The
CRYPTO VIGILANTE

Special Report to Canadians on Crypto Privacy

Mr. X
Technical Crypto Analyst

Mr. A
Crypto Market Technician

Mr. Z
Crypto Asset Analyst

Special Report to Canadians on Crypto Privacy

We at The Crypto Vigilante (TCV) have been humbled and awed at the bravery and leadership displayed by the Canadian Truckers and their supporters. They should be regarded as true heroes for ages to come by all that believe in the power and light which live within the human spirit.

Conversely, the acts of the despicable globalist cabal at Klaus Schwab's World Economic Forum (WEF), along with its idiot-puppet-boy Canadian Prime Minister Justin ~~Trudeau~~ Castreau (who is almost certainly Fidel Castro's illegitimate son) and even more pathetic lackeys, will ultimately be consigned to the 'dung-heap of history'. But until that's achieved, there is much work to be done.

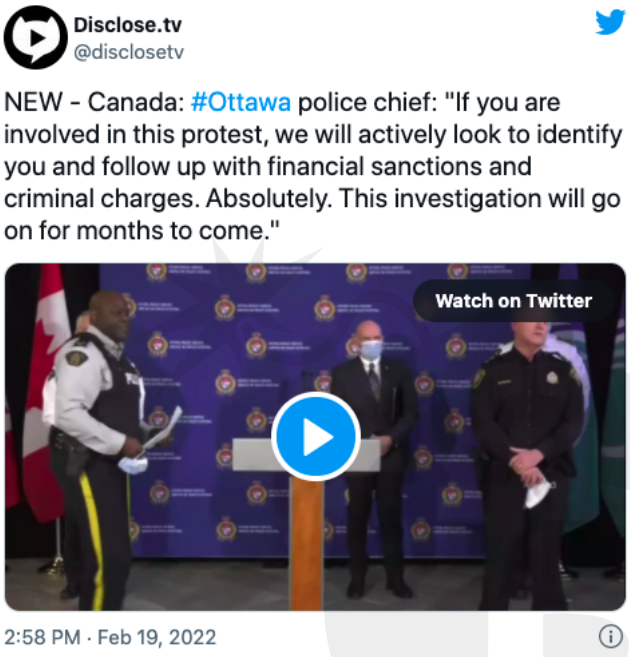
For the time being, they are still sitting in front of levers-of-power which can pack quite a bite. We therefore share this Special Report as a PSA to all those who love real liberty, so that they are armed with the critical information necessary to outmaneuver the evil confronting us all.

While our subscribers have long been made aware of procedures to ensure that their funds cannot be tracked, frozen or stolen by corrupt governments, we are compelled in the interest of what's right to share this primer widely and freely to all those who need to know.

What's Going On

The Canadian government (or more accurately their globalist handlers at the WEF) have taken extraordinary measures to fight the Freedom Convoy. Finance minister Chrystia Freeland, whose grandfather was a prominent Nazi and who herself is a communist WEF Director, has begun freezing bank accounts AND blacklisting crypto wallets of anyone suspected of doing anything they 'don't like'. They are also targeting anyone involved with the protests with criminal charges.

For example, Castreau's Justice Minister David Lametti recently said that being a Trump supporter is one of the factors in determining whether or not Canadians' bank accounts will be seized or frozen.



As of Saturday, February 19, 2022, the Canadian government has already frozen at least 76 bank accounts, worth approximately $3.2 million. There have also been recent rumors about a possible bank run due to some panic regarding temporary banking outages at the top Canadian banks.

Even Americans who have donated to the Canadian trucker convoy efforts have had their personal information exposed in the recent GiveSendGo crowdfunding platform's security breach, and have been publicly targeted and harassed as a result.

While extremely painful for all those caught in the snare, we have no doubt that the Canadian government's actions were something of a "last resort" move.

Why?

Because by doing so, they are drawing attention to the real facts surrounding cryptocurrencies as a tool to escape government oppression.

There's been a carefully orchestrated movement to keep the average joe believing that Bitcoin is private and uncensorable. This has been deliberately done to keep as many people as possible vulnerable to asset-seizures, arrest and censorship should they need to drop the hammer - which they have, of course, now done.

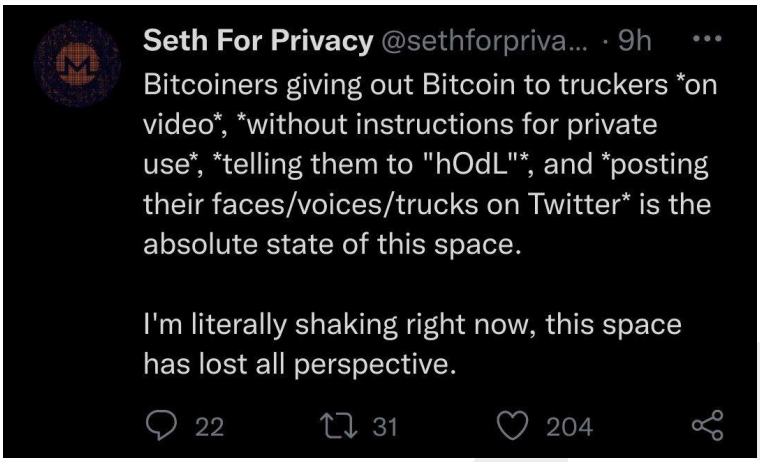
So, without further ado, here's an ultra-crash-course in crypto privacy, and what you should DO about it.

