



Canada Revenue
Agency

Agence du revenu
du Canada

Open Source Intelligence + Crypto

Open Source Information + Tracing = More Complete Story

Open Source

- Many crypto related crimes have a large open source component.
 - Facebook / Twitter / Discord / Reddit
 - Blockchain metadata
 - Etc.
- Open source information helps you understand the human activity behind transactions that you see on blockchains
- Open source information helps you prepare for searches and seizures

Toronto

Ontario court freezes access to funds raised for protest convoy on GiveSendGo platform



Order applies to 'Freedom Convoy 2022' and 'Adopt-a-Trucker' campaign pages

Policy

Canada Sanctions 34 Crypto Wallets Tied to Trucker 'Freedom Convoy'

Bitcoin, Ethereum, Litecoin, Monero and Cardano addresses are all on the list.

Questions

1. How many dollars worth of bitcoins did each trucker receive?
2. What method was used to share the bitcoins – what was being given to the truckers?
3. What wallet were the truckers told to use in order to claim their Bitcoins?
4. How many donations were made to the fundraiser?

OSINT Can Inform Tracing

- OSINT may tell you *activities* what on-chain transactions represent.
- OSINT may show you the intent behind on-chain transactions.
- *OSINT may tell you whether multiple individuals are involved* in conducting transactions.
- OSINT may tell you whether the seizure of virtual assets require multiple keys.

Trucker Protest OSINT Sources





- Social media posts on *YouTube*, *Twitter*, *Reddit*, etc.
- Comments on *donation web pages*
- *Blockchain* data

Protesters were posting information everywhere.

Twitter

- Navigate to the following Twitter web page:
<https://twitter.com/HonkHonkHodl>
- Where were supporters directed to navigate to in order to make donations (i.e. leave tips)?

Two Main Fundraisers

- **Adopt-a-Trucker** 
 - Small amount raised (\$10,000)
 - Multiple cryptocurrencies
 - **Website shut down because of policy violations**
- **HonkHonk Hodl** 
 - Large amount raised (~\$1.2 Million)
 - Bitcoin only
 - Lightning Network donations possible
 - **Website security & privacy has been increased**
 - Donations are still being cashed out



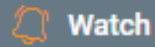
Adoptatrucker.ca

- **Website facilitated donations using fiat payment systems.**
- Linked to GoFundMe
- Bitcoin, Ether, and other cryptocurrencies were accepted.
- Bitcoin address active starting 5 Feb
- Total donations approximately \$10,000

Chainalysis - Adopt-a-Trucker Bitcoin Donation Timeline

Root Address

bc1qvetv213v5081mpral067kghhm6...



Watch

Balance:

0.024366 BTC

Transfers:

82

Sent:

0.132172 BTC

Withdrawals:

9

Received:

0.156919 BTC

Deposits:

73

Total Fees:

0.000379 BTC

Addresses:

2

Overview

Counterparties

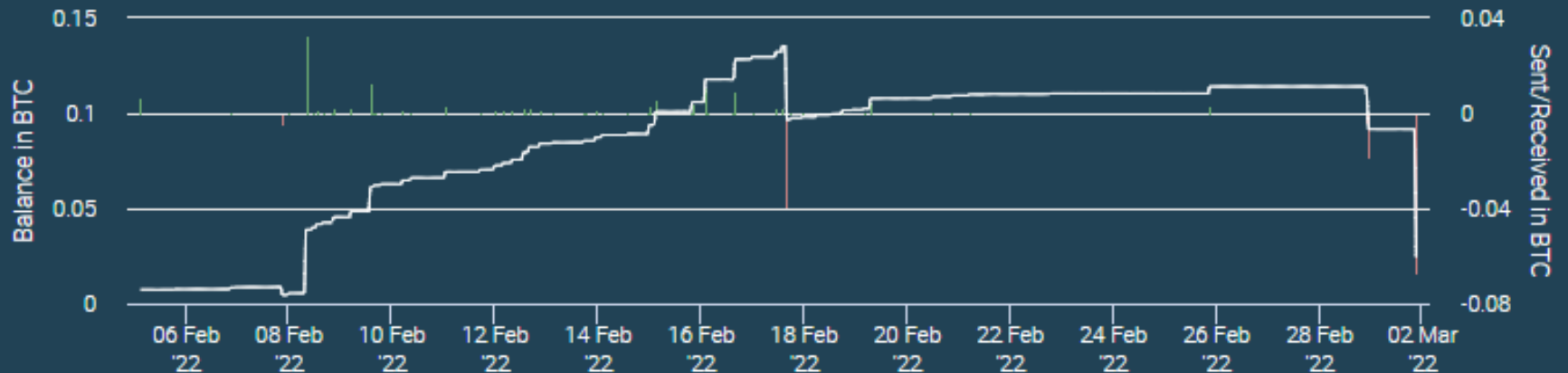
Transfers

Addresses

OSINT



i Both external and internal withdrawal transfers are displayed in the transfers list.



Adopt-a-Trucker donation info was available on Reddit and Twitter

bc1qvetv2l3v508lmpal067kghhm6x6nsm70rgwhx

Ways to donate

"the best way to make sure your donation is received, is always to arrive yourself in Ottawa and deliver the aid, or sponsor someone from your community"

Online	https://givesendgo.com/warroomcanadanet https://givesendgo.com/freedomconvoy2022	
eTransfer	donations@adopt-a-trucker.ca	(set power to: truc'ker)
BTC	bc1qvetv2l3v508lmpal067kghhm6x6nsm70rgwhx	
ETH	0x859481Ef7dAc321078547f50c756C8924EaB183f	
LTC	ltc1qqhzc2dflesccd5gx6ugqqcplzakrk8w1xl8zq	
ADA	addr1qxwxppd3ahfsh43f88h4jn8ngrum64fe6meck3nnwkwtsp6elsk4xhyrdtm5v6tnq3ulw9u9gcmvkhjrj4xcu3sm60hqtz3wuy	
XMR	423nPDQqsPrAagFSHaUBMrYQQCgb2562iLLWu1dZyEGEGsavxfpNxWtDjreSUzwqWQCxi6GrSz8jtYWjS4pW9mK9DoBvdWo	
ETC	0x88CD1D4611D456357eF8620450d3121672305d03	

