

Деанонимизация криптокошелька (на основе анализа блокчейн-транзакций)

Антонов Илья Михайлович

Научный руководитель: Подлесных Дмитрий Артурович, каф. ИВМ МФТИ

Московский физико-технический институт

11 марта 2025 г.

- **Задача:**

- Деанонимизировать владельцев криптовалютных кошельков (связать криптоадреса с реальными субъектами)

- **Мотивация:**

- Повышение эффективности правоохранительной деятельности
- Обеспечение прозрачности и снижение рисков криптовалютной экосистемы

- **Актуальность:**

- Значительный рост и усложнение криптопреступности
- Недостаточная эффективность существующих методов анализа криптотранзакций

Постановка задачи и мотивация

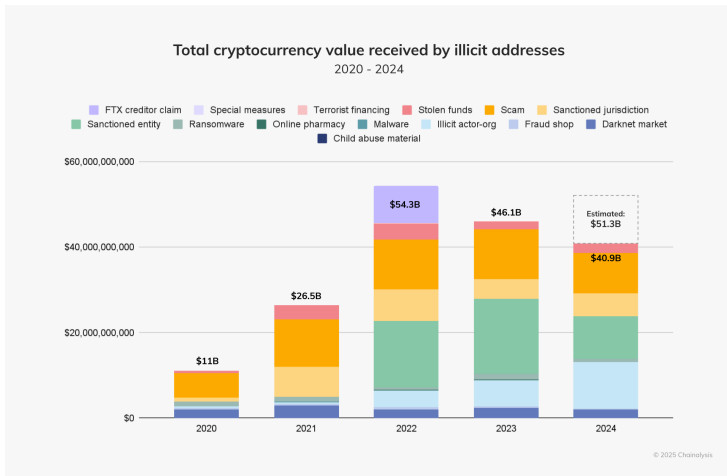


Рис.: 1. Общий объем криптовалюты, полученный адресами, связанными с незаконной деятельностью, за период 2020–2024 годы (по типам преступлений)

Современные методы анализа

- Эвристический подход
- Графовый анализ
- Машинное обучение

- Общий вход (Common Input Heuristic)
- Анализ "сдачи" в транзакциях
- Повторное использование адресов

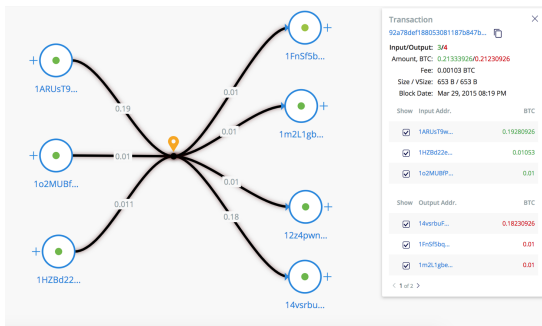


Рис.: 2. Пример Coinjoin-транзакции

Графовый анализ транзакций

- Визуализация сетей транзакций
- Кластеризация адресов
- Выявление "сообществ" адресов

Графовый анализ транзакций

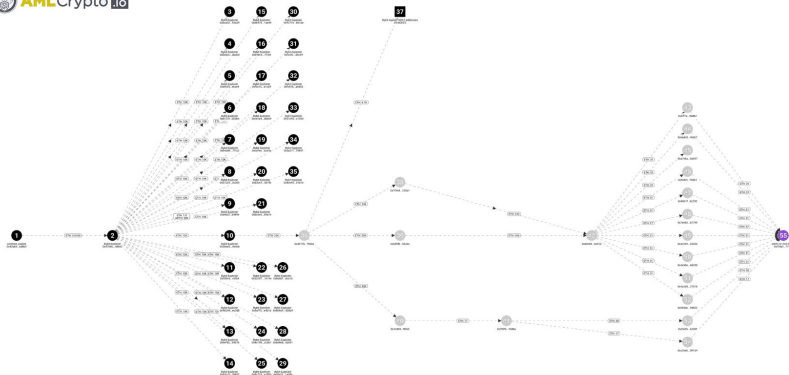


Рис.: 3. Анализ движения криптовалютных средств после взлома биржи Bybit с помощью графа транзакций

Машинное обучение в деанонимизации

- Классификация адресов по типам
- Графовые нейронные сети (GNN)
- Выявление аномалий и паттернов поведения

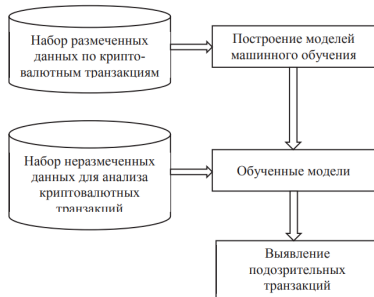


Рис.: 4. Общая архитектура системы машинного обучения для анализа блокчейн-транзакций

Планируемые результаты

- Расширение охвата деанонимизации адресов
- Повышение точности и снижение ошибок классификации
- Разработка практических рекомендаций по улучшению методов

Методы и план исследования

- Этап 1: Сбор данных и формирование датасета
- Этап 2: Эвристическое объединение адресов (кластеризация)
- Этап 3: Графовый анализ транзакций и визуализация
- Этап 4: Разработка и обучение модели машинного обучения
- Этап 5: Экспериментальная проверка и оценка результатов

Заключение и дальнейшая работа

- Эффективность достигается комбинацией методов (эвристики, графовый анализ, ML)
- Дальнейшие исследования будут направлены на улучшение точности и разработку новых подходов

Список литературы

<https://drive.google.com/drive/.....>