OECD International Academy for Tax Crime Investigation

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

OECD

Monitoring, Red-Flagging, Blacklisting & Delisting

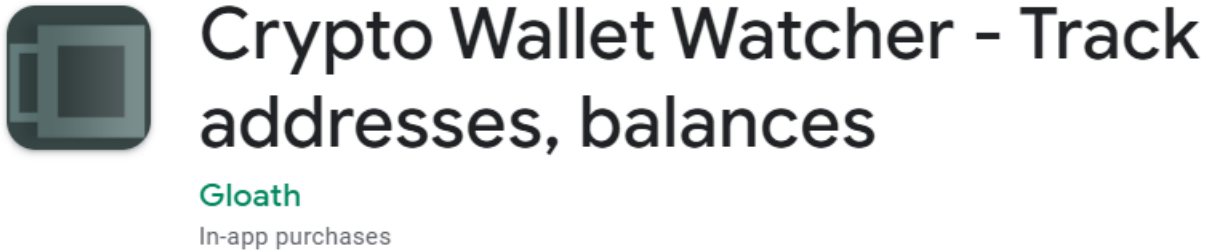
Dealing with "Bad" Addresses

- **Monitoring**: some tools allow you to set up notifications to inform you when assets are transferred.
- **Red-Flagging**: addresses may be reported to government agencies or to private sector entities.
- **Blacklisting & Delisting**: addresses may be banned from platforms, delisted from exchanges or excluded from interacting with smart contracts or DeFi platforms.

MONITORING

Smart Phone Apps

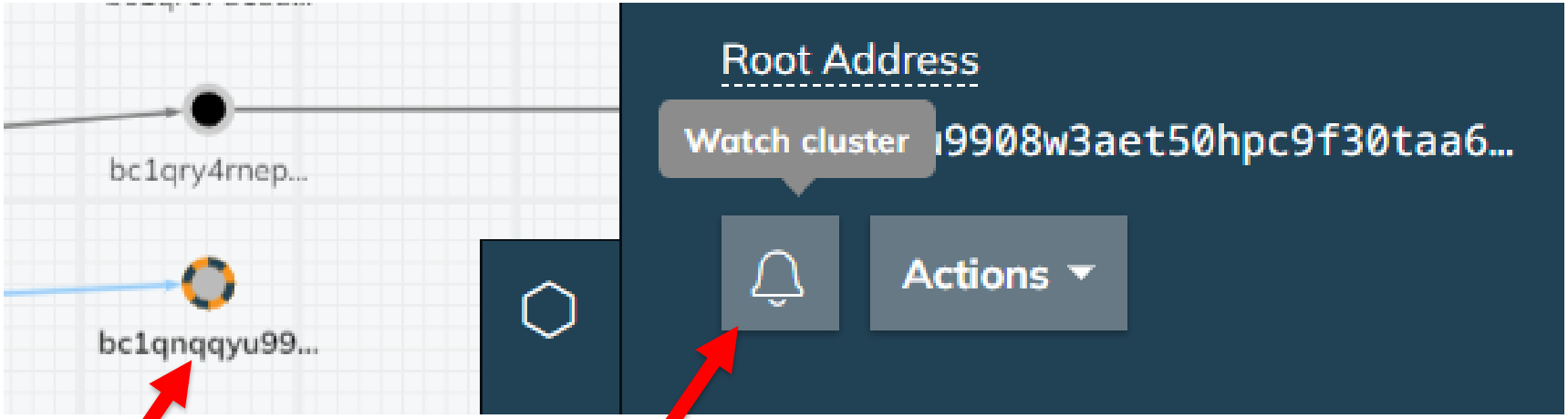
- Crypto Wallet Watcher
- Bitcoin Address Tracker



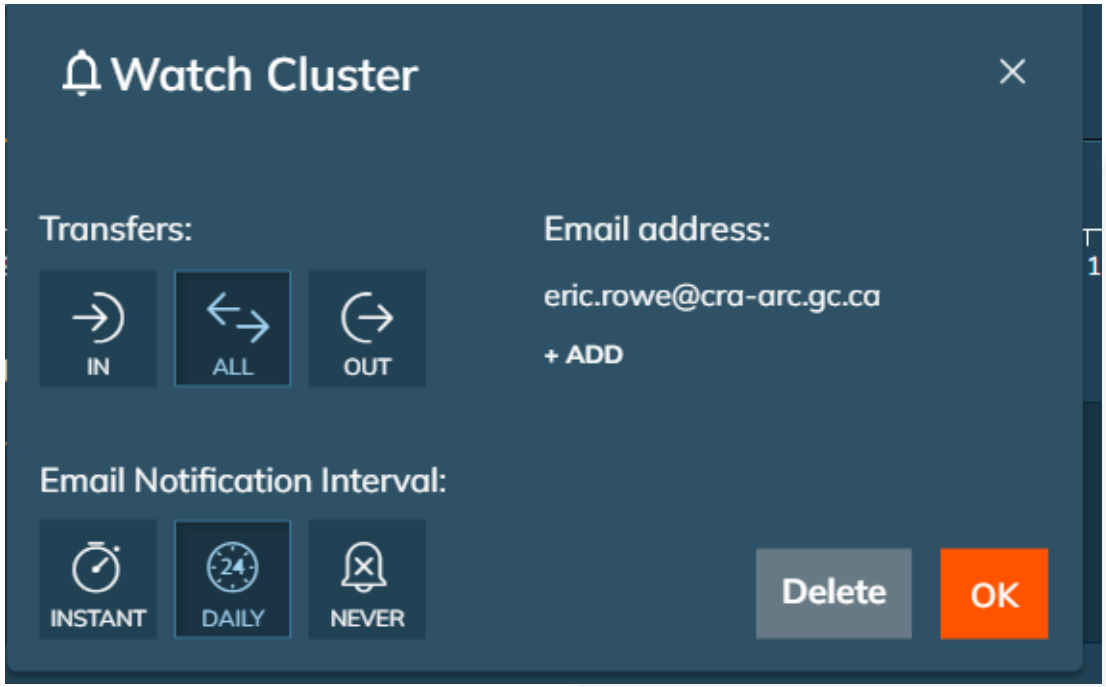
- **Not recommended for Law Enforcement**
  - The tools will see and possibly share addresses that you are watching.
  - Apps may leak data from your smart phone.

Investigation Tools

- Chainalysis and other tracing tools may allow you to monitor addresses and set up automated notifications when assets move to or from them.
  - Email notifications can be set to be sent to multiple individuals.
  - Email notifications may be instant or daily.



