Принципы и методы криптовалютных расследований

Докладчик: Γρηγόριος

whoami

Меня зовут Григорий, я представляю команду ШАРД, платформу безопасности цифровых активов.

Основные направления нашей деятельности:

- оценка криптовалютных рисков
- консультирование в этой области
- блокчейн аналитика
- крипторасследования

Блокчейн как технология

Технология блокчейн (технология распределенных реестров) – выстроенная по определённым правилам цепочка из формируемых блоков транзакций.

- Блокчейн вечно хранит информацию о времени и сумме транзакций
- В блокчейн нельзя внести изменения
- Публичный блокчейн общедоступен

Аналитические инструменты

Иностранные

Chainalysis

ELLIPTIC

CIPHERTRACE

BITFURY Crystal

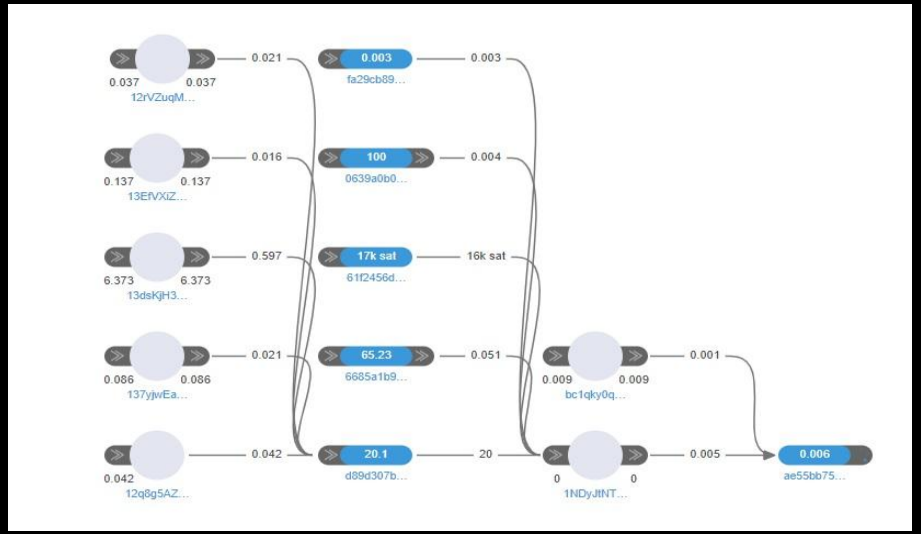
Отечественные

ШАРД

«Прозрачный блокчейн»

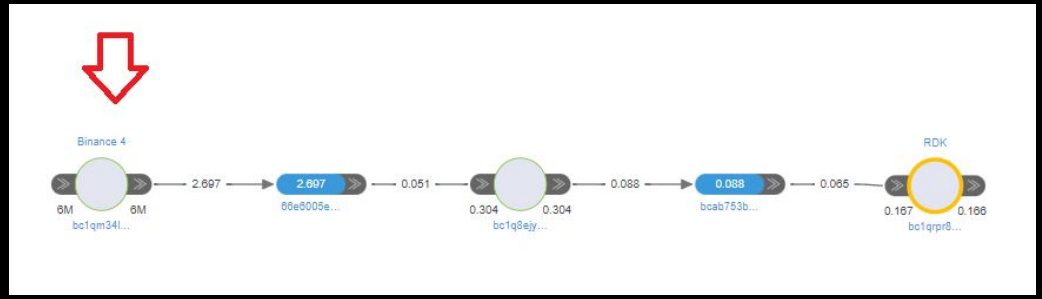
Методы исследования

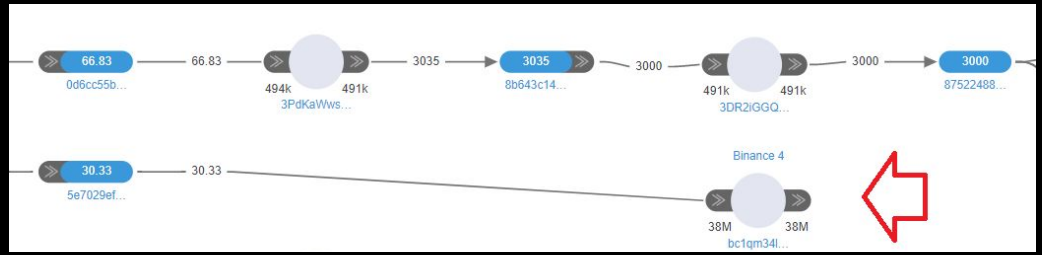
- Визуализация связей
- Кластеризация по эвристикам
- Трейсинг транзакций



