество каждой эвристики

Основные эвристики кластеризации

Эвристика общего входа (Common Input Heuristic)

- Адреса, используемые как входы в одной транзакции, принадлежат одному владельцу
- Основана на необходимости подписывать транзакцию приватными ключами
- **Условие объединения:** Если в транзакции Δ участвуют два или более разных входных скрипта ($n_{in}(\Delta) \geq 2$), все входные скрипты объединяются в один кластер

Основные эвристики кластеризации

Эвристика адреса сдачи

- **Условие объединения:** Если транзакция имеет
  - Ровно 2 выхода;
  - Один выход новый, другой уже встречался раньше

Эвристика одноразового адреса сдачи

- **Условие объединения:** Если транзакция имеет
  - входные и выходные адреса не пересекаются
  - среди выходов ровно один новый адрес

Дополнительные эвристики

- **Эвристика оптимальной сдачи**
  - **Условие объединения:** В транзакции с одним входом и двумя выходами, если один выход имеет "круглое"значение $(v - round(v) < \epsilon)$, а другой нестандартное, то входной адрес и адрес нестандартного выхода объединяются в один кластер

Дополнительные эвристики

Эвристика принудительного объединения входов

- **Условие объединения:** если транзакция
  - содержит $n_{\text{in}} \geq 2$ входа и ровно $n_{\text{out}} = 2$ выхода;
  - все входные адреса и адрес «сдачи» ранее не встречались в блокчейне;
  - суммарная стоимость входов без наименьшего из них меньше платежного выхода:

$$v_{\text{in}} - \min_{i \in \text{in}}(v_i) < v_{\max},$$

  что указывает на вынужденное объединение UTXO;

то все входные адреса и адрес $v_{\min}$ («сдача») объединяются

Дополнительные эвристики

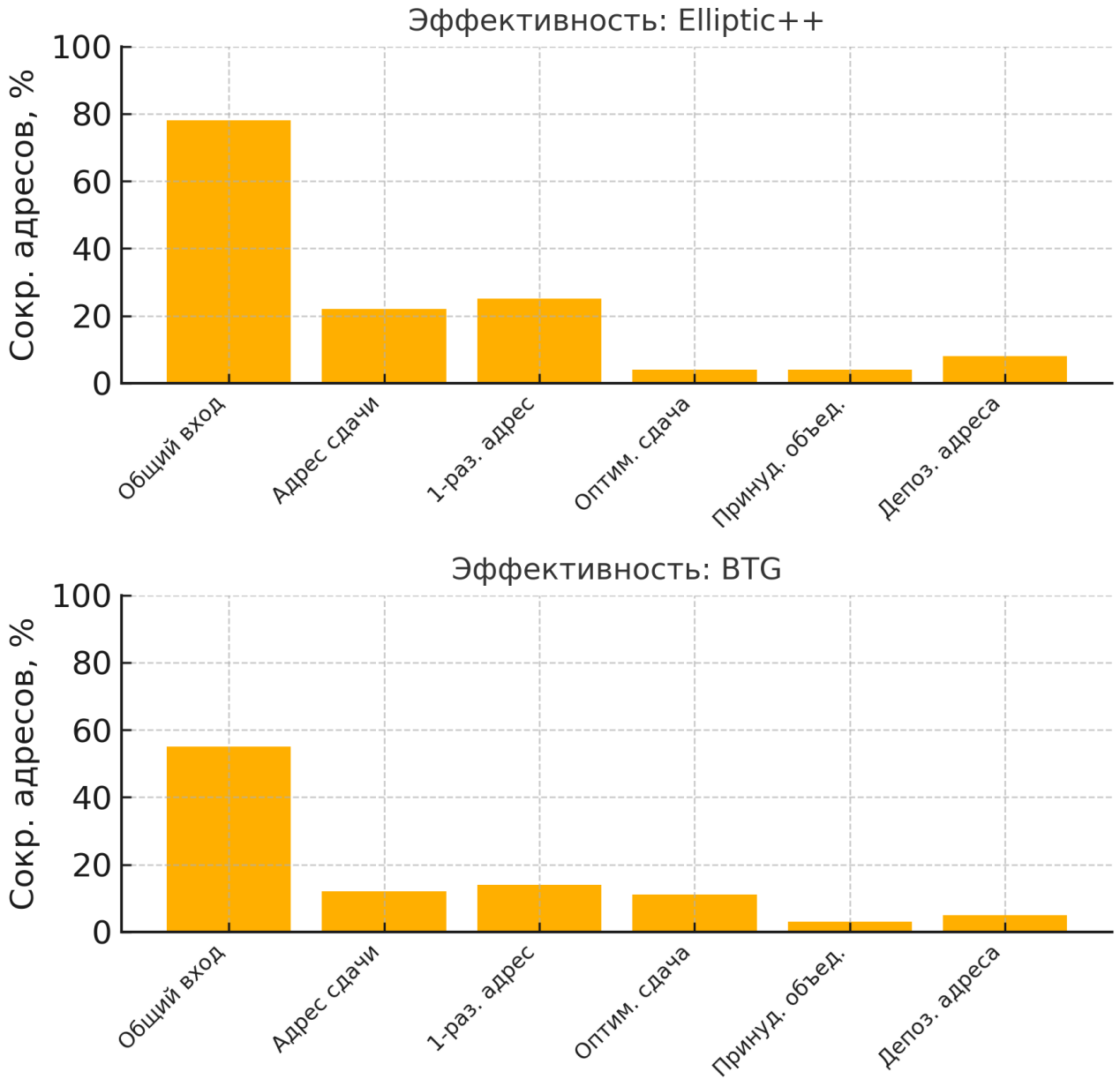
Эвристика депозитных адресов сервиса

- **Условие объединения:** транзакция содержит не менее 50 входов $\left(n_{\text{in}} \geq 50\right)$ и ровно **один** выход $\left(n_{\text{out}} = 1\right)$; тогда все входные адреса объединяются в единый кластер, поскольку с высокой вероятностью принадлежат одному сервису.

