

Как хакеры и мошенники отмывают 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

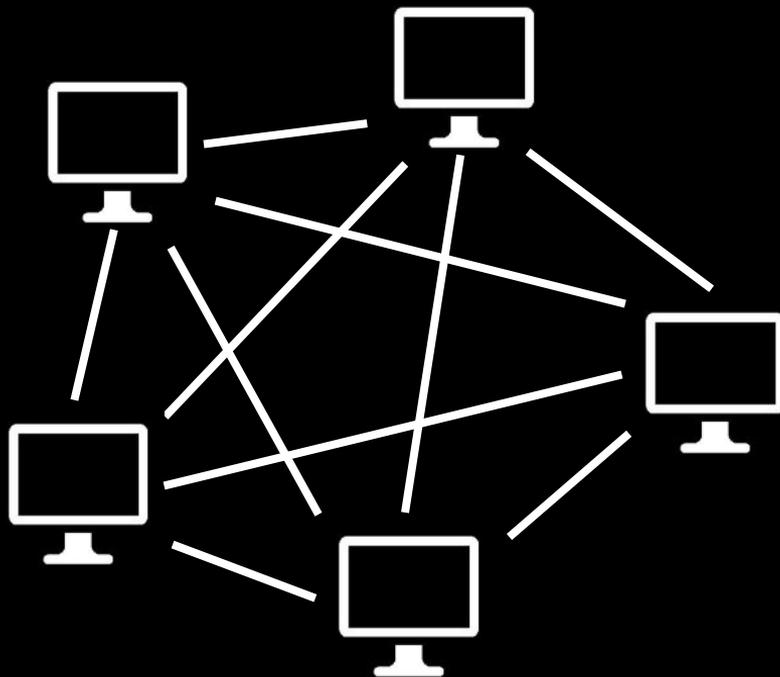


Что такое криптовалюта

P2P сеть

Хранится и обновляется
информация по
алгоритмам консенсуса

Информация
представляет собой
архив совершенных
транзакций

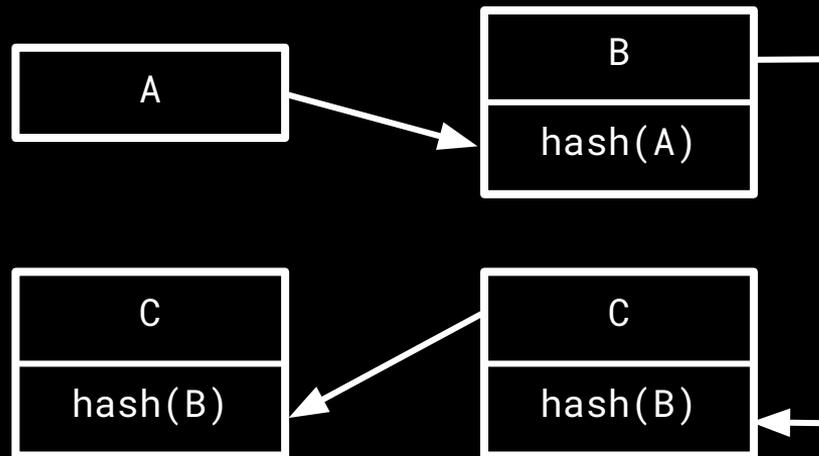


Что такое криптовалюта

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 появления 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": "bc1qm6avcyfhw8f6wg2ywg3dhyf9l56d56wh7pyjl0",
      "witness": [
        "304402202fb5890895355bd9e5bc7e94301ffcfb402b0fe477ab4527bd0de8ddcf17a39902206b2812f5659cc029618fcf3ae8201",
        "020890ebb385a67ee05acd050edcc98dc9dd7eb57f472f3e394236a9fb702f690"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1q9s7jd2g0lkky9hk8e808ndt8fzcxq2rzdgvdv",
      "pkscript": "00142c3d26a90ffdad8216f63e4ef3cdab3a45830143",
      "value": 92973,
      "spent": true,
      "spender": {
        "txid": "4838f8dab5237ab3cb7587f28e2ddeb7b1d8fdd4beb2c564f29d1b860ade89e2",
        "input": 36
      }
    },
    {
      "address": "bc1q6ya2ttm3nf4zz80rcmg3c3g8hvlqtqf6206shvw",
      "pkscript": "0014d13aa5af719a6a211de3c6d11c4507bb3eb0274a",
      "value": 10288359,
      "spent": true,
      "spender": {
        "txid": "cad7792cd526a797301a4ee34671126778f83380af8015388c9ea6c218c1bd70",
        "input": 0
      }
    }
  ]
}
```

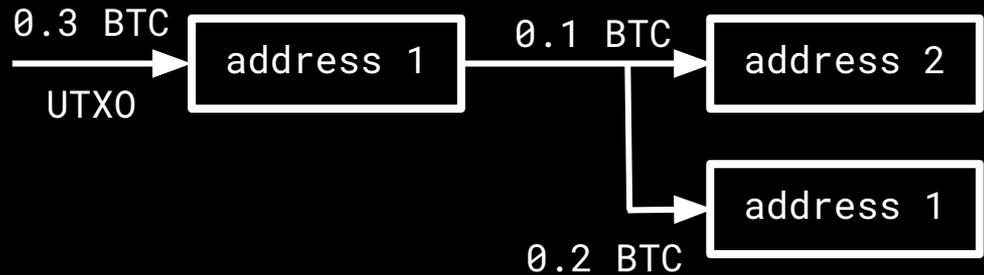
Bitcoin

UTXO - непотраченный
вход

При отправке транзакции
вход тратится полностью

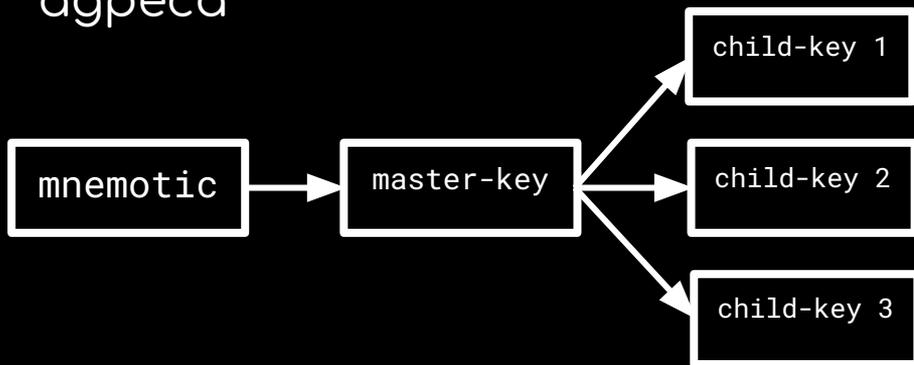
Если необходимо
отправить меньше чем
вход, то сдача
отправляется обратно
владельцу

Если необходимо
отправить больше, то
несколько входов
объединяются



HD-кошелек (BIP-32)

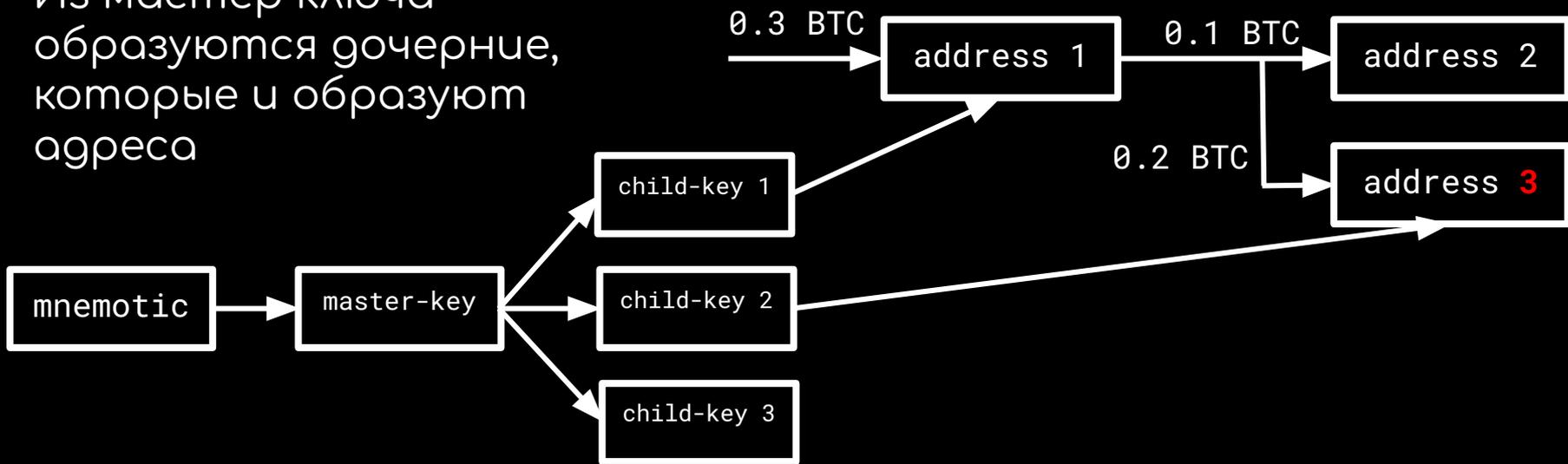
Из мнемотической фразы
образуется мастер ключ
Из мастер ключа
образуются дочерние,
которые и образуют
адреса



The screenshot shows a three-step process: 1. Create password, 2. Secure wallet, and 3. Confirm secret recovery phrase. The current step is 'Write down your Secret Recovery Phrase'. It instructs the user to write down a 12-word phrase and save it in a secure place. It provides tips: save in a password manager, store in a safe deposit box, and write down and store in multiple secret places. The 12 words are: 1. enough, 2. artwork, 3. stadium, 4. school, 5. bargain, 6. reject, 7. secret, 8. van, 9. foam, 10. turn, 11. scissors, 12. atom. There are buttons for 'Hide seed phrase' and 'Copy to clipboard', and a 'Next' button at the bottom.

