OECD International Academy for Tax Crime Investigation

Anti-Money Laundering: Current Trends, Prosecutions, and the Challenges around Cryptocurrencies

OECD

Open Source Intelligence + Crypto

Trucker Freedom Protest (Ottawa) 2022

Open Source Information + Tracing = More Complete Story

Open Source Intelligence

- 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

OSINT Can Inform Tracing

- OSINT may tell you which ***activities*** 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 will require multiple keys.

Exercise

1. Search **YouTube** for "**Canadian freedom truckers bitcoin donations**"
2. Are you able to find a video of Bitcoins being handed out to the truckers?

https://www.youtube.com/

https://www.youtube.com/watch?v=zzW4ieVSejs

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?

Trucker Protest OSINT Sources

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

Protesters were posting information everywhere.

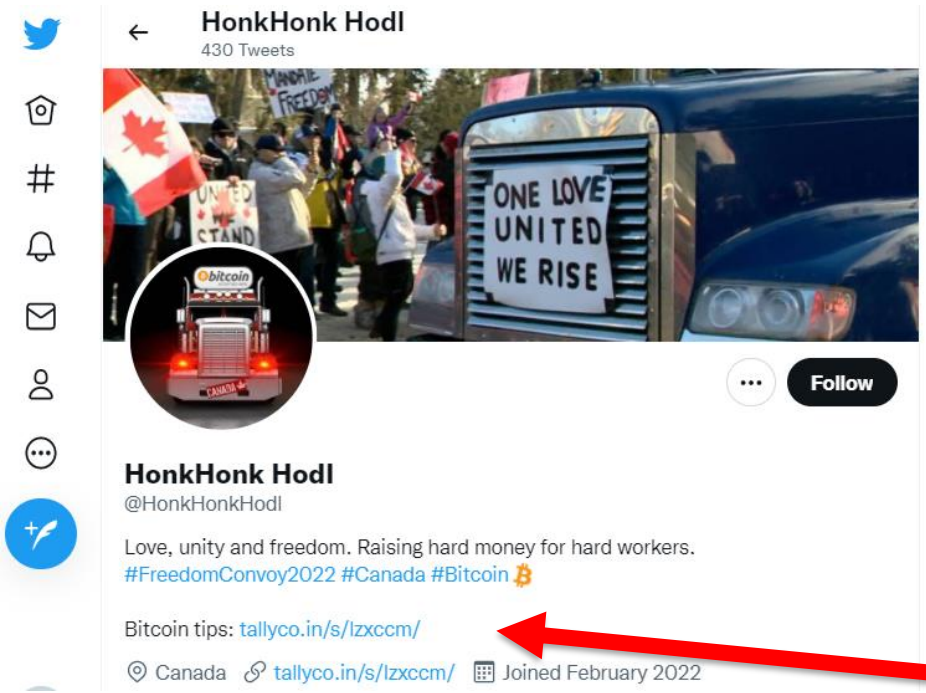
Twitter Exercise

- 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)?

Twitter: https://twitter.com/HonkHonkHodl



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

Two Main Fundraisers

- **Adopt-a-Trucker** gofundme
  - Small amount raised ($10,000)
  - Multiple cryptocurrencies
  - Website shut down because of policy violations

- **HonkHonk Hodl** tallyco.in

  - Large amount raised (~$1.2 Million)
  - Bitcoin only
    - Lightning Network donations possible
  - Website security & privacy has been increased
  - Donations are still being cashed out

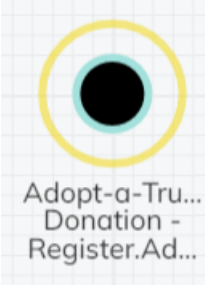
Initial donation site

ADOPT-A-TRUCKER

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

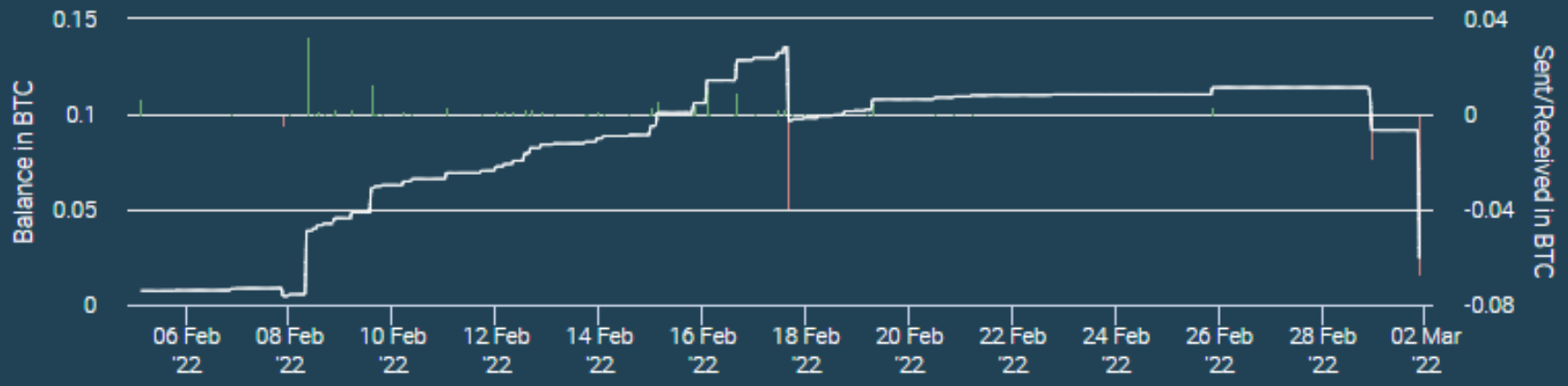


Root Address					
bc1qvetv2l3v508lmpral067kghhm6…	Balance:	0.024366 BTC	Transfers:	82
	Sent:	0.132172 BTC	Withdrawals:	9
	Received:	0.156919 BTC	Deposits:	73
	Total Fees:	0.000379 BTC	Addresses:	2

Watch

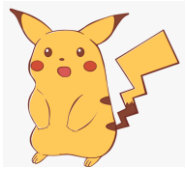
Overview | Counterparties | Transfers | Addresses | OSINT

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

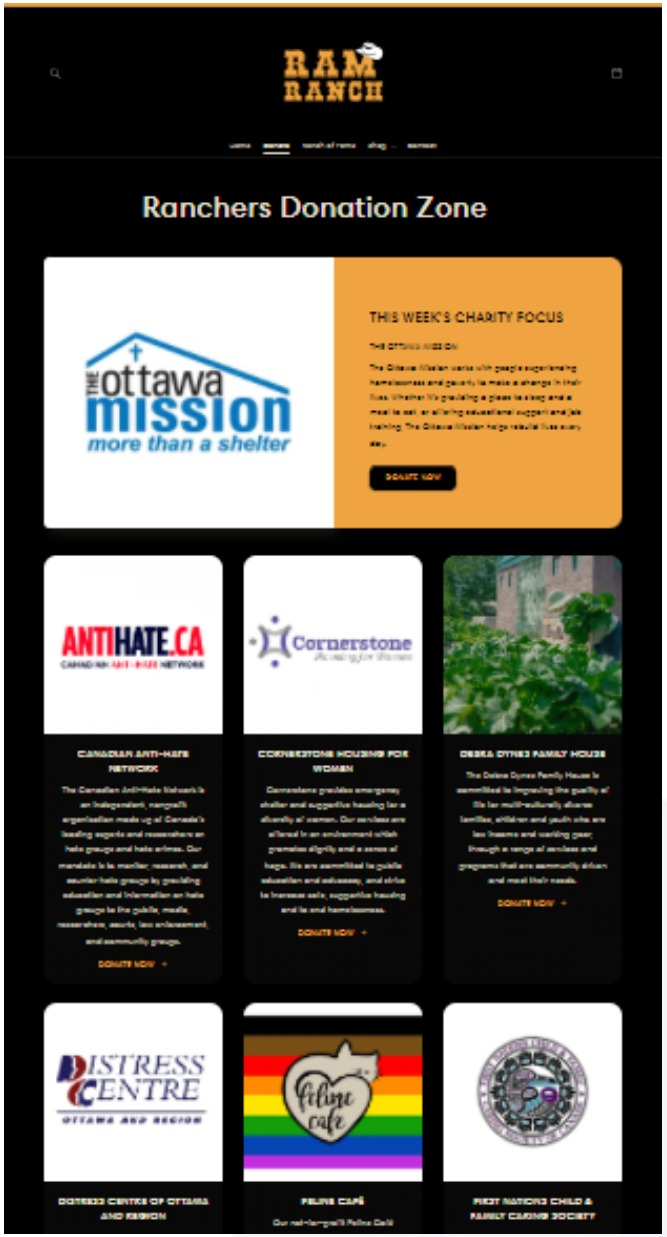


Adoptatrucker.ca

The Adoptatrucker currently redirects to RAM RANCH web site.



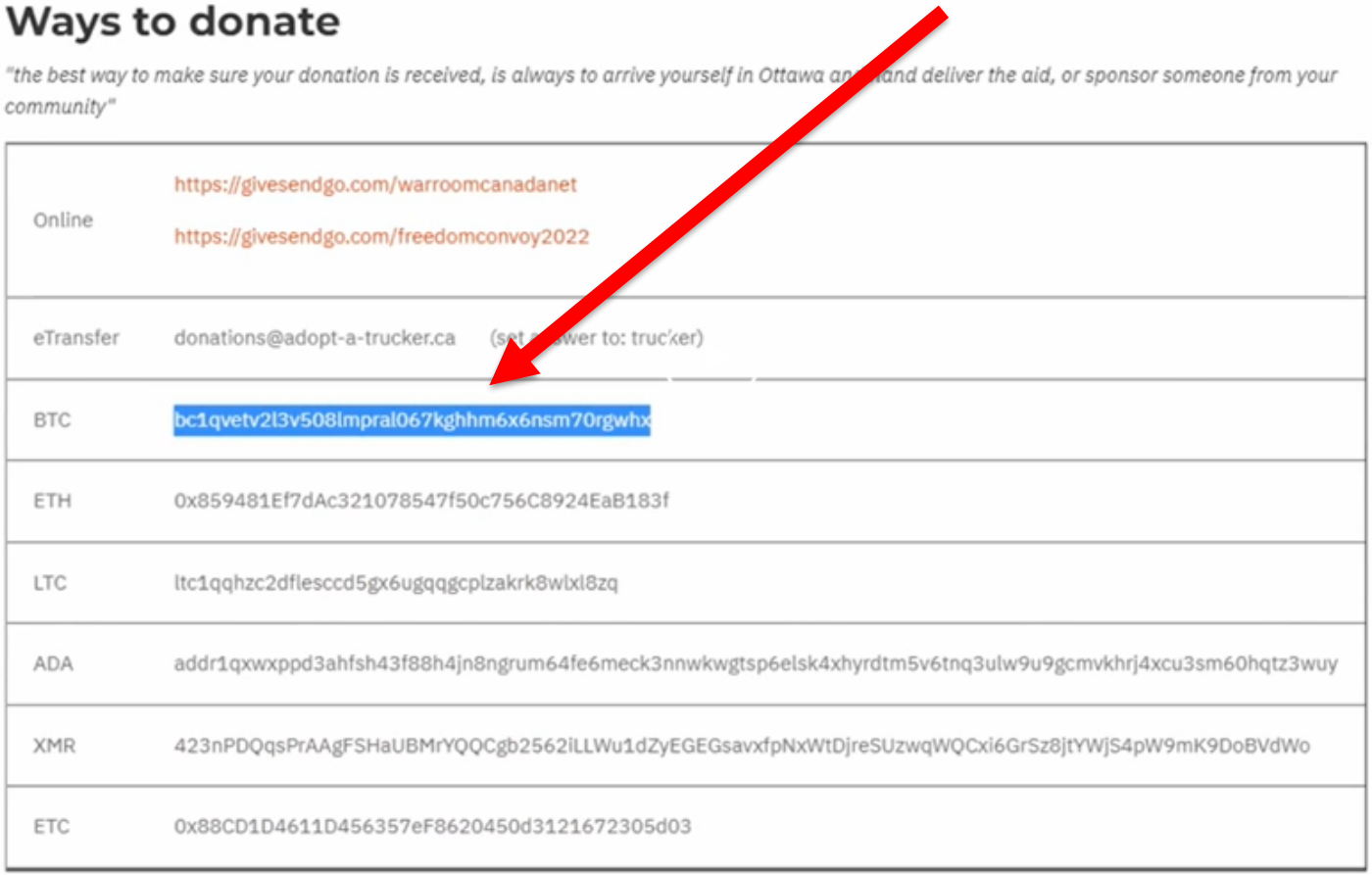
(RAM Ranch is a song by Grant MacDonald which was used to disrupt the trucker communication channels.)



https://ram-ranch.ca/pages/ranchers-donation-zone

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

bc1qvetv2l3v508lmpral067kghhm6x6nsm70rgwhx



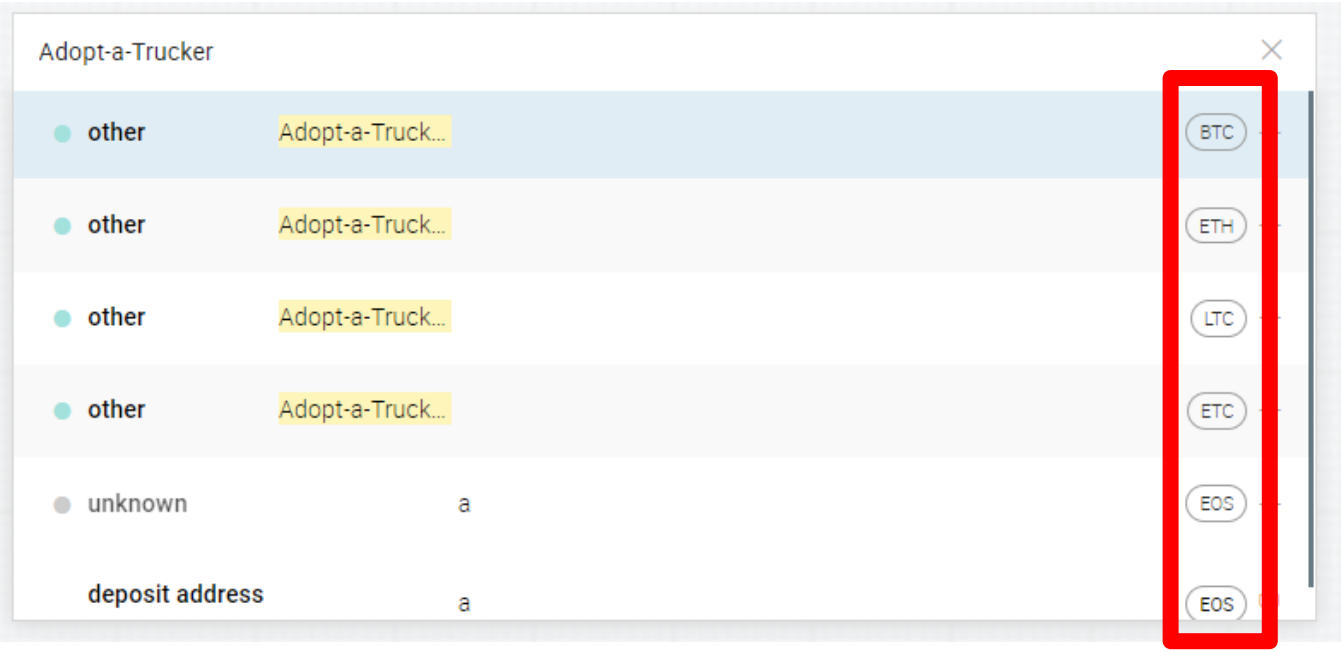
Ways to donate

"the best way to make sure your donation is received, is always to arrive yourself in Ottawa and hand 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 answer to: truc'ker)
BTC	bc1qvetv2l3v508lmpral067kghhm6x6nsm70rgwhx
ETH	0x859481Ef7dAc321078547f50c756C8924EaB183f
LTC	ltc1qqhzc2dflesccd5gx6ugqqgcplzakrk8wlxl8zq
ADA	addr1qxwxppd3ahfsh43f88h4jn8ngrum64fe6meck3nnwkwgtsp6elsk4xhyrdtm5v6tnq3ulw9u9gcmvkhrj4xcu3sm60hqtz3wuy
XMR	423nPDQqsPrAAgFSHaUBMrYQQCgb2562iLLWu1dZyEGEGsavxfpNxWtDjreSUzwqWQCxi6GrSz8jtYWjS4pW9mK9DoBVdWo
ETC	0x88CD1D4611D456357eF8620450d3121672305d03

https://www.reddit.com/r/Monero/comments/su6rx0/monero_says_no/
https://twitter.com/i/status/1494416546529112076