Chainalysis identified additional Adopt-a-Trucker Addresses





BTC: bc1qvetv2l3v508lmpal067kghhm6x6nsm70rgwhx

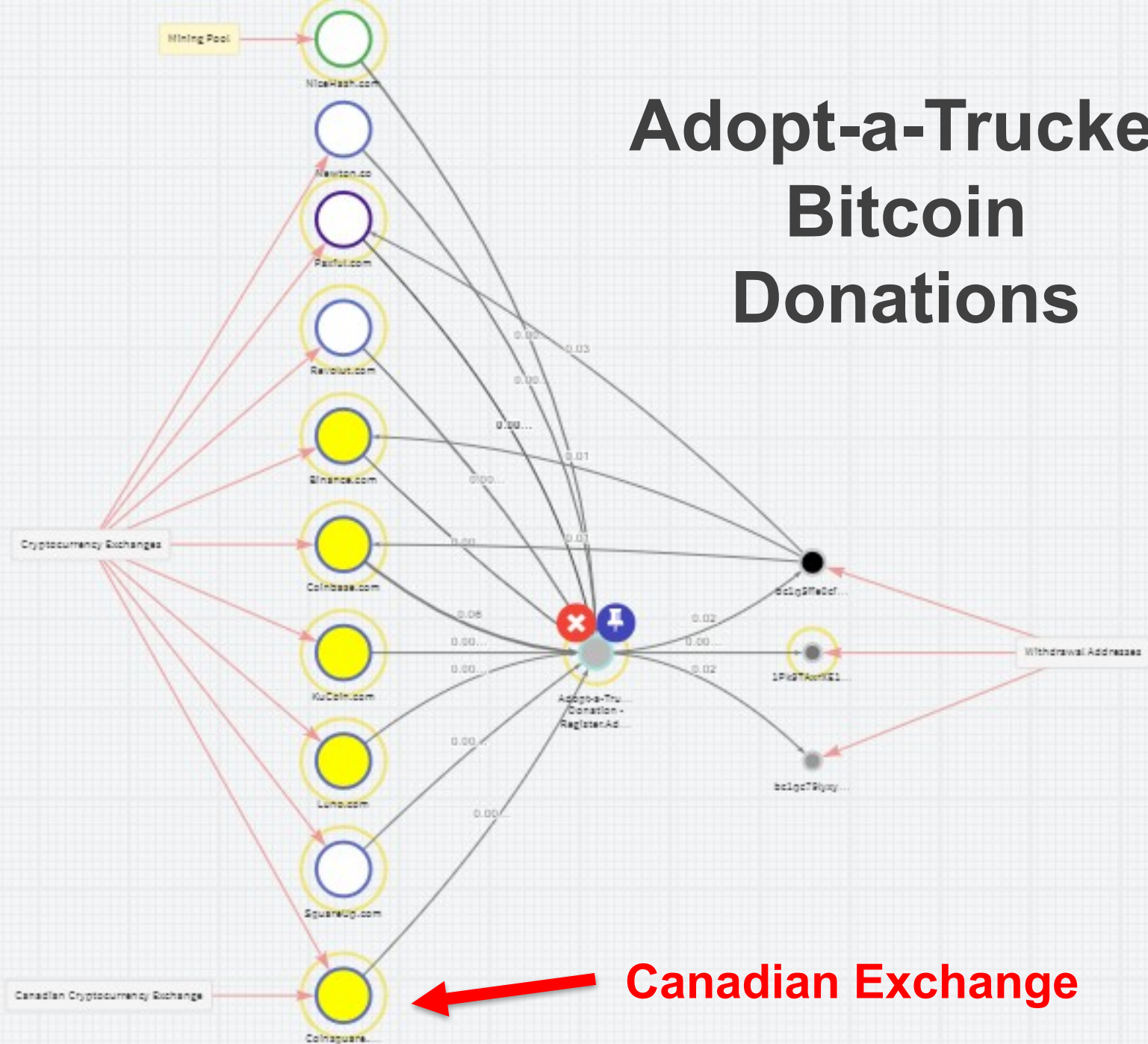
ETH: 0x859481Ef7dAc321078547f50c756C8924EaB183f

LTC: ltc1qqhzc2dflesccd5gx6ugqqgcplzakrk8wlxl8zq

Adopt-a-Trucker - Bitcoin

- Total received = 0.15325265 BTC (~\$7,620 CAD)
- 72 Deposits (i.e. donations)
- 3 Withdrawals
- **OSINT in Chainalysis showed complaints on BitcoinAbuse**

Overview	Counterparties	Transfers	Addresses	OSINT	↓
Source ▾		Date ▴ ▾		Subject ▾	
Chainalysis Identification		02/17/2022 12:00 AM		OTHER: RCMP - Cryptocurrency Alert 2022-02-15 bc1qvetv2l3v508lmp...	
Chainalysis Identification		02/17/2022 12:00 AM		OTHER: RCMP - Cryptocurrency Alert 2022-02-15 bc1q82ejx54e9ra0la9n...	
Bitcoin Abuse		02/15/2022 6:16 AM		crypto scam from freedom convoy adopt-a-trucker.ca	
Bitcoin Abuse		02/15/2022 10:47 AM		other from Recover your lost money	