Chainalysis



Watched Cluster Transfer Notification

Adopt-a-Trucker Donation - Register.Adopt-a-Trucker.ca

Root address: bc1qvetv2l3v508lmpral067kghhm6x6nsm70rgwhx

Graph(s) where this cluster appears:

- Adopt-a-Trucker Donation - Register.Adopt-a-Trucker.ca

2 new transfers:

BTC 0.00015118 Monday, Feb 21 2022, 13:30:03 UTC
0fd41cde1430169151679e829744315d781b585f5af6695ab3aa1a4706889294
and **1** more transfers

Stop watching this cluster

Law Enforcement Tools

- Address Watcher (Europol EC3)
  - May be downloaded from Europol EC3 site
  - Works on several different blockchains
  - **Command line tool:**
    - Uses configuration files
    - Specify address to watch
    - Specify email address to send notifications to

AddressList.txt

Example:

```
BTC;17arLq4ibC4vyWq5TbhCuHkbJoDfcUthMT;4
BTC;1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ
BTC;1PtEnxdU93972S7uPW58mGbLCoZ9EbTRtb;20
```

Config.txt

Example:

```
useMail=true
verbal=2
waitTime=2
mailClient=mail.Police.be
mailSSL = false
mailSMTPPort = 587
mailFrom = Filip.Lacroix@fccu.be
mailTo= Filip.Lacroix@Police.Belgium.eu
mailPwd=
mailUser = Filip.Lacroix
mailDomain = fccu.be
```

RED FLAG INDICATORS

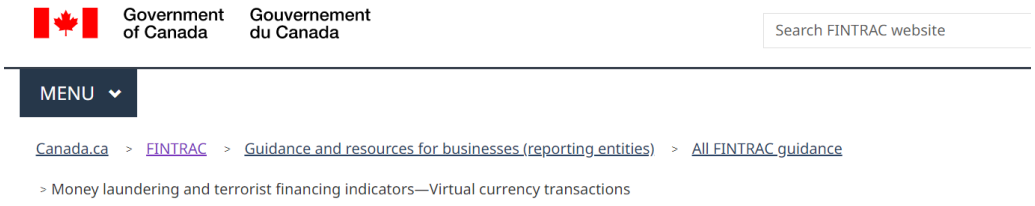
Red Flags

- **Financial Intelligence Units** such as FINTRAC, FINCEN, AUSTRAC maintain lists of red-flagged addresses as well as indicator typologies.
- **Government and international regulatory agencies** may maintain red flag lists or provide red flag indicators.
- **Private sector** lists exist which the public may use to submit addresses and other information.

FIU (FINTRAC)

Money Laundering Red Flag Indicators

https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng



Money laundering and terrorist financing indicators—Virtual currency transactions

- Client portfolio only consists of privacy coins or has a high value in privacy coins. [1]
- Client transfers Bitcoin in large volumes in exchange for privacy coins.
- Client is unwilling or unable to provide information about the source of privacy coins they once held or currently have.
- VC addresses match addresses on recognized watch lists such as the list of the Office of Foreign Assets Control (OFAC) or law enforcement information.
- Many clients register with the exchange within a short period using a shared address, mobile device, phone number, IP addresses and other common identity indicators.
- The client's VC wallet or address is linked to fraudulent activity in media reports and/or cyber security bulletins.
- A platform receives unusual or persistent requests from other exchanges/vendors/service providers in respect of a client's deposited funds or VC.

Potential Red Flags of Money Laundering Activity through NFTs

- Excessive volume of incoming transfers from multiple third parties (individuals/or companies). The funds are then depleted via email money transfers, wire transfers and payments to NFT marketplaces shortly after receipt.
- Payments sent to NFT marketplaces that allow for purchases with credit cards and have minimal KYC procedures.
- Client responded to online job advertisements that require the use of personal bank accounts involving suspected flow-through activity towards NFT marketplaces.

Potential Red Flags of Money Laundering Activity through NFTs

- Frequent trading of NFTs between digital wallets controlled by the same individual.
- Continuous trade of the same NFT over multiple hops involving different wallet addresses.
- Proceeds sent to multiple private wallets, decentralized finance services and mixers (Wasabi Wallet, CoinJoin mixers and Tornado Cash)

FINTRAC, (November 2022). **Exploring the Money Laundering and Terrorist Financing Activity Implications of Non-Fungible Tokens**. SIRA-2022-009. Strategic-stragegique@fintrac-canafe.gc.ca

J5
NFT Red Flag Indicators

https://www.irs.gov/pub/irs-utl/j5-media-release-4-28-2022.pdf

J5 JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT

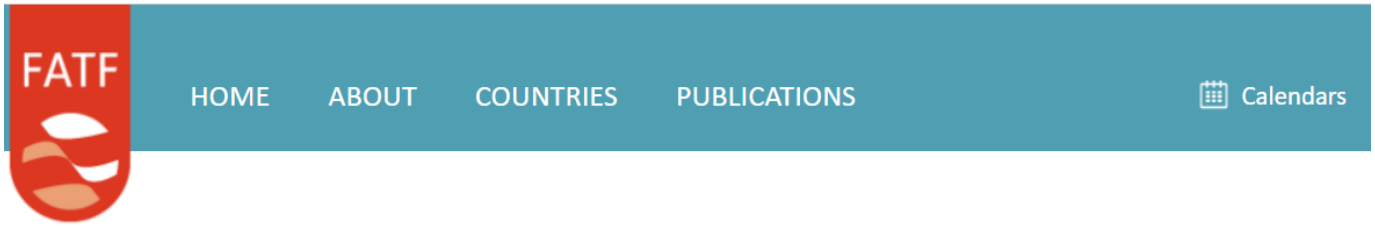
J5 Releases NFT Red Flags to Warn Public of Risks

Strong Indicators:

- Newly minted or secondary market transactions of > USD 100,000 with no observable community.
- A network of sending and receiving parties to the same transaction or group of transactions.
- Newly minted NFTs held by subjects being sold at high price points immediately which is not in line with others in the collection (potentially hiding the true reason for purchase)
- NFTs being sold for large sums and reacquired from the same party or a third party for smaller amounts would be a strong indicator.