Chainalysis identified additional Adopt-a-Trucker Addresses

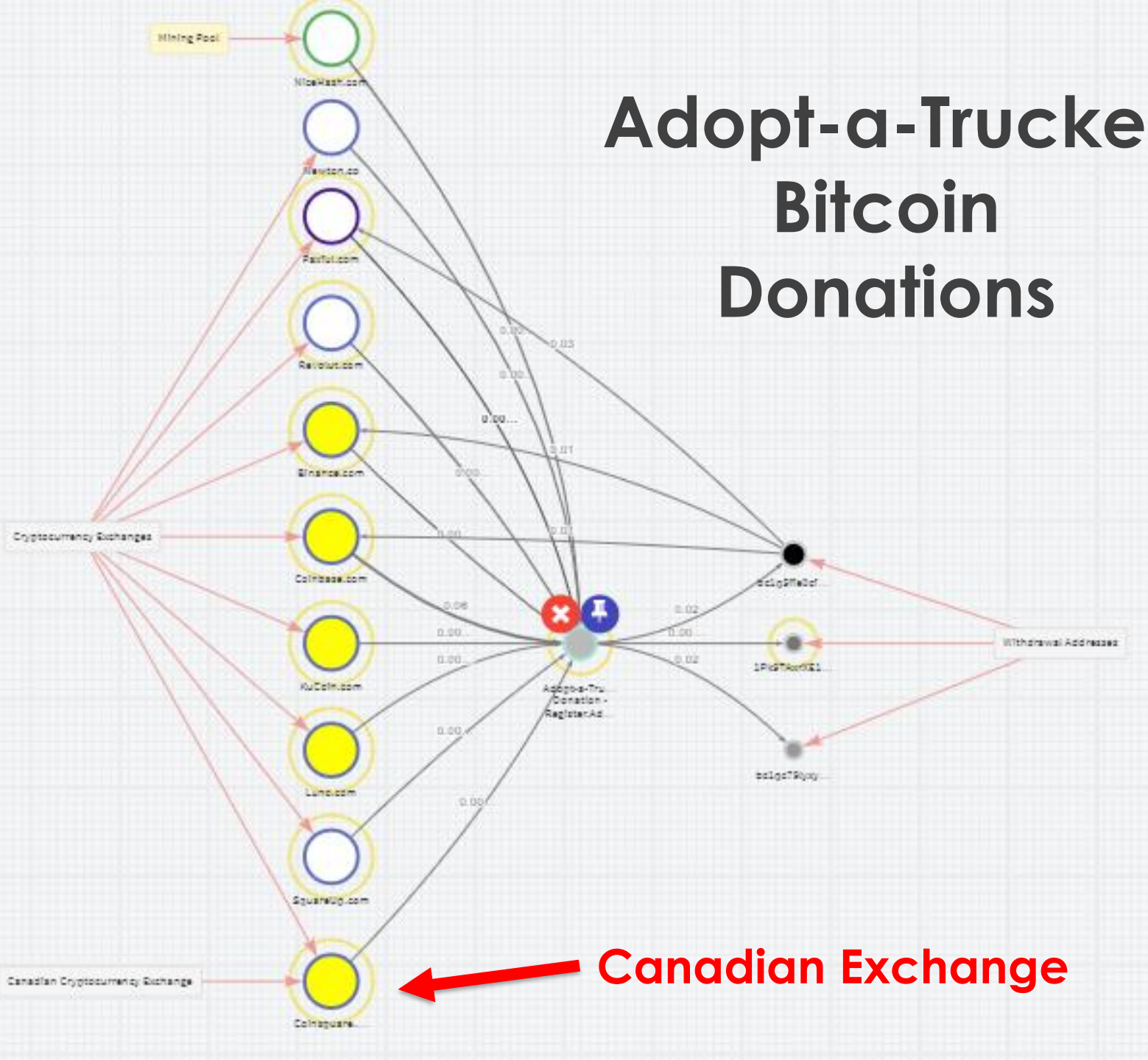


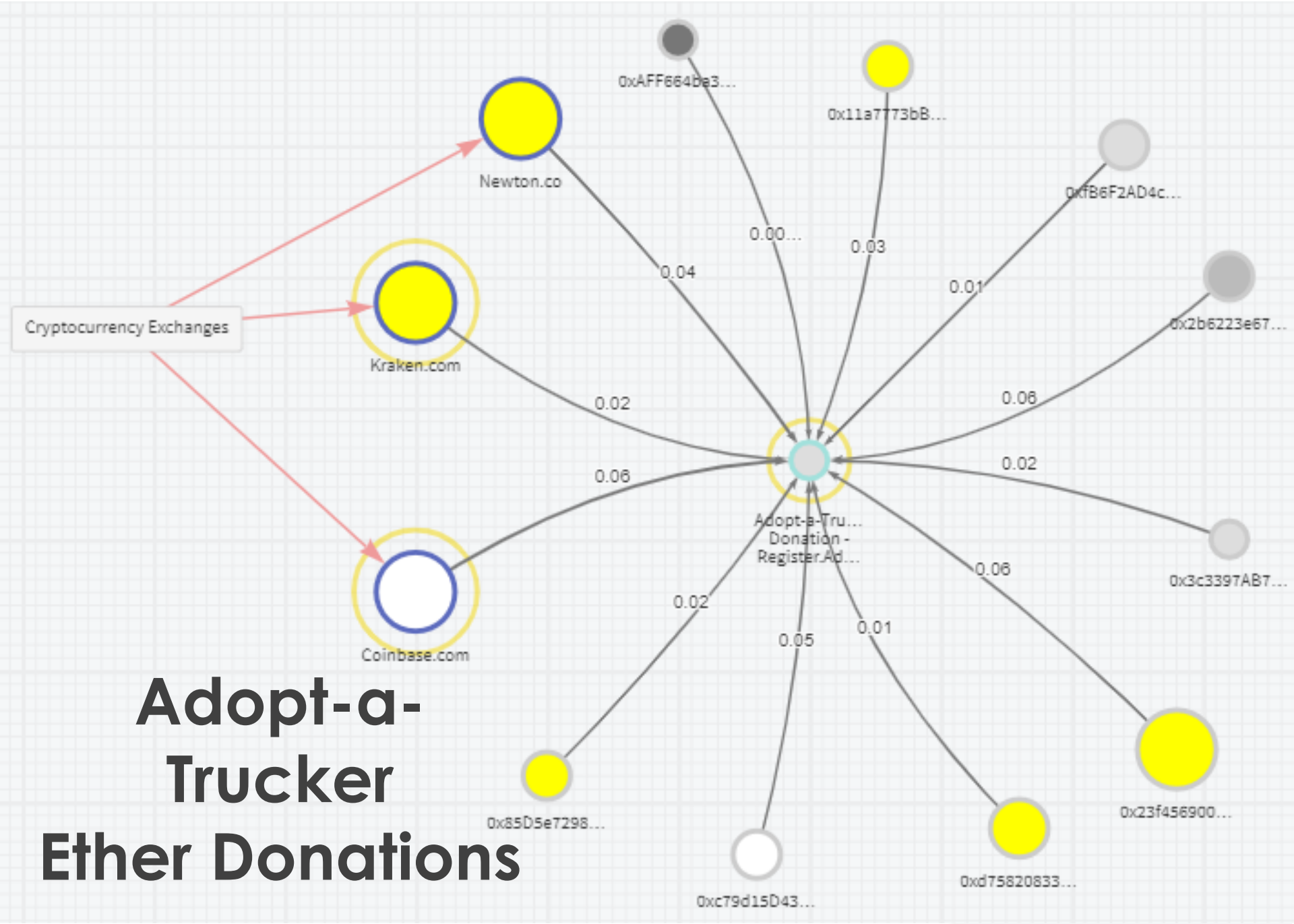
BTC: bc1qvetv2l3v508lmpral067kghhm6x6nsm70rgwhx

ETH: 0x859481Ef7dAc321078547f50c756C8924EaB183f

LTC: ltc1qqhzc2dflesccd5gx6ugqqgcplzakrk8wlxl8zq

Adopt-a-Trucker Bitcoin Donations





Adopt-a-Trucker Ether Donations

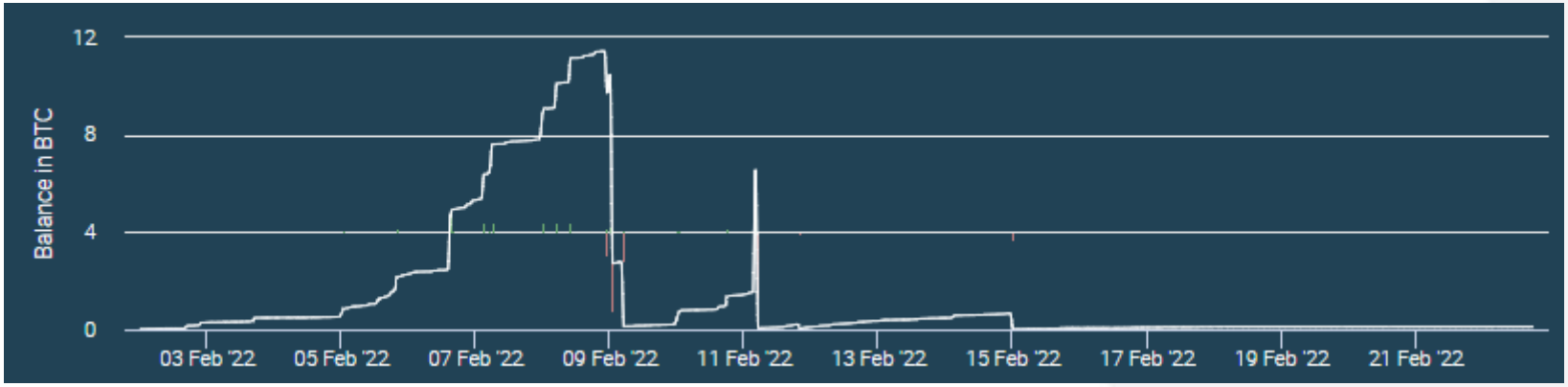
Set up after GoFundMe/Adopt-a-Trucker shut down

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

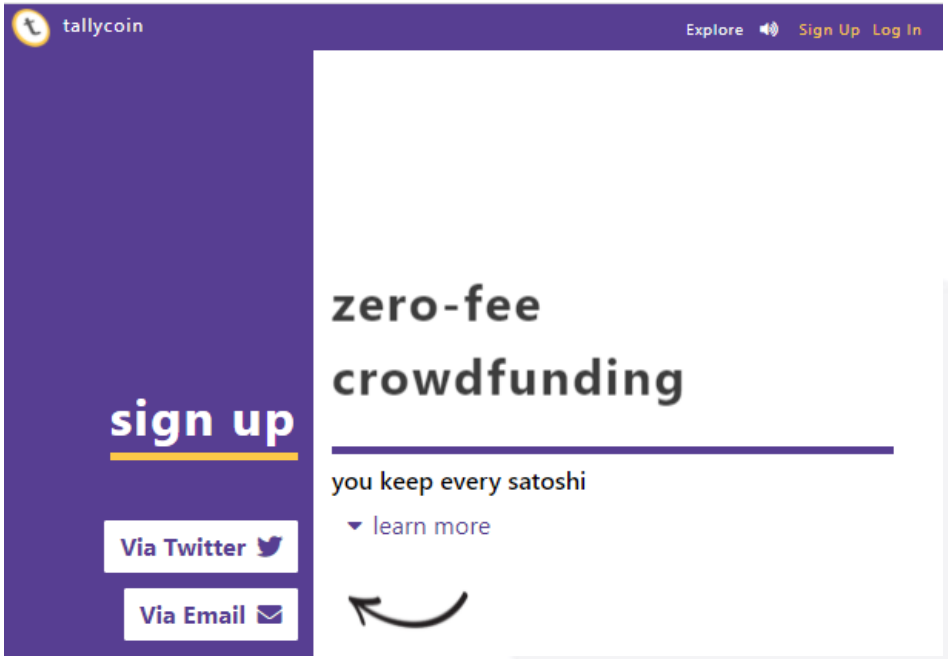
bc1qlc2gpmzrr9gded07d9a40lt2lq7pp2v7h4c5jx

OSINT availability is time sensitive

(but don't worry…)

https://tallyco.in/s/lzxccm/
redirected to
https://tallyco.in/
currently redirects to
https://tallycoin.app/

- **The donation page now redirects to a login page!**
- **As situations change, sites tend to get locked down**



WHAT WERE THE MOTIVATIONS BEHIND THE DONATIONS?