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

From

1 1MXHVCztcy8ki5btP7eisXw9WyMnWGfrgd 5.05278778 BTC • \$132,138

To

1 3JuLSLzwr1VuHG6LS2RN3xyA2U8KrobaeK 5.05261412 BTC • \$132,133

Обозреватели для Bitcoin:

<https://blockchain.com/explorer>

<https://www.walletexplorer.com/>

<https://blockchair.com/>



OSINT? (нпросмо 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

1MXHVCztcy8ki5btP7eisXw9WyMnWGfrgd



⚠ REPORTED ADDRESS

This address has been reported and is under review by Scam Alert. Please take caution when sending any payments to this address. If you have any additional information on this address, please file a report.

[View Details](#)

Reported by [BitcoinAbuse](#)



Posted by u/linkbc 4 years ago

1

Be aware, a fake @peterbrandt on Twitter is doing scam #giveaway. At least 4 transaction so far



Peter Brandt

... · 1h

Currently an upward trend pattern with downtrends in vicinity.

I am really happy how it goes. That's what I thought to organize this:

[tinyurl .com/peterbrandt](https://tinyurl.com/peterbrandt)

To get there, just put the url together and have a look at that page.

6



96



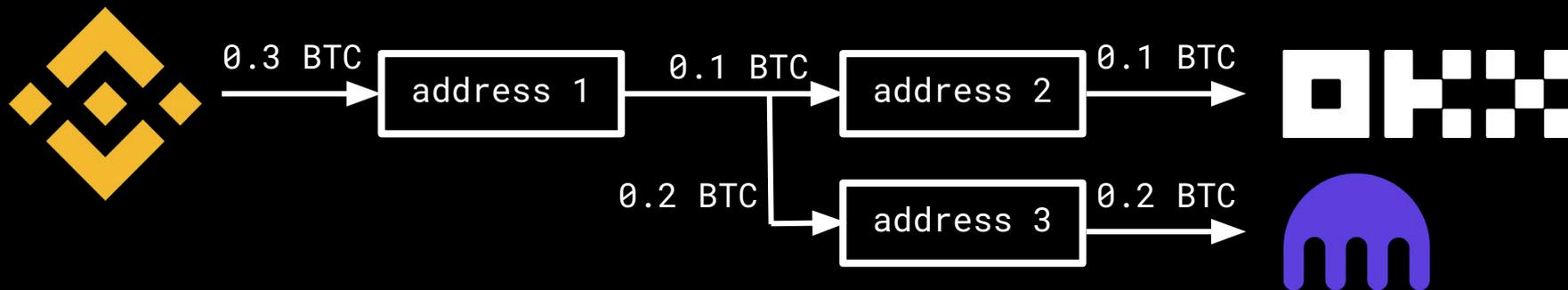
Ход расследования

Источник происхождения средств

Анализ движения средств на
адресе

Конечный получатель

OSINT и запросы в сервисы



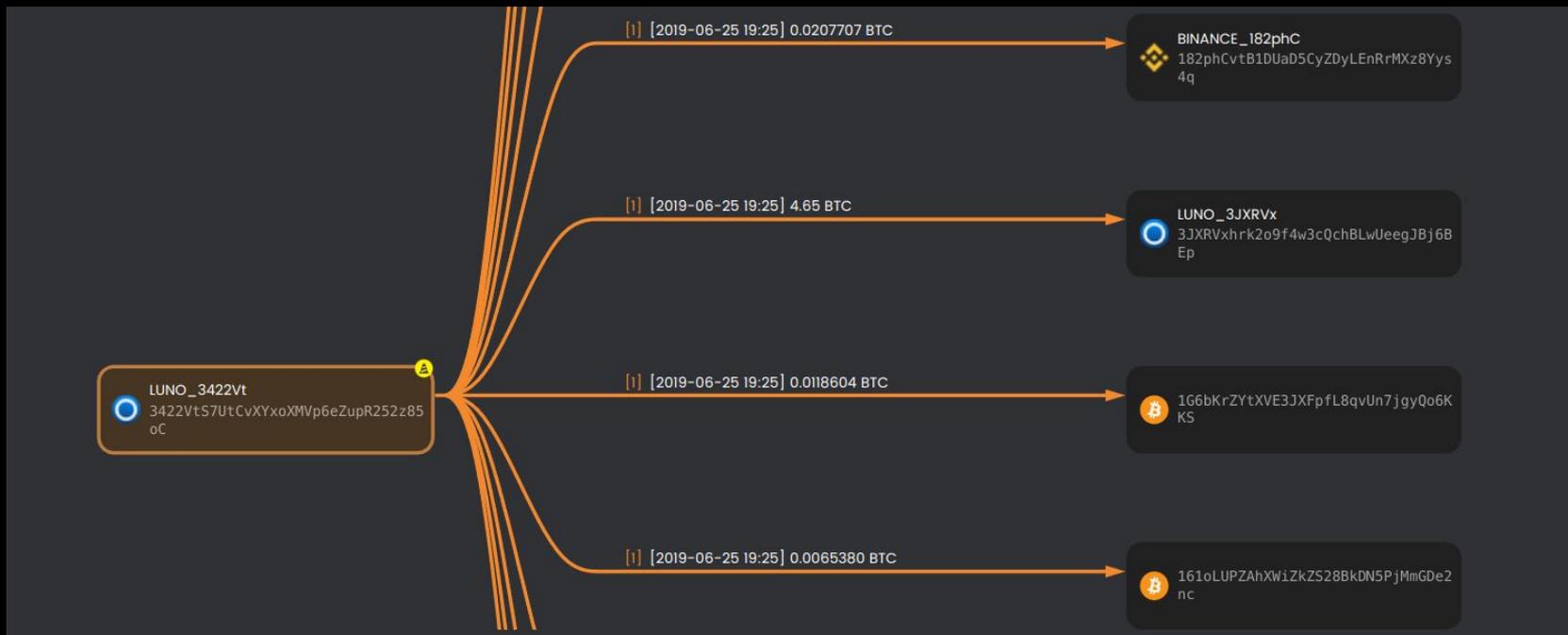
Определяем биржи



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

Поисковые системы



Google



X (Twitter)

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

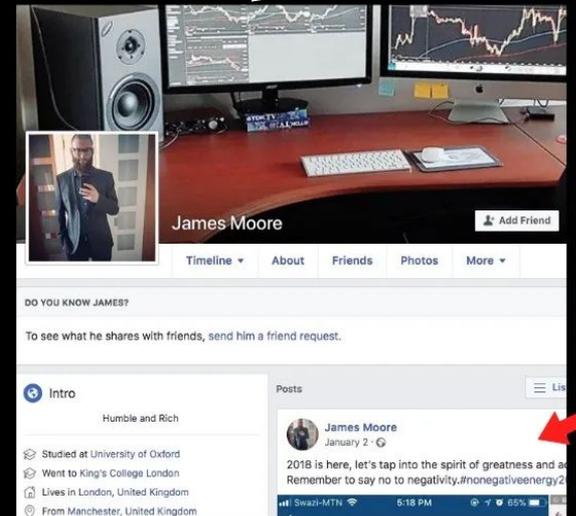
<https://www.bitcoinwhoswho.com/>

<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”.
bc1peu5hzzyj8cnqm051e6ag7uwry0ysmtf3v4uuxv3v8hqhvsatca8ss2vuwx.

Форматы адресов

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

Входы

От

- 1 bc1qs07775cp3y4203h2jpeewas8033r07tqzg0te8 2.12699119 BTC • \$57 757,11
- 2 bc1qs07775cp3y4203h2jpeewas8033r07tqzg0te8 0.57591781 BTC • \$15 638,69
- 3 bc1qs07775cp3y4203h2jpeewas8033r07tqzg0te8 1.25137500 BTC • \$33 980,30

Сдача

Кому

- 1 bc1qfql7qjnz5dzrhryp27d7lqekezwxexqd8yt06m 1.75424100 BTC • \$47 635,31
- 2 1DVMDFR2nuuaRkUC2rgEp2dEZpSiXCgyTK 2.200000000 BTC • \$59 739,61

Сама передача

Визуализация



<https://www.breadcrumbs.app/>



<https://www.ethtective.com/>

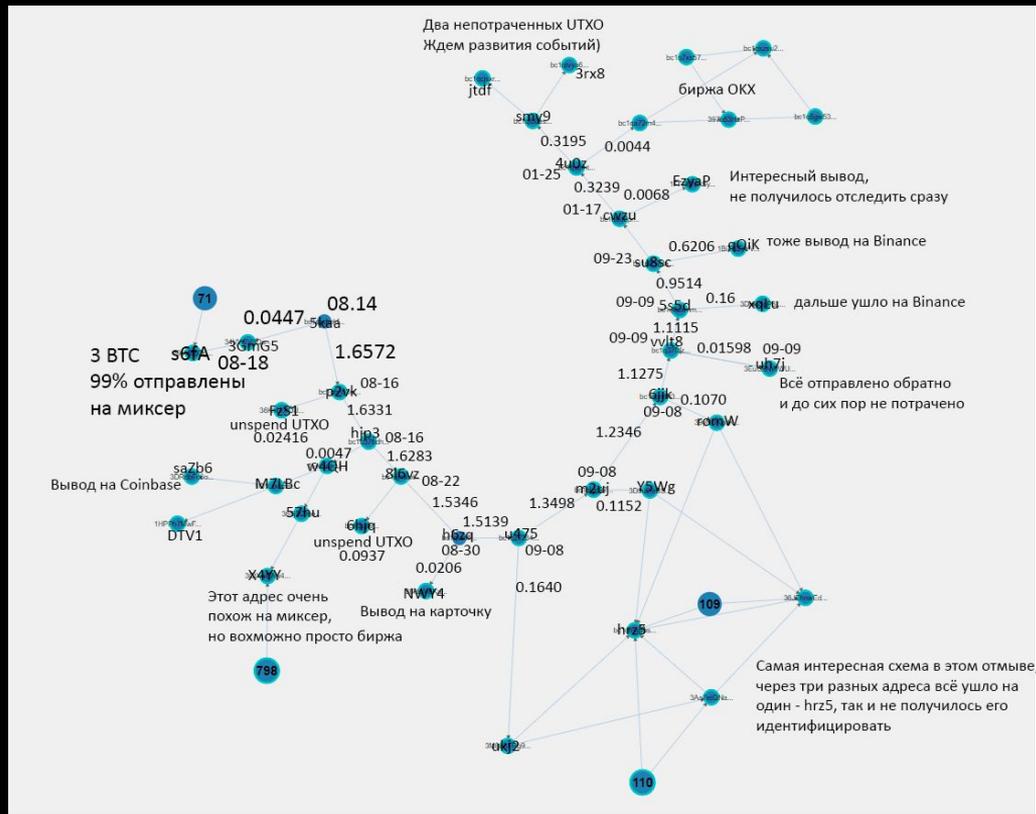


BLOCKSEC
MetaSleuth

<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 16UWajtkDxZwMyDa7pTkRGtLEhgwS3s8PL  
9.00000000 BTC • \$235,032
- 3 1GfptzbHPHYo2ba3Zp8obXawjiJAnDcWCQ  
10.06593219 BTC • \$262,869