FATF
Virtual Asset Red Flag Indicators

https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html



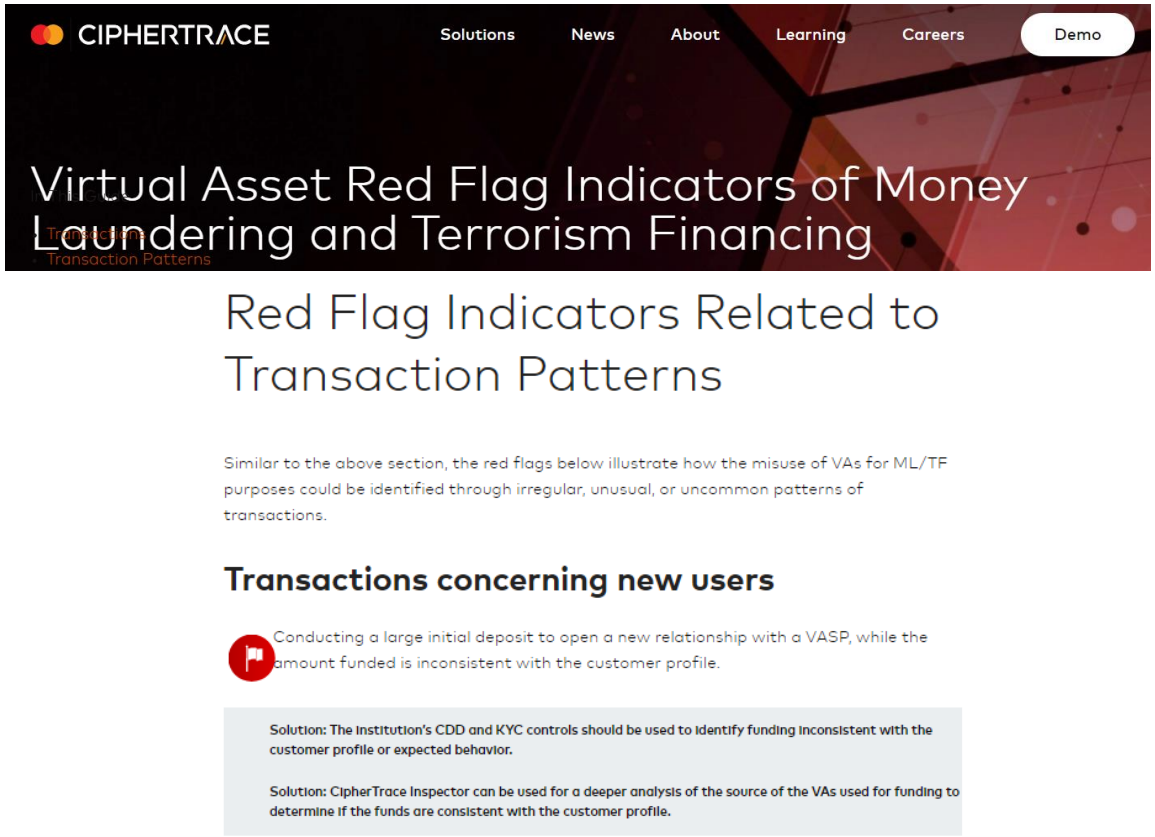
Home / Publications / Methods and Trends / Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

CipherTrace

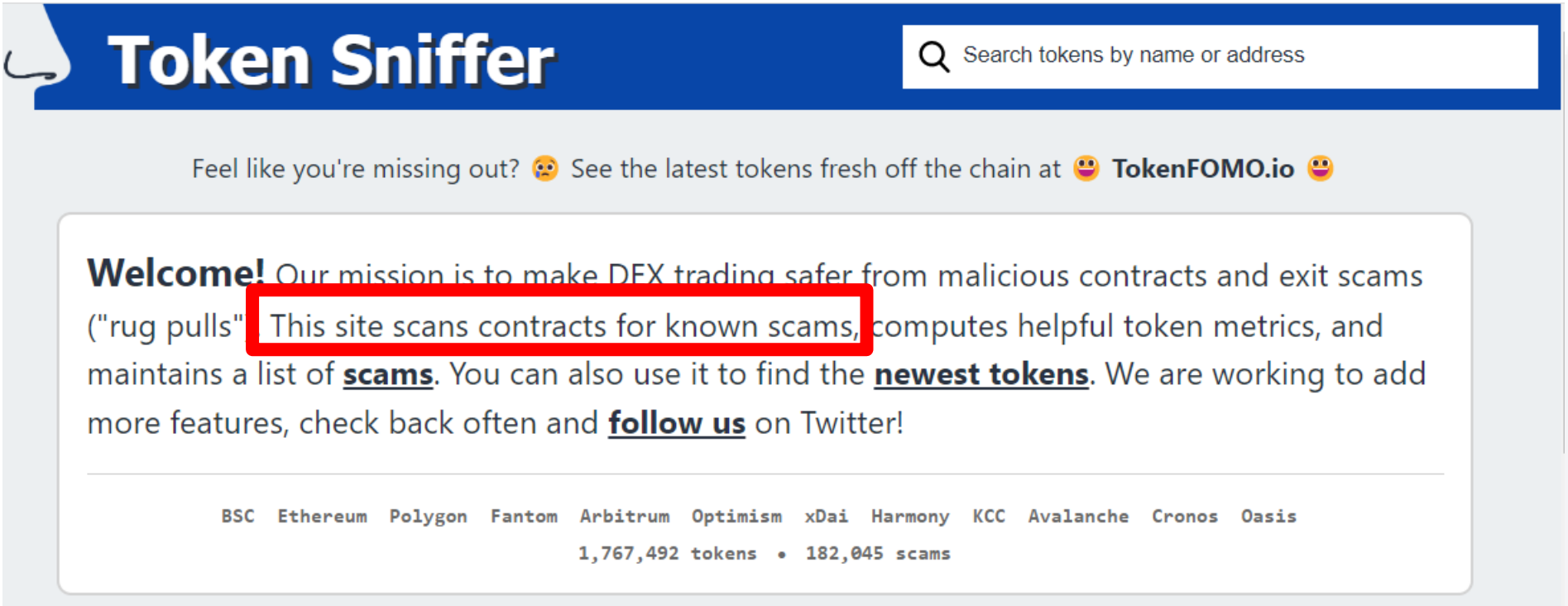
Virtual Asset Red Flag Indicators of Money Laundering and Terrorism Financing

https://ciphertrace.com/virtual-asset-red-flag-indicators-of-money-laundering/



TokenSniffer

- https://tokensniffer.com/



TokenSniffer

https://tokensniffer.com/

- **Performs automated analytics on token projects and addresses:**
  - Is the token sellable?
  - How may tokens are held by the seller
  - Liquidity analysis
- Searchable by name or address
- Metrics may not indicate whether it actually is a scam
- May be useful as a starting point in an evaluation of a token.

Token Sniffer - Exercise

https://tokensniffer.com/

1. Search for “Squid”
2. Compare **Calamari Squid** and **ElonSquidMusk** analytics
3. Do the projects appear to be scams or possibly malicious according to the analytics?
4. Why?
5. Which is more likely to be a scam?

CALAMARI (SQUID)

ETH:0x1951edef4e173900439bd32d4e09bb050f6e350d

Links	Etherscan
Chart	DEX Screener · GeckoTerminal · Etherscan
Deployed	30 Jul 2022 10:18:28 GMT (74 days ago)
	Transaction · Creator

CONTRACT | BUBBLE MAP

Smell Test (automated audit) 45/100

Summary

The audit score 45/100 is a measure of how well the token contract and characteristics meet
may still have hidden malicious code. The score is not advice and should be considered al

Swap Analysis (courtesy of honeypot.is)

✗ Token is sellable (not a honeypot) at this time

This token appears to be unsellable (ignore for presale).