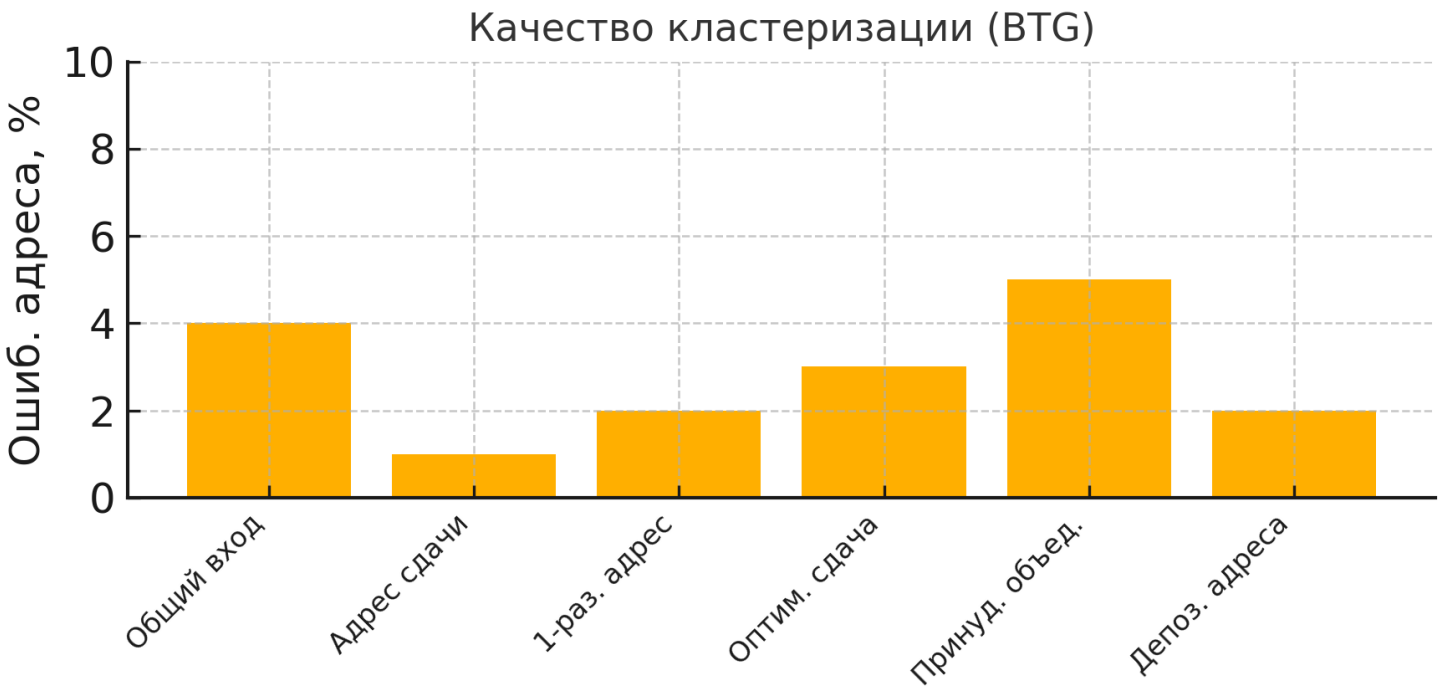
Методология исследования

- **Используемые данные:**
  - *Elliptic++* [1] — транзакции и адреса Bitcoin с **разметкой «законная / нелегальная»**
  - *Bitcoin Transaction Graph Dataset* [2] — адреса с **детальной категоризацией сущностей**
- **План эксперимента:**
  - Для *каждой* эвристики и *каждого* датасета отдельно:
    - рассчитываем эффективность — процентное сокращение числа уникальных адресов/скриптов;
  - Дополнительно **на втором датасете** измеряем качество кластеризации объединение адресов с *разными* метками (напр. «биржа» + «физ. лицо») трактуется как ошибка;

Результаты исследования: эффективность эвристик



Результаты исследования: качество кластеризации



Доля ошибочно объединённых адресов в кластере

Выводы

- **Общий вход** – самое эффективное сжатие графа , при этом даёт лишь $\sim 4\%$ ошибок.
- **Эвристики сдачи** (обычная и одноразовая) убирают 10–25 процентов узлов при ошибках $\leq 2\%$. Оптимальны там, где важна точная привязка сущностей

Источники данных и литература

- **Основные источники данных:**
  1. Elmougy, Y., Liu, L. (2023). “Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics.” *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD ’23)*. doi:10.1145/3580305.3599803
  2. Schnoering, H., Vazirgiannis, M. (2025). “Bitcoin Research with a Transaction Graph Dataset.” . doi:10.1038/s41597-025-04684-8
- **Литература по эвристикам:**
  - Meiklejohn, S., et al. (2013). "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names."
  - Ron, D., Shamir, A. (2013). "Quantitative Analysis of the Full Bitcoin Transaction Graph."
  - Harrigan, M., Fretter, C. (2016). "The Unreasonable Effectiveness of Address Clustering."