Методология расследования

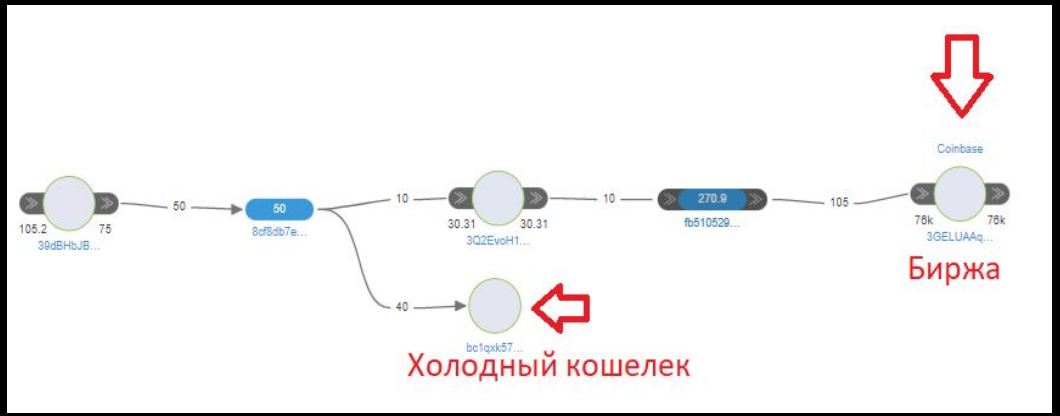
1. Установка целевого адреса
2. Определение путей поступления средств
3. Определение путей вывода средств

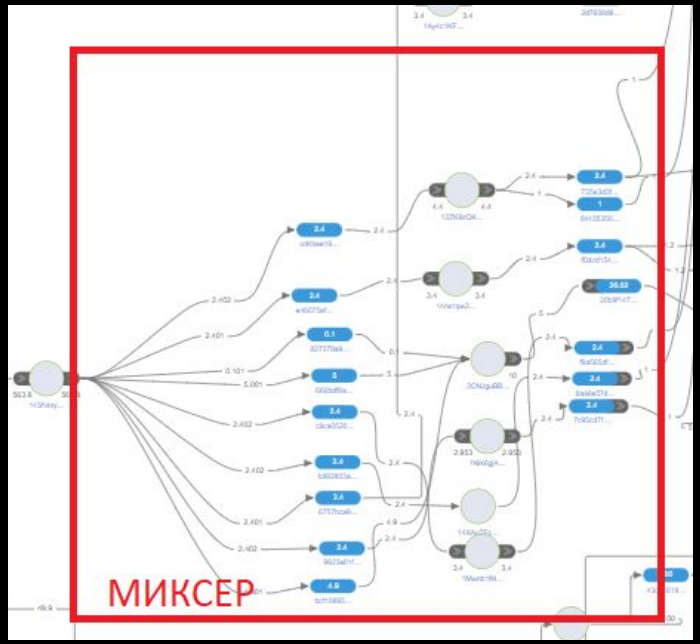




Результаты расследования

1. Криптосервис (биржа/обменный сервис)
2. Холодный кошелек
3. Миксер





Взаимодействие с криптобиржами

Биржи проводят идентификацию пользователя, хранят логи операций.

По обращению правоохранительных органов биржа раскрывает сведения о клиенте.

Биржа раскрывает информацию правоохранителям информацию только о принадлежности аккаунта их гражданину той же страны

Политика сотрудничества с государственными органами для биржи это показатель доверия

Взаимодействие с криптобиржами в эпоху санкций

У многих бирж есть представительства в РФ.

Биржа может заблокировать адреса злоумышленника на основании жалоб пользователей.

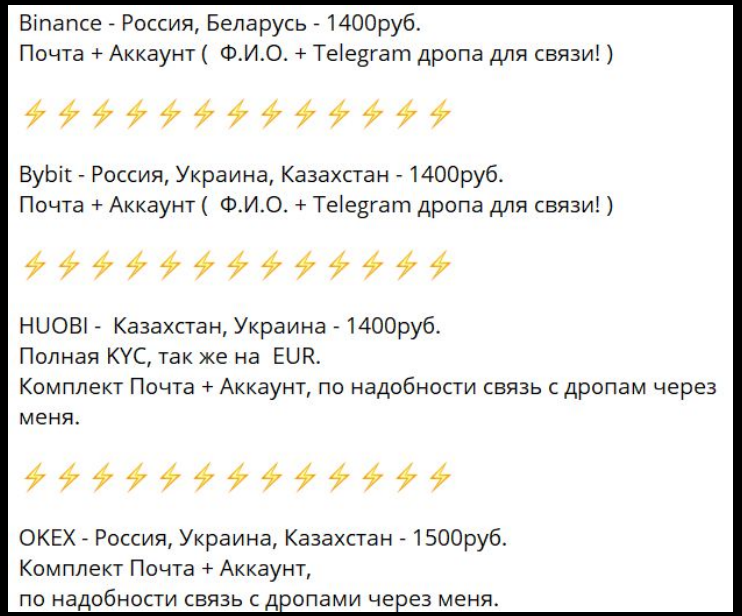
К жалобе можно приложить свое исследование с описанием обстоятельств хищения.

