



Canada Revenue
Agency

Agence du revenu
du Canada

Inteligencia de fuentes abiertas + Criptoactivos

Fuentes abiertas y trazabilidad: claves para entender el
panorama completo

Fuentes abiertas

- Muchos delitos relacionados con criptoactivos tienen un fuerte componente de fuentes abiertas.
 - Facebook / Twitter / Discord / Reddit
 - Metadatos de la blockchain
 - Etc.
- La información de fuentes abiertas permite comprender la actividad humana detrás de las transacciones observadas en la blockchain.
- La información de fuentes abiertas permite planificar mejor los registros e incautaciones

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.

Preguntas

1. ¿Qué valor en dólares recibió cada camionero en bitcoins?
2. ¿Qué método se utilizó para transferir los bitcoins? ¿Qué se les entregaba exactamente a los camioneros?
3. ¿Qué billetera se les indicó usar a los camioneros para reclamar sus bitcoins?
4. ¿Cuántas donaciones se realizaron a la campaña de recaudación?

La OSINT puede contribuir a la trazabilidad

- La OSINT puede ayudar a identificar qué actividades representan las transacciones registradas en la cadena.
- Puede revelar la intención detrás de dichas transacciones.
- Puede indicar si varias personas participaron en la ejecución de las transacciones.
- Puede mostrar si la incautación de activos virtuales requiere múltiples claves.

Fuentes OSINT durante la protesta de camioneros

- Publicaciones en redes sociales como YouTube, Twitter, Reddit, etc.
- Comentarios en páginas de recaudación de fondos
- Datos de la blockchain

Los manifestantes publicaban información en todos lados.

Twitter

- Vaya a la siguiente página de Twitter:
<https://twitter.com/HonkHonkHodl>
- ¿A qué sitio se dirigía a las personas para que hicieran contribuciones (por ejemplo, dejar propinas)?

Dos principales campañas de recaudación



- **Adopt-a-Trucker**



- Monto recaudado: bajo (10.000 USD)
- Se aceptaban múltiples criptomonedas
- **Las autoridades cerraron el sitio por infracciones a las políticas**

- **HonkHonk Hodl**



- Se recaudó una suma considerable (aproximadamente millones de USD)
- Solo se aceptaba bitcoin
 - Se habilitaron donaciones mediante Lightning Network
- **Se reforzaron las medidas de seguridad y privacidad del sitio**
- Todavía se siguen cobrando las donaciones



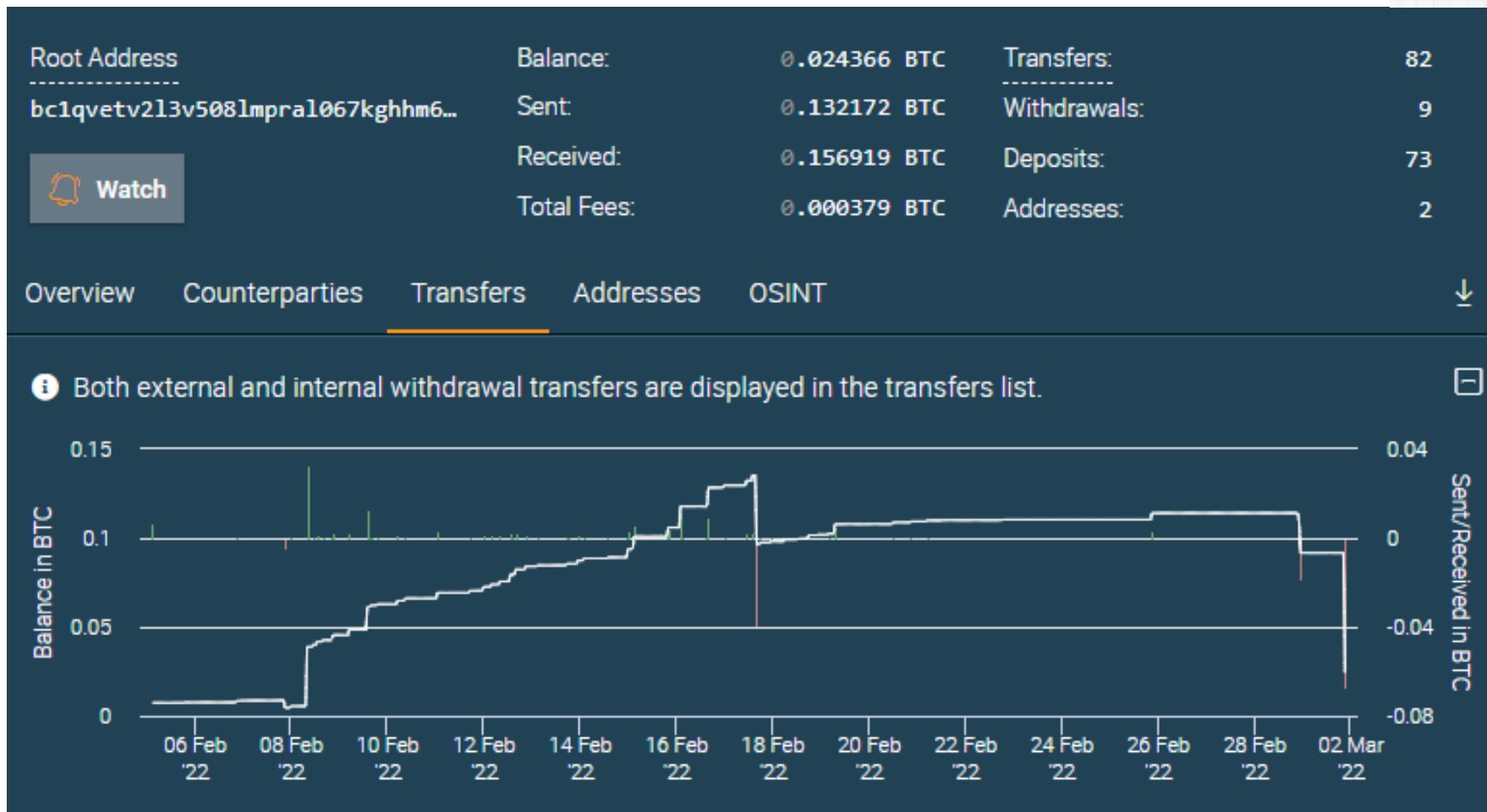
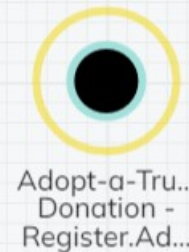
Adoptatrucker.ca



