Как хакеры и мошенники оттывают криптовалюту и что с этим можно сделать

angkasawan

VOLGA CTF international open competition

Обо мне

OSINT-Аналитик

Расследователь криптовалютных преступлений

Спикер PHDays, OFFZONE, OSINTomático, ВШЭ, OSINT Mindset meetup

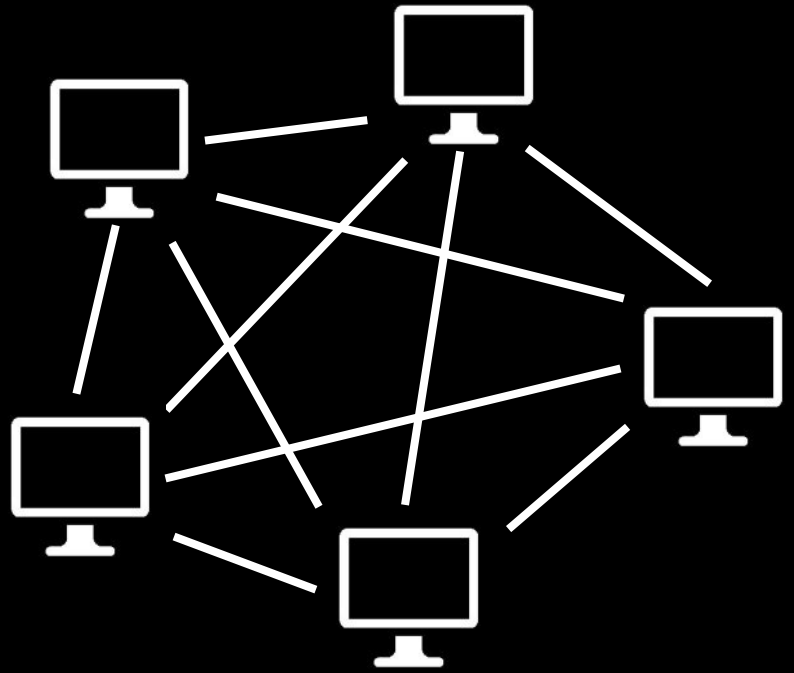
DeFi безопасность

Что такое криптовалюта

P2P сеть

Хранится и обновляется информация по алгоритмам консенсуса

Информация представляет собой архив совершенных транзакций

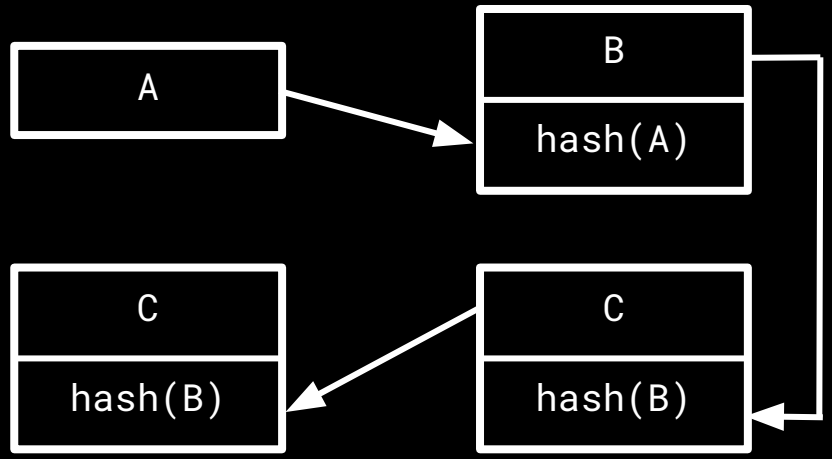


Что такое криптовалюта

P2P сеть

Хранится и обновляется информация по алгоритмам консенсуса

Информация представляет собой архив совершенных транзакций



Bitcoin

Большая бухгалтерская книга

Происхождению любых средств можно определить вплоть до появление в одном из блоков

Сложность расследований заключается в отсутствии развитой экосистемы и сервисов сообщества


```
{
  "txid": "d5fd03388e9b3985bc5e2631c5c2a643ecae9dbff11270b0120832be5b979f83",
  "size": 478,
  "version": 2,
  "locktime": 0,
  "fee": 6749,
  "inputs": [
    {
      "coinbase": false,
      "txid": "f3d427ed0aa171df243e246b3a2ba7f93c7c61e6a7bb12f1911645b3dc7fafa0",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967293,
      "pkscript": "0014debacc113761d3a721447222db9125fd34da69d7",
      "value": 11500000,
      "address": "bc1qm6avcyfhv8f6wg2ywg3dhyf9l56d56wh7pyjl0",
      "witness": [
"304402202fb5890895355bd9e5bc7e94301ffcfb402b0fe477ab4527bd0de8ddcf17a39902206b2812f56
59cc029618fcf3ae8201",
        "020890ebb385a67ee05acd050edcc98dcd9dd7eb57f472f3e394236a9fb702f690"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1q9s7jd2g0lkkcy9hk8e808ndt8fzcxq2rzdgvdy",
      "pkscript": "00142c3d26a90ffdad8216f63e4ef3cdab3a45830143",
      "value": 92973,
      "spent": true,
      "spender": {
        "txid": "4838f8dab5237ab3cb7587f28e2ddeb7b1d8fdd4beb2c564f29d1b860ade89e2",
        "input": 36
      }
    },
    {
      "address": "bc1q6ya2ttm3nf4zz80rcmg3c3g8hvltqf6206shwv",
      "pkscript": "0014d13aa5af719a6a211de3c6d11c4507bb3eb0274a",
      "value": 10288359,
      "spent": true,
      "spender": {
        "txid": "cad7792cd526a797301a4ee34671126778f83380af8015388c9ea6c218c1bd70",
        "input": 0
```

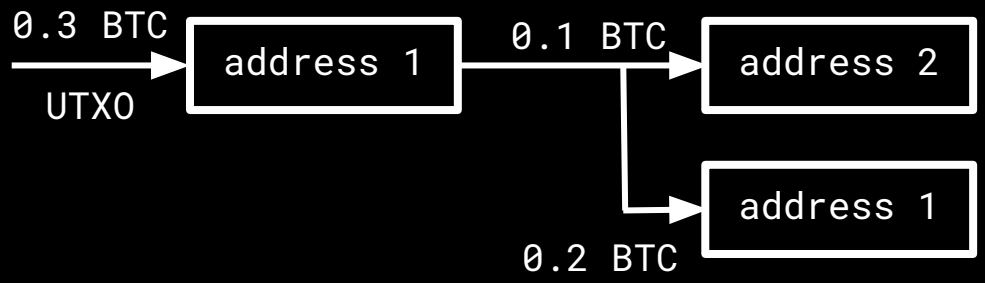
Bitcoin

UTXO - непотраченный вход

При отправке транзакции вход тратится полностью

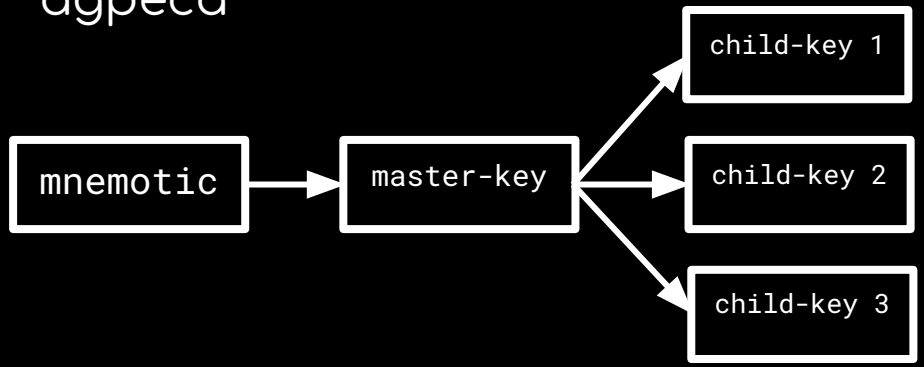
Если необходимо отправить меньше чем вход, то сдача отправляется обратно владельцу

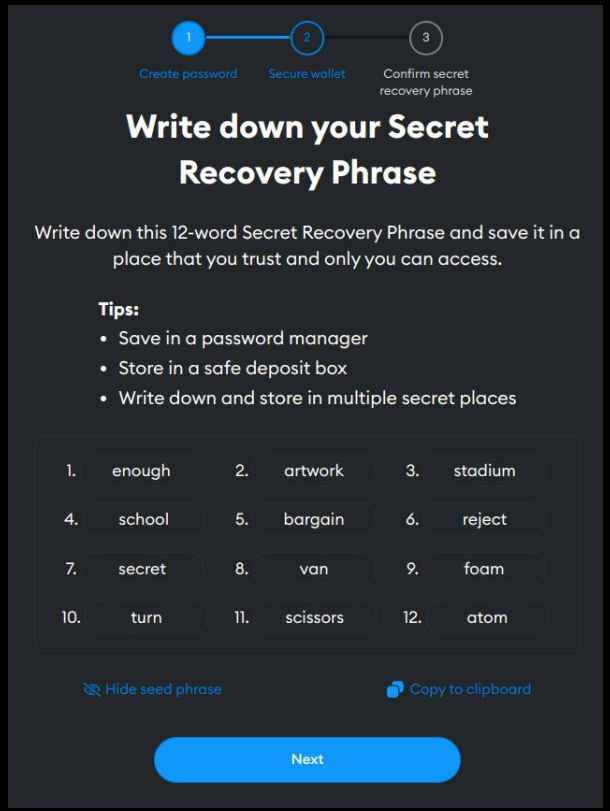
Если необходимо отправить больше, то несколько входов объединяются



HD-кошелек (BIP-32)