Биржа	Адрес для отправки запроса
Binance	case@binance.com
Garantex	support@garantex.ru
OKEx	OKExSeychelles@okex.com
Coinbase	int.sunpoenas@coinbase.com
Kraken	lawenforcement@kraken.com
Huoni	regulatory@huobi.com
Nicehash	support@nicehash.com
ByBit	support@bybit.com
Vexel	legaldep@vexel.com

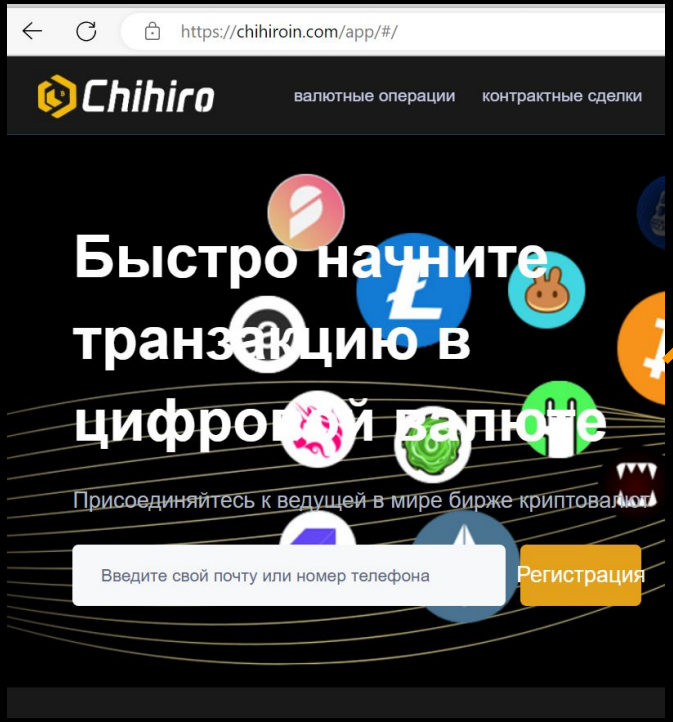
Приобретение и хищение аккаунтов криптобирж

Цены готовых аккаунтов от $30 до $200 в зависимости от биржи, репутации продавца. Ценятся аккаунты, оформленные на жителей Европы без двухфакторной аутентификации.

Хищение уже созданных аккаунтов у пользователей либо регистрация на установочные данные найденные в утечках, с использованием сервисов по отрисовке документов и с обходом программ для фотографирования для прохождения KYC.