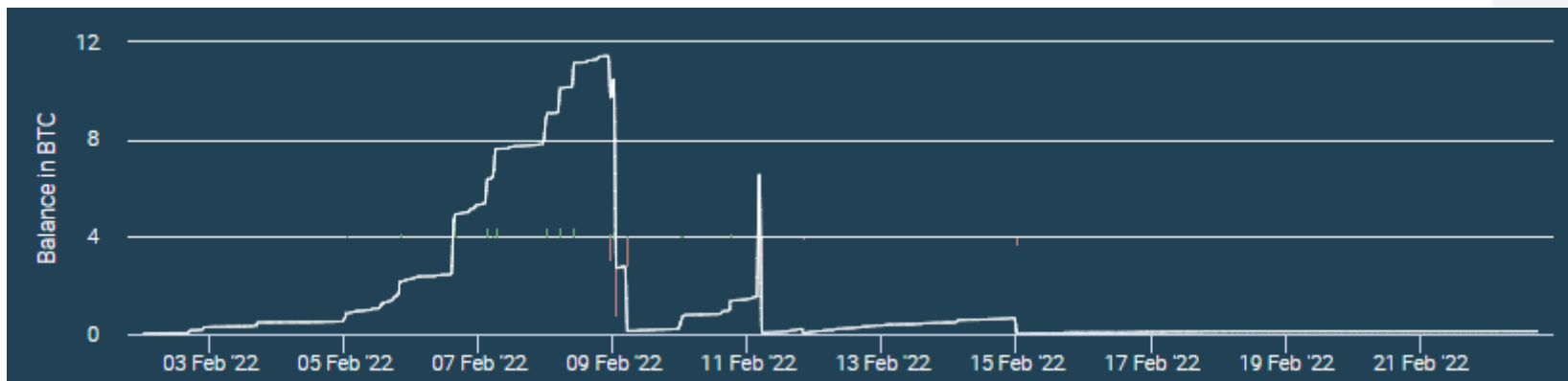
Set up after GoFundMe/Adopt-a-Trucker shut down
HONKHONK HODL



TallyCoin – HonkHonk Hodl

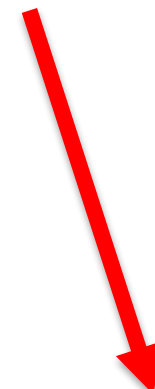
<https://tallyco.in/s/lzxccm/>

- Set up in response to other donation sites being shut down.
- 2339 donations (**not 10s of thousands as claimed**)
- 17 withdrawals
- 20.735 BTC received (**\$1.2 Million CAD**)
- Primarily active from 2 to 15 February, 2022



Donation Web Page (Tallycoin) Shows the Donation Address

bc1qlc2gpmzrr9gded07d9a40lt2lq7pp2v7h4c5jx



tallycoin Explore Sign Up Log In

Details Contributors (5343) Charts Share

BITCOIN FOR TRUCKERS

★ GOAL REACHED ★

CAD \$ 1161857.67 raised goal \$ 1119958.09

Send Bitcoin to Honkhonk Hodi

23832 satoshis

50c	\$1	\$2
\$5	\$10	\$15
\$20	\$30	\$40
\$50	\$100	\$200

BTC Approve: 0.00023832 BTC

Type a Public Message (optional) ...

☒ anonymous or log in

The Canadian Bitcoin community would like to have a second financial access point for #FreedomConvoy2022. Legacy financial infrastructure can sometimes be politicized and clamped down upon, whereas Bitcoin is a truly censorship resistant method of communicating value. Don't allow your voices to be silenced, and don't allow your financial sovereignty to be trampled upon.

Love, unity and freedom - let's raise some hard money for hard workers!

Contributors (5343)

100%

Goal 21 BTC

Raised 21.69934385 BTC

tallyco.in/s/lzxccm/

OSINT availability is time sensitive

(but don't worry...)

- The donation page now redirects to a login page!
- Information is no longer openly available
- As situations change, sites tend to get locked down