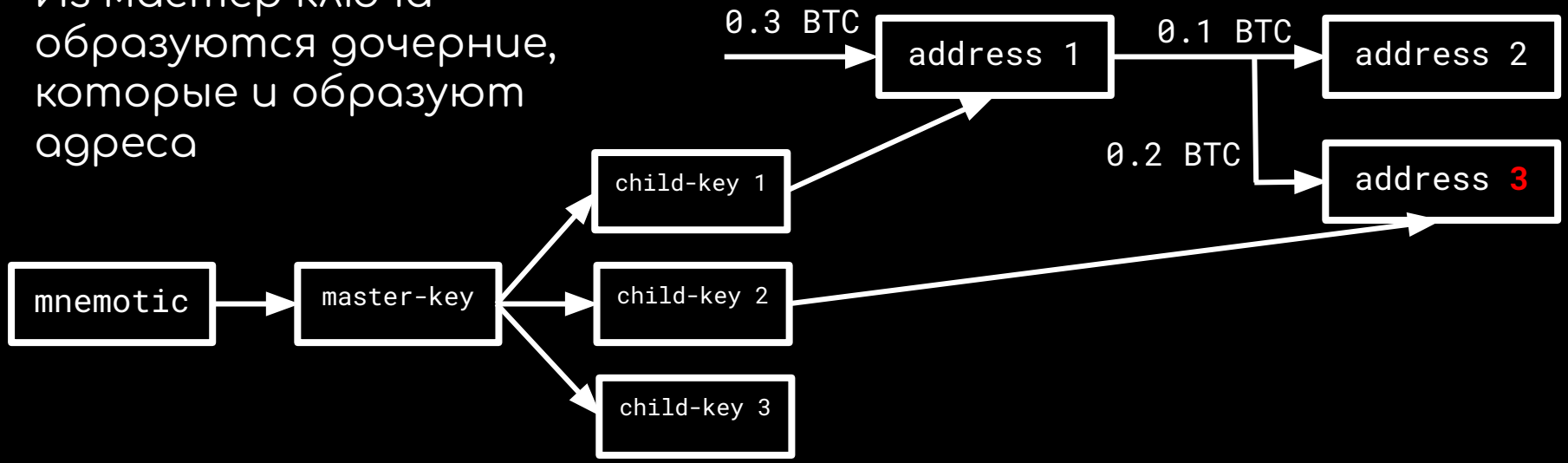
Из мнемотической фразы образуется мастер ключ
Из мастер ключа образуются дочерние, которые и образуют адреса





HD-кошелек (BIP-32)

Из мнемотической фразы образуется мастер ключ
Из мастер ключа образуются дочерние, которые и образуют адреса



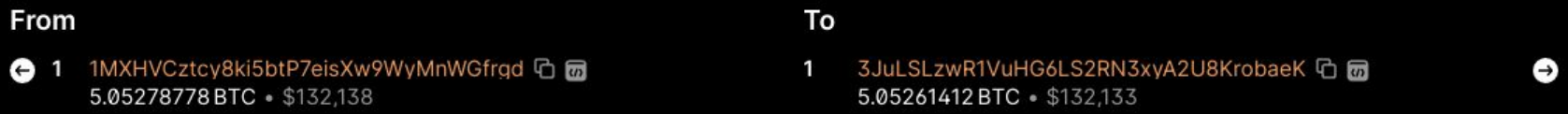
Пример расследования

Мы хотим купить криптовалюту у владельца адреса **3JuLSLzwR1VuHG6LS2RN3xyA2U8KrobaeK**.

Сделка состоится в формате "лицом к лицу". После сделки мы планируем положить криптовалюту на свой счет на бирже Binance. Нам надо узнать источник происхождения средств: легально ли они были получены? И если нелегально, то каким именно образом?

Используем обозреватель

Все средства пришли с адреса
1MXHVCztcy8ki5btP7eisXw9WyMnWGfrgd



Обозреватели для Bitcoin:

https://blockchain.com/explorer

https://www.walletexplorer.com/

https://blockchair.com/

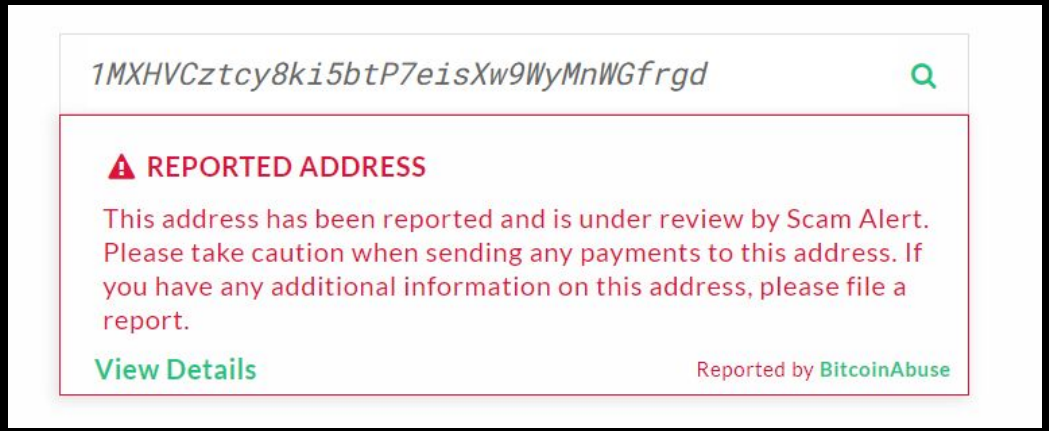
OSINT? (просто Google)

https://www.bitcoinabuse.com › reports

Recently Reported Addresses - Bitcoin Abuse Database

This page contains a list of bitcoin addresses used by hackers and scammers. Click on an address to learn more about how the address was used.

You've visited this page 2 times. Last visit: 11/19/22



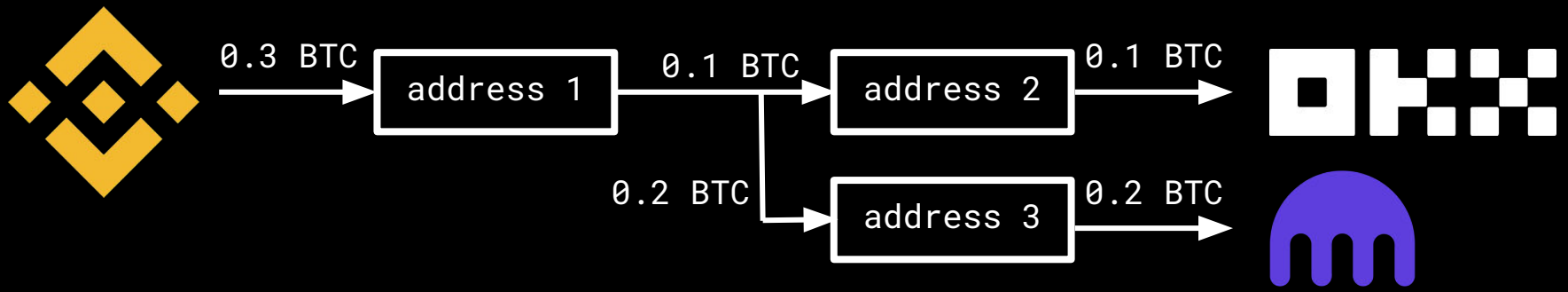
Ход расследования

Источник происхождения средств

Анализ движения средств на адресе

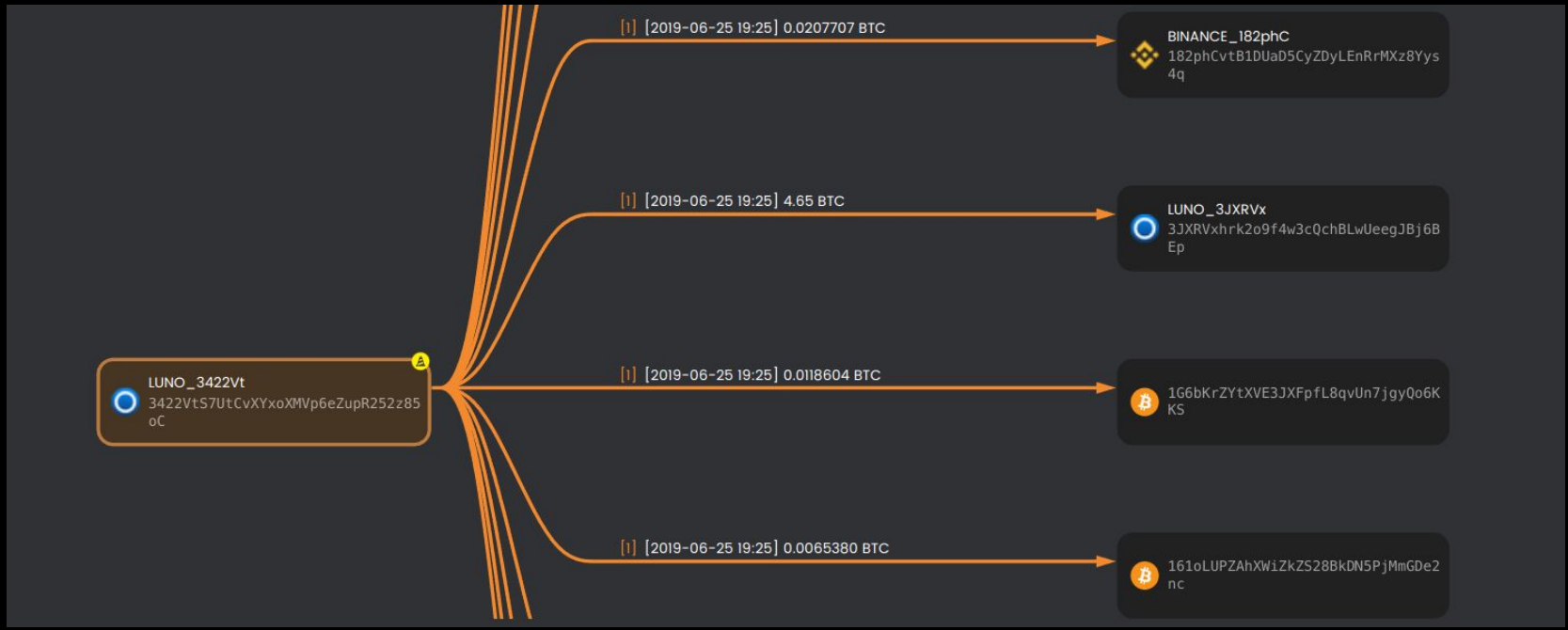
Конечный получатель

OSINT и запросы в сервисы



Определяем биржи

BLOCKSEC MetaSleuth https://metasleuth.io/



Определяем биржи

https://www.walletexplorer.com/

Top wallets

Exchanges:	Pools:	Services/others:	Gambling:	Old/historic:
Huobi.com (2)	BTCCPool	CoinPayments.net	SatoshiDice.com (original)	AgoraMarket
Bittrex.com	SlushPool.com (old) (old2)	Xapo.com	LuckyB.it (chatbot)	BetcoinDice.tm
Luno.com	GHash.io	Cubits.com	BitZillions.com	SilkRoadMarketplace
Poloniex.com	AntPool.com (old) (old2)	Cryptonator.com (old)	999Dice.com	DeepBit.net
Kraken.com (old)	Eligius.st	BitPay.com (old) (old2) (old3)	CloudBet.com	SilkRoad2Market
BTC-e.com (output) (old)	BitMinter.com	BitoEX.com	CoinGaming.io	EvolutionMarket
BitZlato.com	EclipseMC.com (old) (old2) (old3)	HaoBTC.com	PrimeDice.com (old) (old2) (old3) (old4)	Instawallet.org
Bitstamp.net (old)	KnCMiner.com	Cryptopay.me (old)	SatoshiMines.com	UpDown.BT
LocalBitcoins.com (old)	Bitfury.org	AlphaBayMarket (old)	NitrogenSports.eu	AbraxasMarket
MercadoBitcoin.com.br	BW.com	NucleusMarket	SecondsTrade.com	MintPal.com
Cryptsy.com (old)	Kano.is (old)	BitcoinFog	PocketDice.io	SealsWithClubs.eu
Binance.com (old)	Telco214	BitcoinWallet.com	FortuneJack.com	PandoraOpenMarket
Bitcoin.de (old)		CoinJar.com	Rollin.io	MiddleEarthMarketplace
Cex.io		HolyTransaction.com	BitZino.com	BtcDice.com
BtcTrade.com		HelixMixer (old) (old2) (old3) (old4) (old5) (old6) (old7) (old8) (old9) (old10) (old11) (old12) (old13) (old14)	BitcoinVideoCasino.com (old) (old2)	McxNOW.com
CoinSpot.com.au			YABTCL.com	SheepMarketplace
YoBit.net			Betcoin.ag (old)	DiceOnCrack.com
OKCoin.com (2)				BlackBankMarket
				BTCGuild.com