- **El sitio permitía realizar donaciones mediante sistemas de pago en moneda fiduciaria.**
- Estaba vinculado a GoFundMe.
- Se aceptaban bitcoin, ether y otras criptomonedas.
- La dirección de bitcoin comenzó a operar el 5 de febrero.
- Total de donaciones: aproximadamente 10.000 USD

Chainalysis – Adopt-a-Trucker

Cronología de las donaciones en bitcoin



La información sobre las donaciones de Adopt-a-Trucker se publicó en Reddit y 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	ltc1qqhzc2dflesccd5gx6ugqqcplzakrk8wxi8zq	
ADA	addr1qxwxppd3ahfsh43f88h4jn8ngrum64fe6meck3nnwkwgtsp6elsk4xhyrdtm5v6tnq3ulw9u9gcmvkhjrj4xcu3sm60hqtz3wuy	
XMR	423nPDQqsPrAagFSHaUBMrYQQCgb2562iLLWu1dZyEGEGsavxfpNxWtDjreSUzwqWQCxi6GrSz8jtYWjS4pW9mK9DoBvdWo	
ETC	0x88CD1D4611D456357eF8620450d3121672305d03	

Chainalysis identificó direcciones adicionales vinculadas a Adopt-a-Trucker.





BTC: bc1qvetv2l3v508lmpal067kghhm6x6nsm70rgwhx

ETH: 0x859481Ef7dAc321078547f50c756C8924EaB183f

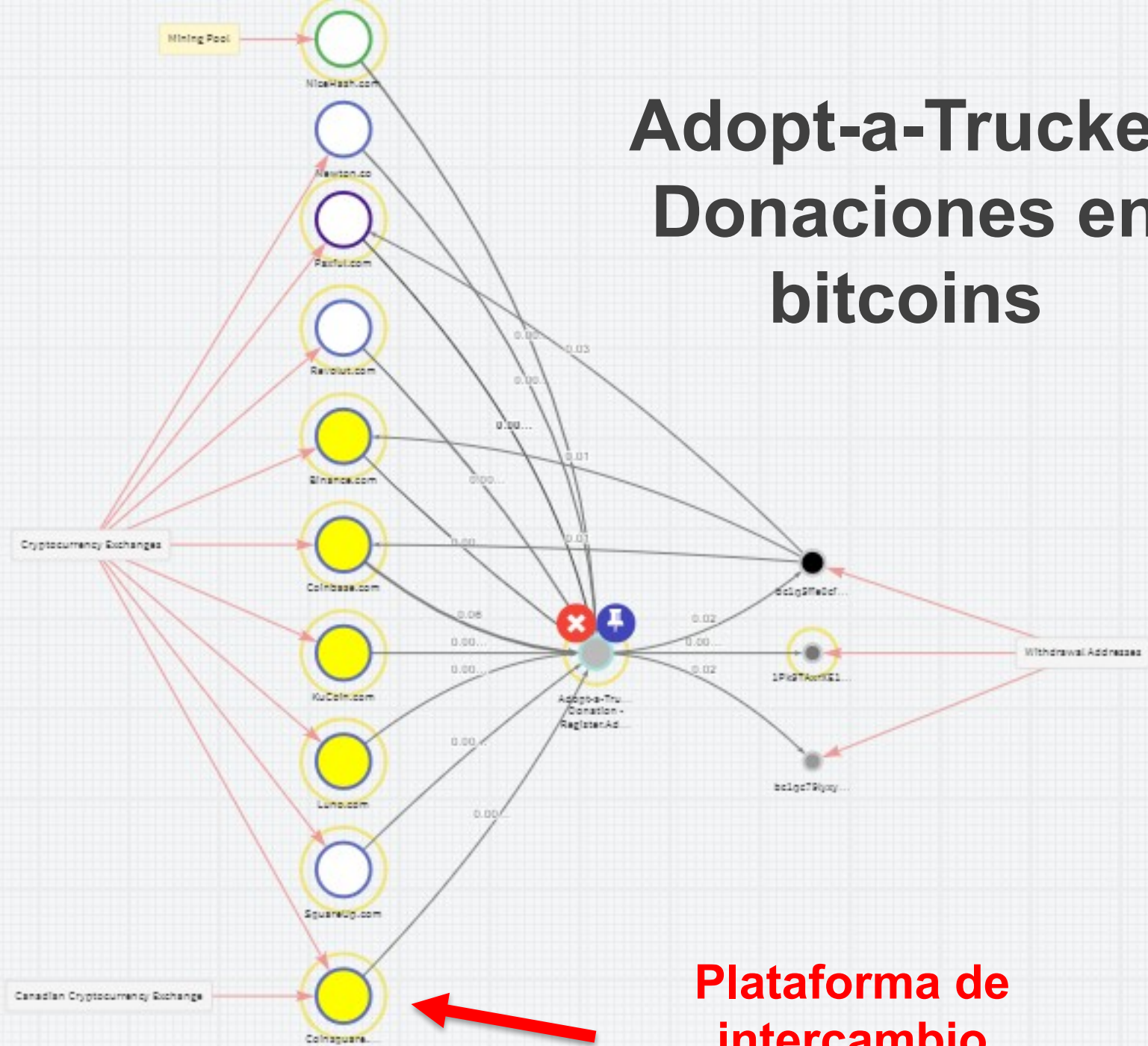
LTC: ltc1qqhzc2dflesccd5gx6ugqqgcplzakrk8wlxl8zq