To

- 1 18zh7JtcxpV116HxbqiAdX6jKTrvSVQNqg   
1.77648465 BTC • \$46,392.42
- 2 1LQejeMyj78KF9J3M2Qk5j5irBKEw8AgLX   
8.27651976 BTC • \$216,139
- 3 1K8RhgF5TrBEViNqLct75Ws1LWbYPxCAMs   
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

- 1 bc1qc5545van8u7zrqlqn0x0jns7jy96435u5uq963  
0.43046721 BTC • \$11 689,20
- 2 bc1qrdhtjlsqr8kq46z3jqk0kqngwqzsas0sqd85x6  
0.33554432 BTC • \$9 111,60
- 3 bc1qycz9hjtswmgvz7emqtzl8l8marvj7802sf007h  
0.28697814 BTC • \$7 792,80
- 4 bc1qum5z8jf9gaz05gpf65ftsh7h9pcmznejev3pe2  
0.28697814 BTC • \$7 792,80
- 5 bc1q5pfk0j23az5c6qq96cv3jjemvunjwnt4s43ujx0  
0.20000000 BTC • \$5 430,93
- 6 bc1qfrkxpcex0c09p0tawyxqna7up6et7m5rf6n3  
0.16777216 BTC • \$4 555,80
- 7 bc1qt0q2wzpqaaaw30nx0995p66673vszmqjnvjvlc  
0.14698574 BTC • \$3 991,35
- 8 bc1q6l8ezd0axa5dvq3qmyjgsw67kv5ymwr0zzrcjt  
0.10000000 BTC • \$2 715,47
- 9 bc1q4yt02dmhx05v9tftcd3j3x9u3hzmz6amtvgsty  
0.10000000 BTC • \$2 715,47
- 10 bc1qtf33thd8ffltygqzatswqn07rauw5alkafjwjp  
0.10000000 BTC • \$2 715,47

[Load 298 More](#)

Кому

- 1 bc1qrl0crc3exeaz4m3ehnn9y6kzy3wgqzew45hj95w   →
0.65306673 BTC • \$17 733,81
- 2 bc1qptnmpj64t2znawa2z06thcx6293lrxvptxt7le   →
0.28697814 BTC • \$7 792,80
- 3 bc1qptlupndpwyfyhfw60uw7pe5nl4d7laumh03kud   →
0.28697814 BTC • \$7 792,80
- 4 bc1q258qmjpe42l6d37trq6txsng2xqw7hrxa4p2dk   →
0.28697814 BTC • \$7 792,80
- 5 bc1q8tr8yk5pm3pltnkgyuahn9nv6snntp287ezce   →
0.14348907 BTC • \$3 896,40
- 6 bc1q0nmk3r5004rz8rczdtm0d0a0469qxvrqc5zjgn   →
0.14348907 BTC • \$3 896,40
- 7 bc1qjrkczy3hrcj32e7ypxuatacw9vh3smr4e74qmzy   →
0.14348907 BTC • \$3 896,40
- 8 bc1qlqqy0wwk080t0343sf7h9sljc0kxqs34fc62y6   →
0.14348907 BTC • \$3 896,40
- 9 bc1qxdkpmvvcsh7mdn7022lac7vxm534j5lqzy6hzu   →
0.09565938 BTC • \$2 597,60
- 10 bc1q236c3skucxja80ds99u30sn5jsqj7swa40zta5   →
0.04782969 BTC • \$1 298,80

[Load 286 More](#)

Пропуск через миксер (Wasabi)

От

- 1 bc1qc5545van8u7zrqlqn0x0jns7jy96435u5uq963  
0.43046721 BTC • \$11 689,20
- 2 bc1qrdhtjlsqr8kq46z3jqk0kqngwqzsas0sqd85x6  
0.33554432 BTC • \$9 111,60
- 3 bc1qycz9hjtswmgvz7emqztl8l8marvj7802sf007h  
0.28697814 BTC • \$7 792,80
- 4 bc1qum5z8jf9gaz05gpf65ftsh7h9pcmznejev3pe2  
0.28697814 BTC • \$7 792,80
- 5 bc1q5pfk0j23az5c6qq96cv3jjemvunjwnt4s43ujx0  
0.20000000 BTC • \$5 430,93
- 6 bc1qfrkxpcex0c09p0tawyxqqa7up6et7m5rf6n3  
0.16777216 BTC • \$4 555,80
- 7 bc1qt0q2wzpqaaaw30nx0995p66673vszmqjnvjvlc  
0.14698574 BTC • \$3 991,35
- 8 bc1q6l8ezd0axa5dvq3qmyjgsw67kv5ymwr0zzrcjt  
0.10000000 BTC • \$2 715,47
- 9 bc1q4yt02dmhx05v9tftcd3j3x9u3hzmz6amtvgsty  