Поисковые системы

Google

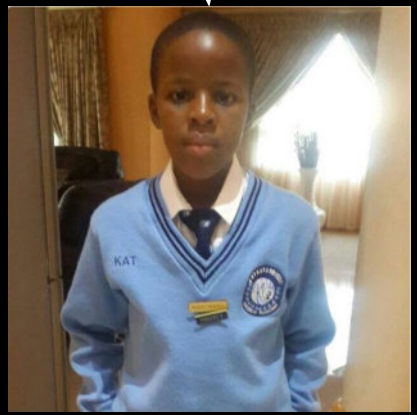
X (Twitter)

С большой осторожностью, но проверяйте тематические форумы scoring и abuse сервисы

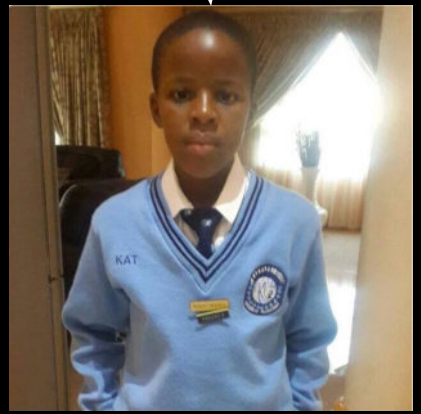
https://www.bitcoinwhoswho.com/

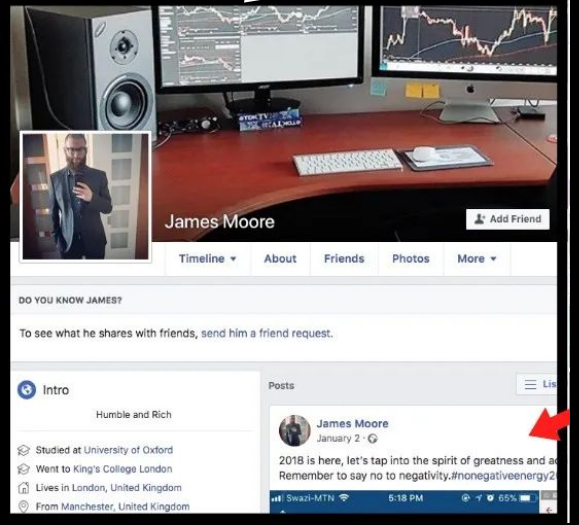
https://checkbitcoinaddress.com/

Если не определить биржу...



Если не определить биржу...





Форматы адресов

Legacy (P2PKH): начинается с цифры 1.
1N4Qbzg6LSXUXyXu2MDuGfzxwMA7do8AyL.

Script (P2SH): начинается с цифры 3.
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy.

SegWit (P2WPKH): начинается с комбинации “bc1q”.
bc1qfg9t7fwn0atn4yf9spca5502vk8dyhq8a9aqd8.

Taproot (P2TR): начинается с комбинации “bc1p”.
bc1peu5hzzyj8cnqm05le6ag7uwry0ysmtf3v4uuxv3v8hqhvsatca8ss2vuwx.

Форматы адресов

Благодаря разному формату адресов можно определять сдачу, кластеризировать адреса и продолжать расследование

Входы

Сдача

Сама передача

Визуализация

breadcrumbs

https://www.breadcrumbs.app/

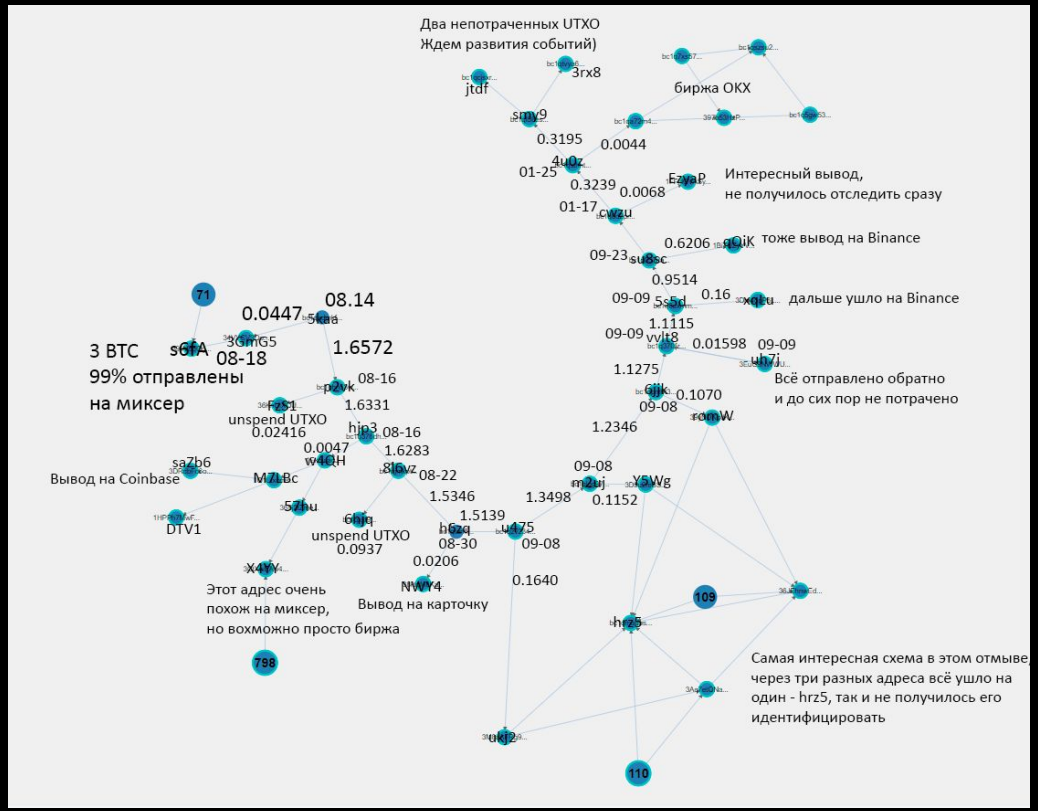
ETHTECTIVE

https://www.ethtective.com/

BLOCKSEC MetaSleuth

https://metasleuth.io/

https://blockpath.com/



CoinJoin

Метод объединения нескольких входов и выходов от разных людей

Используется в миксерах

From

1	17c1kEZtWLTpaKQNteX11mu8TqwigTV2Rj	8.37752724 BTC • $218,776
2	16UWqjtkDxZwMyDa7pTkRGtLEhqwS3s8PL	9.00000000 BTC • $235,032
3	1GfptzbHPHYo2ba3Zp8obXawjiJAnDcWCQ	10.06593219 BTC • $262,869

To

1	18zh7JtcxpV116HxbqiAdX6jKTrvSVQNqq	1.77648465 BTC • $46,392.42
2	1LQejeMyj78KF9J3M2Qk5j5irBKEw8AqLX	8.27651976 BTC • $216,139
3	1K8RhqF5TrBEViNqLCt75Ws1LWbYPxCAMs	8.27651976 BTC • $216,139
4	1No1mRTa3z6ZUtVtQpHiwzcHg8K9tEa2bo	0.72388352 BTC • $18,904.02
5	12yQwNryBEY4oXocdpsXGFH5EB1mFPoFbf	0.11342126 BTC • $2,961.97
6	1H7sF1B1EYj8QTdo9162o1QLLPDqGLLMDv	8.27651976 BTC • $216,139

Пропуск через миксер (Wasabi)

От			Кому		
1	bc1qc5545van8u7zrxlqn0×0jns7jy96435u5uq963	0.43046721 BTC • $11 689,20	1	bc1qrl0crc3exeaz4m3ehn9y6kzy3wqyzew45hj95w	0.65306673 BTC • $17 733,81
2	bc1qrdhtjlsqr8kq46z3jqk0kqnqwqzsas0sgd85×6	0.33554432 BTC • $9 111,60	2	bc1qptnmpj64t2znawa2z06thcx6293lrxvptxt7le	0.28697814 BTC • $7 792,80
3	bc1qycz9hjtswmgvz7emqtzl8l8marvj7802sf007h	0.28697814 BTC • $7 792,80	3	bc1qptlupndpwyfyhfw60uw7pe5nl4d7laumh03kud	0.28697814 BTC • $7 792,80
4	bc1qum5z8jf9gaz05gpf65fktsh7h9pcmznejv3pe2	0.28697814 BTC • $7 792,80	4	bc1q258qmjpe42l6d37trq6txsng2xqw7hrxa4p2dk	0.28697814 BTC • $7 792,80
5	bc1q5pfk0j23az5c6qq96cv3jjemvnjwnt4s43ujx0	0.20000000 BTC • $5 430,93	5	bc1q8tr8yk5pm3pltznkgjuahn9nv6snntp287ezce	0.14348907 BTC • $3 896,40
6	bc1qfrkxpzcex0c09p0tawyxqqna7up6et7m5rf6n3	0.16777216 BTC • $4 555,80	6	bc1q0nmk3r5004rz8rczdtm0d0a0469qxvrqc5zjgn	0.14348907 BTC • $3 896,40
7	bc1qt0q2wzpqaaw30nx0995p66673vszmqjnvjvjlc	0.14698574 BTC • $3 991,35	7	bc1qjrkzcy3hrcj32e7ypxuatcw9vh3smr4e74qmzy	0.14348907 BTC • $3 896,40
8	bc1q6l8ezd0axa5dvq3qmyjqsw67kv5ymwr0zzrcjt	0.10000000 BTC • $2 715,47	8	bc1qlqqy0wwk080t0343sf7h9sljc0kxqs34fc62y6	0.14348907 BTC • $3 896,40
9	bc1q4yt02dmhx05v9tftcd3j3×9u3hmz6amtvjqsty	0.10000000 BTC • $2 715,47	9	bc1qxdkpmtvcsh7mdn7022lac7vxm534j5lqzy6hzu	0.09565938 BTC • $2 597,60
10	bc1qtf33thd8ffltyqqzatswqn07rauw5alkafjwjp	0.10000000 BTC • $2 715,47	10	bc1q236c3skucxja80ds99u30sn5jsqj7swa40zta5	0.04782969 BTC • $1 298,80
Load 298 More			Load 286 More		