Contract Analysis

✓ Verified contract source

✓ Ownership renounced or source does not contain an owner contract

✓ Creator not authorized for special permission

Holder Analysis View Holders | View Bubble Map

— Tokens burned: 4.21%, circulating supply: 957,818,177.493

✓ Creator wallet contains less than 5% of circulating token supply (0%)

✓ All other holders possess less than 5% of circulating token supply

Liquidity Analysis

✓ Adequate current liquidity

1.24 ETH in Uniswap v2 View LP | View Holders

✓ Adequate initial liquidity

1 ETH in Uniswap v2

✓ At least 95% of liquidity burned/locked for 15 days (100%)

100% burned

ElonSquidMusk (SQUID)

BSC:0x26ad6e75c2a69eac18f231ebd02331cc68abb40b

Links	BscScan
Chart	DEX Screener · GeckoTerminal · PooCoin
Deployed	12 Nov 2021 08:38:47 GMT (334 days ago)
	Transaction · Creator

CONTRACT | BUBBLE MAP

Smell Test (automated audit) 0/100

Summary

The audit score 0/100 is a measure of how well the token contract and characteristics meet the criteria for safety. Results may not be applical
still have hidden malicious code. The score is not advice and should be considered along with other factors. Always do your own research a

Swap Analysis (courtesy of honeypot.is)

✓ Token is sellable (not a honeypot) at this time

✓ Buy fee is less than 5% (0%)

✓ Sell fee is less than 5% (0%)

Contract Analysis

✓ Verified contract source

✓ Ownership renounced or source does not contain an owner contract

✓ Creator not authorized for special permission

Holder Analysis View Holders | View Bubble Map

! **A wallet exceeds the circulating token supply (likely a scam)**

✗ Creator wallet contains less than 5% of circulating token supply (132922294578.49%)

The creator wallet contains a substantial amount of tokens which could have a large impact on the token price if sold.

✗ All other holders possess less than 5% of circulating token supply

A wallet contains a substantial amount of tokens which could have a large impact on the token price if sold.

Liquidity Analysis

✗ Adequate current liquidity

< 0.01 BNB in PancakeSwap v2 View LP | View Holders

Not enough liquidity is present which could potentially cause high slippage and other problems when swapping (ignore for presale).

RED FLAGGED ADDRESSES

ChainAbuse

https://www.chainabuse.com/

- Chainabuse is a multi-chain community based tool to report scams, hacks, and exploits.
- Users may file reports as well as upvote or downvote reports.
- The community identifies scams and defines what is most useful for others through upvotes and downvotes.
- **Chainabuse is funded by a collective of web3 communities, businesses, protocols, and foundations as well as TRM Labs**

Reports submitted for

12t9YDPgwueZ9NyMgw519p7AA8isjr6...

wueZ9NyMgw519

7 Scam Reports

SORT BY

FILE NEW REPORT

Ransomware Wannacrypt payment address 2.0

1

Submitted by dubs0 on May 17, 2022

0

Reported Address	115p7UMMngoj1pMvkpHijcR...
Reported Address	12t9YDPgwueZ9NyMgw519p...
Reported Address	13AM4VW2dhxYgXeQepoHk...

Reports by Category

Ransomware	6
Blackmail	1

Chainabuse - Exercise

Search for the following Addresses. What information is given?

1. **12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw** (Wannacry)
2. **Bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh** (Twitter scam)
3. **0xd96f2B1c14Db8458374d9Aca76E26c3D18364307** (Tornado Cash sanctioned address)
4. **0x5DD596C901987A2b28C38A9C1DfBf86fFFc15d77** (Wonderland scammer)
5. **bc1q8fr92crfwta4a9f9j427mh5zwg3uzar85d5hgu** (Instagram Bitcoin scammer)

Bitcoin Abuse Database

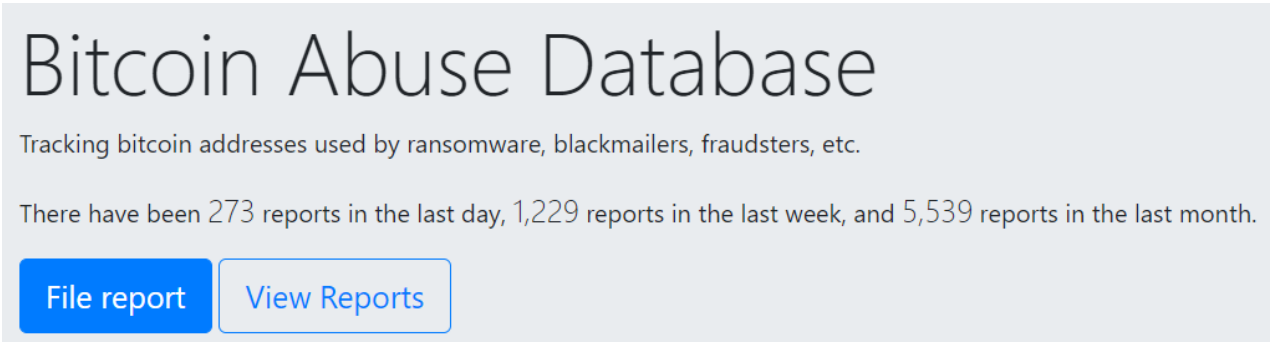
https://www.bitcoinabuse.com/

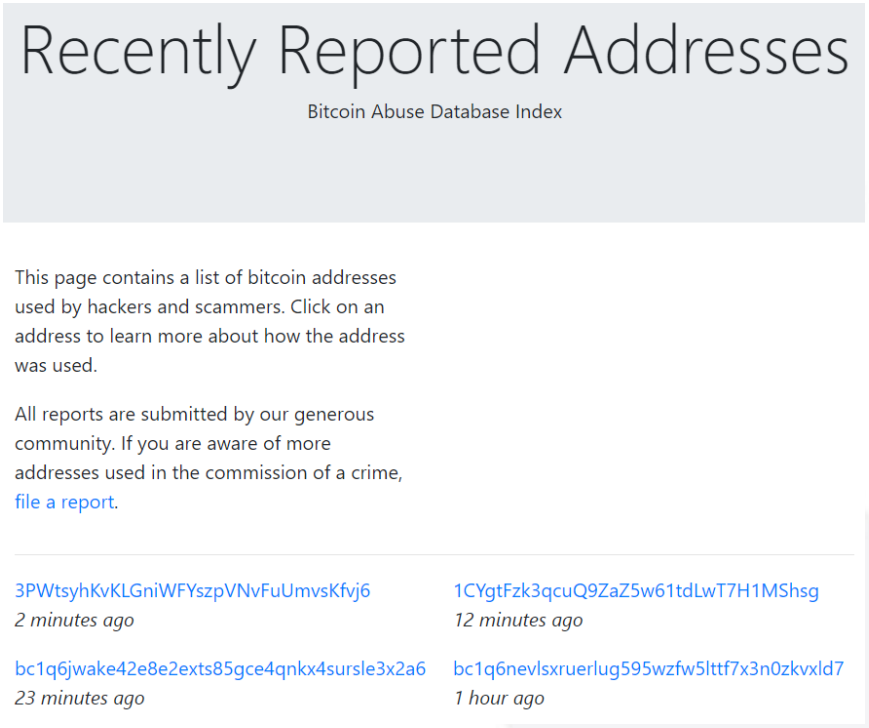
- BitcoinAbuse.com is a public database of bitcoin addresses used by scammers, hackers, and criminals.
- Reports can be made anonymously or with contact information.
  - Complainants can share their contact info and have it shared with law enforcement.
  - https://www.bitcoinabuse.com/reports/create
- **Bitcoin addresses are searchable.**
- Description of the abuse (e.g. sextortion) is included.
- Links to transactions may exist.
- Copies of the database can be downloaded using APIs
  - https://www.bitcoinabuse.com/api-docs