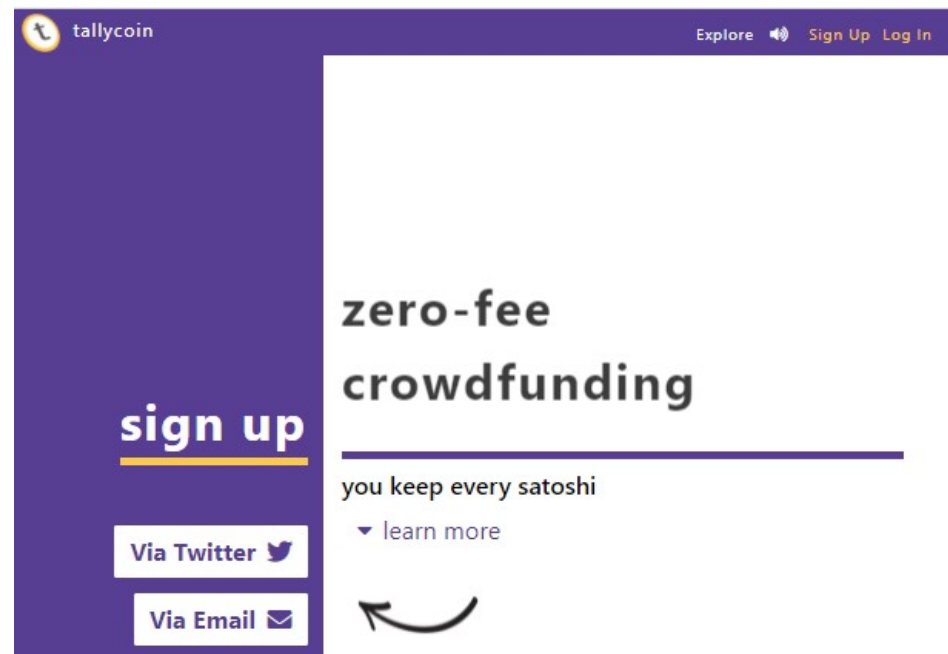
<https://tallyco.in/s/lzxccm/>

redirected to

<https://tallyco.in/>

currently redirects to

<https://tallycoin.app/>



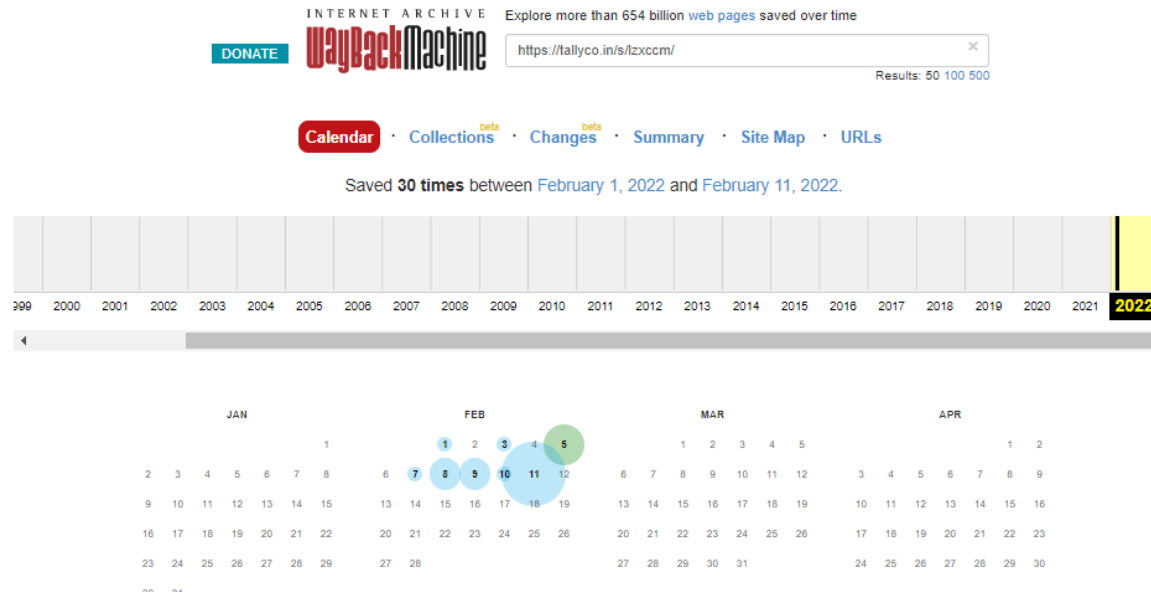
WHAT WERE THE MOTIVATIONS BEHIND THE DONATIONS?

Exercise: Internet Archive

- A locked down site's content may remain available via snapshots taken by the **Internet Archive**.
1. Go to <https://web.archive.org/>
 2. Enter the trucker donation URL from Facebook:
https://tallyco.in/s/lzxccm/
 3. Select a date and open a snapshot.
 4. What information can you see?

Internet Archive has Snapshots

https://web.archive.org/web/*/https://tallyco.in/s/lzxccm/



Each of the snapshots shows 500 donations and **associated messages.**

Users were able to post messages when they donated



- Messages can still be seen
- Messages can be tied to specific donations via amounts
- **Snapshots may be deleted if the site owner requests it.**

Chainalysis



- Displays the donation Date & Time
- Displays precise donation amounts
- Displays the donating addresses

You can link the donation comments to an exported spreadsheet of transactions from Chainalysis

Date & Time – Amount - Address

Root Address

bc1qlc2gpmzrr9gded07d9a401t2lq7pp2...

Watch

Balance:

0.112941 BTC

Transfers:

2,357

Sent:

20.618579 BTC

Withdrawals:

17

Received:

20.737385 BTC

Deposits:

2,340

Total Fees:

0.005864 BTC

Addresses:

1

Overview

Counterparties

Transfers

Addresses

OSINT

Both external and internal withdrawal transfers are displayed

Date (UTC)

Tx Hash

Counterparty

> 02/26/2022 04:21

cf1267cefed4c9e...

d07... ● bc1qmt73k9szt467w...

> 02/23/2022 18:14

87106f227929e25...

d07... ● bc1qvx70aazuemaza...

> 02/22/2022 18:38

0a73188f0f3edd2...

d07... ● bc1qkjinm0zyuzsx9s...

> 02/22/2022 05:23

6f749eb948bfe6e...

d07... ● bc1q06ew9edh6f5mj...

> 02/22/2022 05:23

5207660b2a5ff5e...

0.000213 bc1qlc2gpmzrr9gded07... ● bc1q08z8f28t3vzgw...

> 02/20/2022 15:48

b949d3aed6a4885...

0.000178 bc1qlc2gpmzrr9gded07... ● bc1qr08hx4np5k4rc...

> 02/19/2022 22:28

5fad80a04373107...

0.000124 bc1qlc2gpmzrr9gded07... ● bc1qv08duljezz6h5...

CSV Exports

Export Exposure

Export Exposure USD

Export Counterparties

Export Transfers

Export Transfers with Fees

Export Addresses

Export OSINT

Cluster_transfers_of_Honkhonk_Hodl_-_Canadian_Freedom_Convoy_Donation_-_Tallyco_in_BTC - Excel

File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do

Clipboard Font Alignment Number Styles Cells Editing

G25

A B

1 This file contains a list of all transfer outputs of the cluster identified by the following root address:
2 bc1qlc2gpmzrr9gded07d9a40lt2lq7pp2v7h4c5jx
3 The cluster is also known by the following name:
4 Honkhonk Hodl - Canadian Freedom Convoy Donation - Tallyco.in
5
6 Each line represents a transfer output which is either sent to the cluster or received by the cluster.
7
8 Columns:
9 Hash: The 32 byte hash of the transfer that contains the output.
10 Date: The date when the transfer was confirmed.
11 Receiving Address: If the output is received by this cluster then this will be the address in the cluster that received payment.
12 Counterparty Address: If the output is sent by this cluster then this will be the address in the peer cluster that payment was sent to.
13 Counterparty Cluster Name: The name of the peer cluster if it has been given a name.
14 Counterparty Category: The category of the peer cluster if it has a category.
15 Counterparty Org Name: The org name of the peer cluster if it has been given an organization name.
16 Value: The approximate values.
17 USD value: The approximated USD value converted by using daily average prices. 0 if the price is unknown.
18
19 Hash Date Receiving Address
20
21 4f3d2f959776e505d1e93415da8a23d743f6d53185a7ae6a819934972985b386 2022-02-02 0:09 bc1qlc2gpmzrr9gded07d9a40
22 4cbfb8044d40a5431e4c1c7e48d6ab6e082def6c42be73a595ba580040d8fd05 2022-02-02 0:17 bc1qlc2gpmzrr9gded07d9a40
23 3233ed66b9815e0dbfc308ac9551a30c13179667e1a84d823f8bd2f9609dab42 2022-02-02 1:19 bc1qlc2gpmzrr9gded07d9a40
24 0450edf39a65a2780ff5c8f8e82e8f7ce711e5c74ac003769e1d616e1a23c291 2022-02-02 1:19 bc1qlc2gpmzrr9gded07d9a40
25 811cc80972814086f9e78b1b4944ebf16b2f9c19fe8a2c8fd84691ae46c798df 2022-02-02 1:19 bc1qlc2gpmzrr9gded07d9a40
26 3848a196d735cf080edc3de4eb22cd55abcf6b4e6b4e74f7f3975cb6434cdb53 2022-02-02 1:29 bc1qlc2gpmzrr9gded07d9a40