Кейс №1. Фейковый трейдинг



TSaRZDiBPD8Rd5vrvX8a4zgunHczM9mj8S

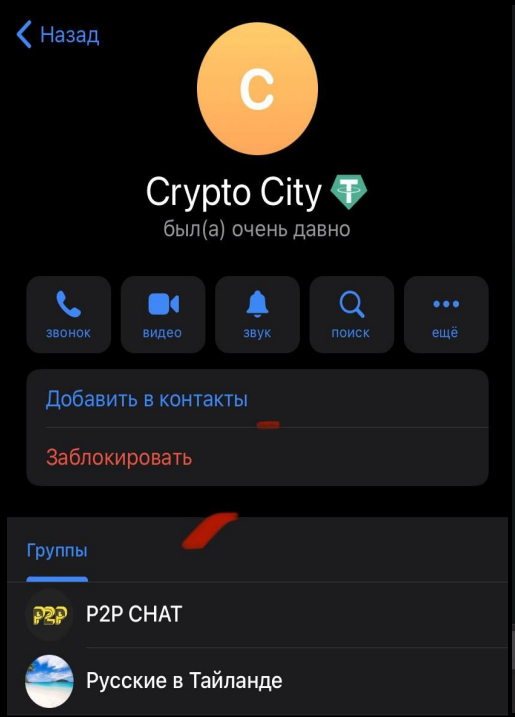
Okex | Add a private tag

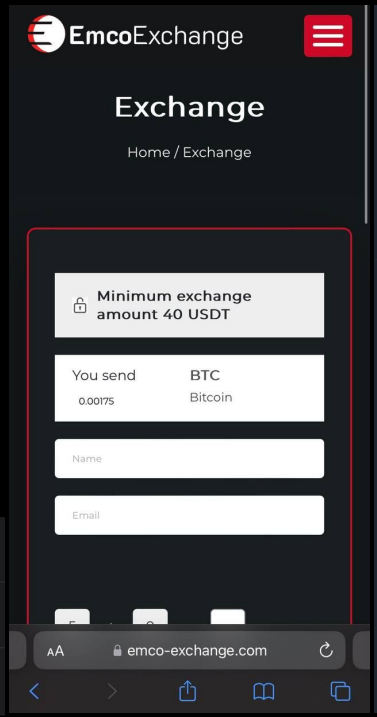
TXTsYYXyk3ZCHwM8mw3M7m3LRRWVBDWUsC

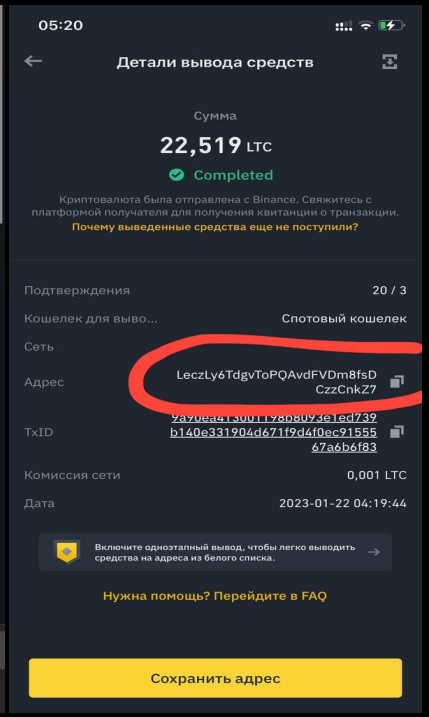
TGj8b8zLXJaxqU5hTokTa9mUH1m1TLDvFd

TCuFKpmbxwxHZYSxeHf9onTz66asxo1JPK

Кейс №2. Фейковый обменник







Обменный сервис после совершения «обмена» поменял адрес приема средств в LTC

Кейс №2. Фейковый обменник

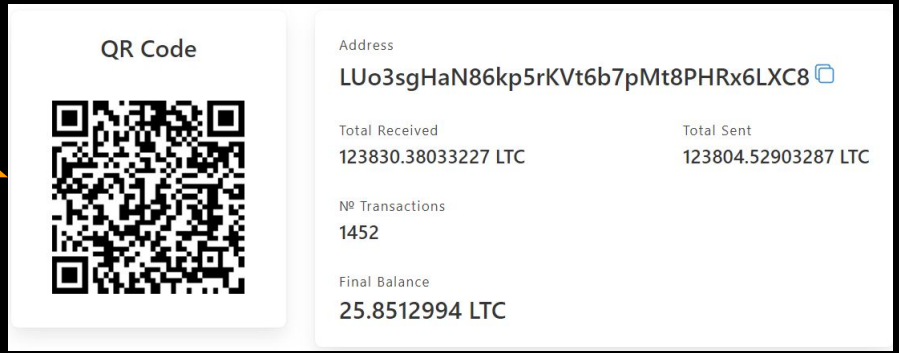
LZEjckteAtWrugbsy9zU8VHEZ4iUiXo9Nm

LeczLy6TdgvToPQAvdFVDm8fsDCzzCnkZ7

M88ZvnPZyNxSiz6v9EVU7KXQvuo3euavz9

Биржа Binance

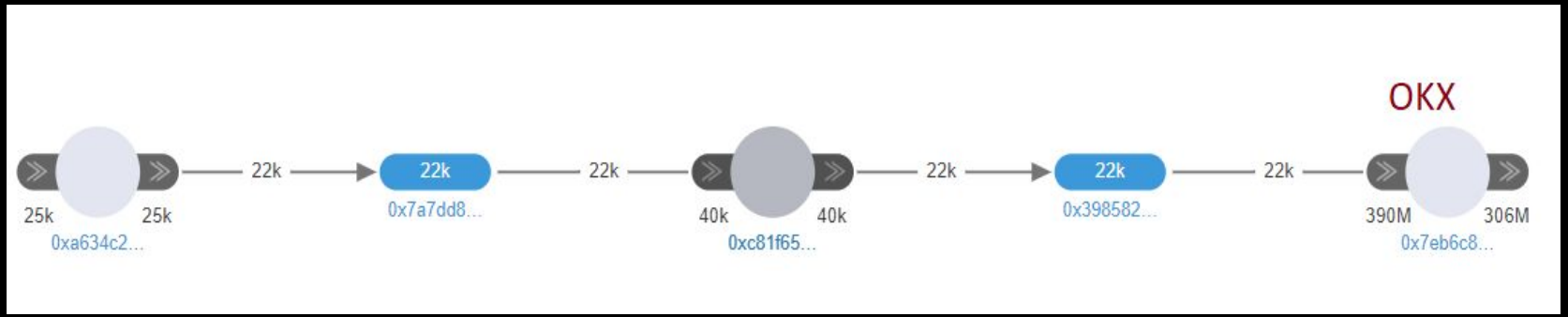
Адрес “Обменника”