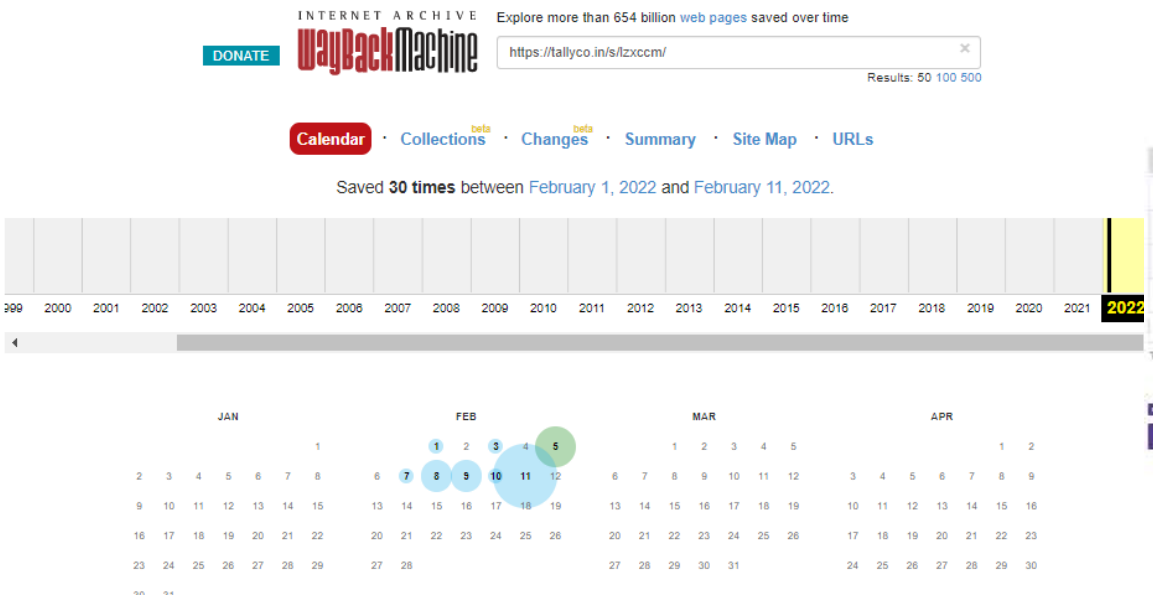
Exercise: Internet Archive

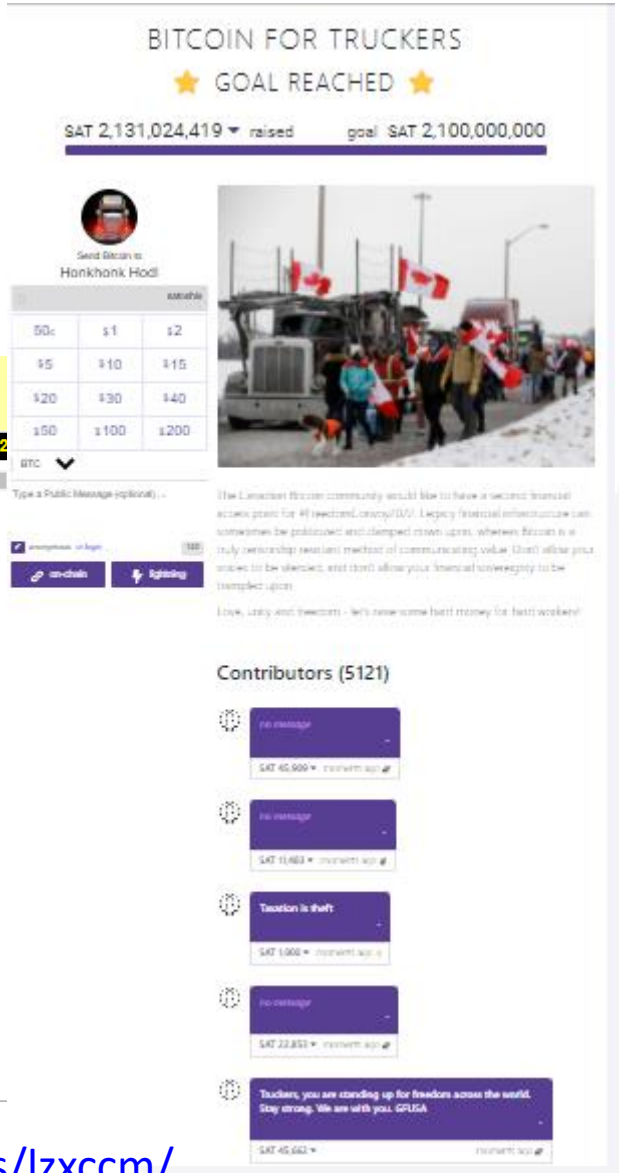
- A locked down site's content may remain available via snapshots taken by the **Internet Archive**.

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/

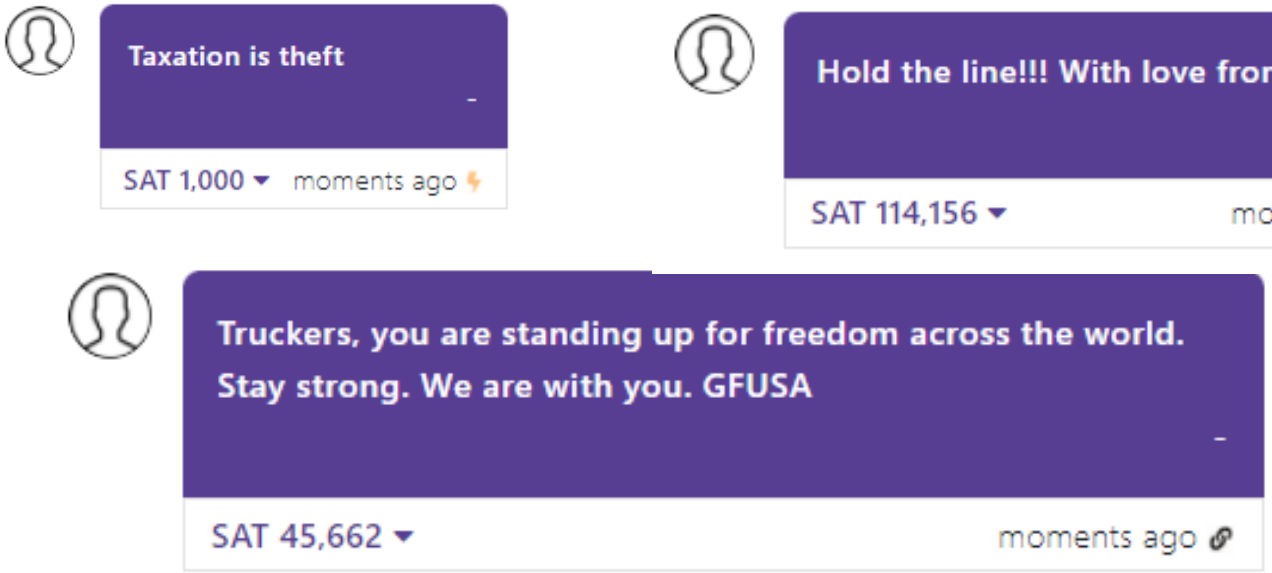




Each of the snapshots shows 500 donations and **associated messages**.

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

Users were able to post messages when they donated



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

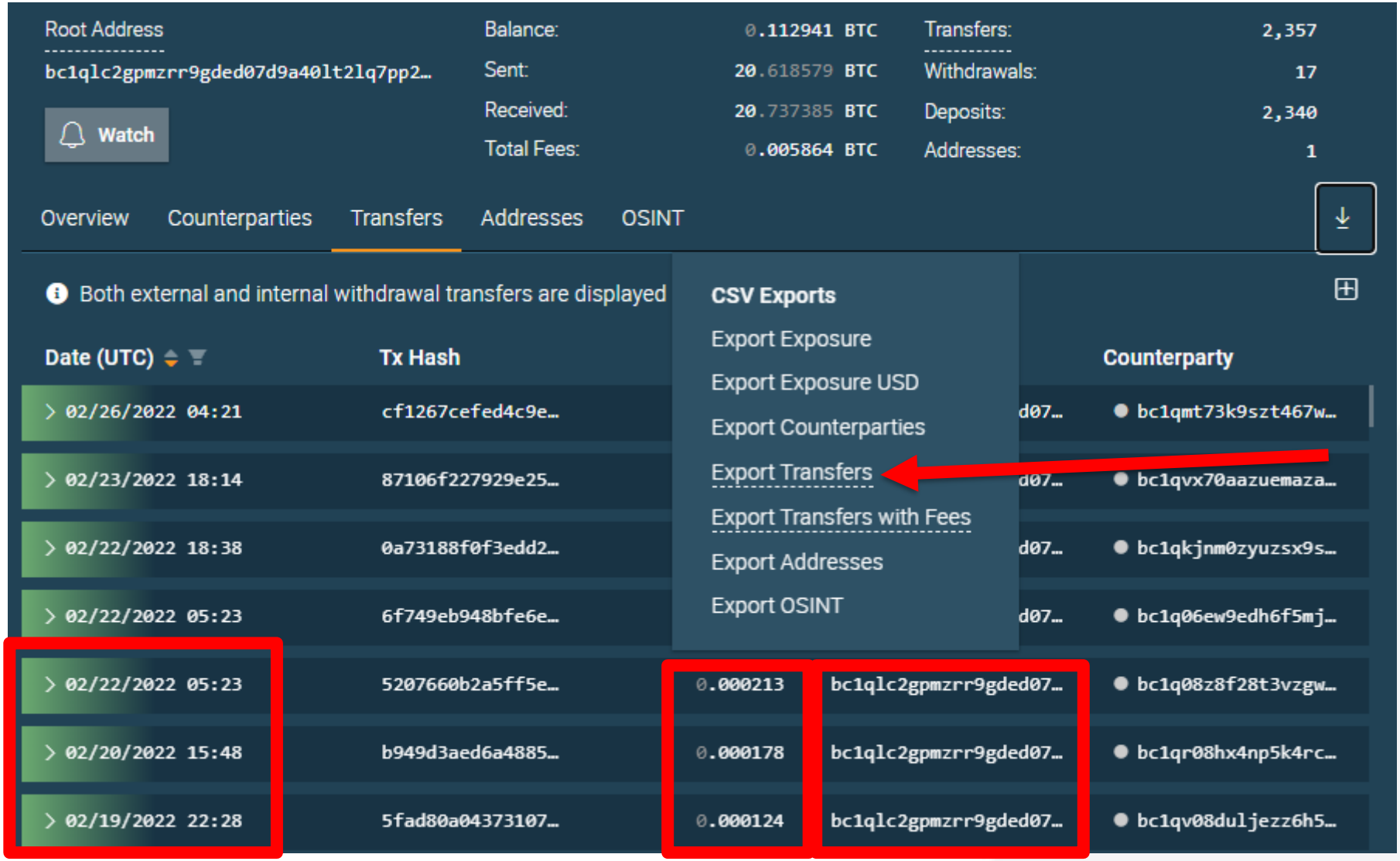
1 BTC= 100 Million Satoshis

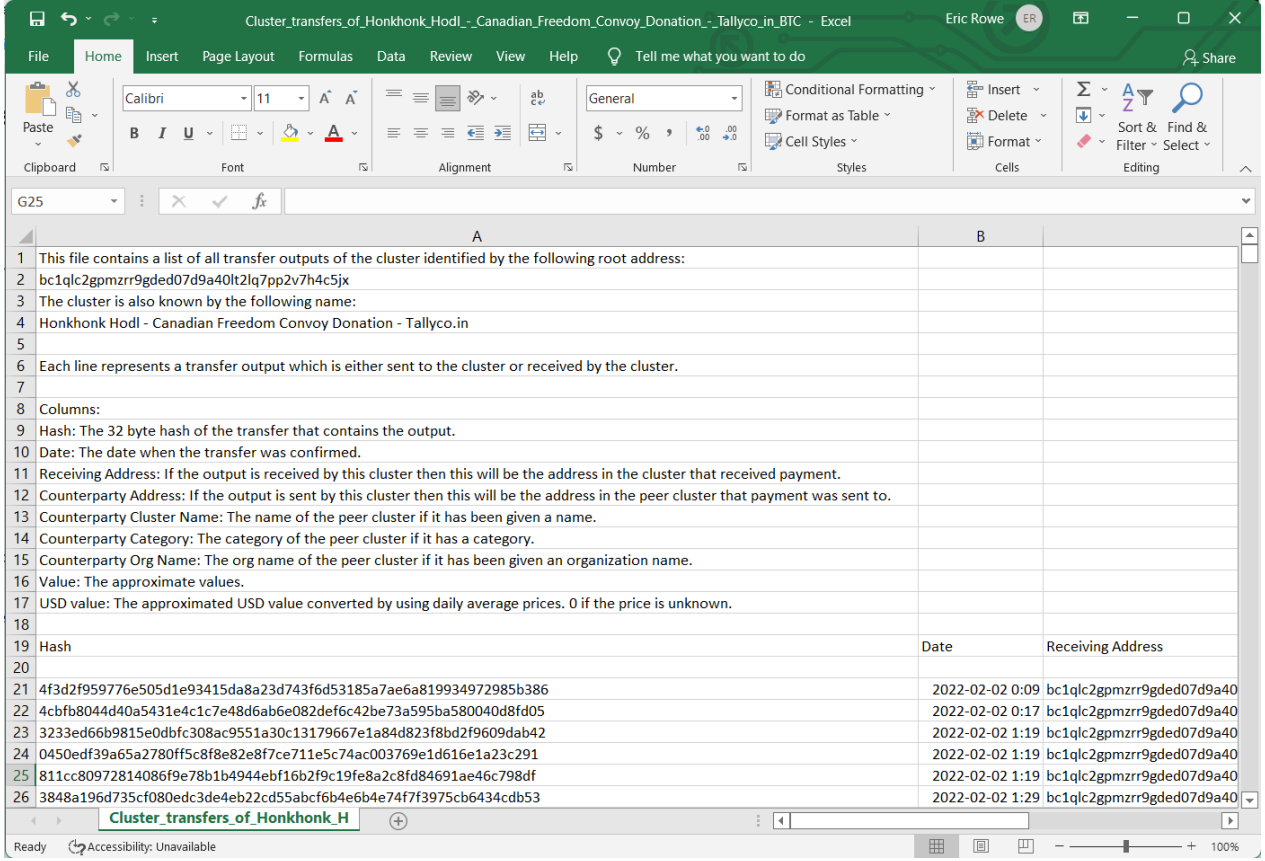
Chainalysis

- 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





Cluster_transfers_of_Honkhonk_Hodl_-_Canadian_Freedom_Convoy_Donation_-_Tallyco_in_BTC - Excel

Eric Rowe

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

Paste Clipboard Calibri 11 Font Alignment General Number Conditional Formatting Format as Table Cell Styles Styles Insert Delete Format Cells Sort & Filter Find & Select Editing

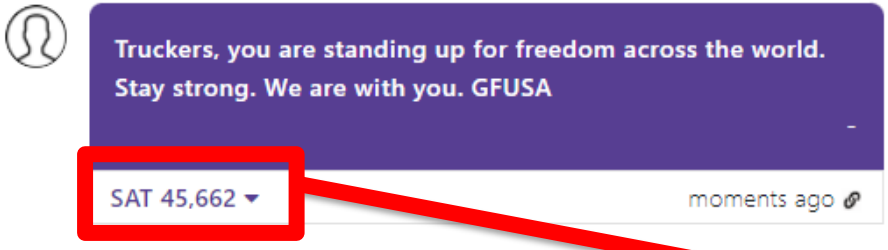
G25

	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 100%

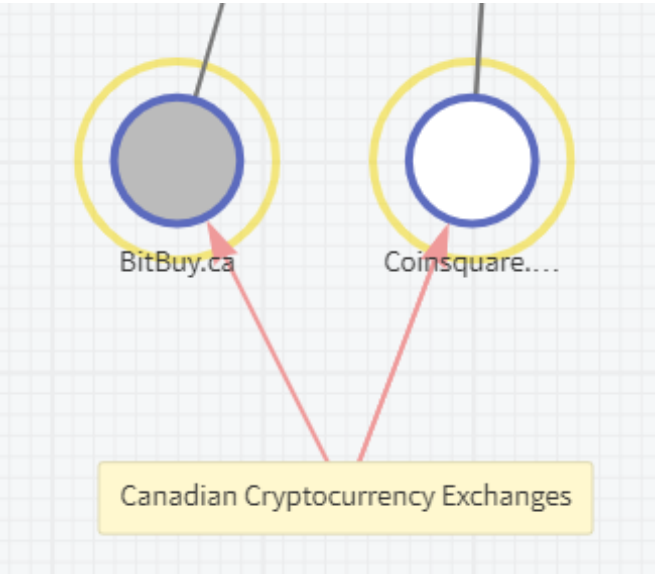
Value	USD Value
0.00025734	9.94711
0.00122121	47.38708
0.00002587	1.00172
0.00129515	50.15014
0.00269025	104.17049
0.00002581	0.99565
0.0012938	49.90997
0.00519532	200.41602
0.00517761	199.98441
0.0005	19.31242
0.01071829	413.99234
0.00012925	5.00475
0.00077416	29.97663
0.000693	26.83399
0.00051623	19.96619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