Cluster_transfers_of_Honkhonk_H

Ready Accessibility: Unavailable

UNCLASSIFIED - NON CLASSIFIÉ

Value	USD Value
0.00025734	9.94711
0.00122121	47.38708
0.00002587	1.00172
0.00129515	50.15014
0.00269025	104.17049
0.00002581	0.99565
0.0012938	49.90997
0.00519532	200.41602
0.00517761	199.98441
0.0005	19.31242
0.01071829	413.99234
0.00012925	5.00475
0.00077416	29.97663
0.000693	26.83399
0.00051623	19.96619
0.00097	37.55985
0.00025989	9.99288
0.00051943	19.9723
0.00025999	9.99672
0.00129947	49.96517
0.00130242	50.43164



Truckers, you are standing up for freedom across the world.
Stay strong. We are with you. GFUSA

SAT 45,662

moments ago

Coinbase.com	exchange	0.00114139	49.68661
		0.00045662	19.93549
		0.0002201	10.00224

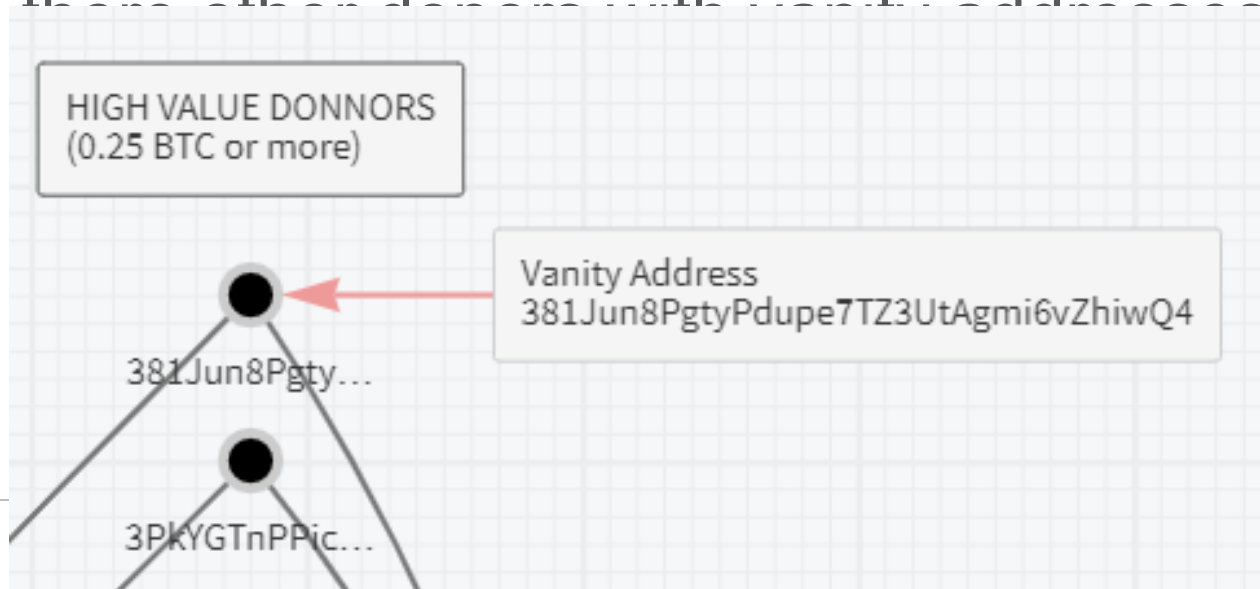
-
- A diagram illustrating the relationship between Canadian Cryptocurrency Exchanges and specific exchanges. At the bottom, a yellow box labeled "Canadian Cryptocurrency Exchanges" has two red arrows pointing upwards to two separate nodes. Each node consists of a yellow outer circle and a blue inner circle. The left node's inner circle is shaded gray and labeled "BitBuy.ca". The right node's inner circle is white and labeled "Coinsquare....".



One large donation used a “Vanity Address”

381Jun8PgtyPdupe7TZ3UtAgmi6vZhiwQ4

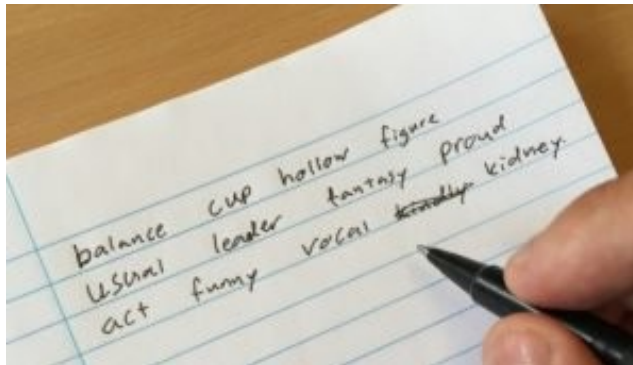
- What does **June 8th** refer to?
- What does **gty** refer to? (Grace to You Church?)
- What does **dupe** refer to?
- Are there other donors with vanity addresses?



WHAT ACTIONS DO THE GRAPHED TRANSACTIONS & ADDRESSES REPRESENT?

Trucker Payouts

- \$8,000 donations
- Disbursed by handing out envelopes to truckers
- Used Seed Word Lists (i.e. wallet backups)
- Used Blue Wallet



If we follow the bitcoins we find transfers of small amounts to 101 addresses

Root Address

bc1q42t9dhpgc6du9pjmdkvxvmke82...

Watch

Balance:

0.00

BTC

Transfers:

102

Sent:

14.679553

BTC

Received:

14.679753

BTC

Total Fees:

0.0002

BTC

Withdrawals:

101

Deposits:

1

Addresses:

1

Overview

Counterparties

Transfers

Addresses

OSINT

Counterparty

Transfers

Sent

Received

02/22

02/22

bc1qww03s6yy3yyqf9sa48vmhfzsdju...