0.10000000 BTC • \$2 715,47
- 10 bc1qtf33thd8fflygqzatswqn07rauw5alkafjwjp  
0.10000000 BTC • \$2 715,47

Load 298 More

Кому

- 1 bc1qrl0crc3exeaz4m3ehn9y6kzy3wgqzew45hj95w  
0.65306673 BTC • \$17 733,81
- 2 bc1qpntmpj64t2znawa2z06thcx6293lrxvptxt7le  
0.28697814 BTC • \$7 792,80
- 3 bc1qptlupndpwyfyhfw60uw7pe5nl4d7laumh03kud  
0.28697814 BTC • \$7 792,80
- 4 bc1q258qmjpe42l6d37trq6txsng2xqw7hrxa4p2dk  
0.28697814 BTC • \$7 792,80
- 5 bc1q8tr8yk5pm3pltnkgjuahn9nv6snntp287ezce  
0.14348907 BTC • \$3 896,40
- 6 bc1q0nmk3r5004rz8rczdtm0d0a0469qvxrqc5zjgn  
0.14348907 BTC • \$3 896,40
- 7 bc1qjrkczy3hrcj32e7ypxuawc9vh3smr4e74qmzy  
0.14348907 BTC • \$3 896,40
- 8 bc1qlqqy0wwk080t0343sf7h9sljc0kxqs34fc62y6  
0.14348907 BTC • \$3 896,40
- 9 bc1qxdkpmvvcsh7mdn7022lac7vxm534j5lqzy6hzu  
0.09565938 BTC • \$2 597,60
- 10 bc1q236c3skucxja80ds99u30sn5jsqj7swa40zta5  
0.04782969 BTC • \$1 298,80

Load 286 More

Отслеживание сдачи в миксере

From

- 1 17c1kEZtWLTpaKQNteX11mu8TqwigTV2Rj  
8.37752724 BTC • \$218,776
- 2 16UWqjtkDxZwMyDa7pTKRGtLEhgwS3s8PL  
9.000000000 BTC • \$235,032
- 3 1GfptzbHPHYo2ba3Zp8obXawjiJAnDcWCQ  
10.06593219 BTC • \$262,869

To

- 1 18zh7JtcxpV116HxbqiAdX6jKTrvSVQNqg   
1.77648465 BTC • \$46,392.42
- 2 1LQejeMyj78KF9J3M2Qk5j5irBKEw8AgLX   
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

$$8.377 - 8.276 = 0.101$$

$$10.065 - 8.276 = 1.789$$

$$9.000 - 8.276 = 0.724$$

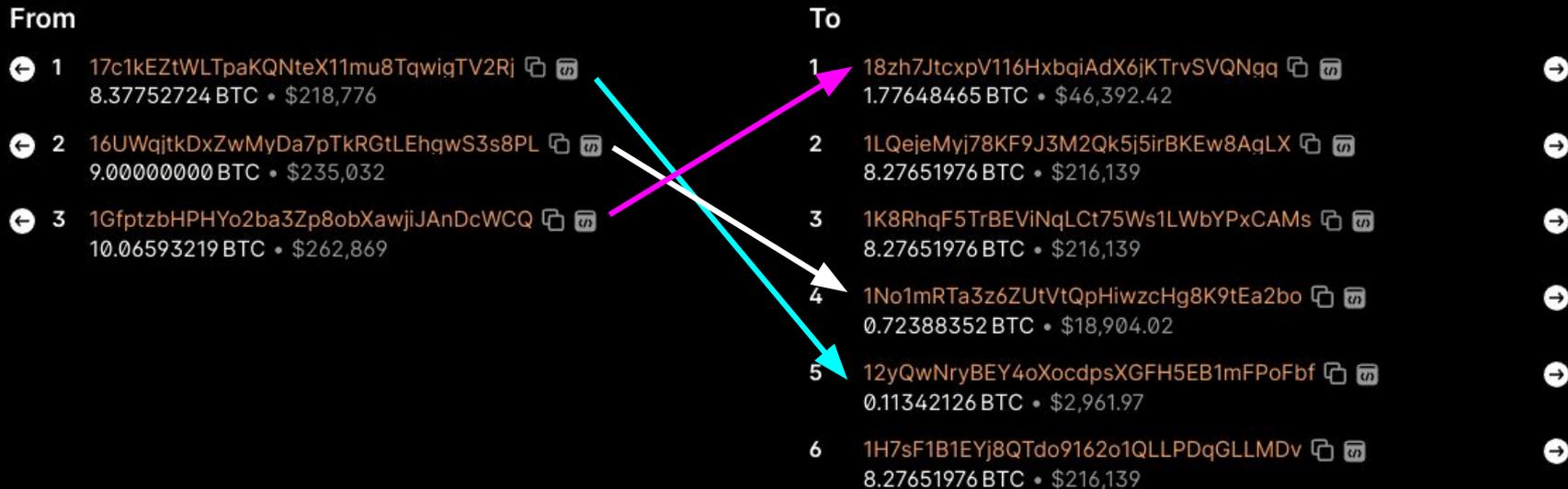
From

- 1 17c1kEZtWLTpaKQNteX11mu8TqwigTV2Rj  
8.37752724 BTC • \$218,776
- 2 16UWqjtkDxZwMyDa7pTkRGtLEhgwS3s8PL  
9.00000000 BTC • \$235,032
- 3 1GfptzbHPHYo2ba3Zp8obXawjiJAnDcWCQ  
10.06593219 BTC • \$262,869

To

- 1 18zh7JtcxpV116HxbqiAdX6jKTrvSVQNga  
1.77648465 BTC • \$46,392.42
- 2 1LQejeMyj78KF9J3M2Qk5j5irBKEw8AgLX  
8.27651976 BTC • \$216,139
- 3 1K8RhgF5TrBEViNqLct75Ws1LWbYPxCAMs  
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 УТХО, так что отслеживать средства
нужно вручную

👁	0xcfc27c7e24d9e4a9a6...	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/>

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

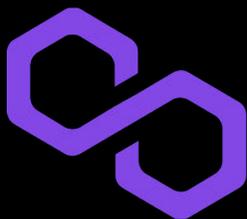


“nickname” + search engines



Mailcat tool

L2-блокчейны



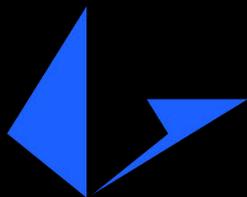
Polygon



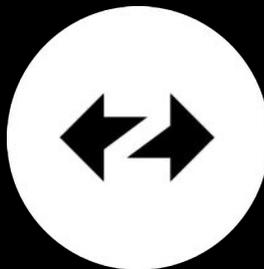
Arbitrum



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

Обзор

JSON

От

← 1 bc1qph5msald49kztjwg025mu2qy98fzr463kxd44q  
0.01621731 BTC • \$421,65

Кому

1 bc1q0yzpjhmq3m7g5qn0xftlvzzqxdt9p457hu4nz6   →
0.01540644 BTC • \$400,56