Adopt-a-Trucker - Bitcoin

- Total recibido = 0,15325265 BTC (aproximadamente 7.620 CAD)
- 72 depósitos
- 3 retiros
- **La OSINT obtenida a través de Chainalysis reveló denuncias registradas en BitcoinAbuse.**

Overview	Counterparties	Transfers	Addresses	OSINT	↓
Source ▾		Date ▾ ▾	Subject ▾		
Chainalysis Identification		02/17/2022 12:00 AM	OTHER: RCMP - Cryptocurrency Alert 2022-02-15 bc1qvetv2I3v508Impral...		
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		

Adopt-a-Trucker Donaciones en bitcoins



**Plataforma de
intercambio**

Se creó después del cierre de GoFundMe/Adopt-a-Trucker

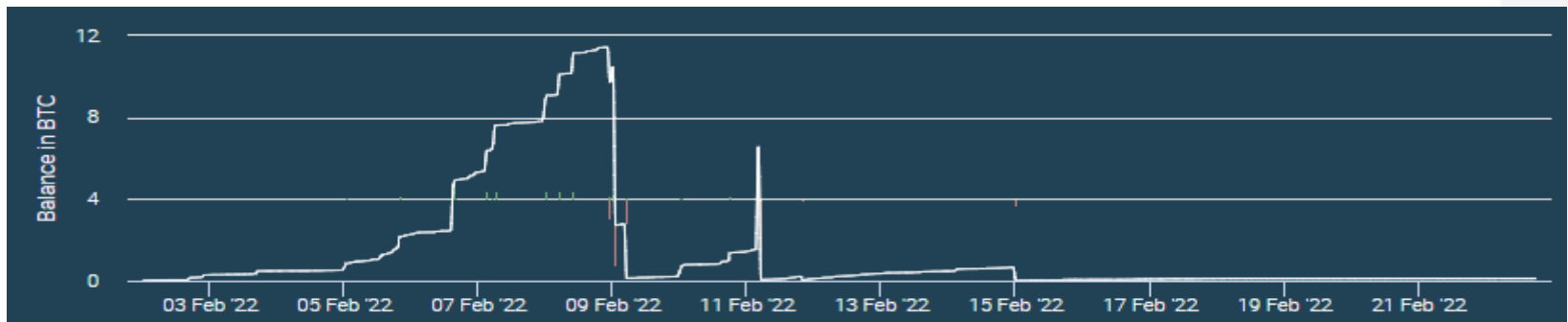
HONKHONK HODL



TallyCoin – HonkHonk Hodl

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

- Se estableció como respuesta al cierre de otros sitios de donaciones
- 2339 donaciones (no decenas de miles, como se había afirmado)
- 17 retiros
- 20,735 BTC recibidos (**1,2 millones de CAD**)
- La mayor parte de la actividad se concentró entre el 2 y el 15 de febrero de 2022.



Página de donaciones (Tallycoin)

Muestra la dirección de donación

bc1qlc2gpmzrr9gded07d9a40lt2lq7pp2v7h4c5jx

The screenshot shows the Tallycoin website interface. At the top, there's a navigation bar with 'tallycoin' logo, 'Explore', 'Sign Up', and 'Log In'. Below this, a sub-navigation bar includes 'Details', 'Contributors (5343)', 'Charts', and 'Share'. The main content area is titled 'BITCOIN FOR TRUCKERS' with a '★ GOAL REACHED ★' banner. It displays 'CAD \$1161857.67 raised' and 'goal \$1119958.09'. A 'Send Bitcoin to Honkhonk Hodi' button is visible. Below the button is a table of donation amounts: 50c, \$1, \$2, \$5, \$10, \$15, \$20, \$30, \$40, \$50, \$100, \$200. A 'BTC' dropdown and 'Approve: 0.00023832 BTC' are also present. A public message field is available, with options for 'anonymous or login' and 'on-chain' or 'lightning' payment methods. A photo of a truck rally with Canadian flags is shown. The text below the photo reads: '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!'. At the bottom, it says 'Contributors (5343)'.

This screenshot shows a different view of the Tallycoin donation page. It features a '100%' progress bar at the top. Below it, the 'Goal' is listed as '21 BTC' and the 'Raised' amount is '21.69934385 BTC'. A large QR code is displayed on the right side. At the bottom, there's a Tallycoin logo and the URL 'tallyco.in/s/lzxccm/'.