1

0.004

0.00

bc1qj7fd7642y7ufcllyspjs7w8p80h...

1

0.004

0.00

bc1q955pcz3pvveflycjns5julkdf24...

1

0.004

0.00

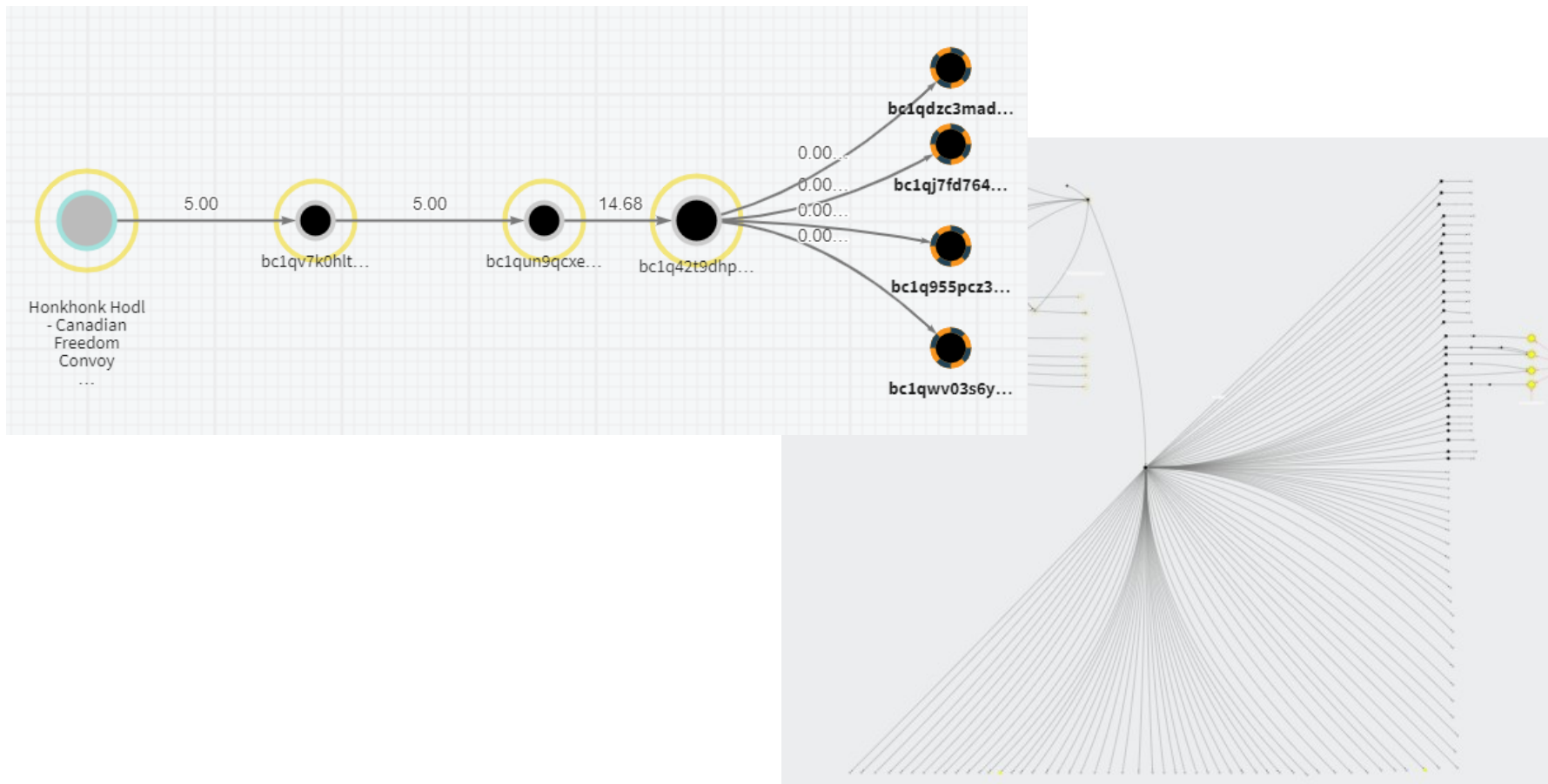
bc1qdzc3mad58rwvydkkf792pdj9ed9...