Bitcoin Abuse Database

- Anyone can submit a report
- Contains a great deal of spam
- May be unreliable – little or no verification

Bitcoin Abuse Database





https://www.bitcoinabuse.com/

Bitcoin Abuse Database

Report history for ***1KjxgUYw2QC53ZiGeAG9uohcSSRUWsSsQA***

Address found in database:

Address	*1KjxgUYw2QC53ZiGeAG9uohcSSRUWsSsQA* View address on blockchain.info
Report Count	7
Latest Report	Fri, 04 Jan 19 09:20:17 +0000 (3 years ago)
Total Bitcoin Received	**0.56848647 BTC**
No. Transactions Received	3

Jul 17, 2018	ransomware	Says he has my password, instructs me to send $3800.
Jul 17, 2018	ransomware	threats to send video to contacts
Jul 17, 2018	other	Wants $3200 or will tell everyone I looked at porn online. Claims to have my password and access to webcam

Bitcoin Abuse - Exercise

https://www.bitcoinabuse.com/

- Search for the following address:
  1QAVaukg4es84us9XRTaPqztYB1XXoXEdA
  1. When was it first reported, and for what abuse type?
  2. When was it last reported, and for what abuse type?
  3. How many reports were made regarding it?
  4. How many deposits were made to the address?
  5. How many withdrawals were made from the address?

Bitcoin Abuse Exercise

https://www.bitcoinabuse.com/

- Search for the following address:
  bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h
  1. When was it first reported, and for what abuse type?
  2. When was it last reported, and for what abuse type?
  3. How many reports were made regarding it?
  4. Is there anything odd about the reports?
  5. How many withdrawals were made from the address?

Bitcoin Abuse Exercise (cont.)

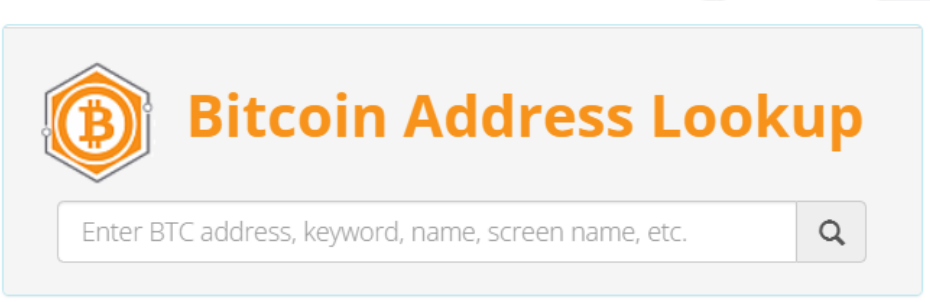
https://bitinfocharts.com/
https://www.bitcoinwhoswho.com/
bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h

- Examine the address in Bitinfocharts.
  - Is the address still active?
  - How may bitcoins are in it?
  - What is the dollar value of the bitcoins in it?
- Examine the address in Bitcoinwhoswho
  - How many billion dollars worth of bitcoin did it receive?
  - What does this indicate about the individuals behind it.

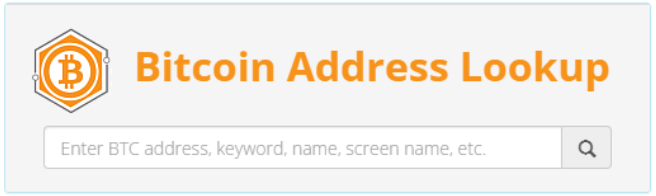
Bitcoin Who's Who

https://www.bitcoinwhoswho.com/

- Track who's who in the world of Bitcoin
- Check Bitcoin Addresses to see if they have been reported as scams.
- Report a scam address.
- Information depends on reports which may not have been properly vetted.



Bitcoin Who's Who



- **Bitcoin Who's Who allows users to check addresses and see whether there have been scam alerts associated with it.**

  http://bitcoinwhoswho.com

- WannaCry: **13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94**
- Quadriga Cold Storage: **1MhgmGaHwLAvvKVyFvy6zy9pRQFXaxwE9M**
- Mueller Investigation: **1LQv8aKtQoiY5M5zkaG8RWL7LMwNzVaVqR**
- Twitter Scam: **bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh**
- Dmitri Karasavidi : **1Q6saNmqKkyFB9mFR68Ck8F7Dp7dTopF2W**

Bitcoin Who's Who Exercise

https://www.bitcoinwhoswho.com/

- Look up the following BTC Address **13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94**

1. Does it show up as a fraudulent address?
2. How many times has it been reported?
3. How many BTC/USD has it received?
4. What scam is it associated with?
5. Can the address be found on web sites?

BITCOIN ADDRESS REPORT

Scam Alert: This address has been reported as fraudulent (1 time)

Watch

BTC Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	**# Website Appearances**	44
Current Balance	0.32843048 = $6,260.34	**Total Received**	20.07353352 = $382,629.65
# Transactions	143	**# Output Transactions**	2
First Transaction	12 May 17	**Last Transaction**	27 May 21
Last Known Input	14LXmEDmQ6... 30 Aug 20	**Last Known Output**	182Neztu7T... 2 Aug 17
Repeated Inputs From (50 most recent transactions)	1LGmE7B3G9... 2	**Repeated Outputs To** (50 most recent transactions)	None
Tags	5 Tags (Please login to see the tags)		

Scam Alert

	Scam Name	URL	Image	Date
−	WannaCry Ransomware			Nov 2nd, 19
	This address is used on WannaCry ransomware			

Website Appearances/Public Sightings

Date Found	Description	More Detail	Website URL	URL Country
30 Aug 21	How to remove BlackMamba Ransomware - virus removal steps (updated)		https://www.pcrisk.com/removal-guides/19732-blackmamba-ransomware	United States
26 Jul 21	What Is WannaCry? Analyzing the Global Ransomware Attack	What is WannaCry and how does it work? We provide analysis and insight for what has become the largest ransomware attack in history.	https://www.recordedfuture.com/wannacry-ransomware-analysis/	United States
26 Jul 21	WannaCry Profits		https://wanna-cry-profits.herokuapp.com/	United States

by exploiting bugs/flaws of outdated software. Trojans are malicious programs that can cause chain infections by installing other software of this kind. Note that malware can only be distributed in this way if Trojans are already installed on computers.