2 bc1qph5msald49kztjwg025mu2qy98fzr463kxd44q  
0.00078651 BTC • \$20,45

3 Неизвестно
0.00000000 BTC • \$0.00

Отслеживание

Прочтение документации

Анализ структуры транзакции

Подтвержденный

Эта транзакция имеет 163 Подтверждения. It was mined in Block 805 483

Эта транзакция эффективна, проблем не обнаружено.

Decoded OP_Return
=:ETH.ETH:0xc55B5B8D77d5de79E1e8C83c00E7D6835E522821:23315661:tr:0

Обзор

JSON

От

1 bc1qph5msald49kztjwg025mu2qy98fzr463kxd44q 0.01621731 BTC • \$421,65

Кому

- 1 bc1q0yypjhmq3m7g5qn0xftlvzzqxdt9p457hu4nz6 0.01540644 BTC • \$400,56
- 2 bc1qph5msald49kztjwg025mu2qy98fzr463kxd44q 0.00078651 BTC • \$20,45
- 3 Неизвестно 0.00000000 BTC • \$0.00

Отслеживание

Прочтение документации

Анализ структуры транзакции

More Info

PRIVATE NAME TAGS

+ Add

CONTRACT CREATOR

THORCHAIN: Deployer  at txn 0x5bf3dd4913410a7f0...

From:

0x0274AE37f8fE22675B963f43662C064b9FB60869 

To:

 0xD37BbE5744D730a1d98d8DC97c42F0Ca46aD7146  

L Transfer 0.24093825 ETH From 0xD37BbE...46aD7146 To 0xc55B5B...5E522821

Value:

0.24093825 ETH \$397.34

Transaction Fee:

0.00239016 ETH \$3.94

Gas Price:

60 Gwei (0.00000006 ETH)



Отслеживание

Транзакция в сети Arbitrum

Используется мост Multichain

From: 0x5ac79c6850424997560f6d3953d8610fed4f214a

Interacted With (To): Contract 0xc30141b657f4216252dc59af2e7cdb9d8792e1b0 (Socket: Registry)

ERC-20 Tokens Transferred: 4

- From 0x5ac79c6850424... To Socket: Anyswap I... For 18,843.146018 (\$18,843.15) Bridged USDC (USDC.e)
- From Socket: Anyswap I... To Multichain: anyUS... For 18,843.146018 (\$18,843.15) Bridged USDC (USDC.e)
- From Null: 0x000...000 To Socket: Anyswap I... For 18,843.146018 USD Coin (Ar... (anyUSD...))
- From Socket: Anyswap I... To Null: 0x000...000 For 18,843.146018 USD Coin (Ar... (anyUSD...))

Отслеживание

Транзакция в сети Arbitrum

Используется мост Multichain

Transaction Details

Overview

Logs (9)

Advanced TxInfo

Comments

Transaction Hash:

0x4f38e0027ad5

Status:

Success

From: 0x5ac79c6850424997560f6d3953d8610fed4f214a

Interacted With (To): Contract 0xc30141b657f4216252dc59af2e7cdb9d8792e1b0 (Socket: Registry)

ERC-20 Tokens Transferred: 4

- From 0x5ac79c6850424... To Socket: Anyswap I... For 18,843.146018 (\$18,843.15) Bridged USDC (USDC.e)
- From Socket: Anyswap I... To Multichain: anyUS... For 18,843.146018 (\$18,843.15) Bridged USDC (USDC.e)
- From Null: 0x000...000 To Socket: Anyswap I... For 18,843.146018 USD Coin (Ar... (anyUSD...))
- From Socket: Anyswap I... To Null: 0x000...000 For 18,843.146018 USD Coin (Ar... (anyUSD...))