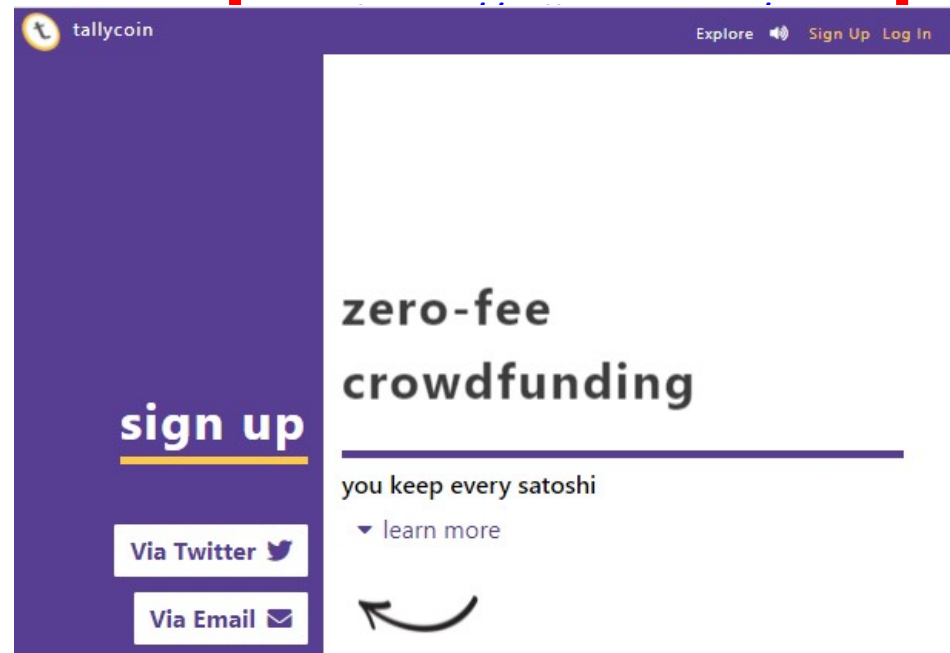
La disponibilidad de OSINT está sujeta a limitaciones temporales

(pero no se preocupe...)

- La página de donaciones ahora redirige a una página de inicio de sesión.
- La información ha dejado de estar disponible al público
- A medida que cambian las circunstancias, los sitios tienden a restringirse.

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

redirige a
<https://tallyco.in/>
que actualmente
redirige a



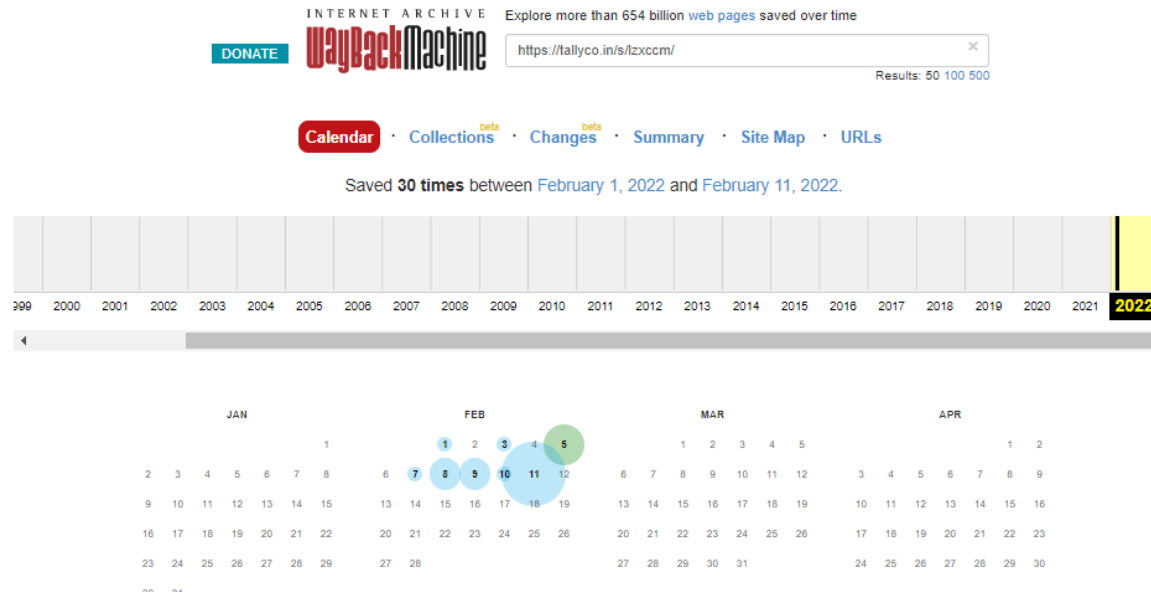
¿QUÉ MOTIVÓ A LAS PERSONAS A HACER DONACIONES?

Ejercicio: Internet Archive

- Es posible que el contenido de un sitio restringido siga siendo accesible a través de las capturas de pantalla archivadas por **Internet Archive**.
1. Ingrese a <https://web.archive.org/>
 2. Ingrese la URL de donaciones de los camioneros tomada de Facebook: ***https://tallyco.in/s/lzxccm/***
 3. Seleccione una fecha y abra una captura.
 4. ¿Qué información puede ver?

Internet Archive contiene capturas

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



Cada una de las capturas muestra 500 donaciones y los **mensajes asociados.**

Los usuarios podían publicar mensajes al realizar una donación.