Unofficial activation ('cracking') tools are illegal programs that supposedly activate licensed software free of charge and bypass activation, however, they often install other malicious programs instead.

Threat Summary:	
Name	BlackMamba virus
Threat Type	Ransomware, Crypto Virus, Files locker.
Ransom Demanding Message	Pop-up window
Ransom Amount	USD$30 in Bitcoins
BTC Wallet Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Cyber Criminal Contact	cobra_locker666@protonmail.ch
Detection Names	Avast (Win32:MalwareX-gen [Trj]), BitDefender (Gen:Variant.Bulz.276557), ESET-NOD32 (A Variant Of MSIL/Filecoder.AER), Kaspersky (HEUR:Trojan-Ransom.MSIL.Encoder.gen), Microsoft (Trojan:Win32/Wacatac.B!ml), Full List Of Detections (VirusTotal)

https://wanna-cry-profits.herokuapp.com

WannaCry Profits

Stats for each known BTC address associated with the WannaCry ransomware:

LAST UPDATED 8/24/2021

Blockchain Address: 1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY

Current BTC Value: 3.25249956 BTC

Current USD Value: $62,153.05

Blockchain Address: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Current BTC Value: 14.87769994 BTC

Current USD Value: $284,302.73

Blockchain Address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Current BTC Value: 19.69028255 BTC

Current USD Value: $376,267.91

Blockchain Address: 15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Current BTC Value: 1.71956125 BTC

Current USD Value: $32,859.65

Blockchain Address: 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Current BTC Value: 20.07353352 BTC

Current USD Value: $383,591.58

Dune Analytics
(Ethereum based tokens)

https://dune.xyz/

- **Dune Analytics lists stablecoins which have been banned inside their smart contracts**.
- You will need to examine the addresses further in EtherScan or other tools to obtain details.
- Banned stablecoin Addresses Overview https://dune.xyz/bt/Stablecoins:-Addresses-Banned
  - **Tether** (USDT) https://dune.xyz/phabc/usdt---banned-addresses
  - **USD Coin** (USDC) https://dune.xyz/phabc/usdc-banned-addresses
  - **Paxos Standard Token** (PAX) https://dune.xyz/phabc/pax---banned-addresses

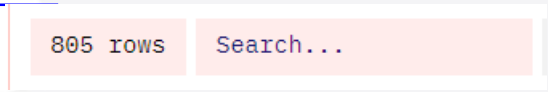
Dune Analytics (USDT)

Search for the following addresses in Dune:

1. 0x4688a8b1f292fdab17e9a90c8bc379dc1dbd8713
2. 0xc1bec32be8a68346ad9dabbb0a67ce220d43997c
3. 0xeb963da0ea2d53bfb930edc76f994fca2de7fe5f
4. 0xf5e9f38e559cf86b5eca5e78c4dc71e2268660d0
5. 0x9faf5515f177f3a8a845d48c19032b33cc54c09c

When were they banned?

https://dune.xyz/phabc/usdt---banned-addresses
https://dune.com/queries/5866/11619



BLACK-LISTING & DELISTING

Black Lists

- Addresses or Individuals may be **banned from cryptocurrency or token platforms**.
- Addresses may be blacklisted and **banned from interacting with smart contracts** (including decentralized platforms).
- Problematic tokens or cryptocurrencies may be **delisted from Exchanges** or other services.
- Often this is done to reduce financial or legal risks to the business.

Blacklists are just lists of addresses

- Anyone can create a blacklist
- Blacklists can be integrated into tools and software
- Virtual asset service providers (VASP) may use blacklists to flag activity or deny services.

Canada RCMP Blacklists Truckers' Bitcoin Addresses

February 16, 2022 by Edna Rico

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

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

RCMP Alert sent to Exchanges & FINTRAC

s 2022

CoinDesk

Layer 2

Business Tech Policy Indices TV & Videos Podcasts Crypto Explainer+ Events Research About

020.62 -0.56% Ethereum $2,576.59 -1.64% XRP $0.783985 +6.01% Terra $89.84 -7.34% Solana Crypto Price

Policy

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

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

By Aoyon Ashraf, Danny Nelson · Feb 16, 2022 at 5:35 p.m. GMT · Updated Feb 17, 2022 at 4:44 p.m. GMT

Government of Canada / Gouvernement du Canada

Search PSPC

MENU

Home > How government works > Treaties, laws and regulations > Canada Gazette > Publications > Part II: Vol. 156 (2022)

Emergency Economic Measures Order: SOR/2022-22

Canada Gazette, Part II, Volume 156, Extra Number 1

Registration
SOR/2022-22 February 15, 2022

EMERGENCIES ACT

P.C. 2022-108 February 15, 2022

RCMP·GRC

OPP

CRYPTOCURRENCY ALERT

The Ontario Provincial Police and Royal Canadian Mounted Police are currently investigating cryptocurrency donations being collected in relation to illegal acts falling under the scope of the *Emergency Measures Act*.

Pursuant to the *Emergency Economic Measures Order*, under subsection 19(1) of the *Emergencies Act*, there is a duty to cease facilitating any transactions pertaining to the following cryptocurrency address(es):

Any information about a transaction or proposed transaction in respect of these address(es), is to be disclosed immediately to the Commissioner of the Royal Canadian Mounted Police, at CryptocurrencyNHQ-CryptomonnaieDG@rcmp-grc.gc.ca.

Asset	Address
LTC	ltc1qqhzc2dflesccd5gx6ugqqgcplzakrk8wlxl8zq
ADA	addr1qxwxppd3ahfsh43f88h4jn8ngrum64fe6meck3nnwkwgtsp6elsk4xhyrdtm5v6tnq3ulw9u9gcmvkhrj4xcu3sm60hqtz3wuy
XMR	423nPDQqsPrAAgFSHaUBMrYQQCgb2562iLLWu1dZyEGEGsavxfpNxWtDjreSUzwqWQCxi6GrSz8jtYWjS4pW9mK9DoBVdWo
ETH	0x859481ef7dac321078547f50c756c8924eab183f
ETC	0x88cd1d4611d456357ef8620450d3121672305d03
BTC	bc1qvetv2l3v508lmpral067kghhm6x6nsm70rgwhx
BTC	1Pk9TAxrXE1sQeYx3KXN77TfNjBDPxeEnk
BTC	bc1q82ejx54e9ra0la9n5whcaqegdr2f5j6ep0kep7
BTC	bc1qlc2gpmzrr9gded07d9a40lt2lq7pp2v7h4c5jx
BTC	bc1q2xjld87z45k2fuz48dqhntgh3e0k80ft0a46jd3ftwrqt4fnnyjqftd0ur
BTC	bc1q3jsfd54ja2jxnumjwq2ds6qn0yt0mye7lwvdmyft3a8a5w9d8hkqxfg6az

Bitcoin addresses can be blacklisted

- Bitcoin addresses associated with criminal activity, terrorist financing, or other activities can be blacklisted.
- Bitcoin addresses associated with such as gambling, high risk exchanges or other entities or entities can be flagged in tracing, reporting or monitoring tools.