Отслеживание

Смотрим логи (события) транзакции

Address `0xc931f61b1534eb21d8c11b24f3f5ab2471d4ab50`



`LogAnySwapOut (index_topic_1 address token, index_topic_2 address from, index_topic_3 address to, uint256 amount, uint256
Name fromChainID, uint256 toChainID) View Source`

Topics 0 `0x97116cf6cd4f6412bb47914d6db18da9e16ab2142f543b86e207c24fbd16b23a`

1 `Dec` → `0x3405a1bd46b85c5c029483fbecf2f3e611026e45`

2 `Dec` → `0x8537307810fc40f4073a12a38554d4fff78efff41`

3 `Dec` → `0x5ac79c6850424997560f6d3953d8610fed4f214a`

Data amount : 18843146018

fromChainID : 42161

toChainID : 1

Dec Hex

Отслеживание

Читаем документацию Multichain

EVM Layer 2			
Name	Chain ID	Currency	Explorer
Arbitrum	<u>42161</u>	ETH	https://arbiscan.io/
Name	Chain ID	Currency	Explorer
Avalanche C-Chain	43114	AVAX	https://snowtrace.io/
Ethereum	<u>1</u>	ETH	https://etherscan.io/

Отслеживание

Идем в Ethereum

0x2A038e100F8B85DF21e4d44121bdBfE0c288A869 (Multichain: Executor) 

 0x6b7a87899490EcE95443e979cA9485CBE7E71522 (Multichain: Router V4)  

▶ **From Null: 0x000...000 To 0x5ac79c...eD4f214A For 18,833.246018**  USDC... (anyUSD...)