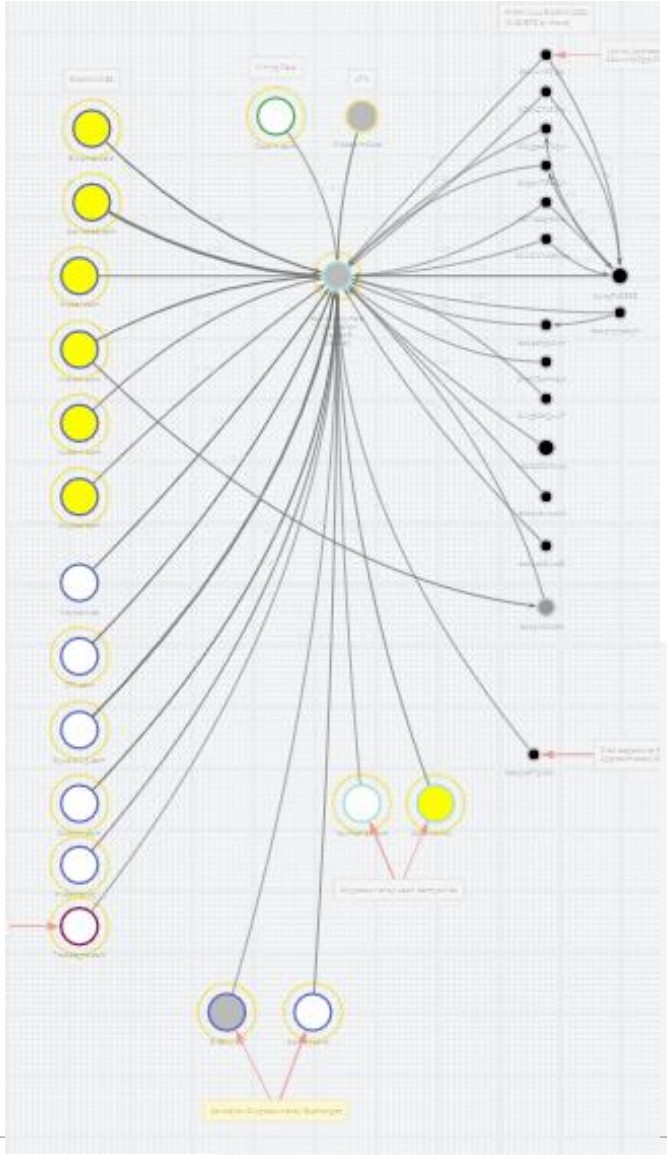


			0.00114139	49.68661
Coinbase.com		exchange	0.00045662	19.93549
			0.0002291	10.00224

Donations from Exchanges & Large Donations

- **One donation was for 5 BTC ($250,000 CAD)**
- **Many donations came directly from Exchanges**

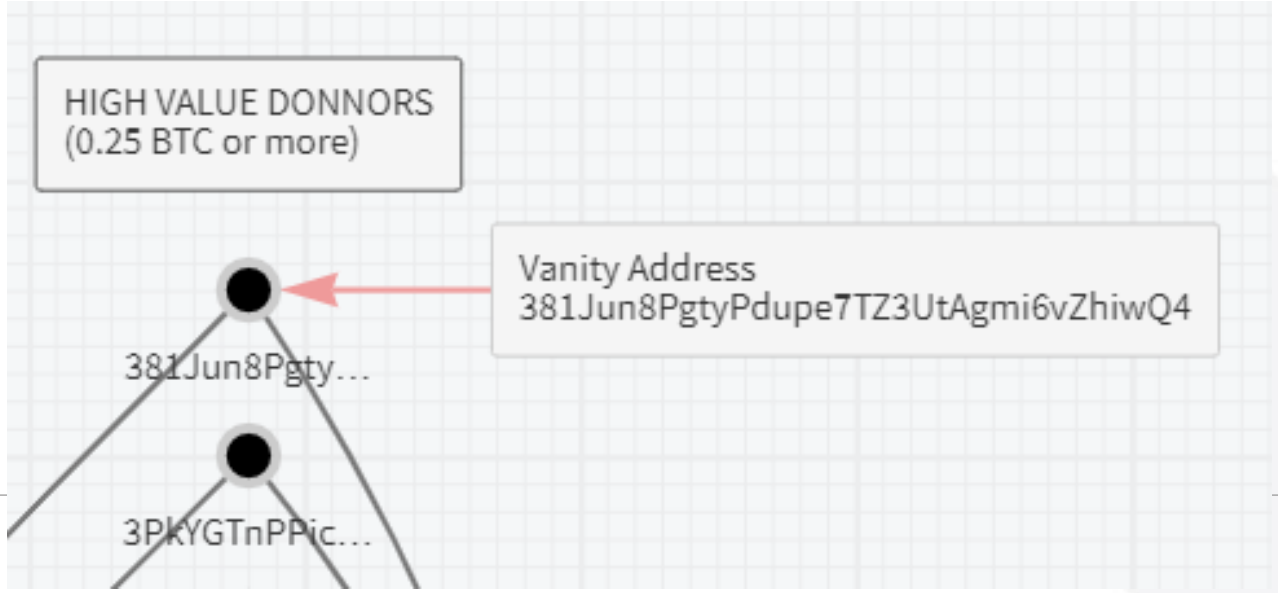




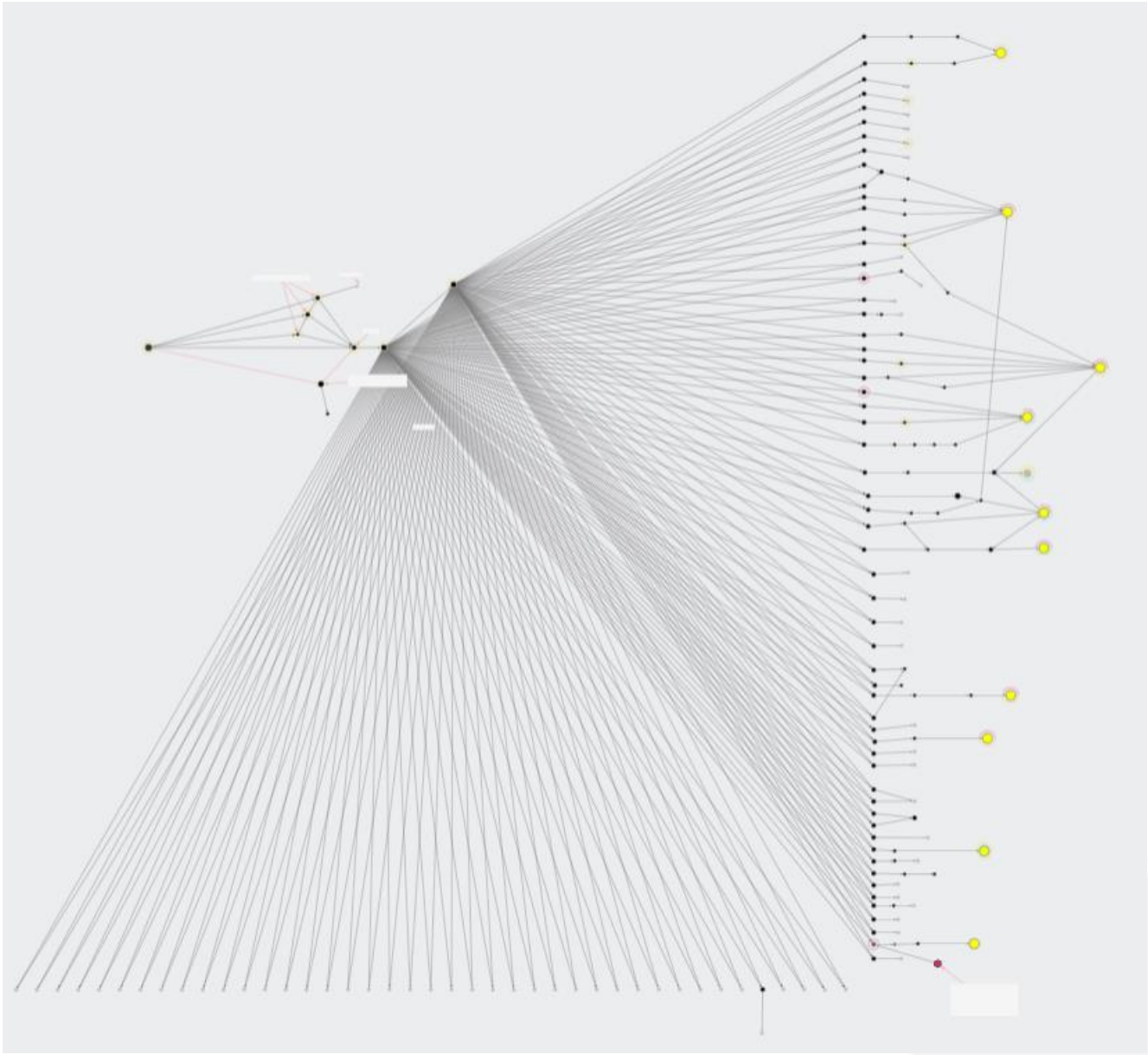
One large donation used a “Vanity Address”

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?

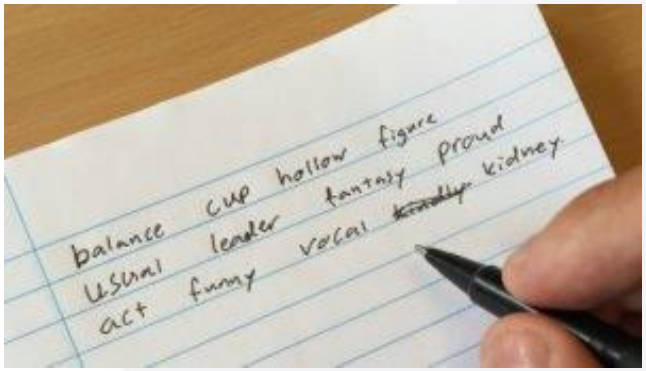


WHAT ACTIONS DO THE GRAPHED TRANSACTIONS & ADDRESSES REPRESENT?



Trucker Payouts

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



Disbursement was discussed on Twitter feeds and other social media

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet

← Thread

Peter Todd
@peterktodd

I need to talk about distributing BTC funds to truckers.

This is a complex topic, and aspects of it are quite counter-intuitive.

First, let's start with what a protest actually is, and what it accomplishes:

Tim Pastoor (@timp@x0f.org) @timpastoor · Feb 18
Trucker receives $8k in bitcoin on livestream:
Show this thread

B diplomat
@NobodyCaribou

This thread is worth a read for those who want to understand the complex situation we are dealing with in Ottawa re: distributing btc funds to truckers

Peter Todd @peterktodd · Feb 18
I need to talk about distributing BTC funds to truckers.

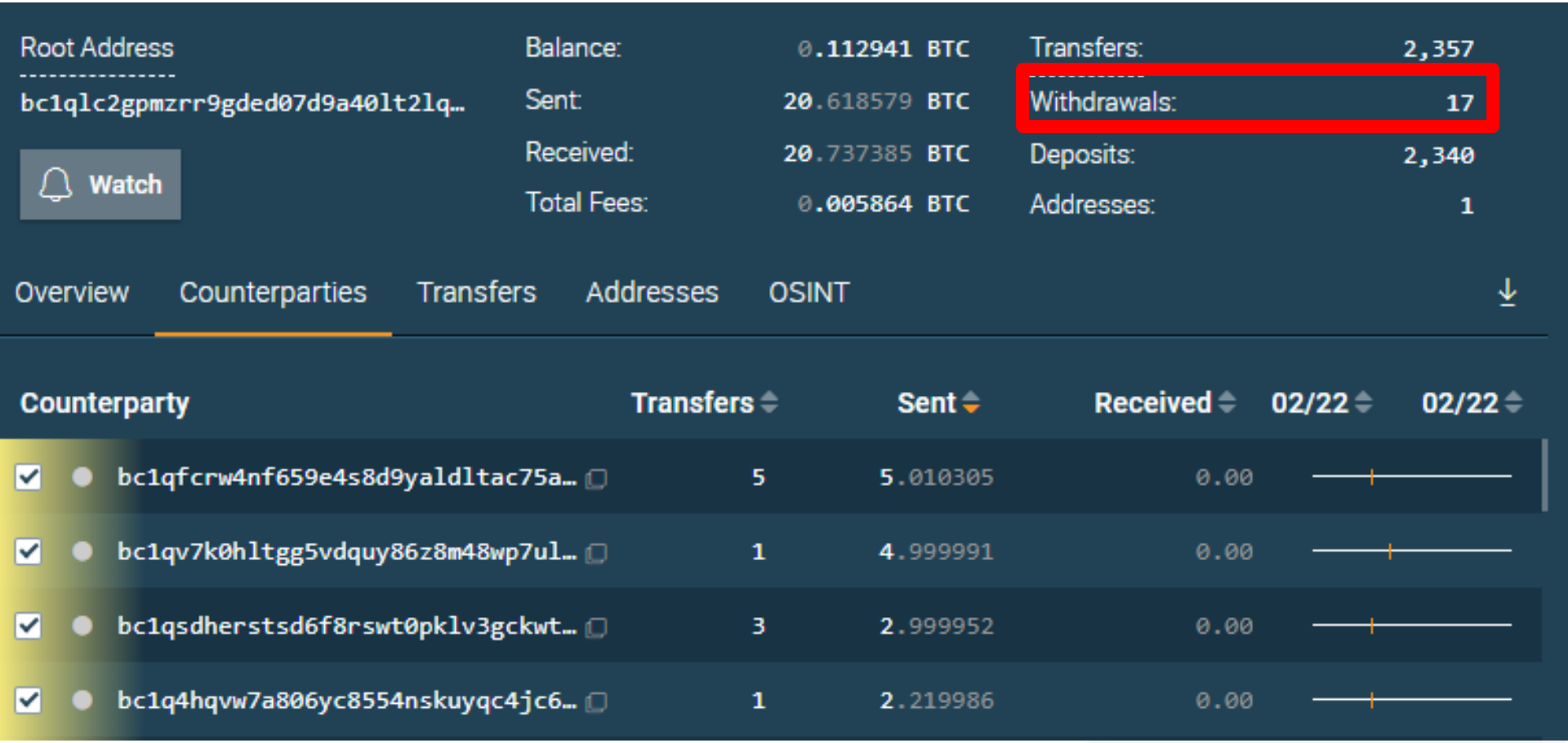
This is a complex topic, and aspects of it are quite counter-intuitive.