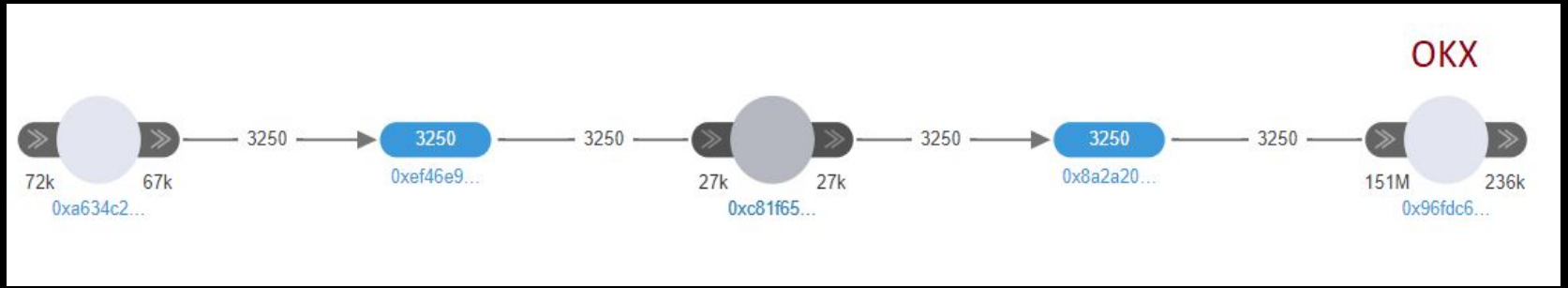


Кейс №3. Ограбление блогера

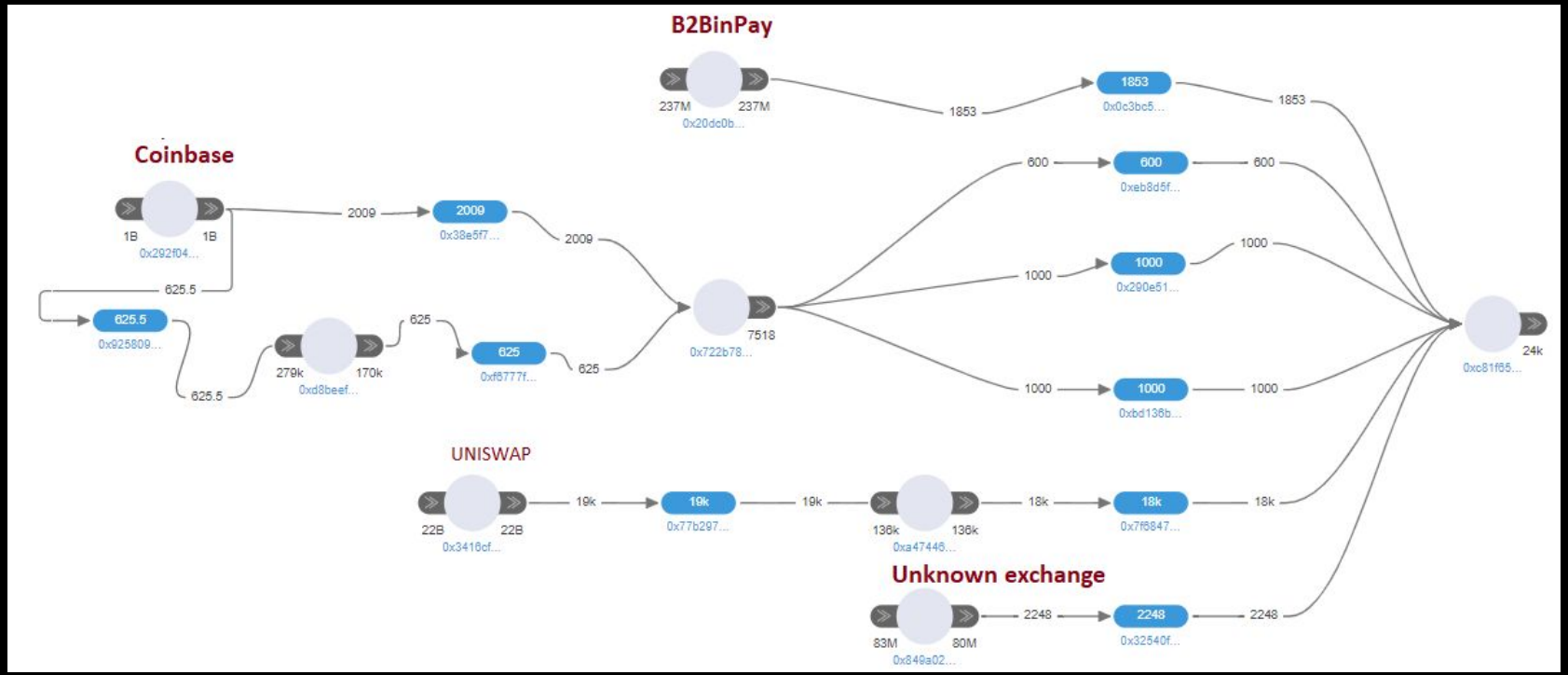
Вооруженное ограбление произошло в декабре 2022 года на участников одного криптопроекта. Угрожая огнестрельным оружием, похитители вынудили жертв открыть доступ к криптовалютным кошелькам на мобильных телефонах и перевести им на криптокошелек $25 000 в криптовалюте USDT.