Пропуск через миксер (Wasabi)

От		Кому	
1	bc1qc5545van8u7zrxlqn0×0jns7jy96435u5uq963 0.43046721 BTC • $11 689,20	1	bc1qrl0crc3exeaz4m3ehn9y6kzy3wqyzew45hj95w 0.65306673 BTC • $17 733,81
2	bc1qrdhtjlsqr8kq46z3jqk0kqnqwqzsas0sgd85×6 0.33554432 BTC • $9 111,60	2	bc1qptnmpj64t2znawa2z06thcx6293lrxvptxt7le 0.28697814 BTC • $7 792,80
3	bc1qycz9hjtswmgvz7emqtzl8l8marvj7802sf007h 0.28697814 BTC • $7 792,80	3	bc1qptlupndpwyfyhfw60uw7pe5nl4d7laumh03kud 0.28697814 BTC • $7 792,80
4	bc1qum5z8jf9gaz05gpf65fktsh7h9pcmznejv3pe2 0.28697814 BTC • $7 792,80	4	bc1q258qmjpe42l6d37trq6txsng2xqw7hrxa4p2dk 0.28697814 BTC • $7 792,80
5	bc1q5pfk0j23az5c6qq96cv3jjemvnjwnt4s43ujx0 0.20000000 BTC • $5 430,93	5	bc1q8tr8yk5pm3pltznkgjuahn9nv6snntp287ezce 0.14348907 BTC • $3 896,40
6	bc1qfrkxpzcex0c09p0tawyxqqna7up6et7m5rf6n3 0.16777216 BTC • $4 555,80	6	bc1q0nmk3r5004rz8rczdtm0d0a0469qxvrqc5zjgn 0.14348907 BTC • $3 896,40
7	bc1qt0q2wzpqaaw30nx0995p66673vszmqjnvjvjlc 0.14698574 BTC • $3 991,35	7	bc1qjrkzcy3hrcj32e7ypxuatcw9vh3smr4e74qmzy 0.14348907 BTC • $3 896,40
8	bc1q6l8ezd0axa5dvq3qmyjqsw67kv5ymwr0zzrcjt 0.10000000 BTC • $2 715,47	8	bc1qlqqy0wwk080t0343sf7h9sljc0kxqs34fc62y6 0.14348907 BTC • $3 896,40
9	bc1q4yt02dmhx05v9tftcd3j3×9u3hmz6amtvjqsty 0.10000000 BTC • $2 715,47	9	bc1qxdkpmtvcsh7mdn7022lac7vxm534j5lqzy6hzu 0.09565938 BTC • $2 597,60
10	bc1qtf33thd8ffltyqqzatswqn07rauw5alkafjwjp 0.10000000 BTC • $2 715,47	10	bc1q236c3skucxja80ds99u30sn5jsqj7swa40zta5 0.04782969 BTC • $1 298,80
Load 298 More		Load 286 More	

Отслеживание сдачи в миксере

From

1 17c1kEZtWLTpaKQNteX11mu8TqwiqTV2Rj
8.37752724 BTC • $218,776

2 16UWqjtkDxZwMyDa7pTkRGtLEhqwS3s8PL
9.00000000 BTC • $235,032

3 1GfptzbHPHYo2ba3Zp8obXawjiJAnDcWCQ
10.06593219 BTC • $262,869

To

1 18zh7JtcxpV116HxbqiAdX6jKTrvSVQNqq
1.77648465 BTC • $46,392.42

2 1LQejeMyj78KF9J3M2Qk5j5irBKEw8AqLX
8.27651976 BTC • $216,139

3 1K8RhqF5TrBEViNqLCt75Ws1LWbYPxCAMs
8.27651976 BTC • $216,139

4 1No1mRTa3z6ZUtVtQpHiwzcHg8K9tEa2bo
0.72388352 BTC • $18,904.02

5 12yQwNryBEY4oXocdpsXGFH5EB1mFPoFbf
0.11342126 BTC • $2,961.97

6 1H7sF1B1EYj8QTdo9162o1QLLPDqGLLMDv
8.27651976 BTC • $216,139

Включаем математику

8.377 - 8.276 = 0.101 10.065 - 8.276 = 1.789 9.000 - 8.276 = 0.724

From

1 17c1kEZtWLTpaKQNteX11mu8TqwigTV2Rj
8.37752724 BTC • $218,776

2 16UWqjtkDxZwMyDa7pTkRGtLEhgwS3s8PL
9.00000000 BTC • $235,032

3 1GfptzbHPHYo2ba3Zp8obXawjiJAnDcWCQ
10.06593219 BTC • $262,869

To

1 18zh7JtcxpV116HxbqiAdX6jKTrvSVQNqq
1.77648465 BTC • $46,392.42

2 1LQejeMyj78KF9J3M2Qk5j5irBKEw8AqLX
8.27651976 BTC • $216,139

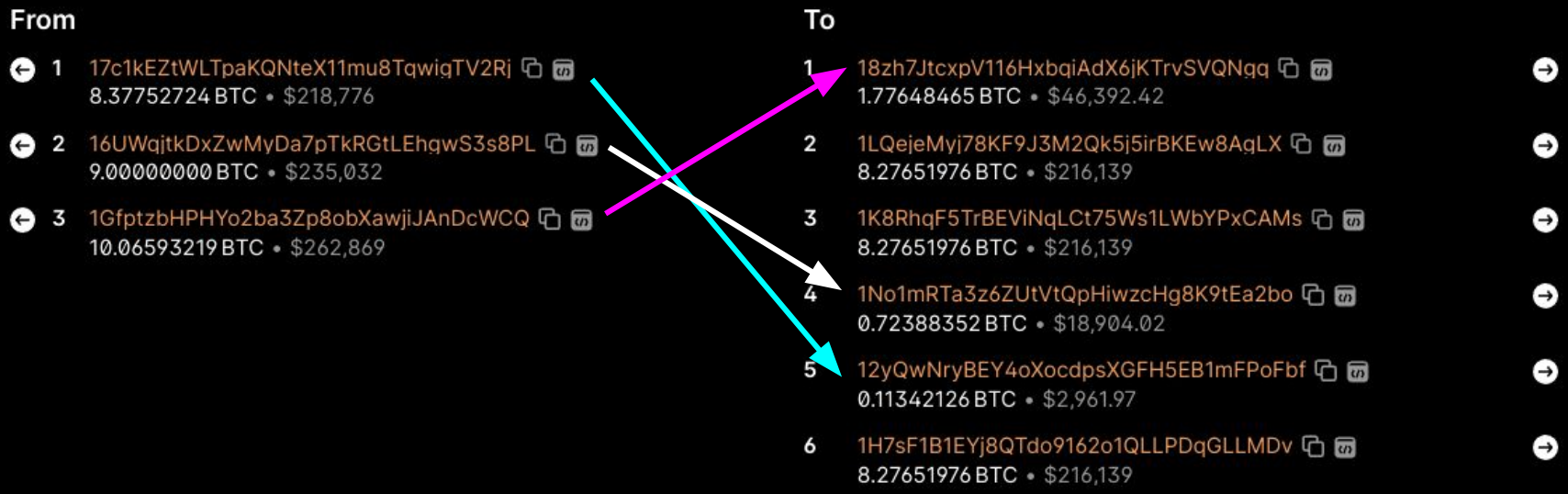
3 1K8RhqF5TrBEViNqLCt75Ws1LWbYPxCAMs
8.27651976 BTC • $216,139

4 1No1mRTa3z6ZUtVtQpHiwzcHg8K9tEa2bo
0.72388352 BTC • $18,904.02

5 12yQwNryBEY4oXocdpsXGFH5EB1mFPoFbf
0.11342126 BTC • $2,961.97

6 1H7sF1B1EYj8QTdo9162o1QLLPDqGLLMDv
8.27651976 BTC • $216,139

Связываем адреса в миксере



Сеть Ethereum

Такая же P2P сеть

На каждой полноценной ноде запущена EVM

Помимо базы транзакций хранится состояние сети

Транзакции между собой не связаны

Большое количество связанных сервисов, есть простор для расследований

Состояние Ethereum

Адрес	Баланс ETH	nonce	EVM байткод	Хранилище смарт-контракта
0xBffeCdCD5033	0.0014	10		
0x1f9090aaE28b	198	257	0x608060805260	key:value
0x388C818CA8B9	1.554	30		
0x02cEca3504ec	2.71	260		
0xDB65702A9b26	5922	1050	0x608060805260	key:value
0x3d3be777790b	3.2	23905		
0x68b3465833fb	120	19300	0x608060805260	key:value
0x5d39ABaa161e	0	1	0x608060805260	key:value