First, let's start with what a protest actually is, and what it accomplishes:
twitter.com/timpastoor/sta...
Show this thread

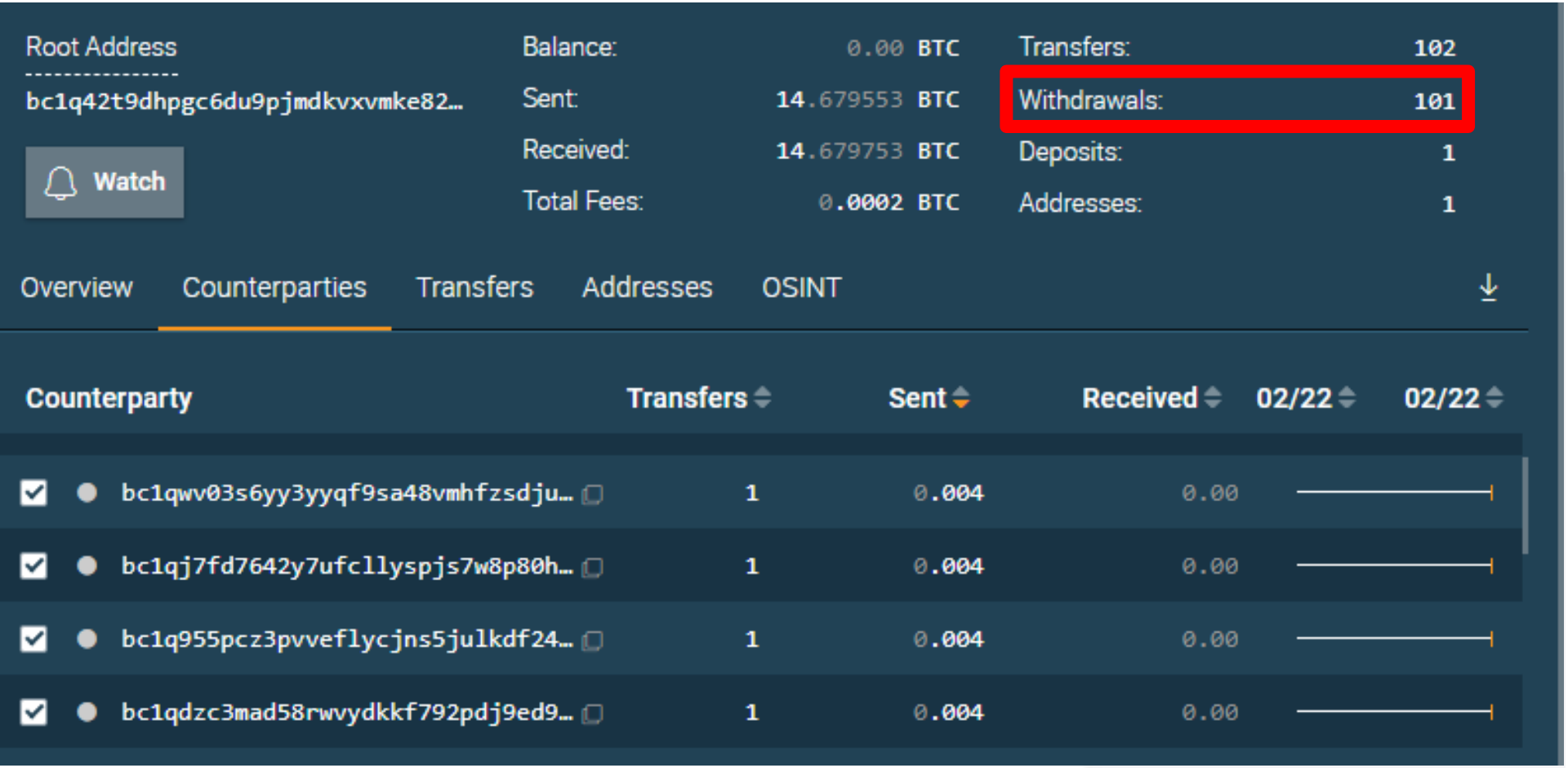
5:49 PM · Feb 19, 2022 · Twitter for iPhone

https://twitter.com/peterktodd/status/1494776972777558021
https://twitter.com/NobodyCaribou/status/1495093206194741264

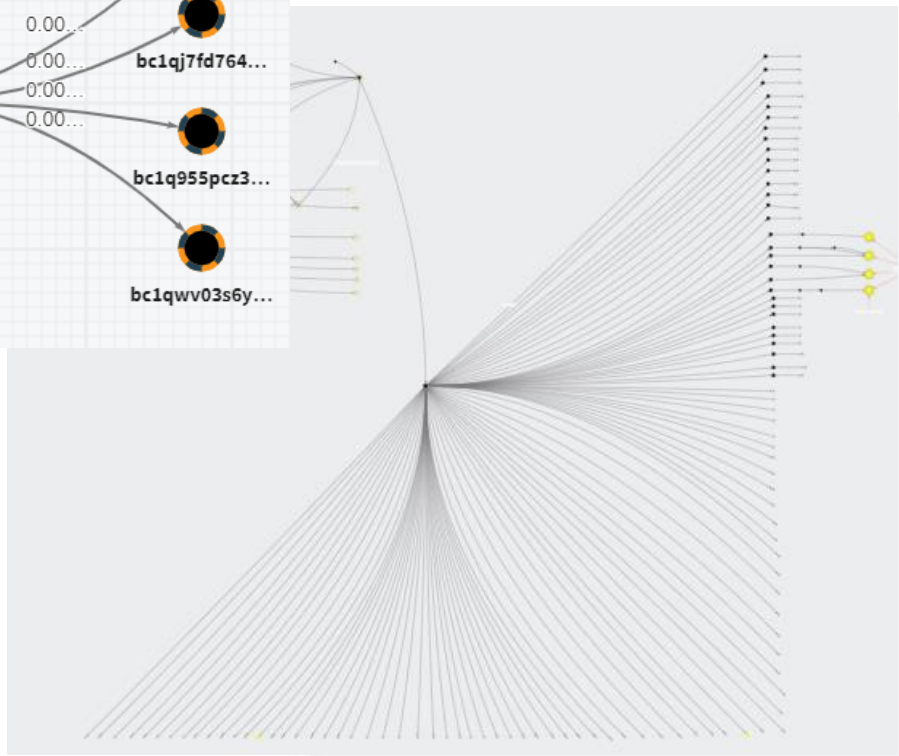
HonkHonk Hodl donation address shows 17 Withdrawals to 11 Addresses



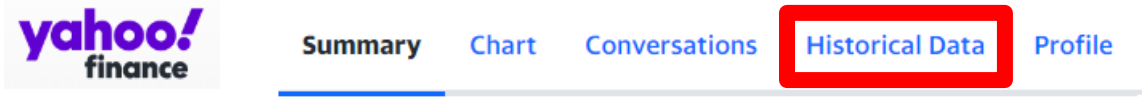
If we follow the bitcoins we find transfers of small amounts to 101 addresses



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



Exercise



1. Go to Yahoo Finance for BTC to CAD

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

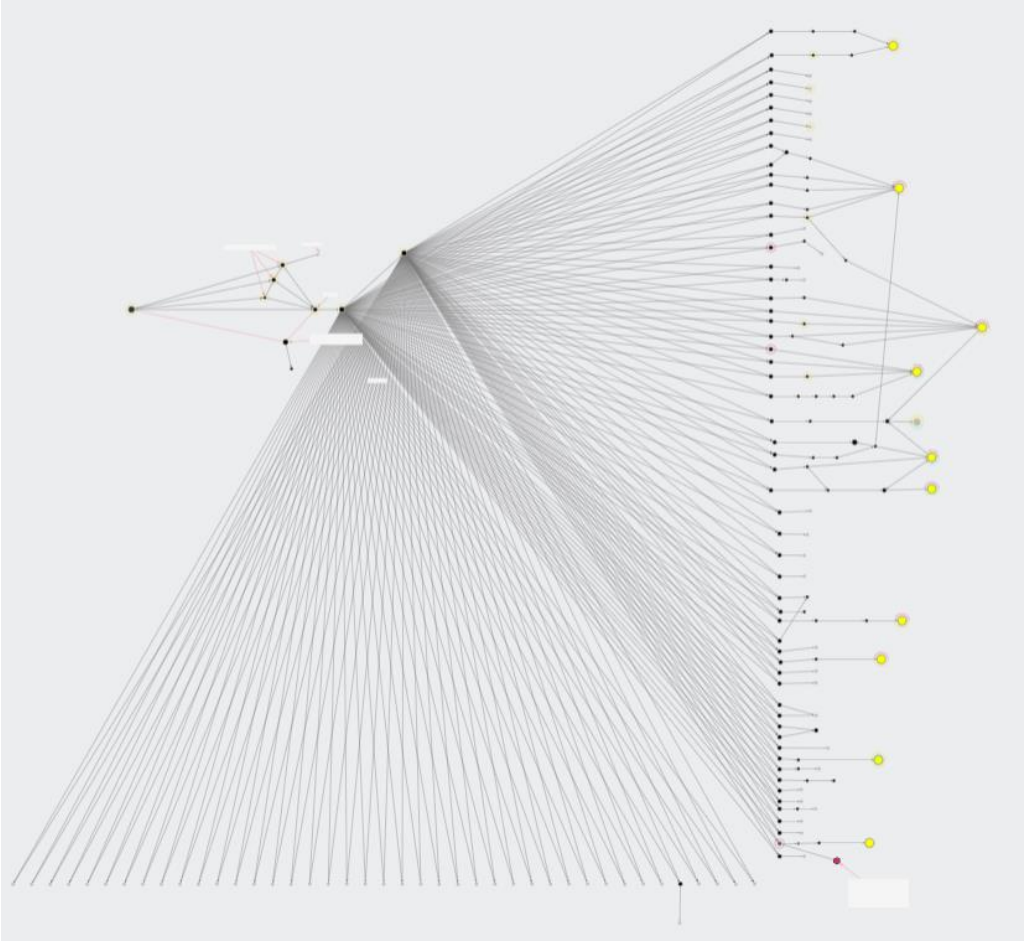
2. Navigate to the **Historic Data**
3. Look up how much 1 BTC was worth in CAD on 14 February 2022
4. Calculate how much 0.14 Bitcoins were worth
5. Compare this amount to the $8000 amount mentioned in the YouTube video

Chainalysis – Disbursement Graph

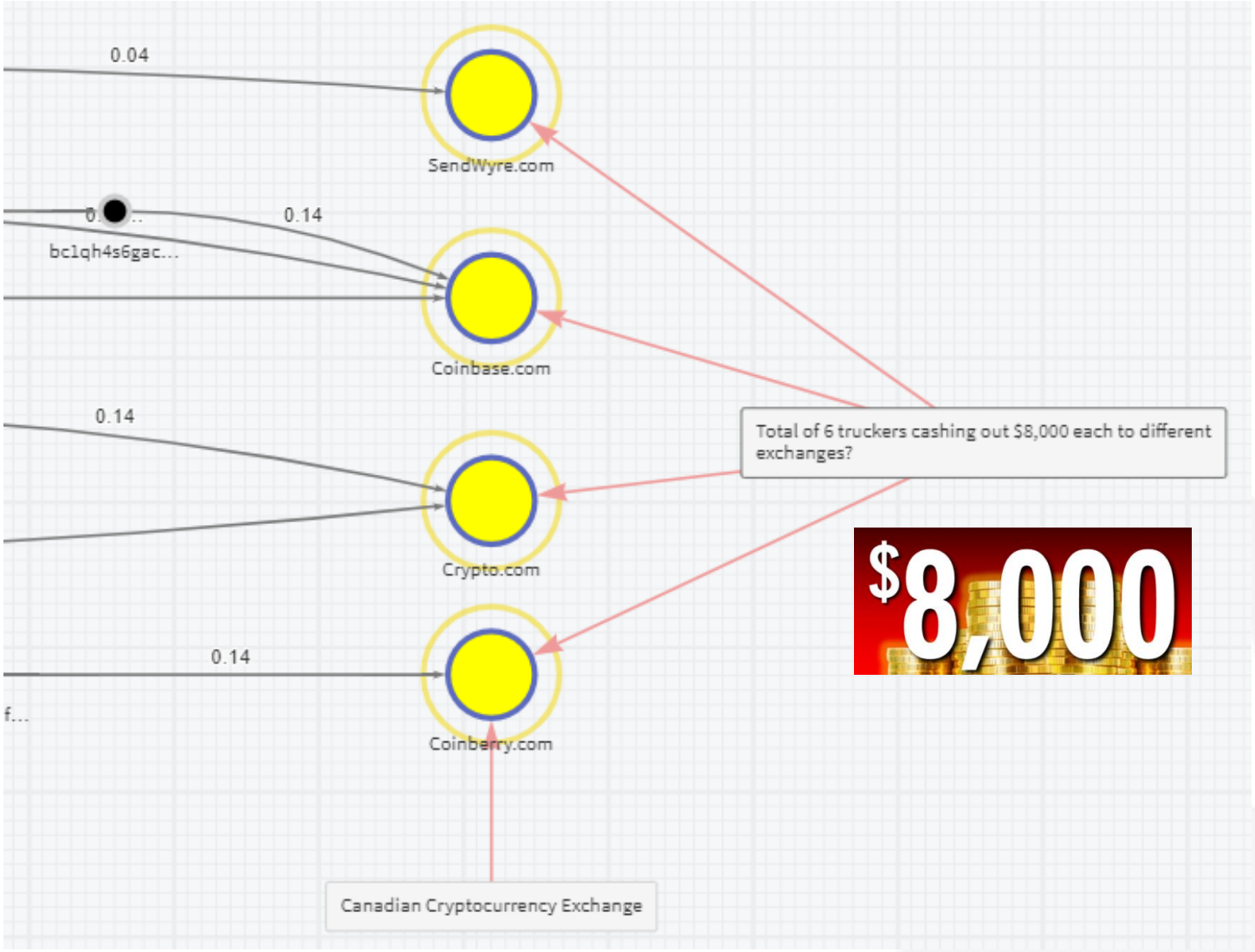
Donation site is on the far left.

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

Far right are addresses cashing out at exchanges.