Кейс №3. Ограбление блогера





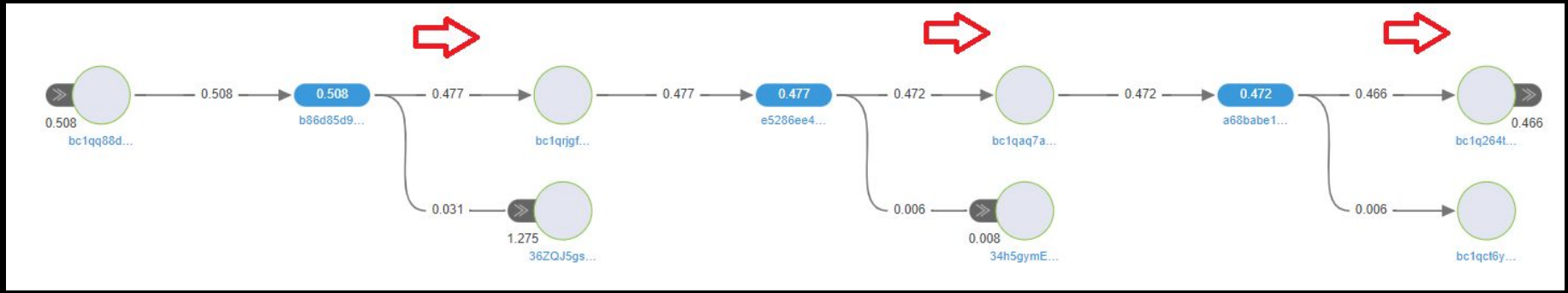
Кейс №3. Ограбление блогера



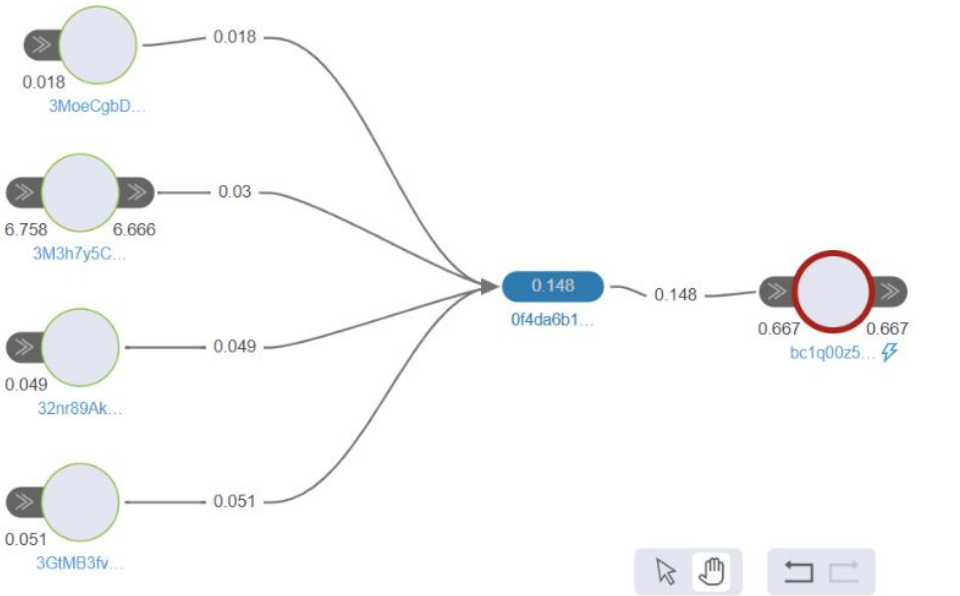
Методы деанонимизации криптовалютных адресов

- Эвристические методы
- Анализ графа транзакций
- Сбор информации в сети (Web-scraping): репорты пользователей, санкционные списки, форумы, утечки, информация из бирж и сервисов
- Расследования, ловушки
- OSINT (в том числе Google Dorks)