Etherscan

Основной инструмент для аналитики и анализа счета в Ethereum

Адреса большинства сервисов уже определены

В Ethereum не требуется UTXO, так что отслеживать средства нужно вручную

0xcf27c7e24d9e4a9a6...	Transfer	17632331	56 days 8 hrs ago	0x2345Ac...596729C1	IN	0x41aFd2...B5D7024d	0.03 ETH	0.0012204
0x197ece3c3c61979f3...	Transfer	17632316	56 days 8 hrs ago	0x068f19...5E883C79	IN	0x41aFd2...B5D7024d	0.01 ETH	0.00123138
0xb2d49d7fa823941b...	Transfer	17434133	84 days 5 hrs ago	0x41aFd2...B5D7024d	OUT	Rickroll: RICKROLL T...	0 ETH	0.00109562
0x61e9dad074279be2...	Approve	17364325	94 days 1 hr ago	0x41aFd2...B5D7024d	OUT	0x5Ad816...378AD0d2	0 ETH	0.00195997
0x8069e9976faa88fd7...	Swap Exact E...	17364324	94 days 1 hr ago	0x41aFd2...B5D7024d	OUT	Uniswap V2: Router 2	0.07 ETH	0.0045659

https://etherscan.io/

VOLGA CTF

ENS

Никнейм, владелец которого записан в блокчейн

Отображается через любой обозреватель

Дает большое пространство для исследования

0xd756fa374f6cfd05fe...	Commit	18017088	2 days 12 hrs ago	vca.eth	OUT	0x000000...c09DE67C	0 ETH	0.00190349
0x2284780fdea8e7275...	Batch Renew ...	18012356	3 days 4 hrs ago	vca.eth	OUT	0x5d81ce...4c7b2245	0.01770247 ETH	0.00178889
0xa1e7b6f8fa9931282...	Transfer	18012347	3 days 4 hrs ago	Luno 2	IN	vca.eth	0.09606442 ETH	0.00058994
0x7dff481f3ce45b944...	Register	17985037	6 days 23 hrs ago	vca.eth	OUT	0x000000...c09DE67C	0.00252635 ETH	0.0094666

Поиск по никнеймам

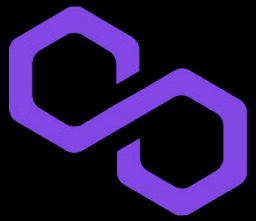
Maigret tool by soxoj

opensea.io

“nickname“ + search engines

Mailcat tool

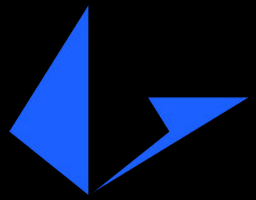
L2-блокчейны



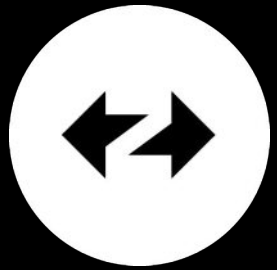
Polygon

Arbitrum

Optimism



LoopRing



zkSync

dYdX

Crosschain - мосты

Позволяют передавать средства из одного блокчейна в другой

Чаще всего реализованы через смарт-контракты

Активы замораживаются или сжигаются в одной сети и появляются в другой чаще всего в виде обернутого токена с приставкой **W**, например **WBTC**.