- Los mensajes aún pueden visualizarse.
- Es posible vincular cada mensaje con su donación correspondiente a través del monto.
- **Las capturas pueden eliminarse si así lo solicita el propietario del sitio.**

Chainalysis



- Muestra la fecha y hora de la donación
- Muestra el monto exacto donado
- Muestra las direcciones desde las que se realizó la donación

Puede vincular los comentarios de las donaciones con una hoja de cálculo exportada de transacciones desde Chainalysis

Fecha y hora – Monto – Dirección

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...	d07... ● bc1q08z8f28t3vzgw...
> 02/20/2022 15:48	b949d3aed6a4885...	d07... ● bc1qr08hx4np5k4rc...
> 02/19/2022 22:28	5fad80a04373107...	d07... ● 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

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

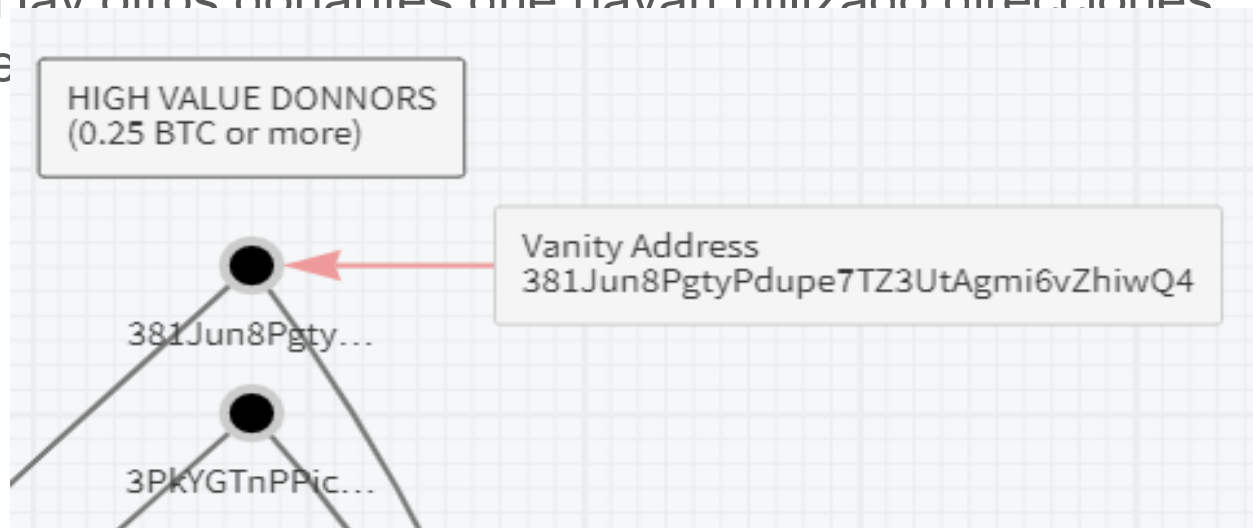
-
- Canadian Cryptocurrency Exchanges
- BitBuy.ca
- Coinsquare....
- The diagram illustrates the relationship between Canadian Cryptocurrency Exchanges and two specific entities. At the bottom, a yellow box labeled "Canadian Cryptocurrency Exchanges" has two red arrows pointing upwards to two circular nodes. The left node is a grey circle with a blue border, labeled "BitBuy.ca". The right node is a white circle with a blue border, labeled "Coinsquare....". Both nodes are enclosed within a larger yellow circle, and a black line extends from the top of each yellow circle.



Una gran donación utilizó una “dirección personalizada”

381Jun8PgtyPdupe7TZ3UtAgmi6vZhiwQ4

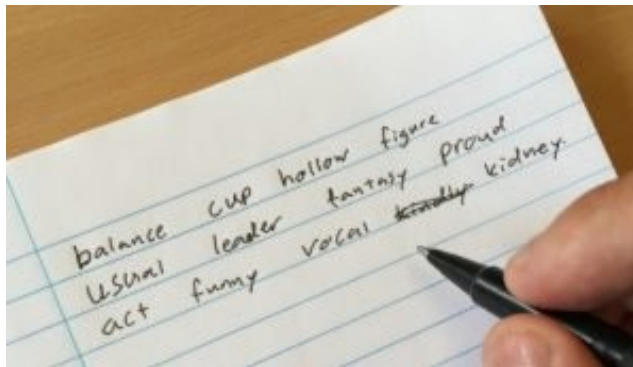
- ¿Qué significa “8 de junio”?
- ¿Qué significa “gty”? (¿Grace to You Church?)
- ¿Qué significa “dupe”?
- ¿Hay otros donantes que hayan utilizado direcciones pe



¿QUÉ ACCIONES REPRESENTAN LAS
TRANSACCIONES Y DIRECCIONES QUE
APARECEN EN EL GRÁFICO?

Pagos a camioneros


- Donaciones por \$ 8.000
- Distribuidas entregando sobres en mano a los camioneros
- Se utilizaron listas de palabras semilla (es decir, copias de seguridad de billeteras)
- Se utilizó Blue Wallet



Si seguimos el rastro de los bitcoins, se observan transferencias de pequeños montos a 101 direcciones

Root Address

bc1q42t9dhpgc6du9pjmdkvxvmke82...