Blacklisting a Bitcoin address does not stop the address from receiving or sending bitcoins.

Ethereum addresses can be blacklisted

- Ethereum addresses can be added to many blacklists.
- Tokens constructed on the Ethereum Blockchain can be blacklisted on platforms
- Blacklisted Ethereum as well as Blacklisted Tokens can be flagged in tracing, reporting and monitoring tools.

Blacklisting an Ethereum address does not stop its owner from receiving or sending ether.

Blacklisted Ethereum addresses or Token addresses may result in the freezing, receiving or the spending of tokens.

Blacklisting ETH Tokens

- **Tether** (USDT) started blacklisting addresses in 2017
- When **CENTRE** (USDC) executes its blacklist function for a particular address, the USDC in the address is locked and cannot be used for on-chain transactions.
- Blacklisting and freezing tokens has been used to return stolen funds.
  - This is not usually possible however.

Whether or not a token can be frozen depends on whether that functionality has been programmed into its smart contract.

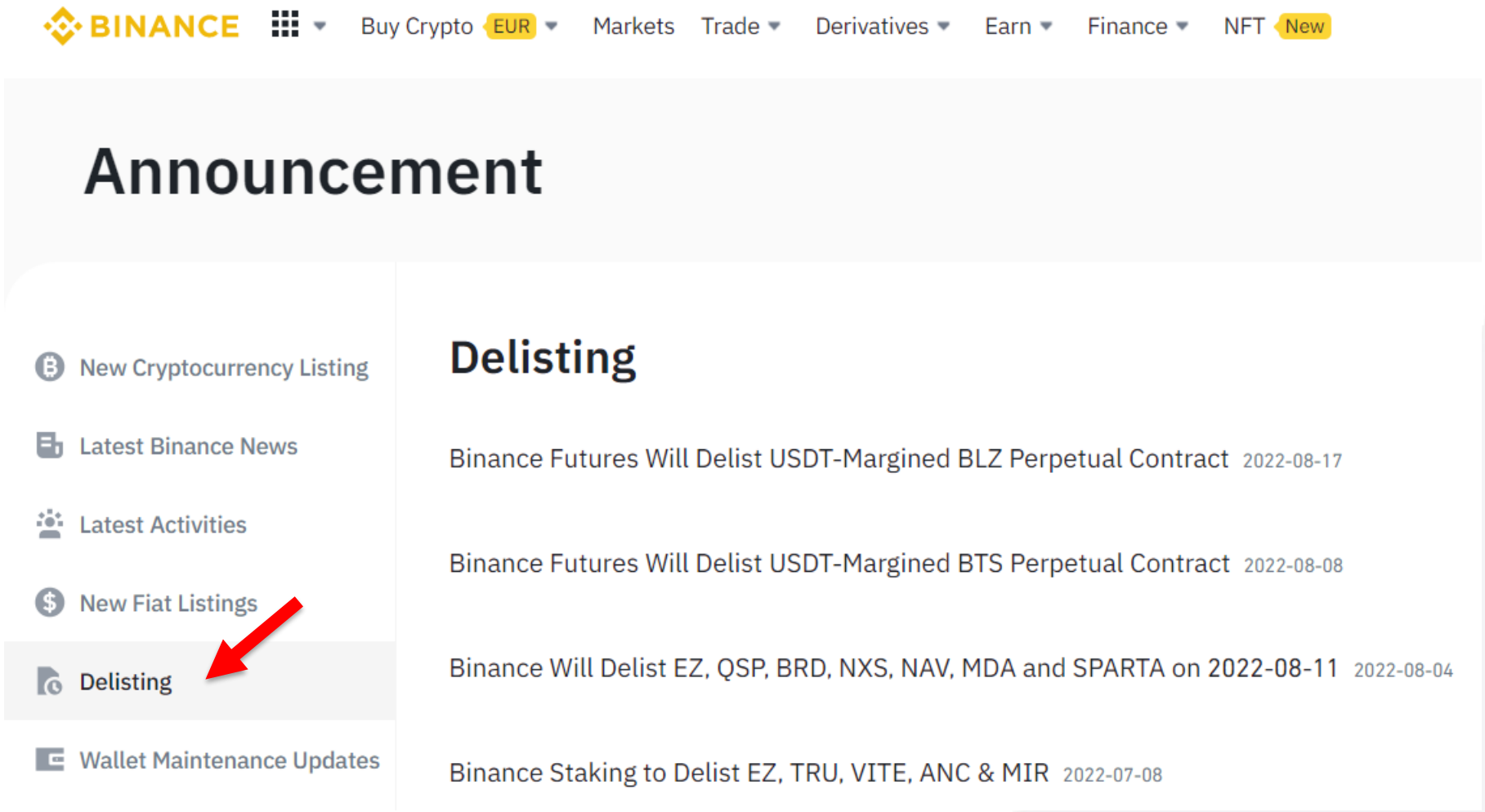
https://cryptobriefing.com/tether-can-freeze-your-usdt-39-addresses-containing-millions-blacklisted/
https://cryptobriefing.com/100000-usdc-blacklisted-highlighting-importance-decentralized-stablecoins/

Blacklists can be coded into software

- In 2014 a coder for Linux Gentoo blacklisted a number of address prefixes.
- Other coders fought back with a patch.