▶ **From 0x5ac79c...eD4f214A To Null: 0x000...000 For 18,833.246018**  USDC... (anyUSD...)

▶ **From Multichain: anyUSDC Token To 0x5ac79c...eD4f214A For 18,833.246018 (\$18,833.25)**  USD Coin... (USDC...)

Отслеживание



<https://platform.arkhamintelligence.com/>

OpenSea User (0x5ac)

\$62.90 -\$2.36

PORTFOLIO		HOLDINGS BY CHAIN		PORTFOLIO ARCHIVE	
CHAIN	USD VALUE	TOP HOLDING	ASSETS		
ETHEREUM	\$18.03 29%	ETH			
ARBITRUM	\$16.47 26%	ETH			
OPTIMISM	\$11.37 18%	ETH			
POLYGON	\$8.09 13%	MATIC			
BNB CHAIN	\$6.91 11%	BNB			

Tornado Cash

<https://tornado.cash/>



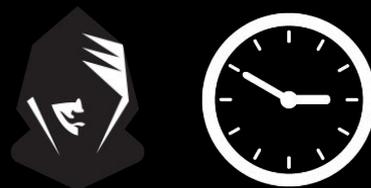
Tornado Cash

zk-SNARK протокол



Tornado Cash

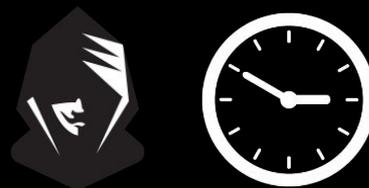
zk-SNARK протокол



несколько дней

Tornado Cash

zk-SNARK протокол



несколько дней



Tornado Cash

Как хакеры и мошенники
отмывают криптовалюту
VolgaCTF 2023
angkasawan



<https://tutela.xyz/>

0x12d66f87a04a9e220743712ce6d9bb1b5616b8fc

about your input

OVERALL INFO ON THE 0.1 ETH TORNADO CASH POOL

uncompromised equal user deposits: 11956 / 17548

TORNADO CASH ANONYMITY SET

total equal user deposits: 17548

compromised deposits:

- all reveals: 5592
- address match reveals: 3553
- unique gas price reveals: 5