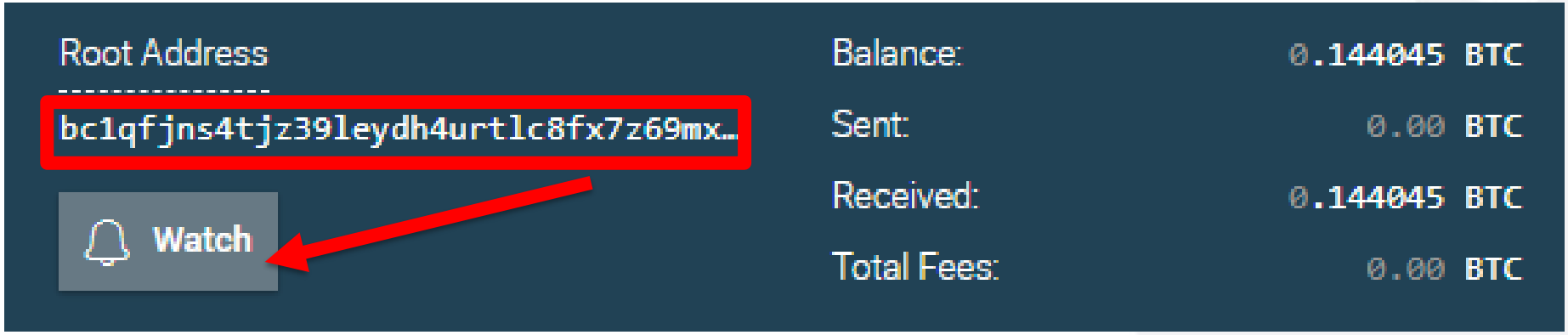


Truckers cashing out at Exchanges

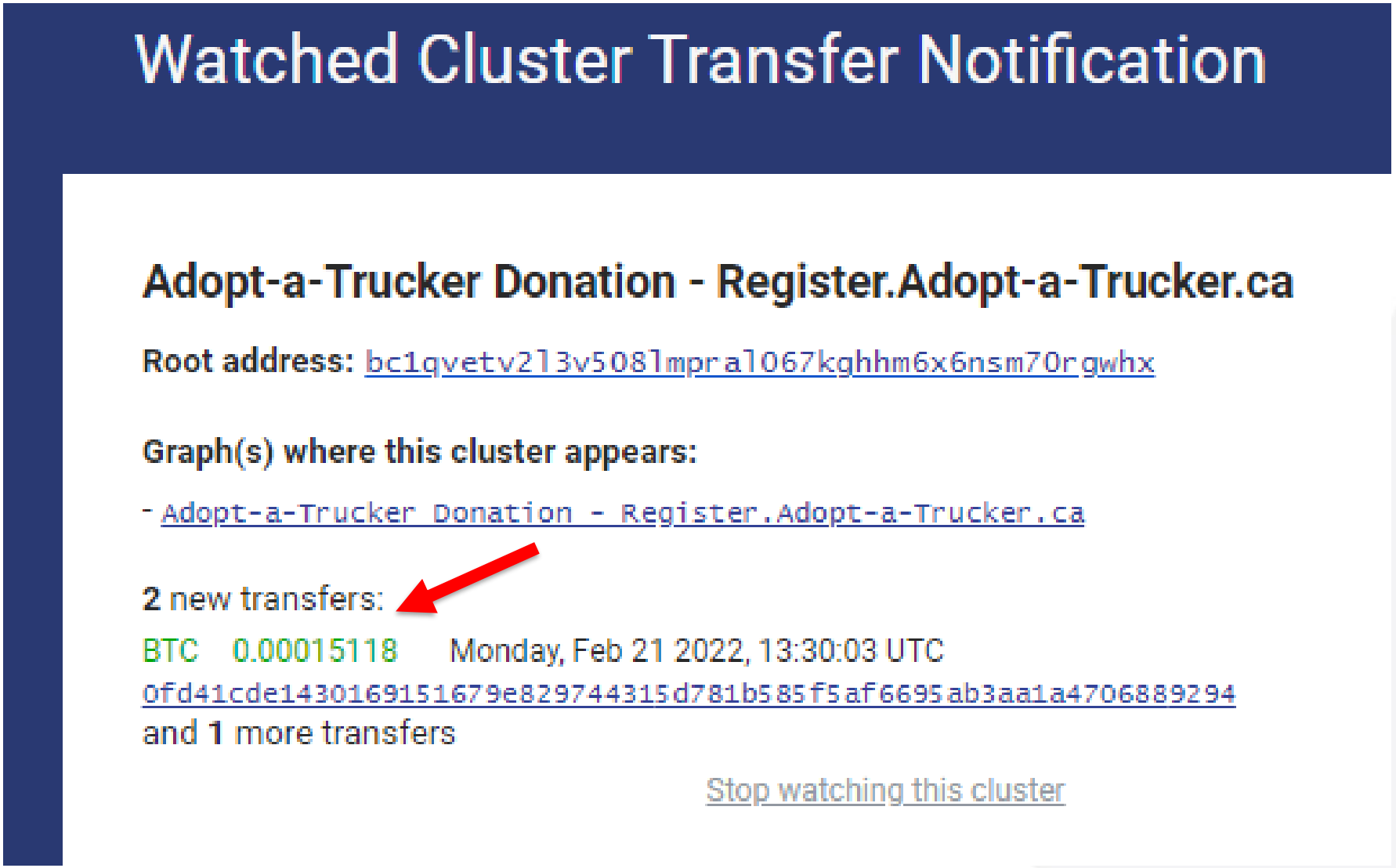


Movement of cryptocurrency out of the $8,000 addresses can be monitored by tools (e.g. Chainalysis)

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



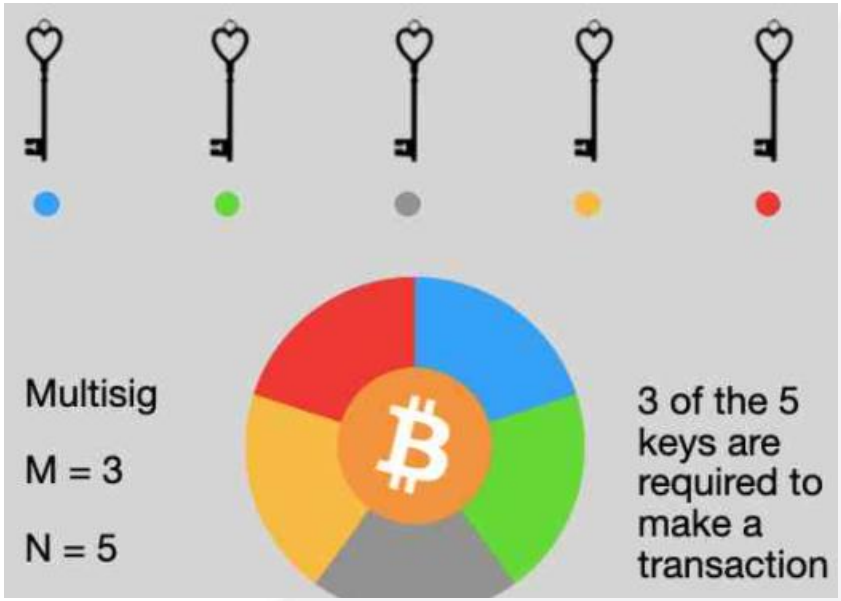
Notifications of transfers may be sent via Email to the investigator



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 by the HonkHonkHoddle organizers?

- If multi-signature address are being used, this 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 the addresses.
- Identifying who may hold the keys helps help you coordinate searches.
- Seed Word Lists may help?

Exercise

Google: "**Freedom Truckers Multisig Bitcoin**"

1. Are there indications that multisig addresses were used?
2. How many keys were created?
3. Can you find the names of any key holders?
4. How many keys will be required to seize?
5. What wallet was used?

Are the donation addresses "multisig"?

A committee of five bitcoin advocates — Bitcoiner Greg Foss, YouTuber BTC Sessions, Nobody Caribou, author Jeff Booth and Bull Bitcoin CEO Francis Pouliot — have organized bitcoin fundraising using Twitter and fundraising site Tallycoin.

Committee member Foss told *Bitcoin Magazine* that donations to the official bitcoin wallet will be anonymous and safe. The donations are being stored in a multisig wallet, so in order to access the donated funds the wallet requires three out of five key signatures to release any funds.

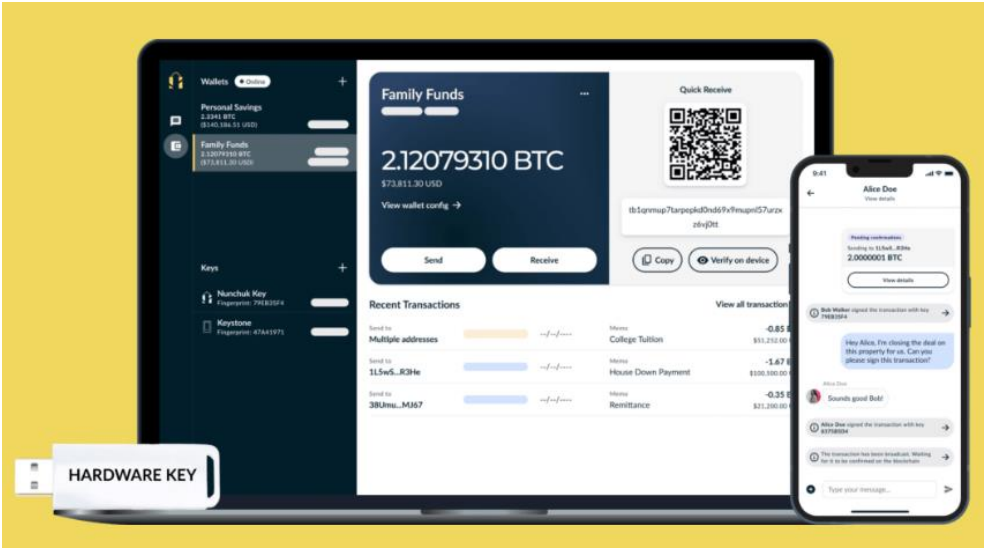
BITCOIN MAGAZINE®

https://bitcoinmagazine.com/culture/bitcoin-donation-drive-for-freedom-truckers

https://nunchuk.io/

NUNCHUK

80% of funds raised are being consolidated into a multisig wallet. They are using nunchuk.io multisig wallet because “it makes collaborative custody through multisig intuitive and easy to use for non technical users,” protest organizer and Bitcoin activist, Nobody Caribou told *Bitcoin Magazine*.

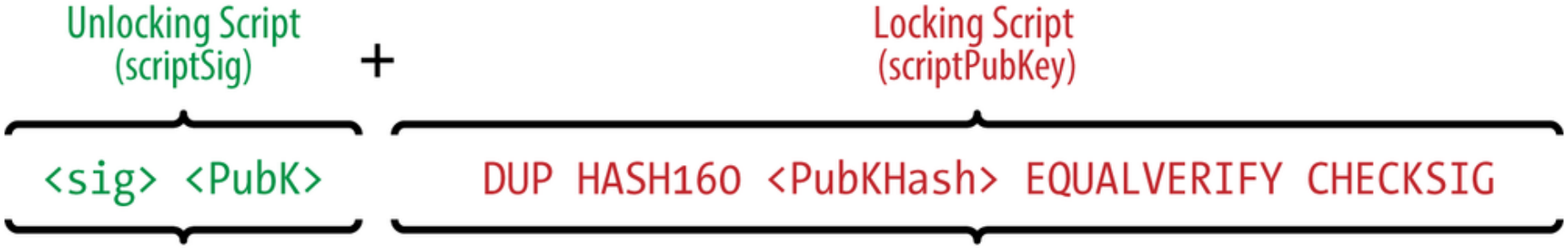


YOUR BITCOIN. GUARD IT.

Use Nunchuk multisig wallet

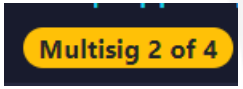
https://bitcoinmagazine.com/markets/bitcoin-fundraising-canada-ottawa-truckers-freedom-convoy

Bitcoin transactions are scripts



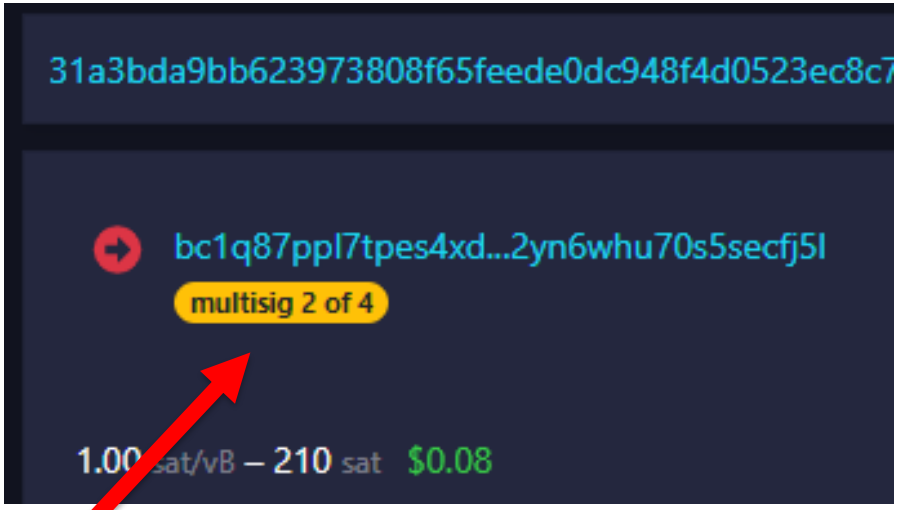
- Scripts may contain special instructions in the form of **OP_CODES**
  - Time Lock
  - **Multisignature**
  - Etc.
- Scripts are preserved on the Blockchain and can be accessed using a blockchain explorer

Multisig Transactions may be identified using a blockchain explorer

- When a multisig address sends cryptocurrency, it must use multiple signatures to authorize and sign the transaction.
- Multiple signatures in a sending transaction will be identified and tagged by some blockchain browsers such as **Mempool.Space**. 

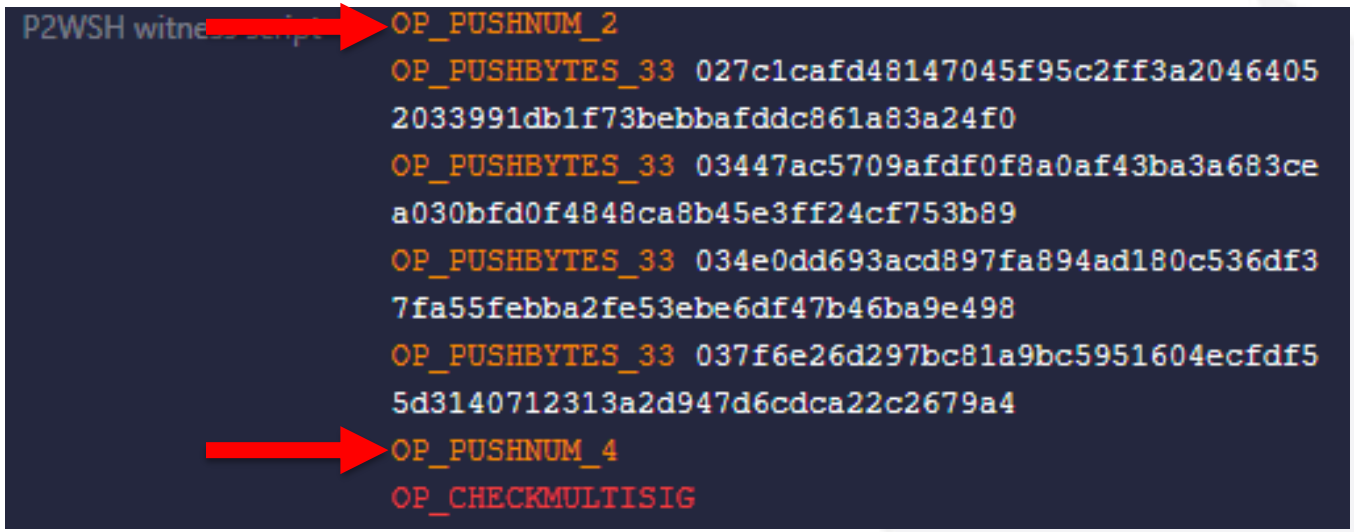
- If you want to know if an address is multisig and identify how many keys it has and how many are required to spend from it, you need to **look at its spending transactions**.