1

0.004

0.00

Each of 101 smaller addresses contain **0.144048 BTC**





Summary

Chart

Conversations

Historical Data

Profile

Exercise

1. Go to Yahoo Finance for BTC to CAD

<https://ca.finance.yahoo.com/quote/BTC-CAD/>

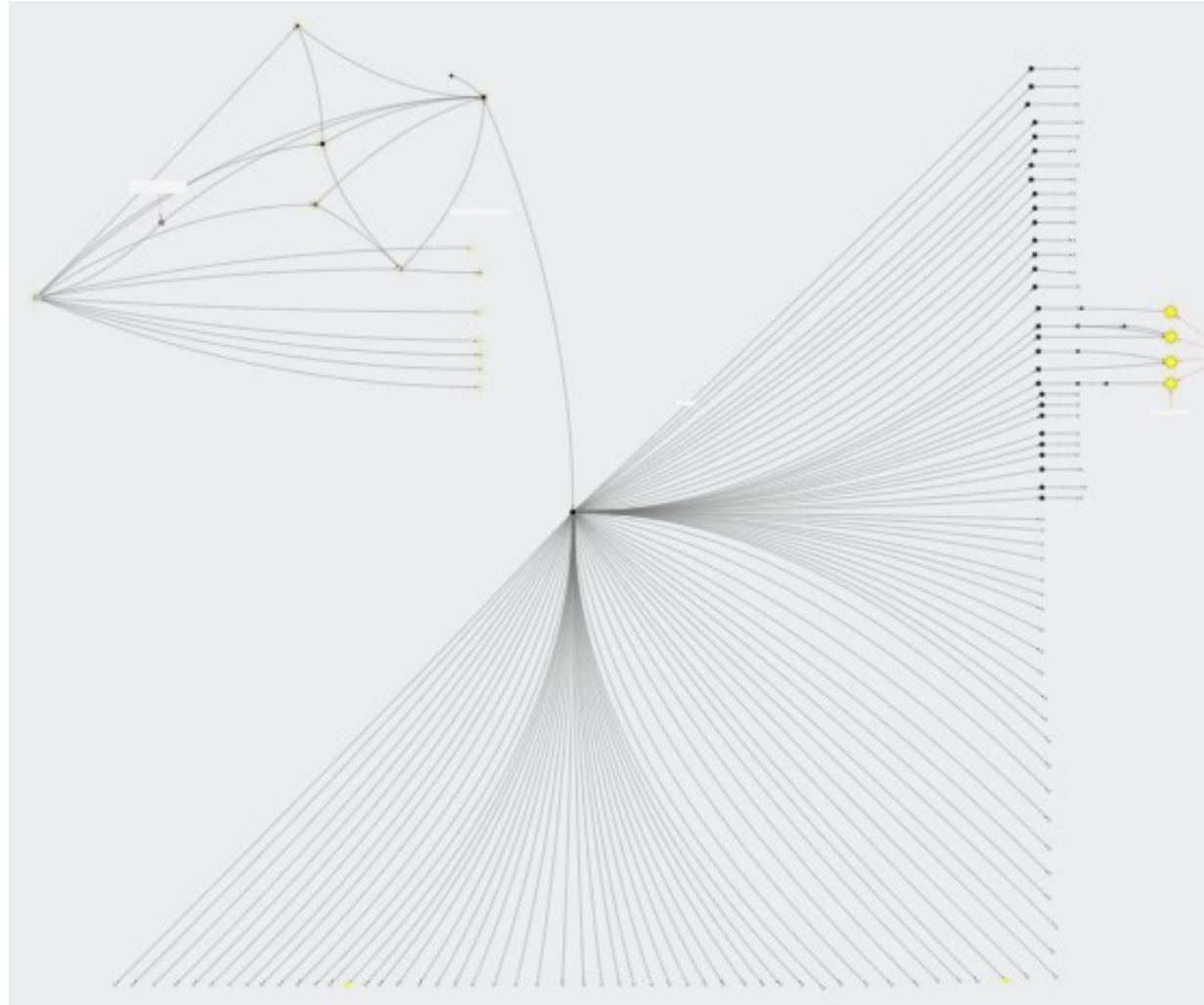
2. Navigate to the **Historic Data**
3. Look up how much 1 BTC was worth in CAD on 14 February 2022
4. Calculate how much 0.14 Bitcoins were worth
5. Compare this amount to the \$8000 amount mentioned in the YouTube video

Chainalysis – Disbursement Graph

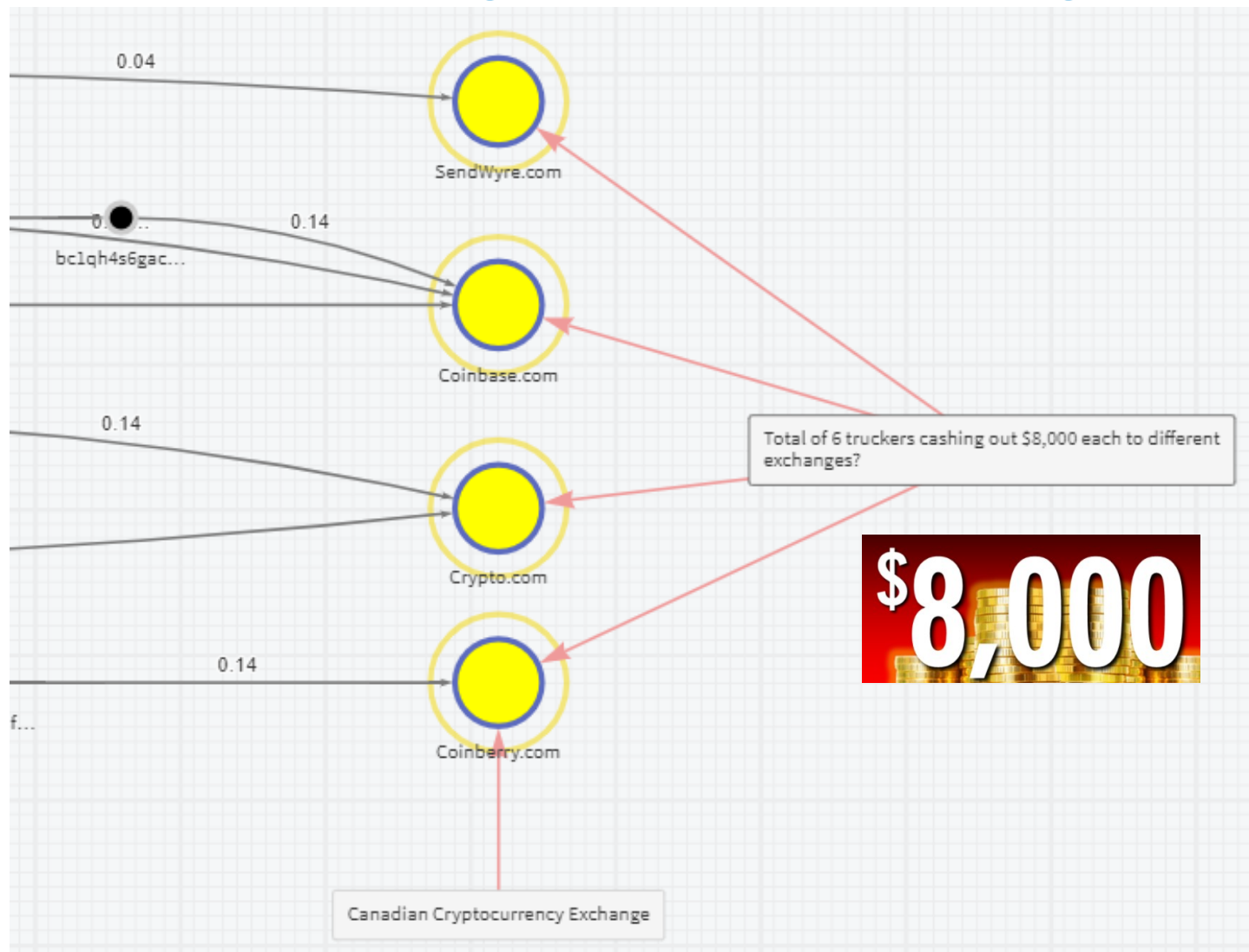
Donation site is on the far left.