- multi-denom reveals: 1303
- linked address reveals: 2420
- TORN mining: 29

uncompromised deposits : 11956

check if your transactions have been compromised

YOUR COMPROMISED TXNS IN THIS POOL

enter a deposit or withdrawal address used with this pool to check for compromised txs

Анонимные валюты



Monero

CryptoNote



Zcash

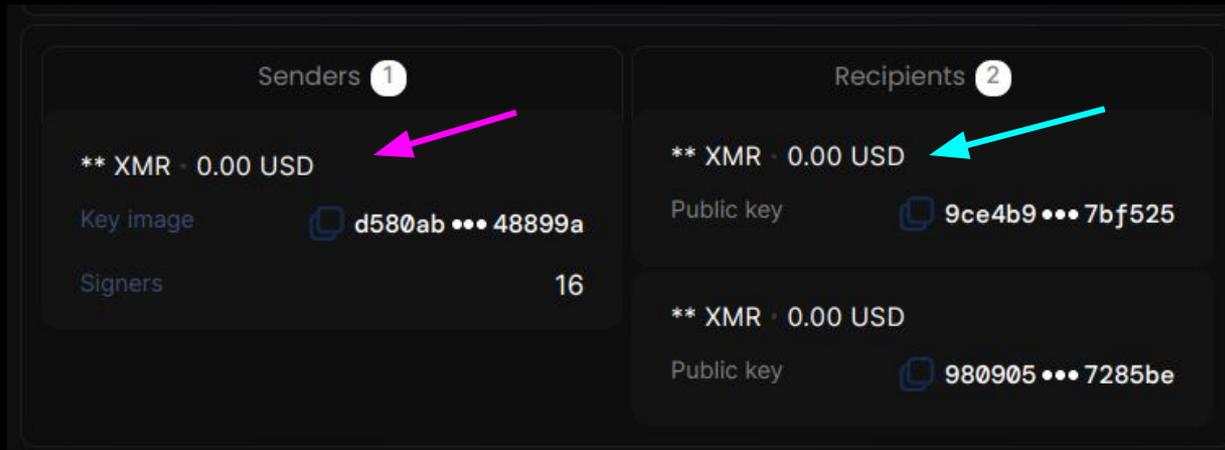
zk-SNARK



Dash

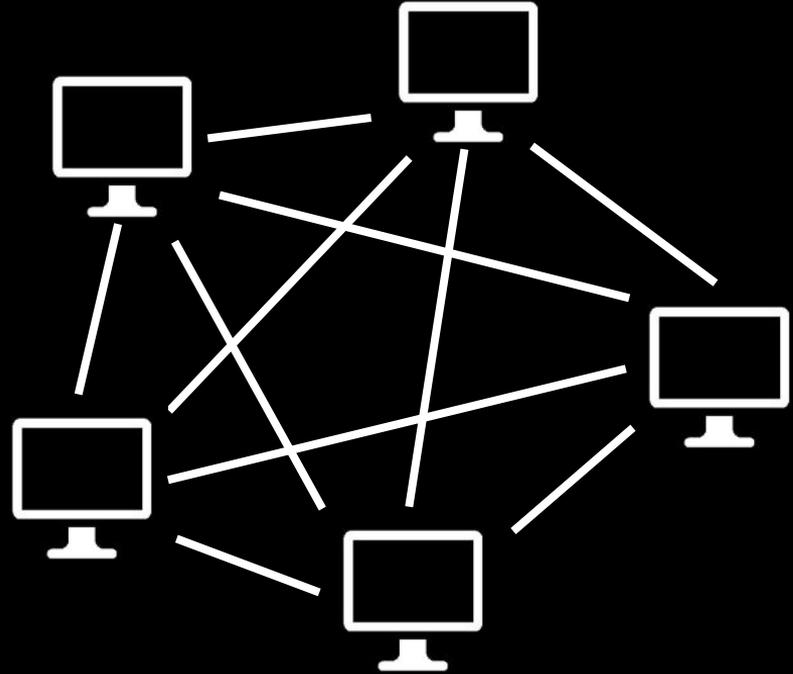
CoinJoin

Анонимные валюты

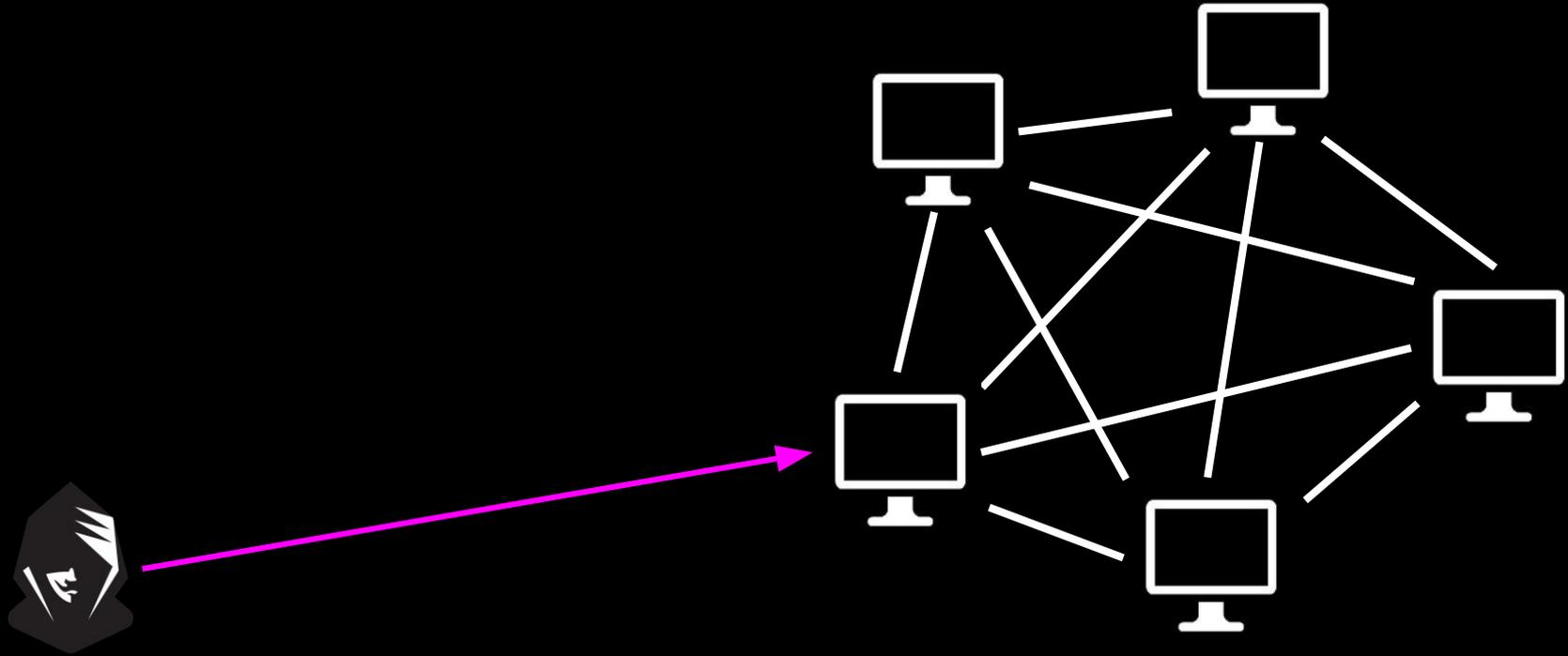


Ни входов, ни выходов, ни количества

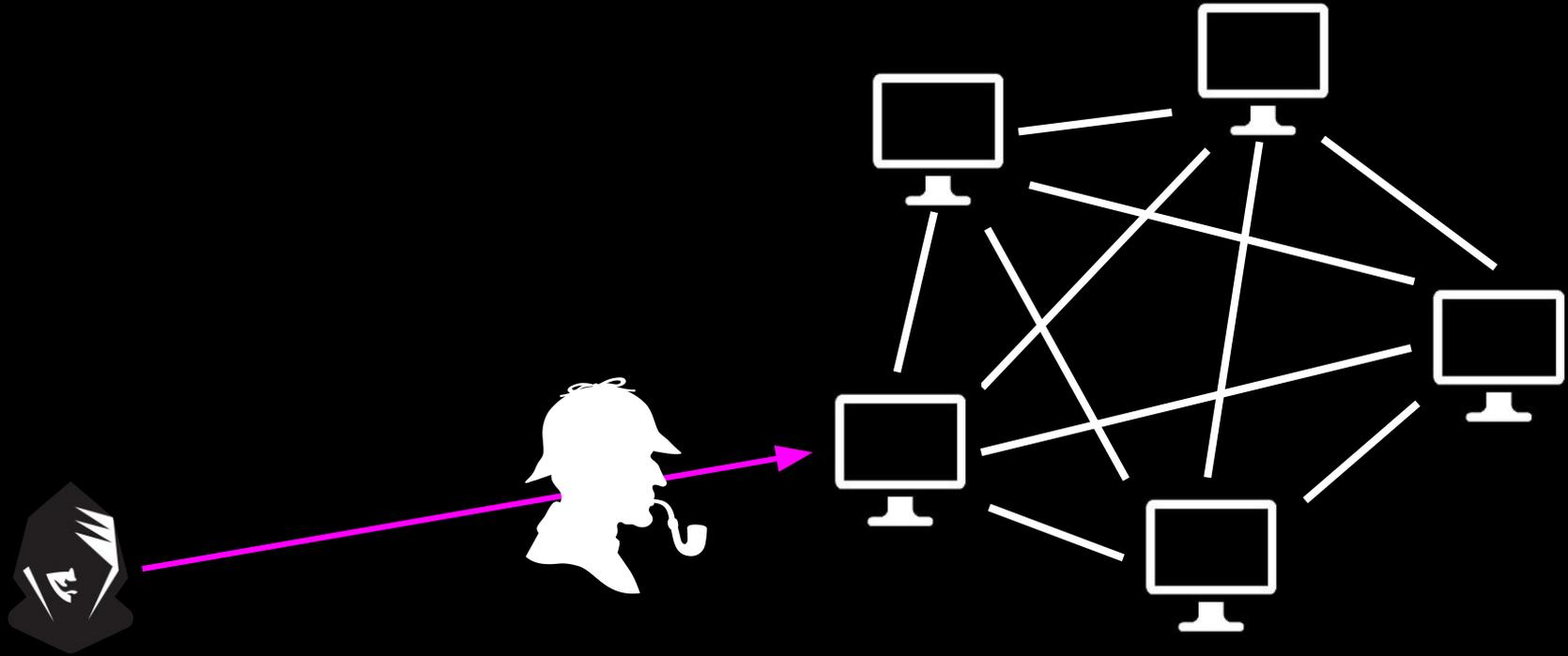
Перехват IP



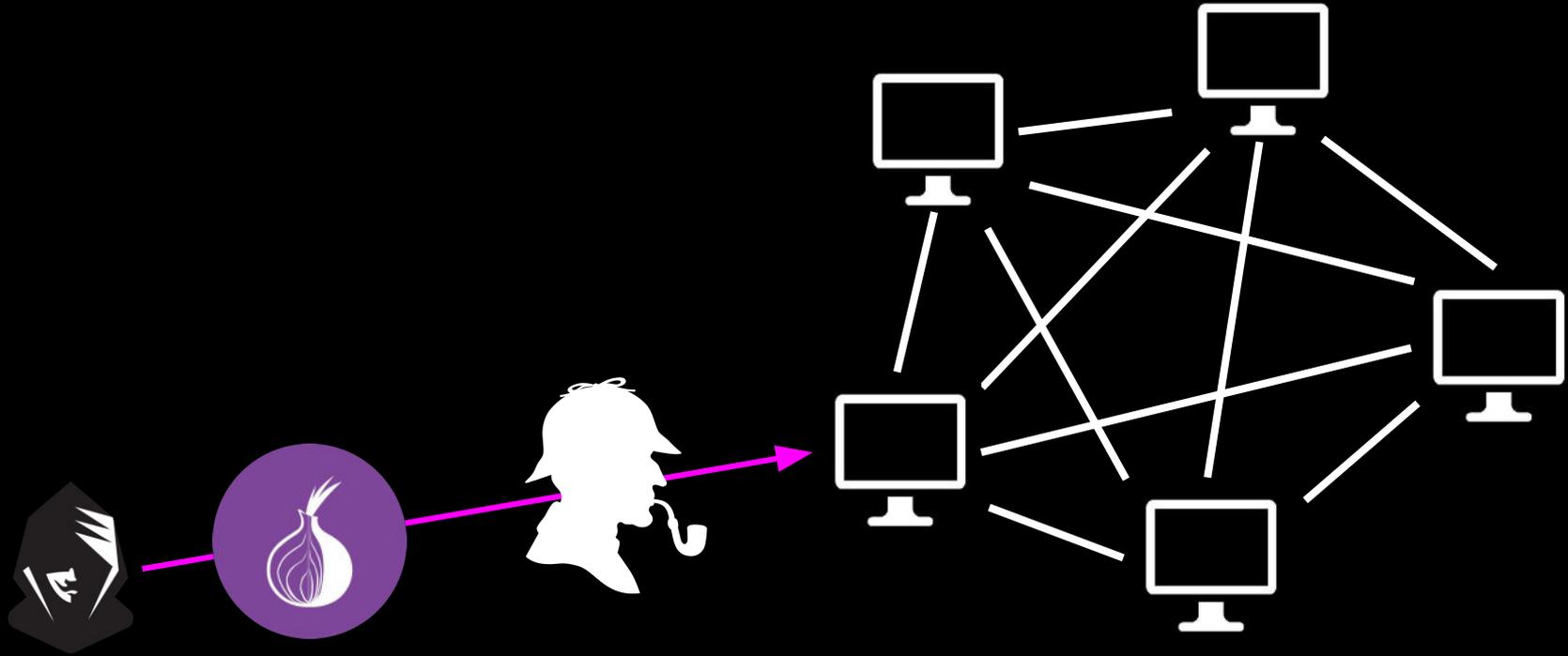
Перехват IP



Перехват IP



Перехват IP



Сколько веревочке ни виться...

Monero

zk-SNARK

Tornado Cash

Zcash

Вся криптография

Bitcoin и Ethereum

Сколько веревочке ни виться...

Monero

zk-SNARK

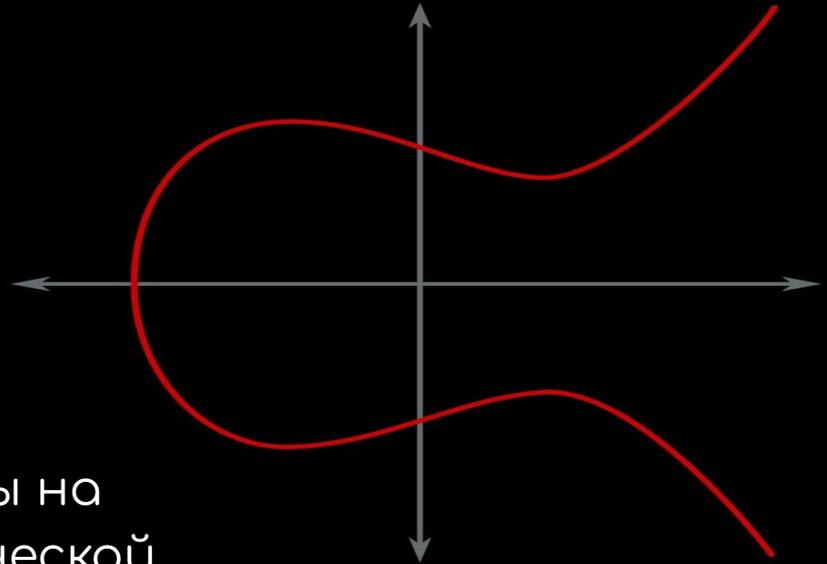
Tornado Cash

Zcash

Вся криптография

Bitcoin и Ethereum

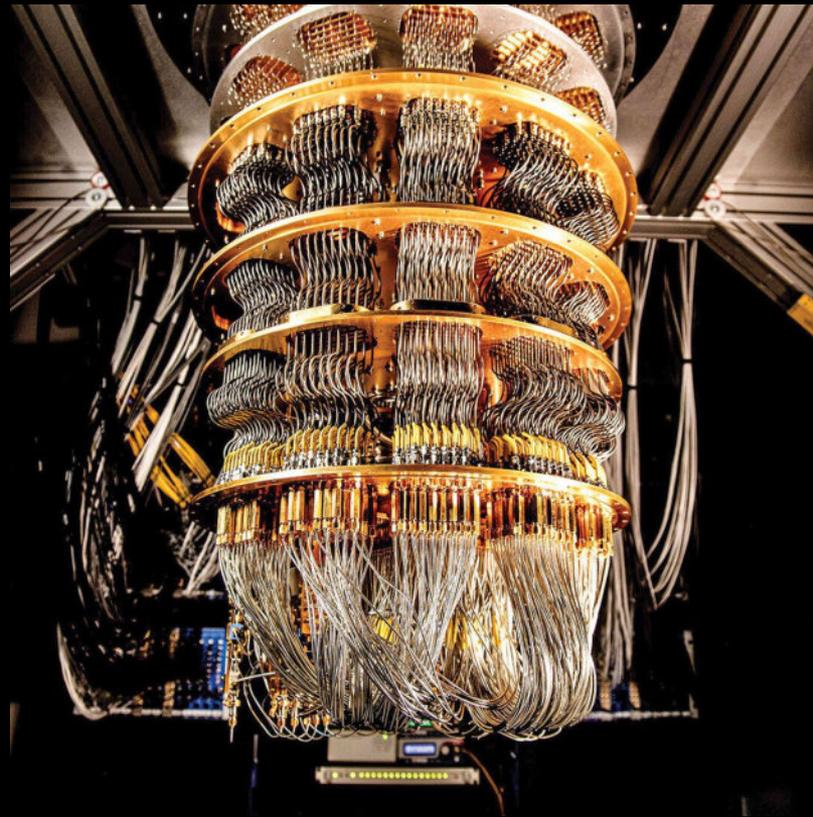
Основаны на
эллиптической
криптографии



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/5KSkJOTgMtvqC36v1GqZ987N-_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