Multisig Transactions can be identified Using a Blockchain Explorer

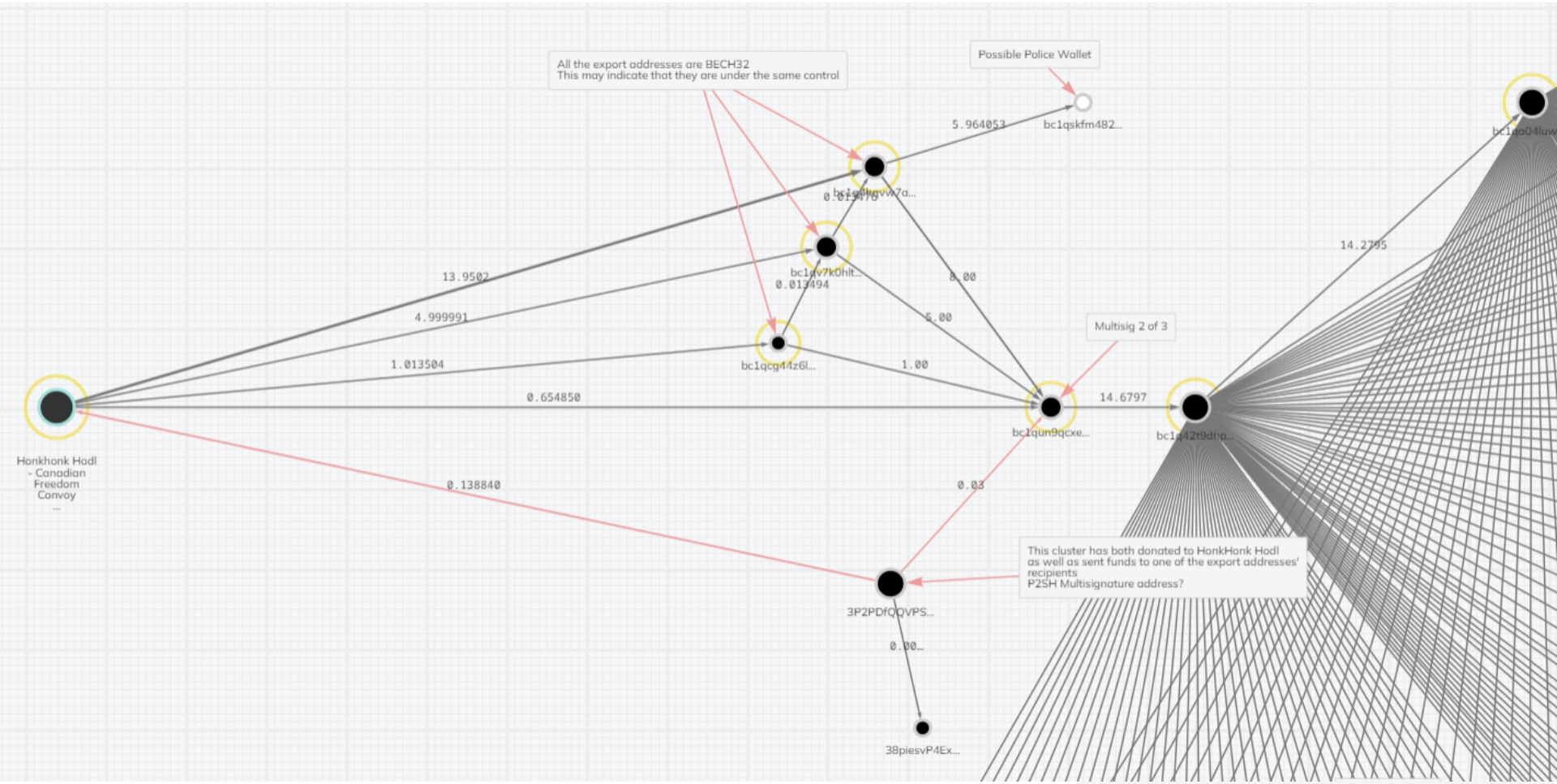


mempool.space

https://mempool.space/address/bc1q87ppl7tpes4xd9upan4q56fqes3h0vu2nzls8j3d2yn6whu70s5secfj5l



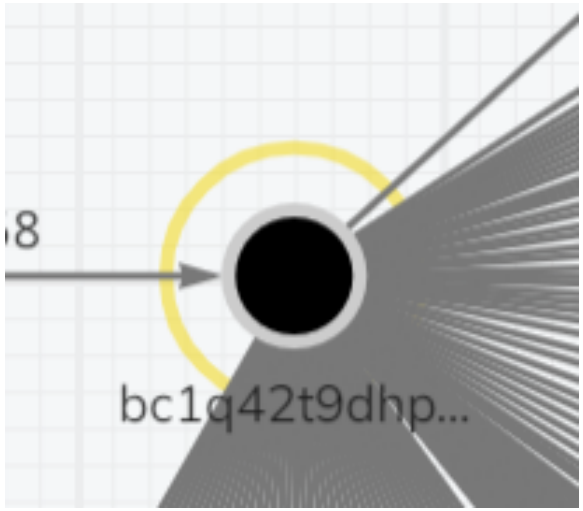
HonkHonkHodl Possible Multisig

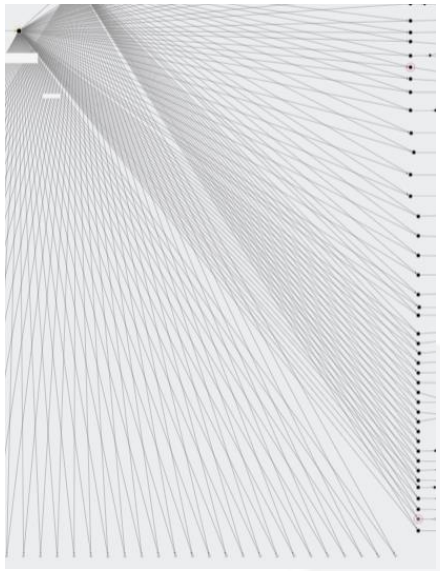


Exercise

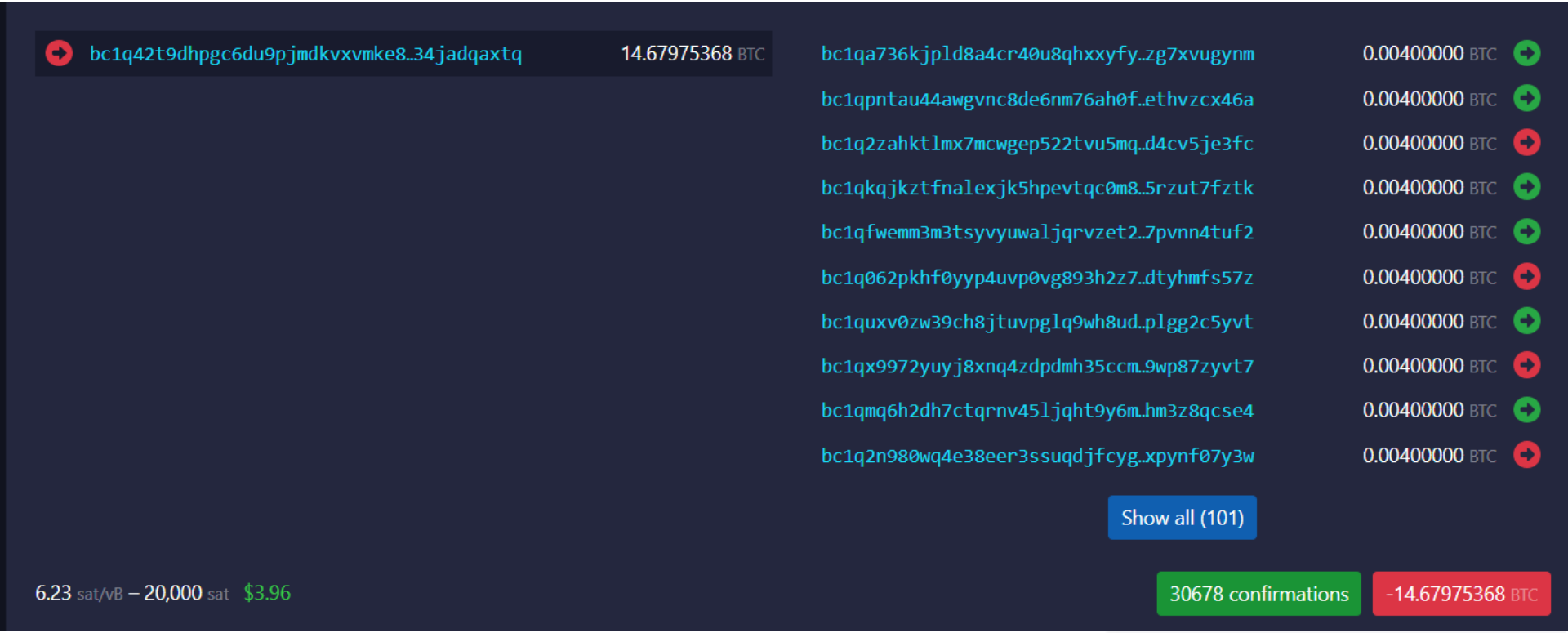
bc1q42t9dhpgc6du9pjmdkvxvmke82fl34jadqaxtq

1. Go to https://mempool.space/
2. Search for the address and determine whether it is multisig by looking at one of its **sending transactions**.



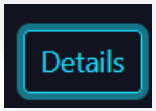


No Multisig bubble under the address

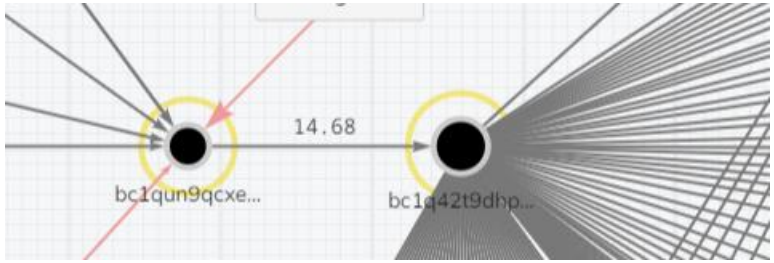


Exercise

bc1qun9qcxesc6avaa30anl0jvs36h3cy6nq7xh36yvx9frmqc8v6khq4nwnv0

1. Go to https://mempool.space/
2. Search for address **bc1qun9…**
3. Find it on the left hand side of a transaction (sending) and see if it has a multisig bubble.
4. Click on the ***transaction ID* aa73c785c…** to view the details of the transaction
5. Click on the **Inputs & Outputs "Details"** button 

6. Scroll down and look at the **P2WSH witness script**
7. What does it tell you?



bc1qun9qcxesc6avaa30anl0jvs36..6khq4nwnv0 0.03000000 BTC

Multisig 2 of 3

bc1qx499qzmpj4fa889tj8tfx0s32..rgtf6clhse 0.00010000 BTC

bc1qltgmfmv25gnj5298swxhdpxee..g2wq84g9ru 0.02988867 BTC

6.01 sat/vB – 1,133 sat $0.22

30712 confirmations -0.03000000 BTC

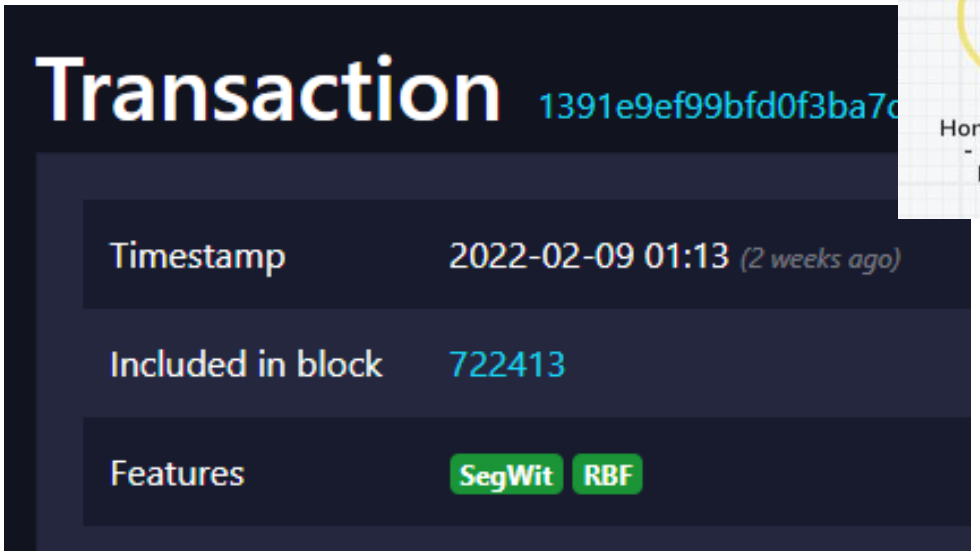
P2WSH witness script

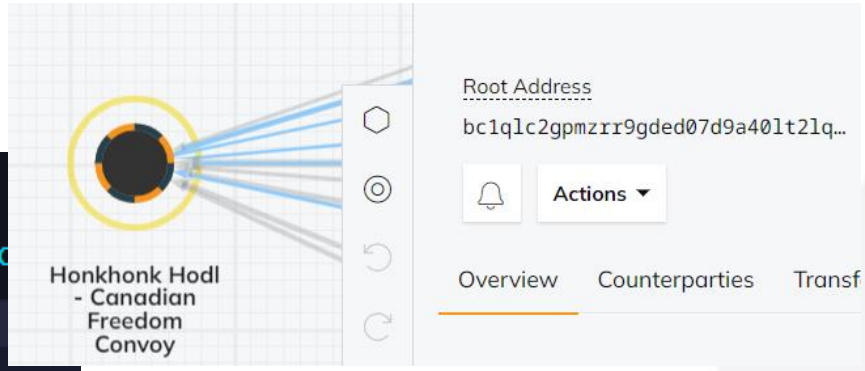
```
OP_PUSHNUM_2
OP_PUSHBYTES_33 027133445ff18c4164ab80f700ec7251c
af71ca38df5b020f7c690b5709a19e094
OP_PUSHBYTES_33 028c8c43b8523b5b2872e59b9571a0591
f756840c3b60dd16cd6a1fb3699472f8c
OP_PUSHBYTES_33 03c9b9ff3de4c712f13564d3aa12d3a9a
3eb157e9a360f86c8cd06e6cc18fdc130
OP_PUSHNUM_3
OP_CHECKMULTISIG
```

Is the HonkHonk Hodl Donation Address Multisig?

bc1qlc2gpmzrr9gded07d9a40lt2lq7pp2v7h4c5jx

- Sent large amounts to secondary addresses
- **Not Multisig**

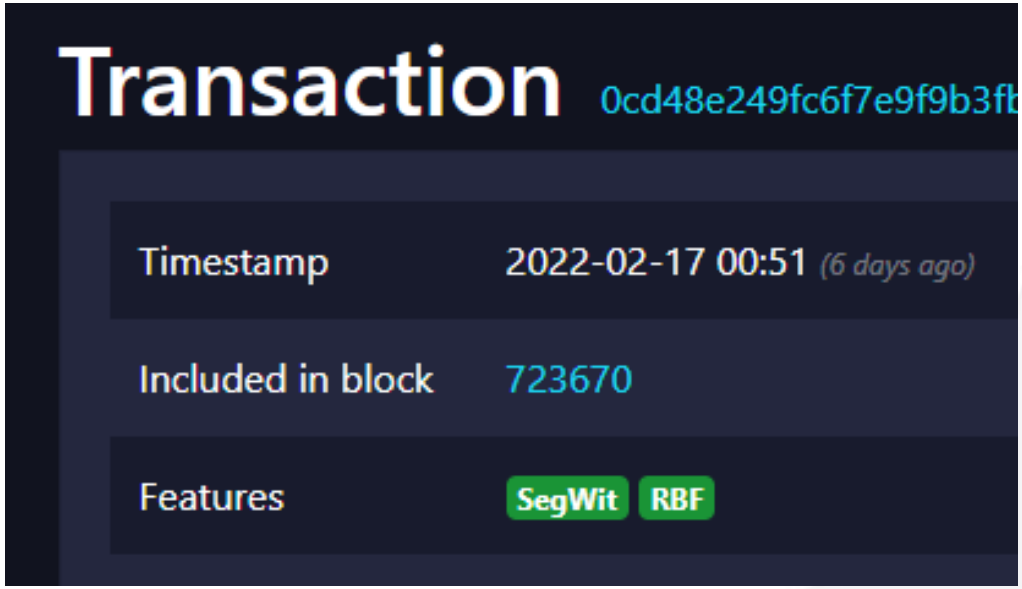




Is the Address that set up the wallets containing $8,000 Multisig?

bc1q42t9dhpgc6du9pjmdkvxvmke82fl34jadqaxtq

- Sent bitcoins to the $8,000 Trucker addresses
- **Not Multisig**



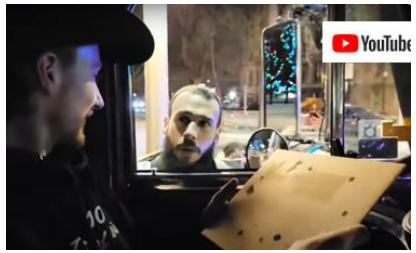
Multisig Conclusion?