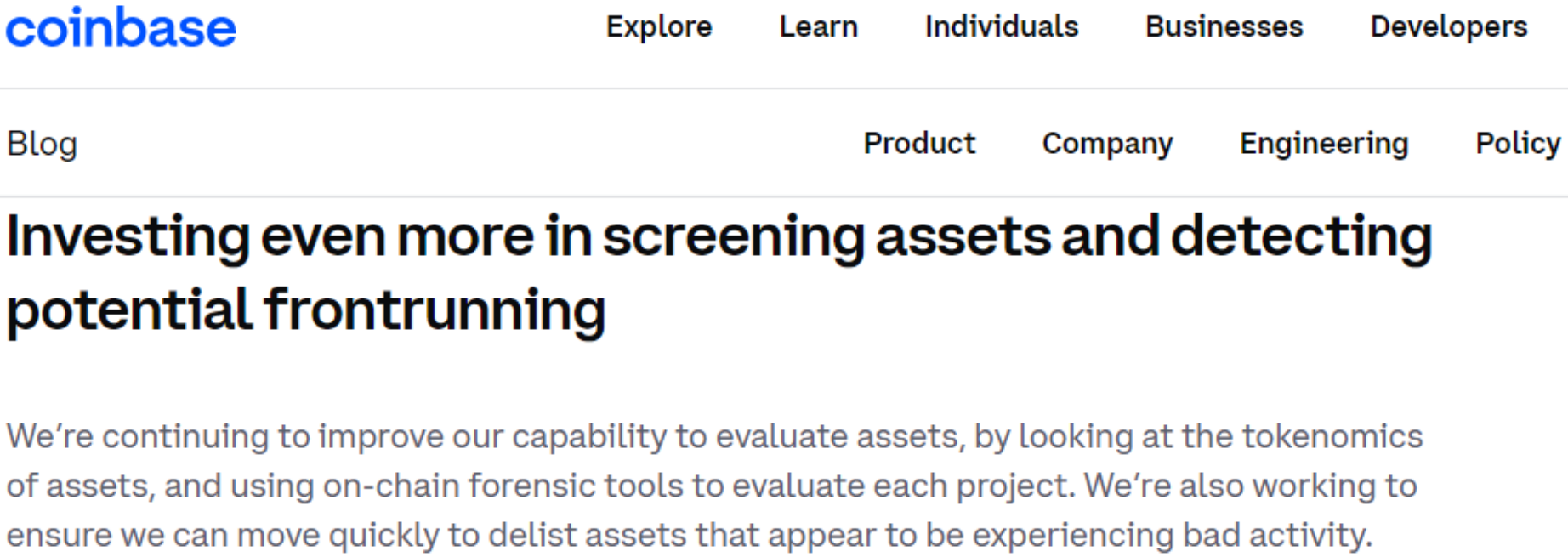
```
struct BlacklistEntry {
    uint32_t begin;
    uint32_t end;
    const char *name;
};

static struct BlacklistEntry BlacklistedPrefixes[] = {
    {0x946cb2e0, 0x946cb2e0, "Mastercoin"},
    {0x06f1b600, 0x06f1b6ff, "SatoshiDice"},
    {0x74db3700, 0x74db59ff, "BetCoin Dice"},
    {0xc4c5d791, 0xc4c5d791, "CHBS"},  // 1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T
    {0x434e5452, 0x434e5452, "Counterparty"},
    {0x069532d8, 0x069532da, "SatoshiBones"},
    {0xda5dde84, 0xda5dde94, "Lucky Bit"},
};
```

Binance and other Exchanges actively delist tokens



https://www.binance.com/en/support/announcement/c-161

Coinbase delists tokens

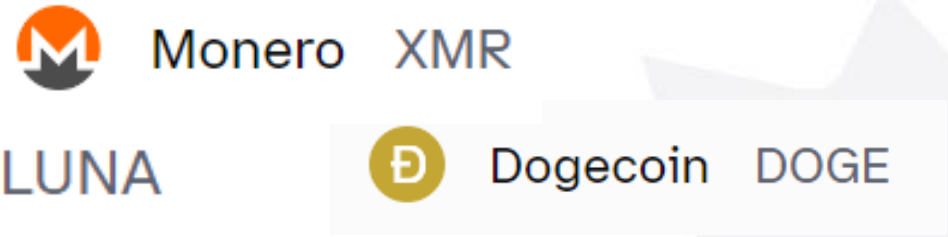


Coinbase exercise

- Search Coinbase to see if the following tokens are listed on Coinbase:
  - Monero
  - Terra Luna
  - Doge

https://www.coinbase.com/browse

- Search the Internet to discover why some of these popular coins may have been delisted.

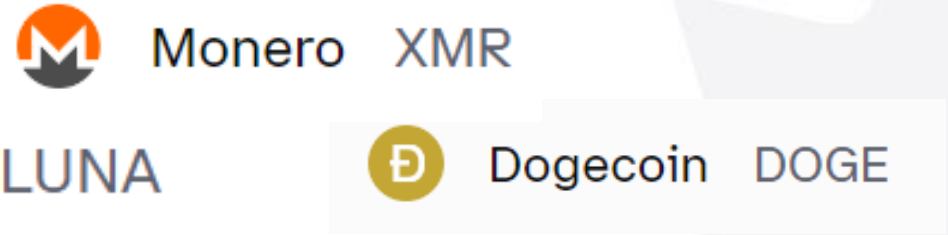


Binance Exercise

Go to the Binance Exchange web site:

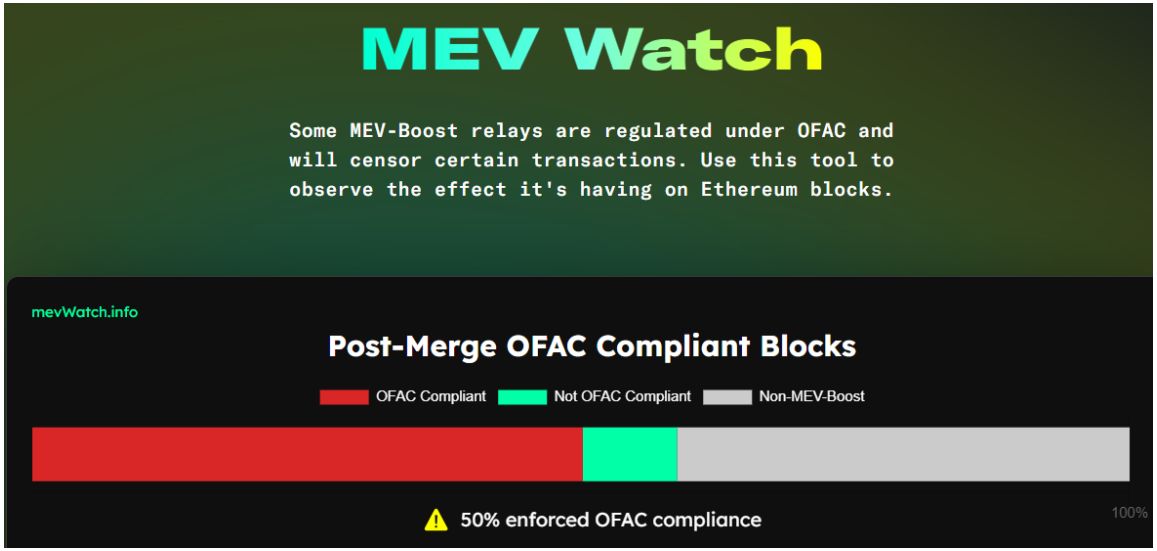
https://www.binance.com/en/buy-sell-crypto

1. Are you able to buy **Monero** (XMR)?
2. Are you able to buy **Dogecoin** (DOGE)?
3. Are you able to purchase **Terra** (LUNA)?
4. Why do you think that one of the coins can be purchased on Binance but not on Coinbase?



Some miners may refuse to mine blacklisted tokens

- Miners choose the transactions that they wish to mine
- Miners use **MEV programs** (Maximum Extractable Value) to decide which transactions to include in a block.
- Miners' MEV programs may examine addresses to see if they are blacklisted or sanctionned and refuse to mine them if they are.
- This is currently being seen on the Ethereum blockchain.



https://www.mevwatch.info/