 Watch

Balance:0.00 BTC

Sent:14.679553 BTC

Received:14.679753 BTC

Total Fees:0.0002 BTC

Transfers:102

Withdrawals:101

Deposits:1

Addresses:1


Overview





Counterparties

Transfers

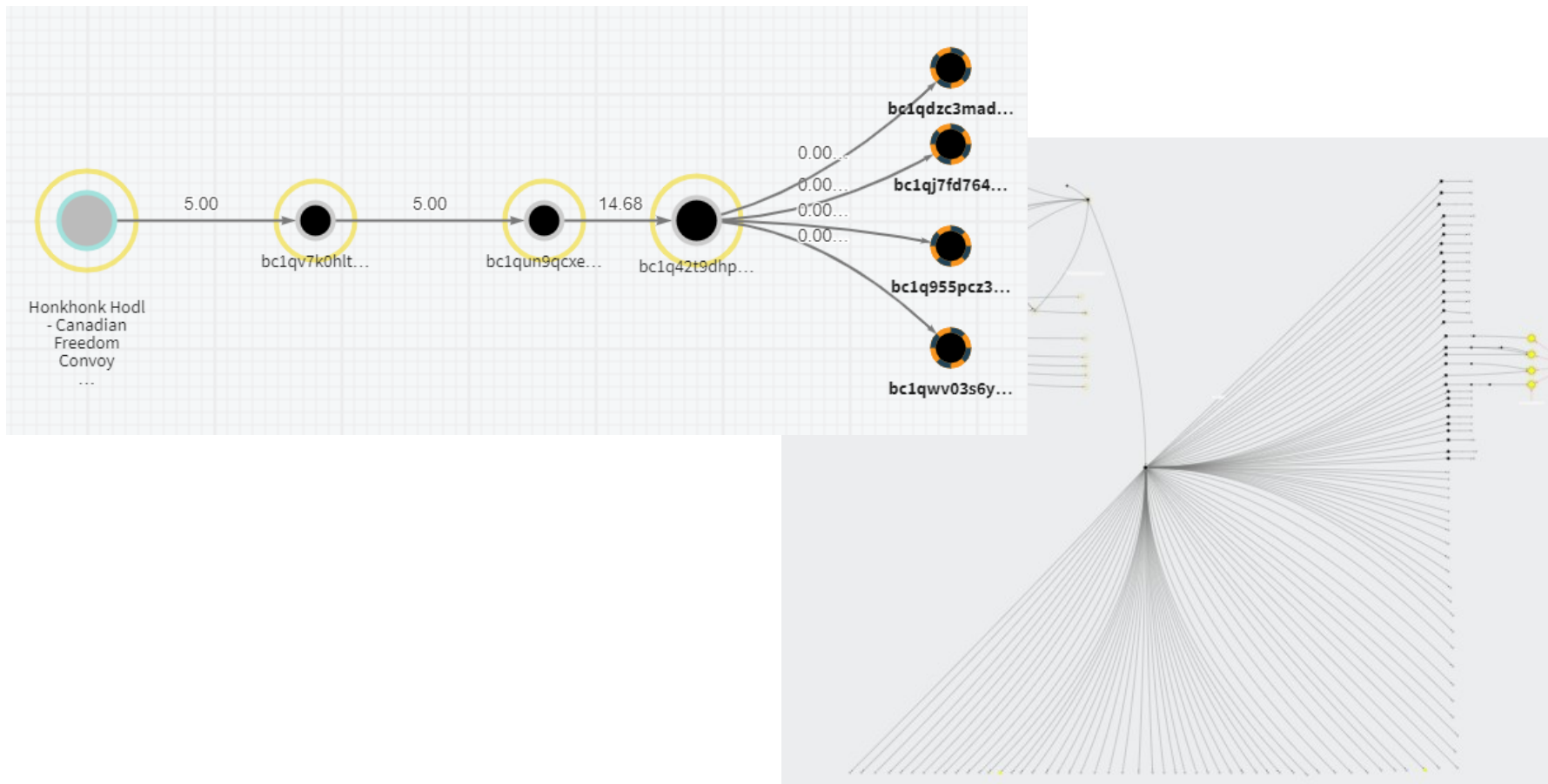
Addresses

OSINT



Counterparty	Transfers	Sent	Received	02/22	02/22
<div><div><input checked="" type="checkbox"/></div><div><div></div></div><div>bc1qww03s6yy3yyqf9sa48vmhfzsdju...</div><div></div></div>	1	0.004	0.00	<div></div>	<div></div>
<div><div><input checked="" type="checkbox"/></div><div><div></div></div><div>bc1qj7fd7642y7ufcllyspjs7w8p80h...</div><div></div></div>	1	0.004	0.00	<div></div>	<div></div>
<div><div><input checked="" type="checkbox"/></div><div><div></div></div><div>bc1q955pcz3pvveflycjns5julkdf24...</div><div></div></div>	1	0.004	0.00	<div></div>	<div></div>
<div><div><input checked="" type="checkbox"/></div><div><div></div></div><div>bc1qdzc3mad58rwvydkkf792pdj9ed9...</div><div></div></div>	1	0.004	0.00	<div></div>	<div></div>

Cada una de las 101 direcciones contiene **0.144048 BTC**



Ejercicio

[Summary](#)[Chart](#)[Conversations](#)[Historical Data](#)[Profile](#)