THORChain

MultiChain

Отслеживание

Прочтение документации

Анализ структуры транзакции

Отслеживание

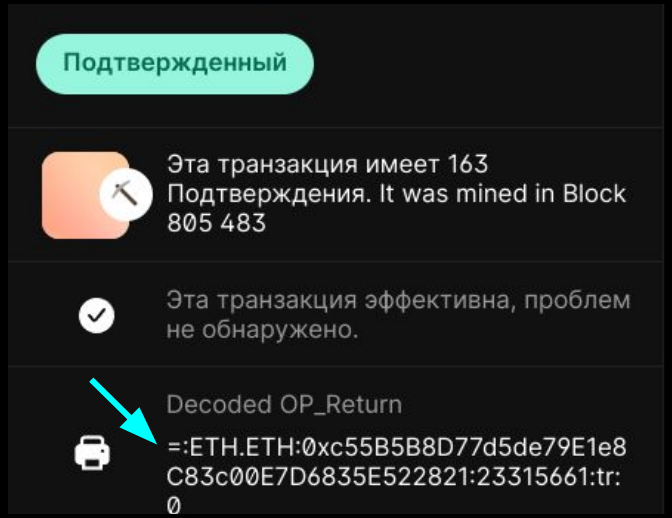
Прочтение документации

Анализ структуры транзакции

Отслеживание

Прочтение документации

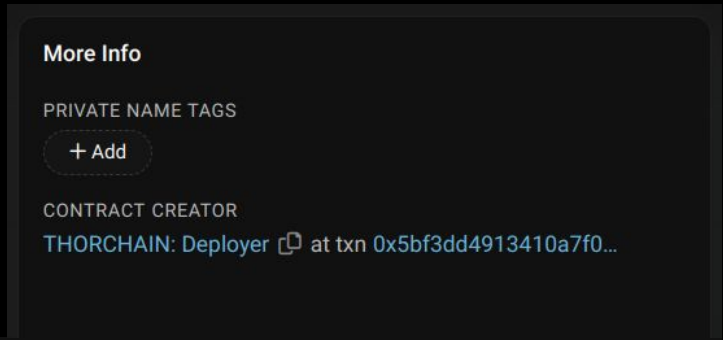
Анализ структуры транзакции

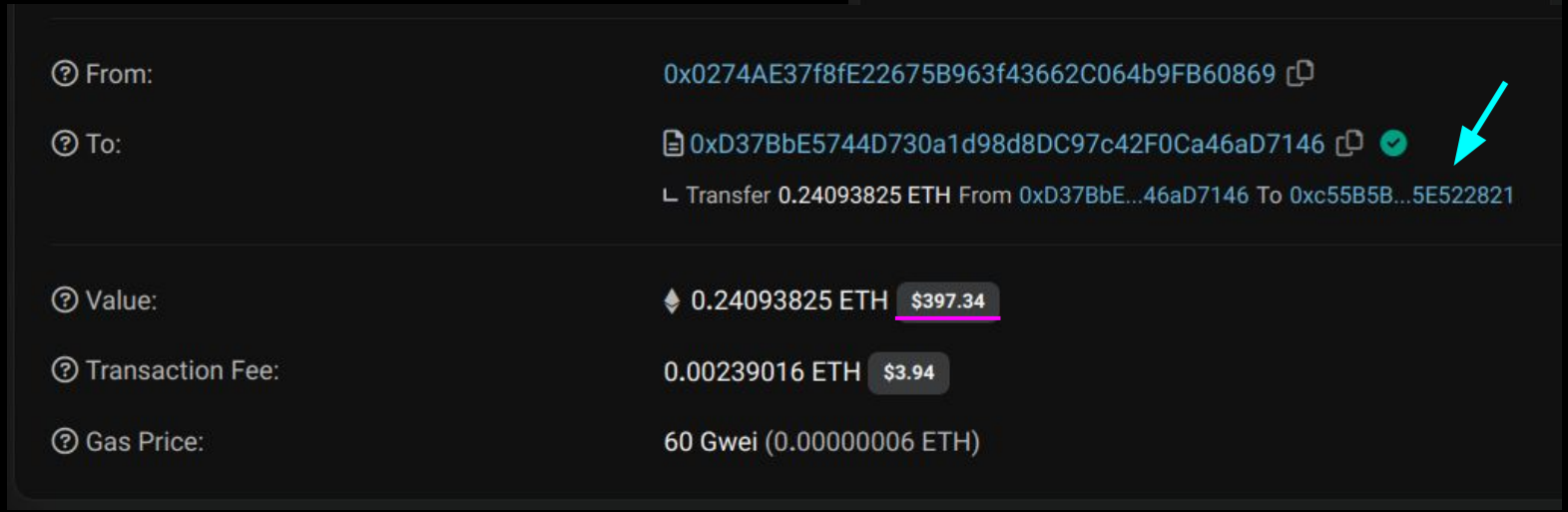


Отслеживание

Прочтение документации

Анализ структуры транзакции





Отслеживание

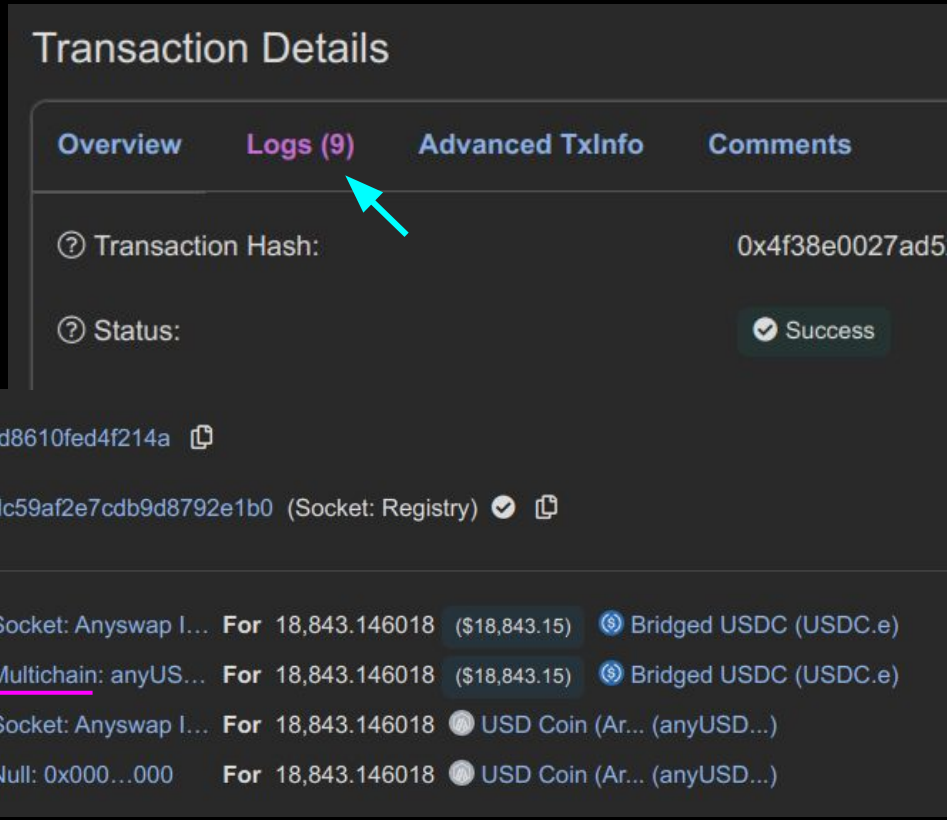
Транзакция в сети Arbitrum

Используется мост Multichain

Отслеживание

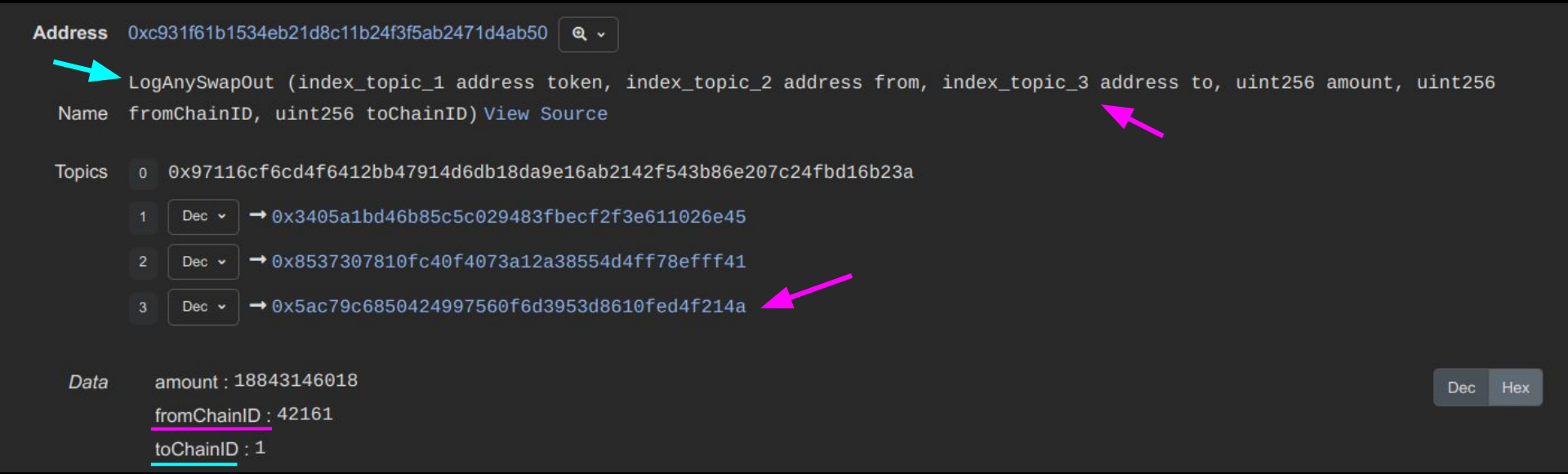
Транзакция в сети Arbitrum

Используется мост Multichain



Отслеживание

Смотрим логи (события) транзакции



Отслеживание

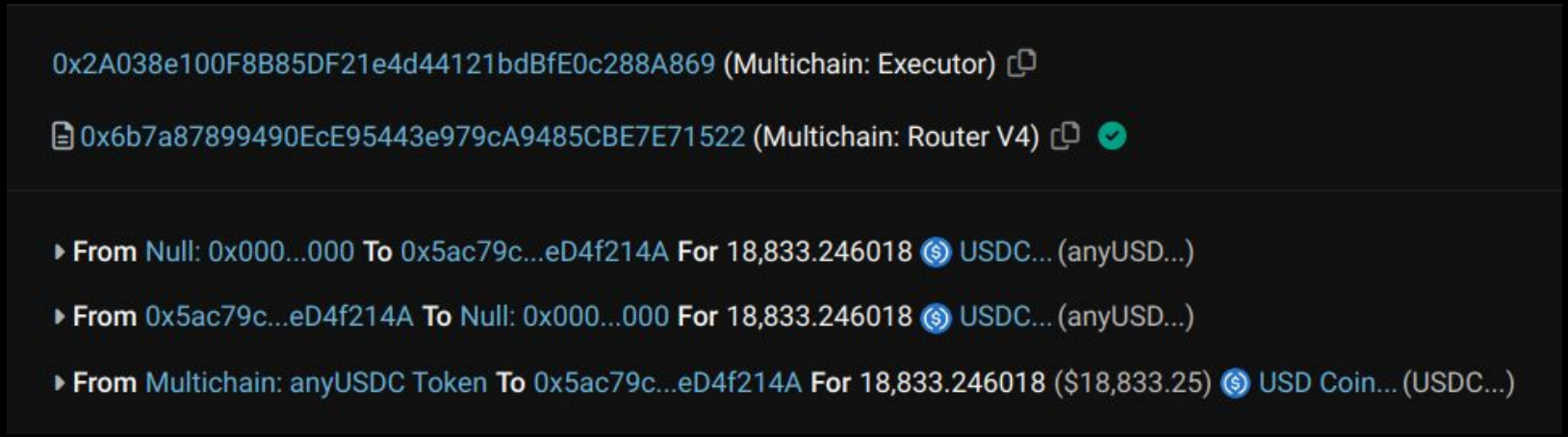
Читаем документацию Multichain

EVM Layer 2

Name	Chain ID	Currency	Explorer
Arbitrum	42161	ETH	https://arbiscan.io/
Avalanche C-Chain	43114	AVAX	https://snowtrace.io/
Ethereum	1	ETH	https://etherscan.io/