Эвристика наибольшей суммы



Эвристика общей траты



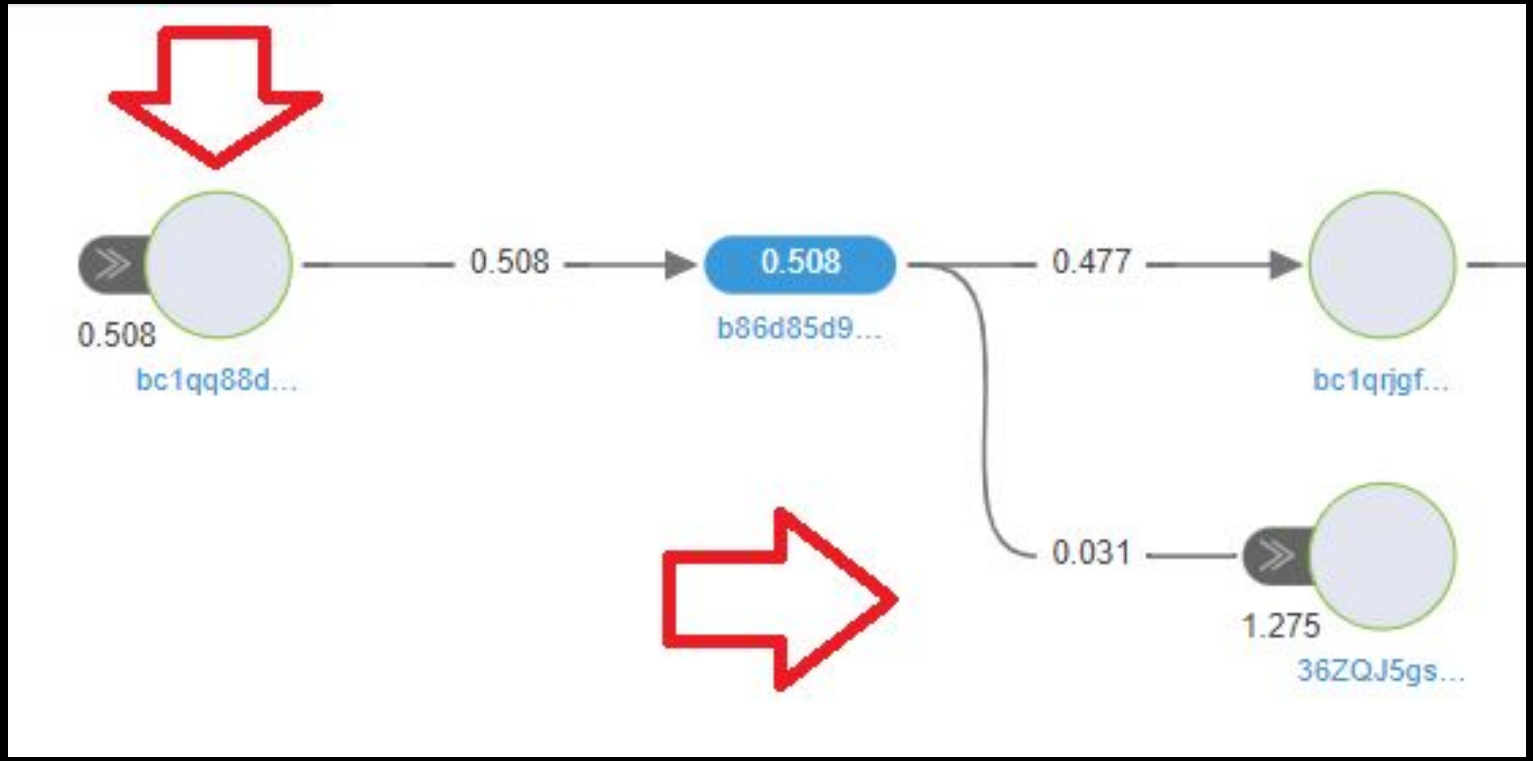
Входящие адреса

	АДРЕС	СУММА
☑	3MoeCgbD9f...	0.018
☑	3M3h7y5Cz5...	0.03
☑	32nr89AkYu...	0.049
☑	3GtMB3fv5T...	0.051