Edges of the triangle are 101 addresses each containing approximately \$8k in bitcoins.

Far right are addresses cashing out at exchanges.



Truckers cashing out at Exchanges



Movement of cryptocurrency out of the \$8,000 addresses can be monitored by tools (e.g. Chainalysis)

- Chainalysis is able to send investigators notifications when the truckers cash out or transfer the bitcoins into their own cryptocurrency wallets.

Root Address

bc1qfjns4tjz39leydh4urtlc8fx7z69mx...

Balance: 0.144045 BTC

Sent: 0.00 BTC

Received: 0.144045 BTC

Total Fees: 0.00 BTC

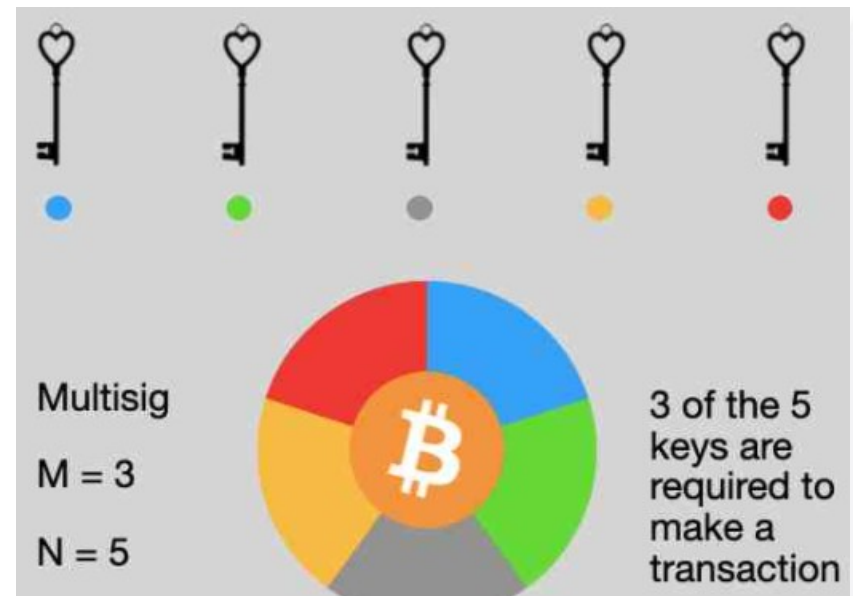


Watch

WERE MULTIPLE INDIVIDUALS
INVOLVED IN TRANSACTIONS?

Multisig Addresses

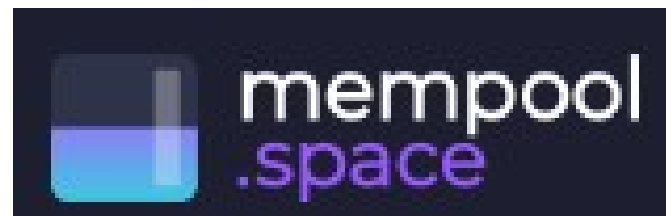
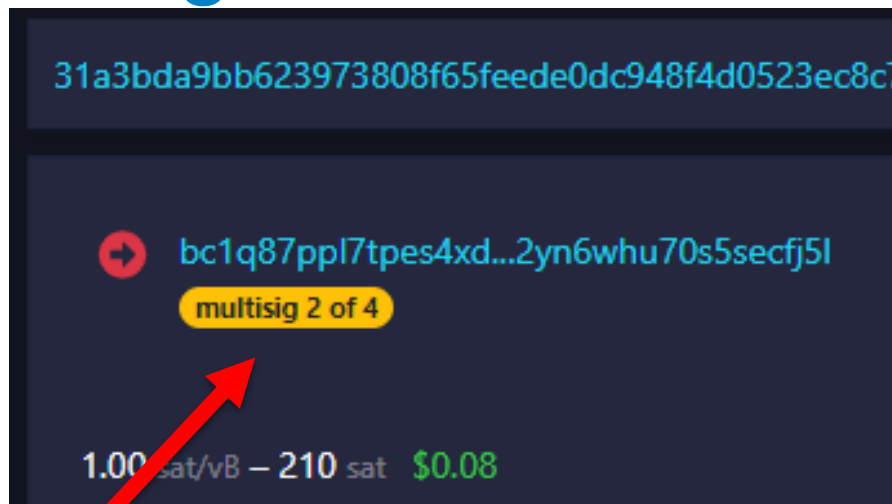
- **Multi-signature (multisig) addresses require more than one key to spend any cryptocurrency held in them.**
- Limit on the number of keys varies depending on the address type.
- Upper limit is 16-20 keys.
- Standard is 3 keys.



Were multisig addresses used?

- If multi-signature address are being used, this usually implies that more than one person was involved.
- If multisig addresses are being used, law enforcement will need more than one key to seize assets held at an address.
- Identifying who has the keys may help you coordinate searches.
- Seed Word Lists may help?

Multisig Transactions can be identified Using a Blockchain Explorer



<https://mempool.space/address/bc1q87ppl7tpes4xd9upan4q56fqes3h0vu2nzls8j3d2yn6whu70s5secfj5l>

```
P2WSH witness script
→ OP_PUSHDNUM_2
OP_PUSHBYTES_33 027c1cafd48147045f95c2ff3a2046405
2033991db1f73bebbafddc861a83a24f0
OP_PUSHBYTES_33 03447ac5709afdf0f8a0af43ba3a683ce
a030bfd0f4848ca8b45e3ff24cf753b89
OP_PUSHBYTES_33 034e0dd693acd897fa894ad180c536df3
7fa55febba2fe53ebe6df47b46ba9e498
OP_PUSHBYTES_33 037f6e26d297bc81a9bc5951604ecfdf5
5d3140712313a2d947d6cdca22c2679a4
→ OP_PUSHDNUM_4
OP_CHECKMULTISIG
```


Recent Snapshot