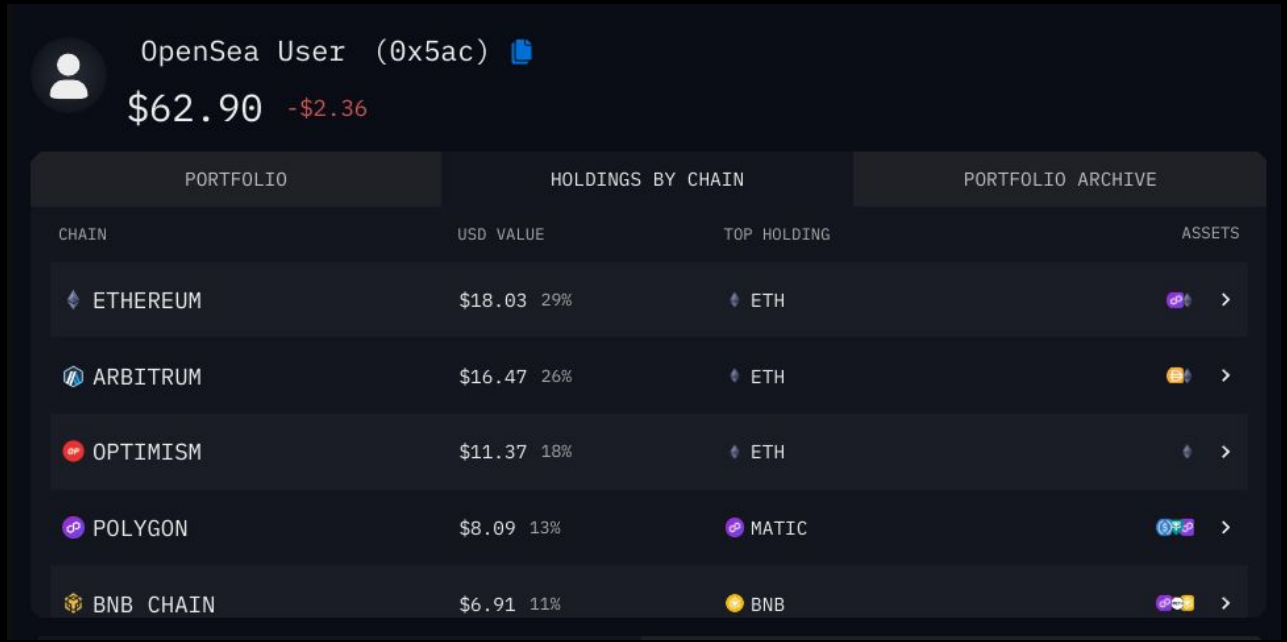
Отслеживание

Идем в Ethereum



Отслеживание

https://platform.arkhamintelligence.com/



Tornado Cash

https://tornado.cash/

Tornado Cash

zk-SNARK протокол

Tornado Cash

zk-SNARK протокол

несколько дней

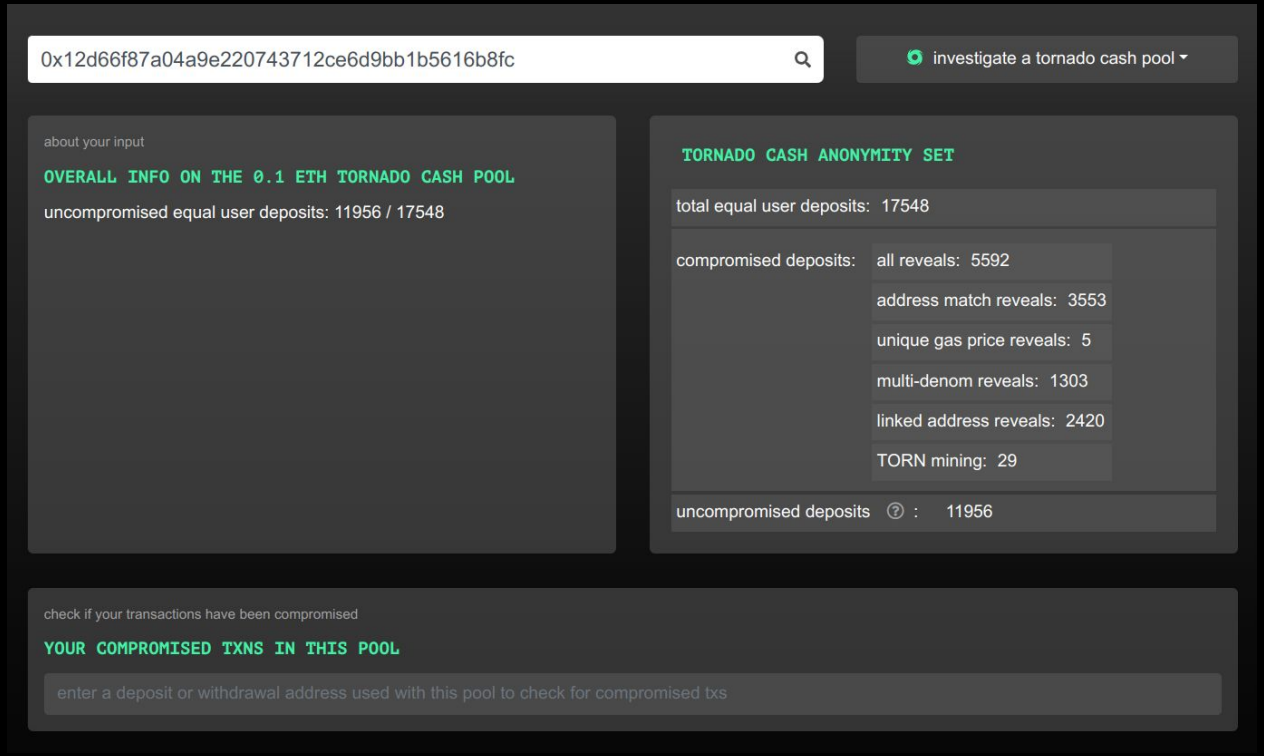
Tornado Cash

zk-SNARK протокол

несколько дней

Tornado Cash

https://tutela.xyz/



Анонимные валюты

Monero

CryptoNote

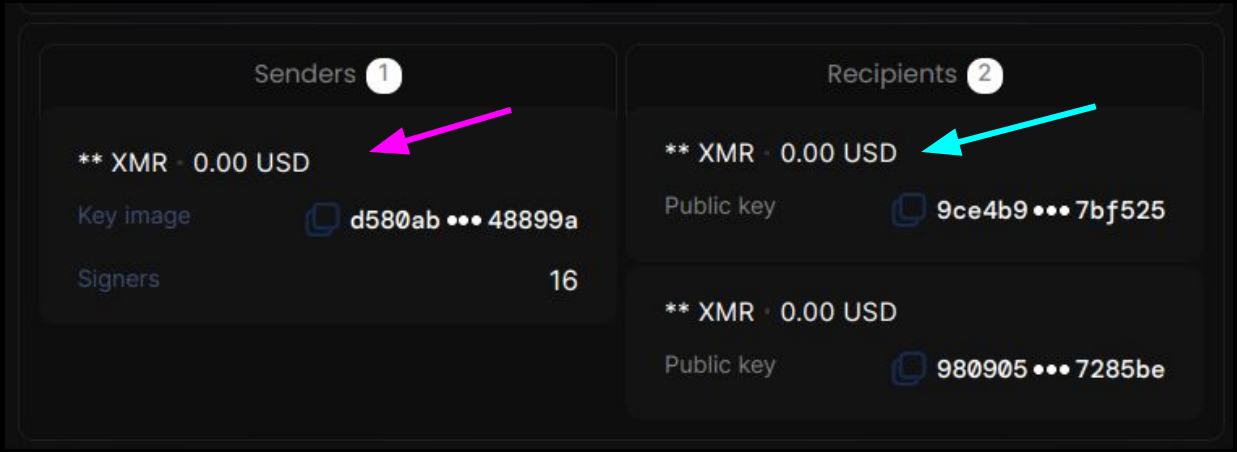
Zcash

zk-SNARK

Dash

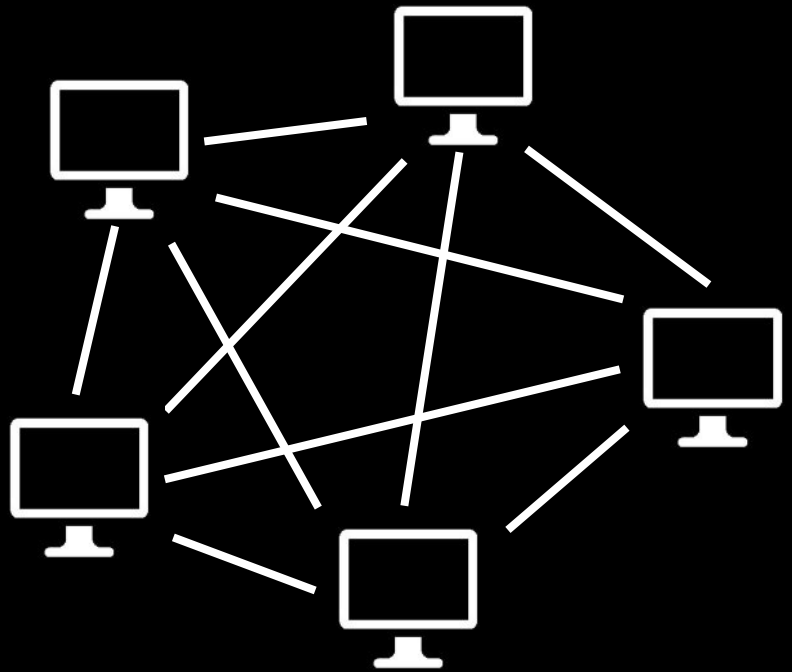
CoinJoin

Анонимные валюты

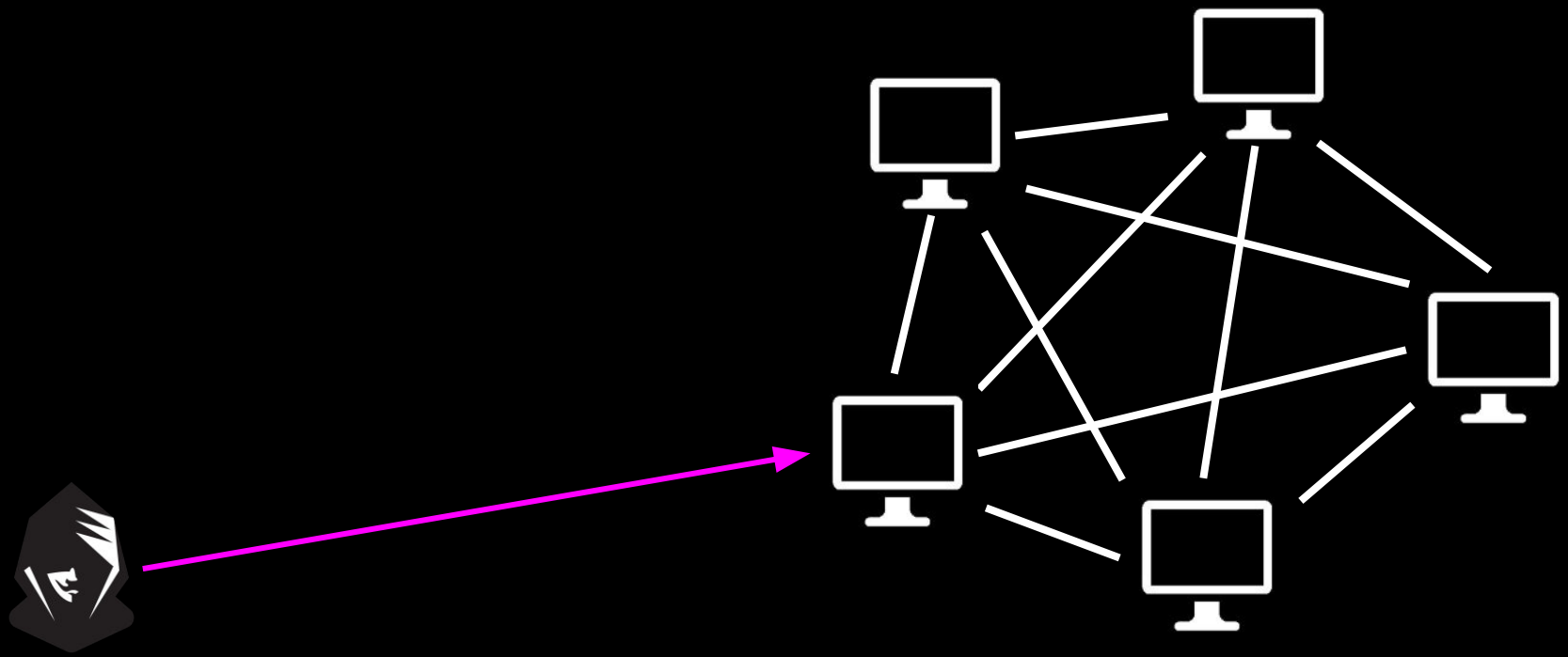


Ни входов, ни выходов, ни количества

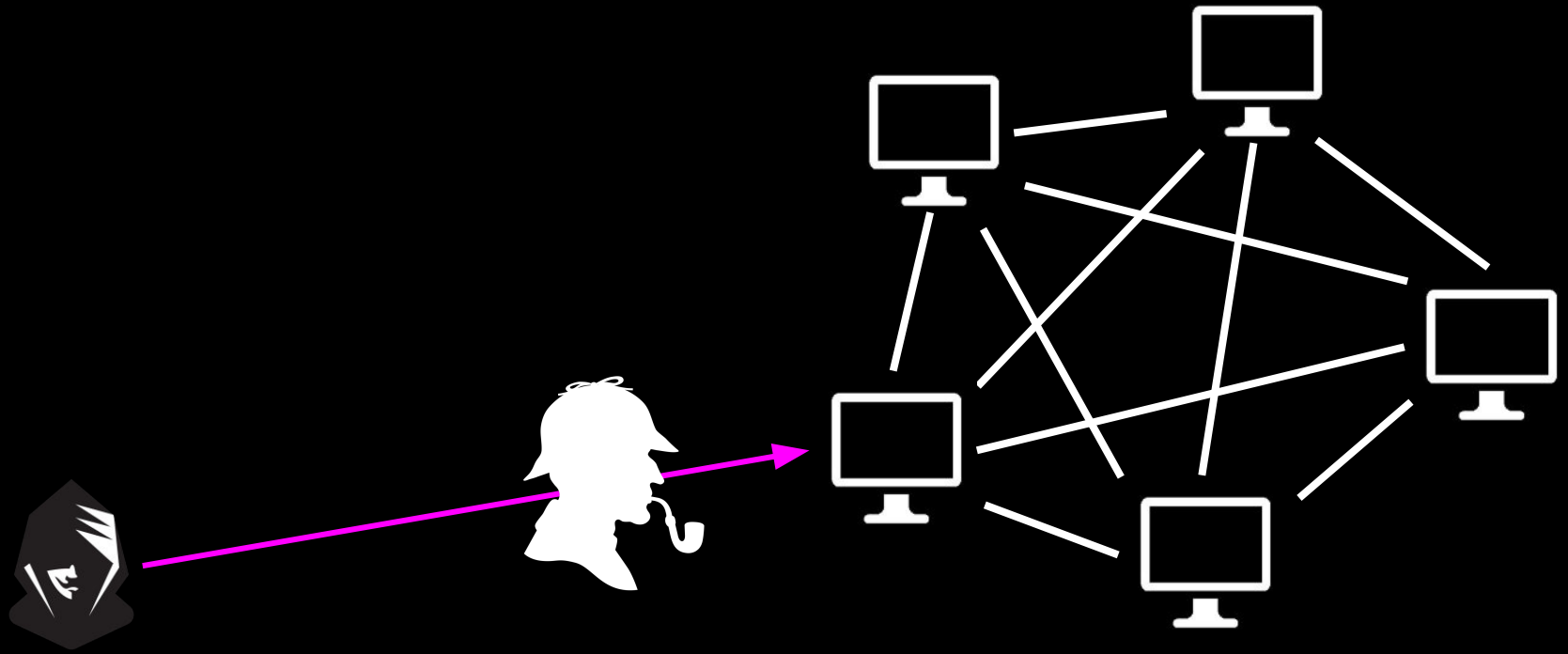
Перехват IP



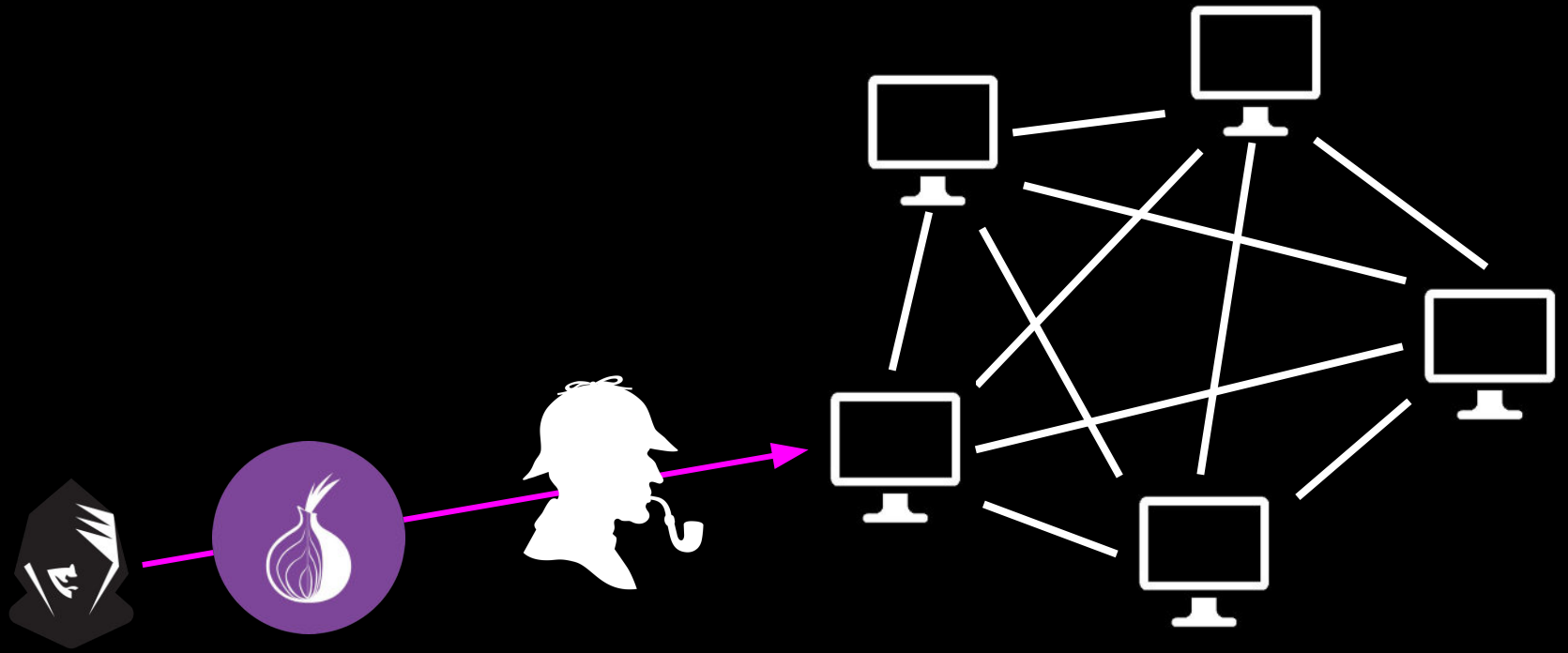
Перехват IP



Перехват IP



Перехват IP



VOLGA CTF

Сколько веревочке ни виться...

Monero

zk-SNARK

Tornado Cash

Zcash

Вся криптография
Bitcoin и Ethereum

Сколько веревочке ни виться...

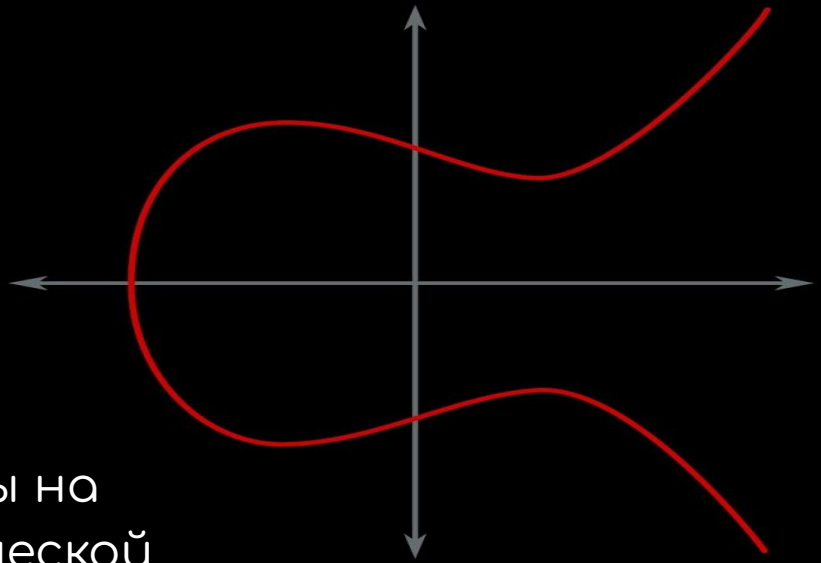
Monero

zk-SNARK

Tornado Cash

Zcash