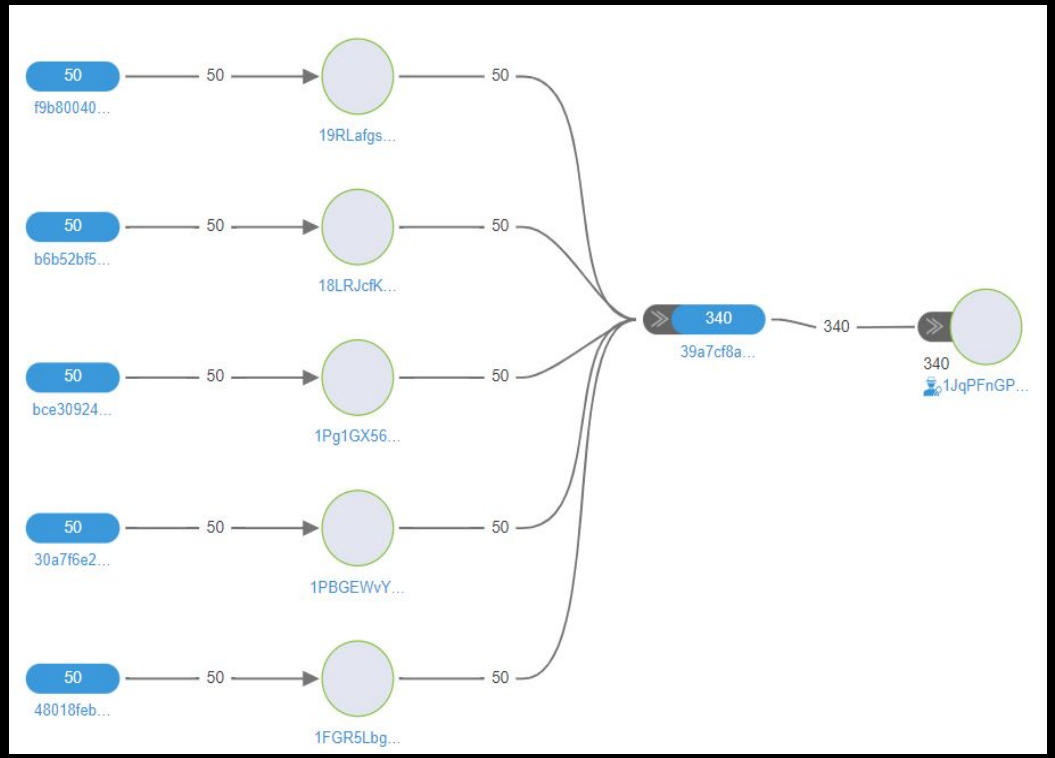
Исходящие адреса

	АДРЕС	СУММА
☑	bc1q00z5uf...	-0.148

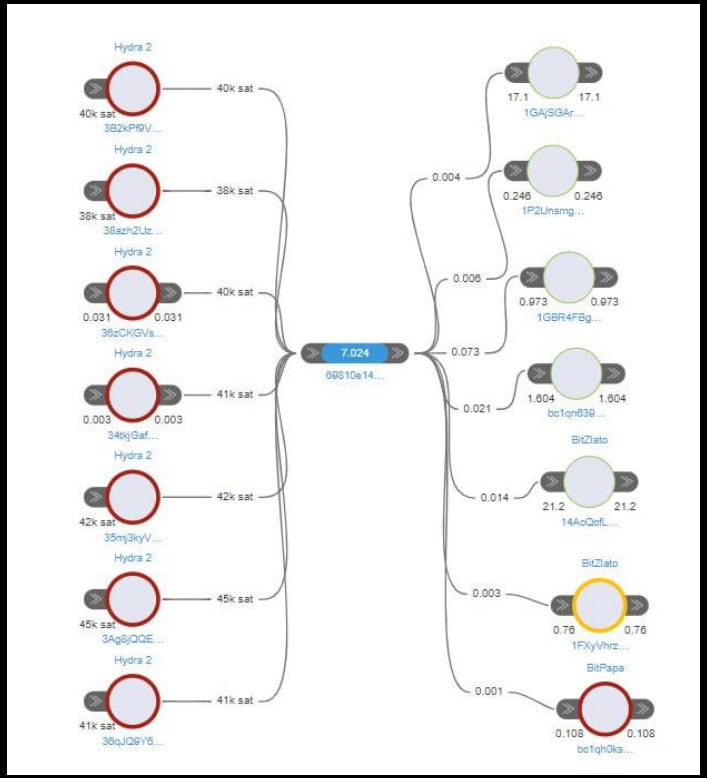
Эвристика общей сдачи



Coinbase транзакции

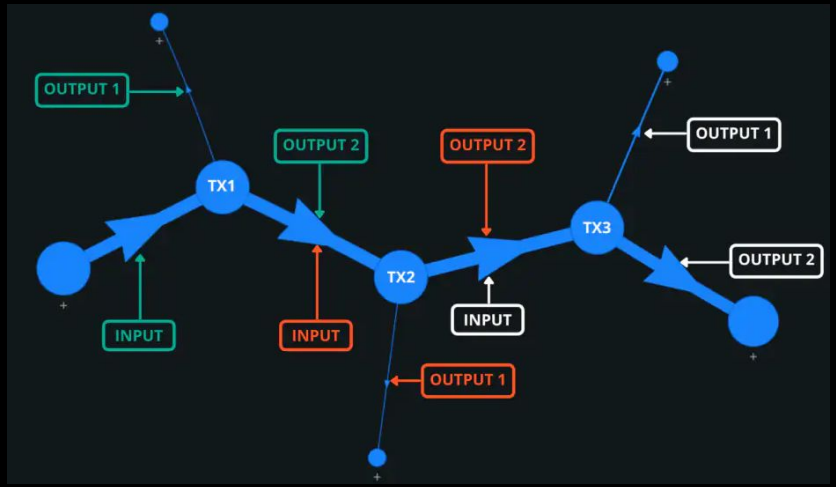


Эвристика смешанной транзакции



Методика деанонимизации по графу

- Крупнейший выход делает предполагаемый выход со сдачей легко заметным.
- Выход со сдачей всегда выплачивается на P2PKH-адреса.
- Выход со сдачей чаще всего является вторым из двух выходов транзакции.
- Поиск аналогичных паттернов транзакций на графе



Анонимизация VS Деанонимизация

Борьба тех кто хочет оставаться анонимным, с регуляторами, правоохранительными органами и криптосервисами, которые требуют раскрыть данные.

+ Всегда найдутся новые методы анонимизации

+ У кого больше ресурсов скрыться либо раскрыться тот эффективнее решает задачу

Контакты

121099, г. Москва, ул. Новый Арбат, д. 30/9, помещ. 2н ком./офис 2/22

Тел. +7 495 225 90 22

info@shard.ru

https://shard.ru

СПАСИБО. ВОПРОСЫ?

ШАРД

https://shard.ru

https://t.me/osint_mindset

https://t.me/+smhN69qD2mkxMTEy