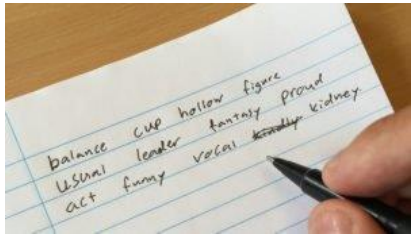
1. Was more than one individual moving bitcoins from the donation wallet?
   - **No**
2. Was more than one individual helping hold and move funds in an intermediate wallet?
   - **Yes**
3. Was more than one individual moving the bitcoins which eventually funded the 100 trucker wallets?
   - **No**

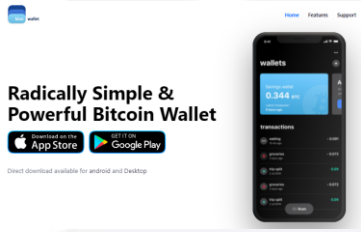
OSINT IMPLICATIONS FOR SEARCH & SEIZURE

OSINT & Search Implications

- **Search for:**
  - Donation envelopes
  - Seed word lists
  - Wallet set up instructions
  - Blue Wallets on digital devices
  - Nunchuck wallets on digital devices
  - Cryptocurrency exchange data in browser







OSINT – Seizure Implications

- Be prepared to re-create **Blue Wallets** on site
- Seizure should be possible with just one key/wallet

- Be prepared to recreate **Nunchuck Wallets** on site
- Seizure will be impossible without at least 2 keys

Postscript – Search & Seizure

VICE

The 'Freedom Convoy' Bitcoin Donations Have Been Frozen and Seized

Bitcoin was supposed to be a financial lifeline for vaccine mandate protesters in Canada. That hasn't exactly worked out to plan.

"Officers forcibly removed me from my apartment and took me to an unmarked police vehicle," St. Louis said. "Police wanted the seed phrases for my crypto wallets. Under police compulsion I provided my seed phrases."

https://financialpost.com/fp-finance/cryptocurrency/police-task-force-seized-some-crypto-connected-to-trucker-protest-fundraiser-says-in-court-documents

Postscript - Organizer comments

FINANCIAL POST

FP Finance / Cryptocurrency

Behind HonkHonk Hodl: The story of the trucker convoy's 'bitcoin team lead'

"***St. Louis said of his experience: "I think it took five years off my f—ing life."*** The lawsuit, he said, was the cost of supporting what he deemed to be "freedom-loving, law abiding, peaceful Canadians." **St. Louis started another bitcoin donation drive to fund his defence**."

https://financialpost.com/fp-finance/cryptocurrency/behind-honkhonk-hodl-the-story-of-the-trucker-convoys-bitcoin-team-lead

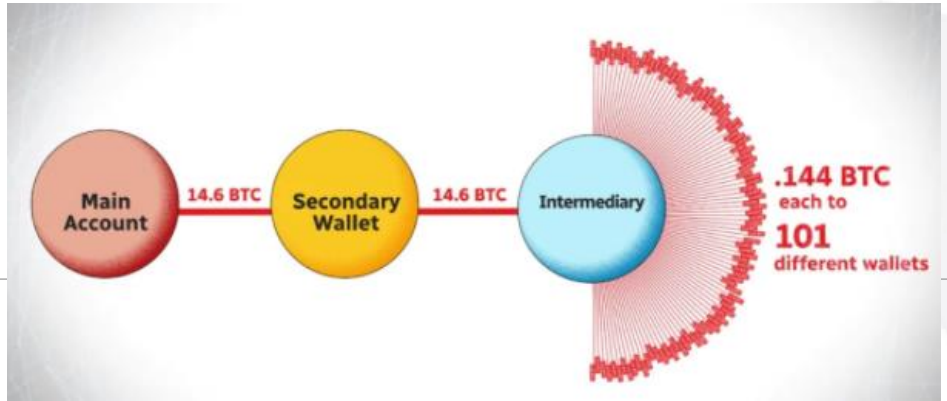
Postscript – Police Seizure

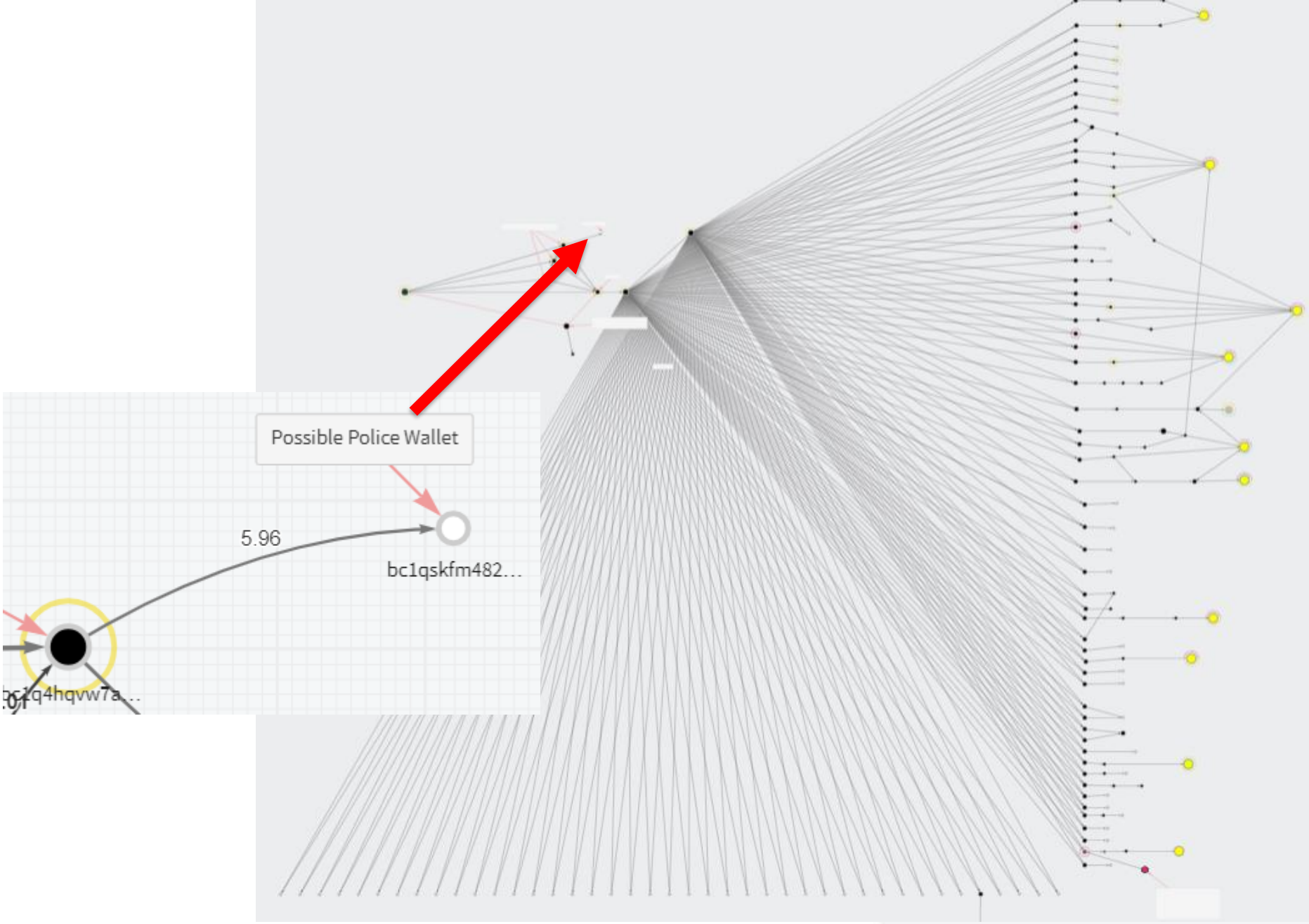
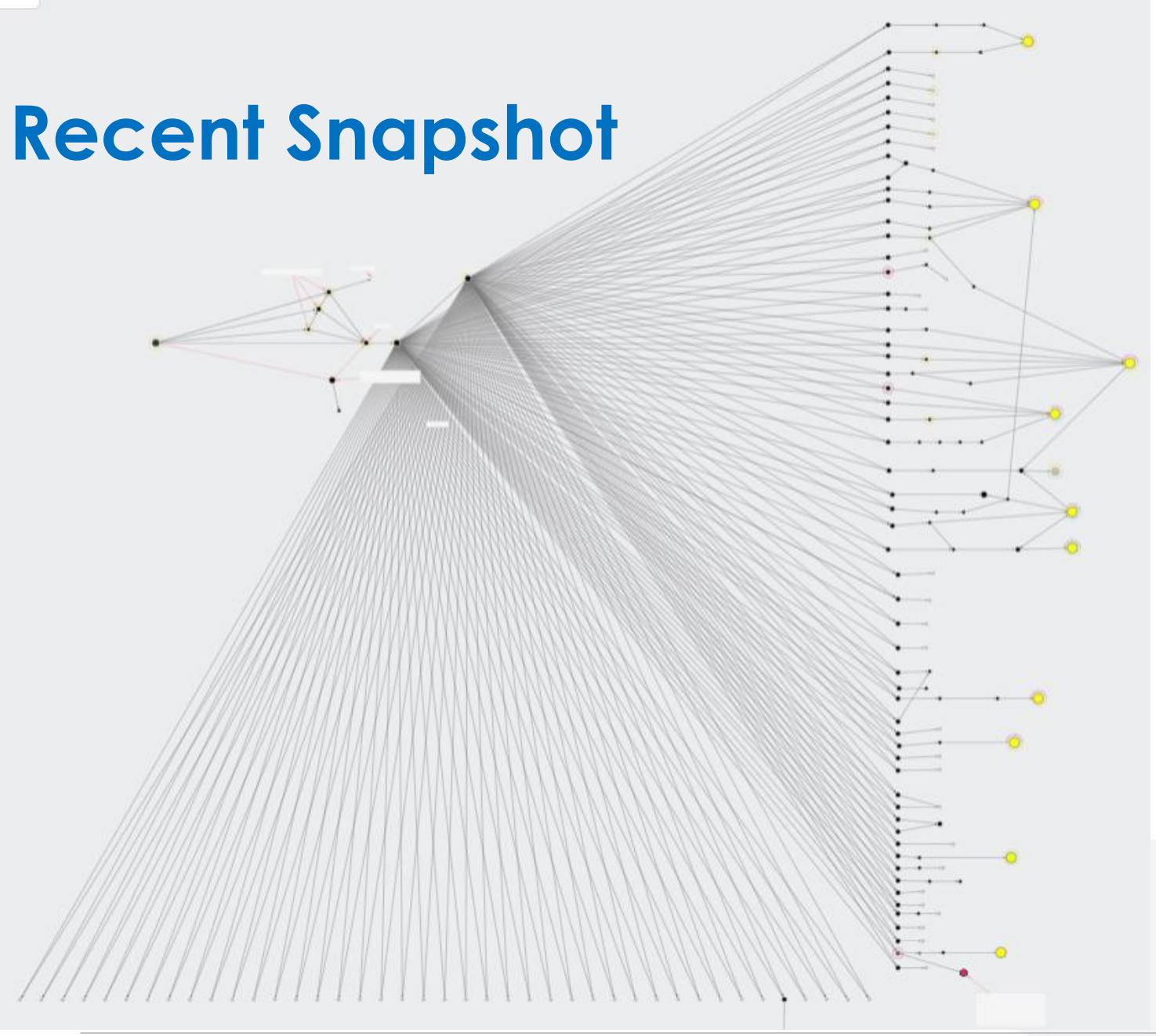
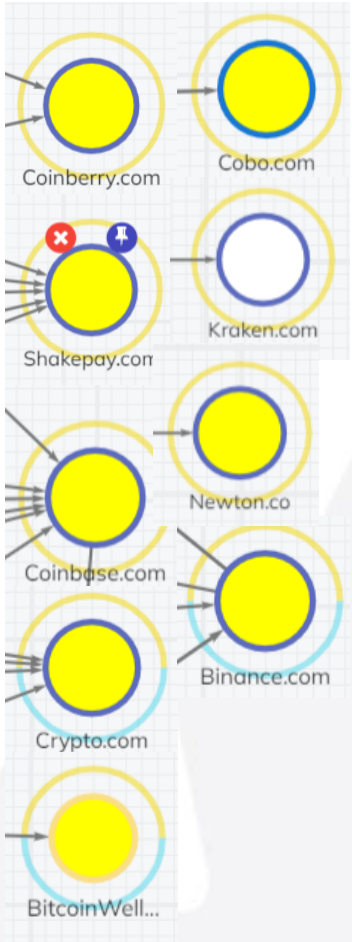
Ottawa · CBC Investigates

Digital currency donations for Freedom Convoy evading seizure by authorities

70 per cent of digital currency assets have been drained from original source

Most of the roughly $1 million in known donations raised in digital currency for the Freedom Convoy appears to have evaded seizure by authorities more than a month after the federal government invoked the Emergencies Act to freeze convoy assets, according to a CBC News investigation.




Possible Police Wallet
5.96
bc1qskfm482…

Recent Snapshot