1. Ir a Yahoo Finance para consultar la cotización de BTC a CAD

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

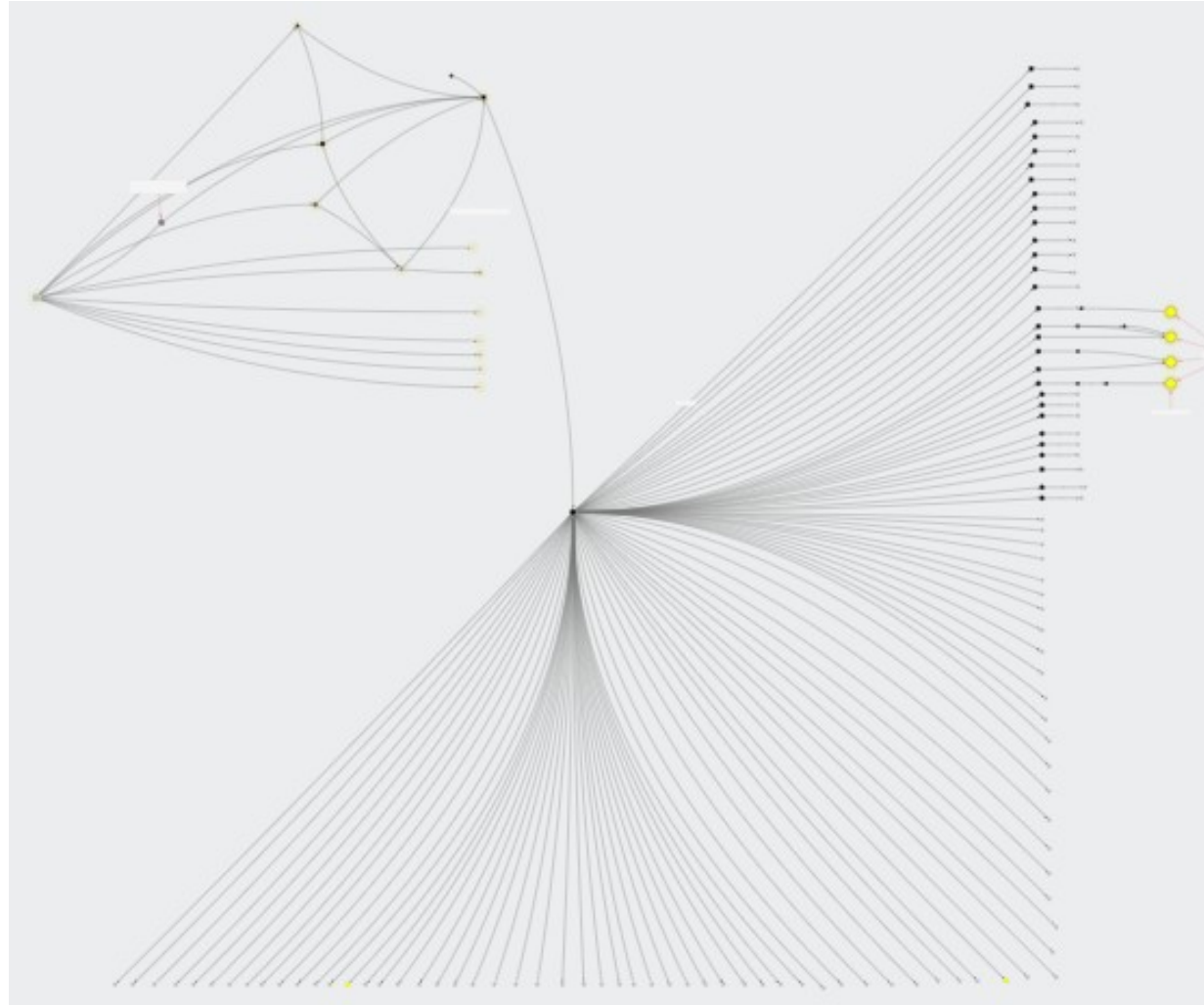
2. Navegar hasta la sección de **datos históricos**
3. Consultar el valor de 1 BTC en CAD el 14 de febrero de 2022
4. Calcular cuánto valían 0,14 bitcoins
5. Comparar este valor con los 8.000 dólares mencionados en el video de YouTube