Вся криптография
Bitcoin и Ethereum

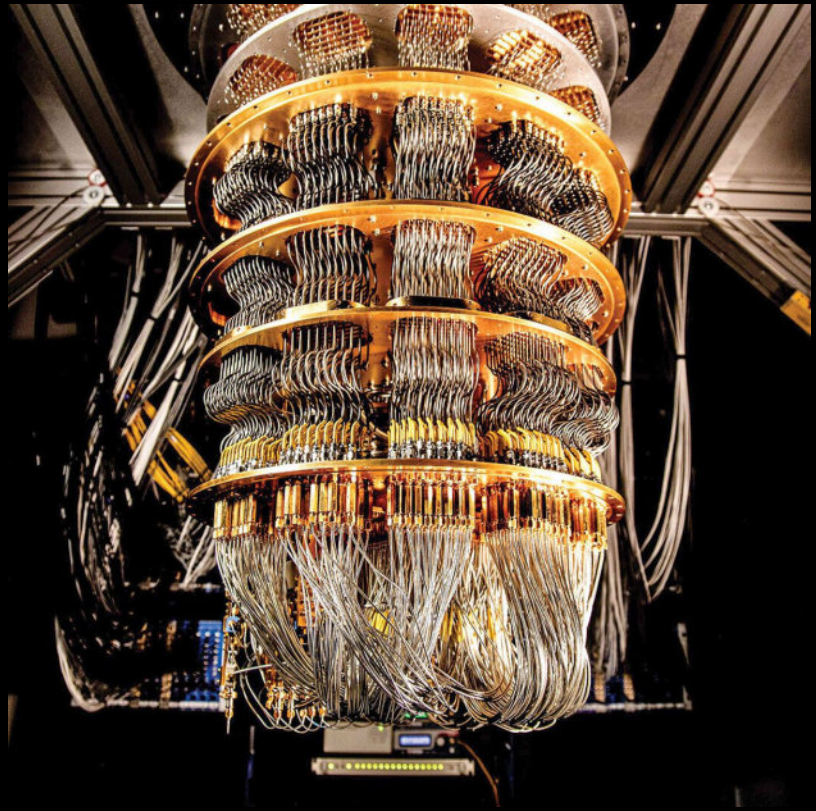


Основаны на
эллиптической
криптографии

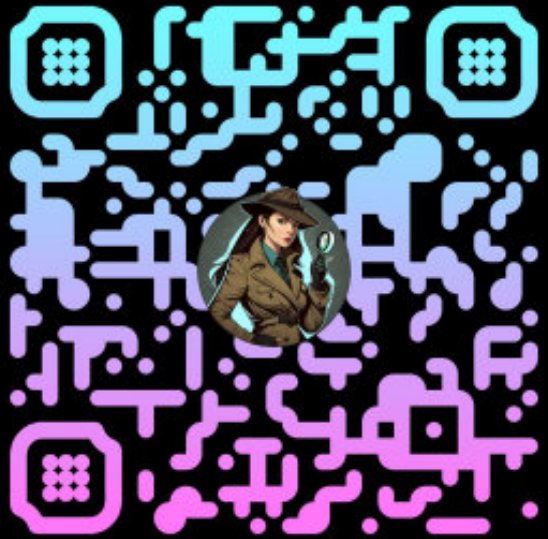
Сколько веревочке ни виться...

Эллиптическая криптография не устойчива к квантовым вычислениям

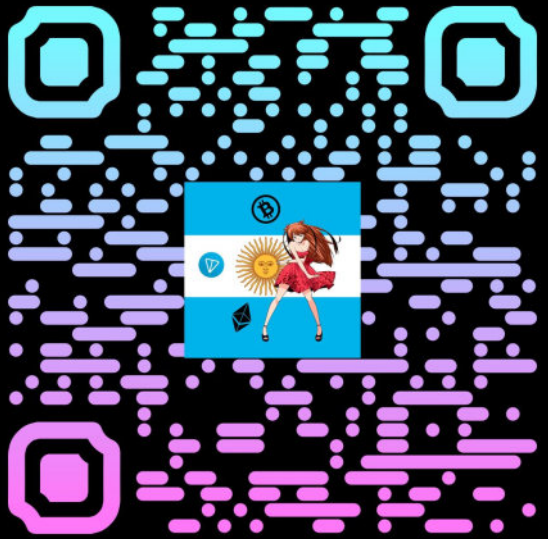
Возможно, через много лет нас ждут очень интересные расследования



Спасибо за внимание!



Наш форум расследований



Мой канал

Материалы

Доклады:
https://www.youtube.com/watch?v=kJf_lc4reEI
https://www.youtube.com/watch?v=MidqWdQuQDs
https://www.youtube.com/watch?v=JE_19ZrjWto
Полезные статьи:
https://officercia.mirror.xyz/BFzv17UwH6QG4q711NAljtSiP8eKR17daLjTdmAgbHw
https://officercia.mirror.xyz/5KSkJOTgMtvgC36v1GqZ987N-_Oj_zwvGatOk0A47Ws
https://zachxbt.mirror.xyz/8k0TmMxxieSiwUfUlqFFKGDVoOx2SnneYti31hoHwUk
Инструментарий:
https://github.com/OffcierCia/On-Chain-Investigations-Tools-List
https://start.me/p/ek4rxK/cryptocurrency
https://github.com/aaarghhh/awesome_osint_criypto_web3_stuff