Chainalysis – Gráfico de distribución

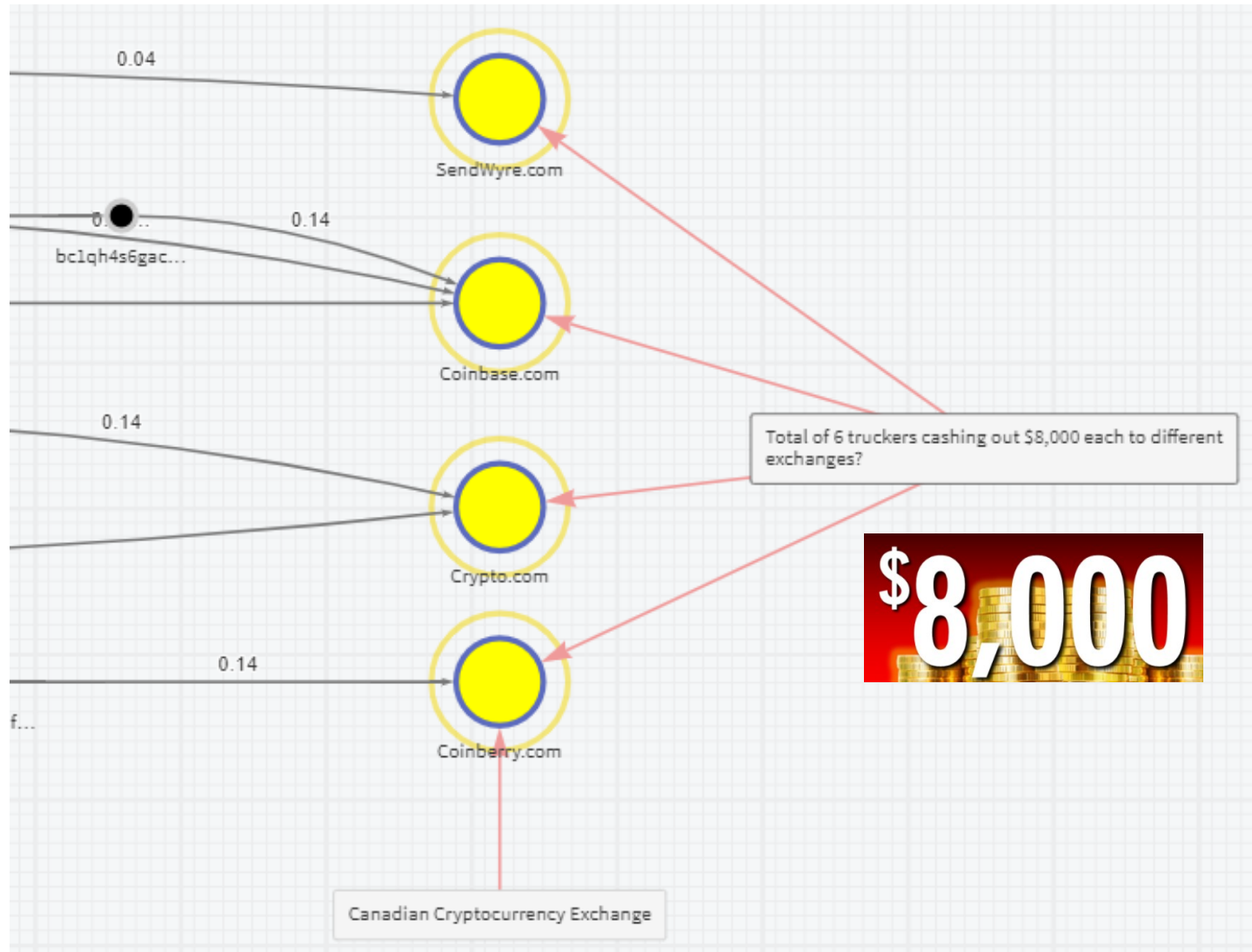
El sitio de donaciones aparece en el extremo izquierdo.

Los bordes del triángulo representan 101 direcciones que contienen aproximadamente 8.000 USD en bitcoins cada una.

En el extremo derecho aparecen direcciones que realizan retiros de fondos en plataformas de intercambio.



Retiros de camioneros en plataformas de intercambio



Herramientas como Chainalysis permiten rastrear las transferencias realizadas desde las direcciones que contienen aproximadamente 8.000 USD en criptomonedas.

- Chainalysis puede enviar notificaciones a los investigadores cuando los camioneros retiran fondos o transfieren los bitcoins a sus propias billeteras de criptomonedas.

Root Address

bc1qfjns4tjz39leydh4urt1c8fx7z69mx...

Balance: 0.144045 BTC

Sent: 0.00 BTC

Received: 0.144045 BTC

Total Fees: 0.00 BTC



Watch

¿PARTICIPARON MÚLTIPLES PERSONAS EN LAS TRANSACCIONES?

Direcciones multisig

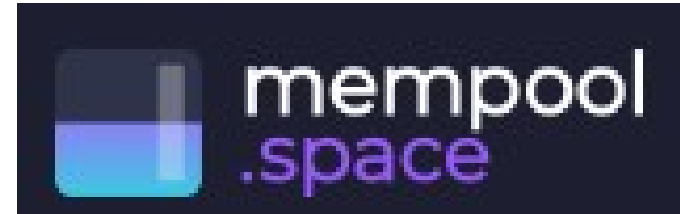
- Las direcciones multifirma (multi-signature, multisig) requieren más de una clave para poder gastar los criptoactivos almacenados.
- El número máximo de claves varía según el tipo de dirección.
- El límite superior es de 16 a 20 claves.
- El estándar es de 3 claves.



¿Se usaron direcciones multisig?

- Cuando se utilizan direcciones multifirma, suele implicar que hay más de una persona involucrada.
- Si se están usando direcciones multisig, las autoridades necesitarán más de una clave para incautar los activos almacenados en ellas.
- Identificar quiénes poseen las claves puede facilitar la coordinación de registros.
- ¿Pueden ayudar las listas de palabras semilla?

Las transacciones multisig pueden identificarse mediante el uso de un explorador de blockchain



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

```
P2WSH witness script
→ OP_PUSHNUM_2
  OP_PUSHBYTES_33 027c1cafd48147045f95c2ff3a2046405
  2033991db1f73bebbafddc861a83a24f0
  OP_PUSHBYTES_33 03447ac5709afdf0f8a0af43ba3a683ce
  a030bfd0f4848ca8b45e3ff24cf753b89
  OP_PUSHBYTES_33 034e0dd693acd897fa894ad180c536df3
  7fa55febb2fe53ebe6df47b46ba9e498
  OP_PUSHBYTES_33 037f6e26d297bc81a9bc5951604ecfdf5
  5d3140712313a2d947d6cdca22c2679a4
→ OP_PUSHNUM_4
  OP_CHECKMULTISIG
```


Captura reciente