BITCOIN IS NOT PRIVATE, and therefore, it can be effectively frozen, censored, and used to track you down and persecute you for your actions.

Also not private? Ethereum, Litecoin, Zcash, Dash or BTC payments made on the Lightning Network.

These are what we at TCV refer to as SURVEILLANCE COINS.

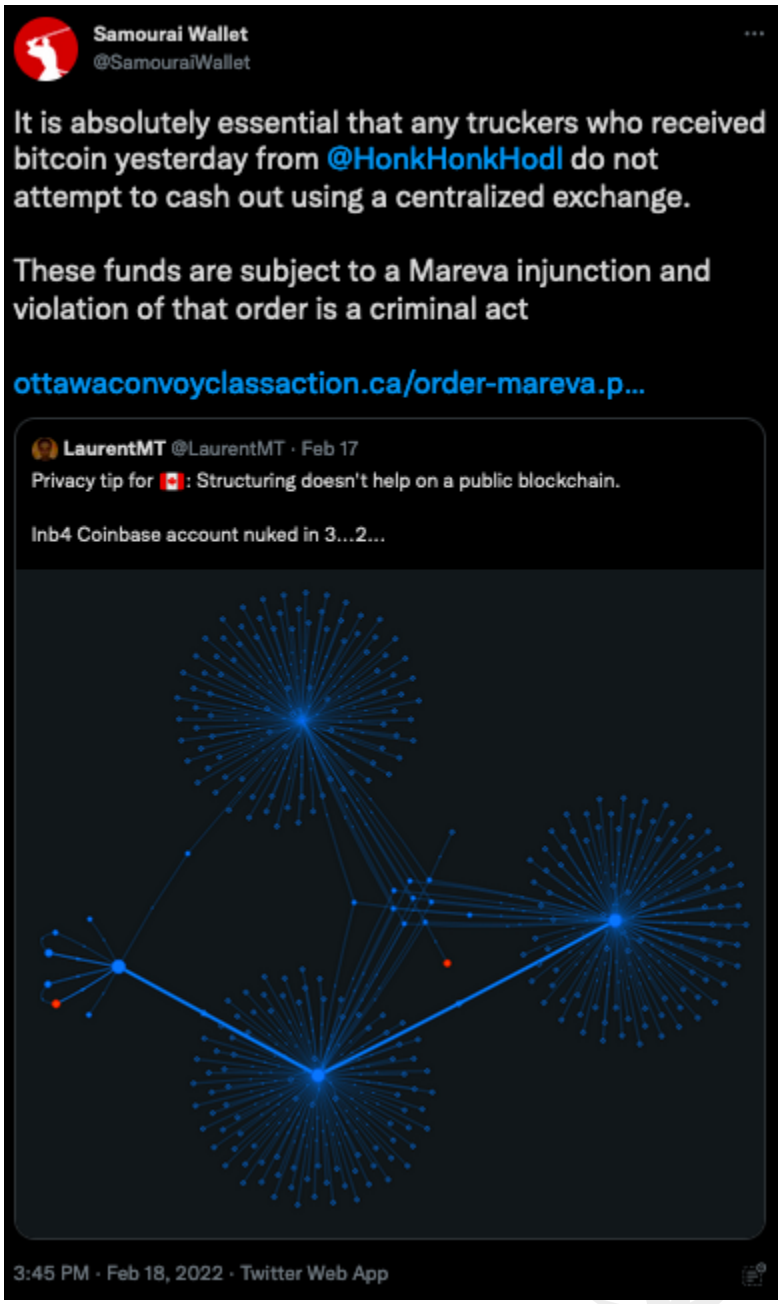
When the GoFundMe funds were stolen by the government and people shouted "Bitcoin fixes this!" we all shook our heads, because we knew that Bitcoin does NOT fix this.



https://twitter.com/sethforprivacy/status/1494772839924355079

Bitcoin, like every public cryptocurrency can be censored at an exchange or even wallet level if TPTSB decide they want to (as they now have). But even more than that, your identity can be linked to your

activity via blockchain analysis, leaving you vulnerable to further prosecution if you 'dared to donate a few satoshis' to anything that is considered out of favor with our 'Dear Leader'.



https://twitter.com/SamouraiWallet/status/1494699654491029510

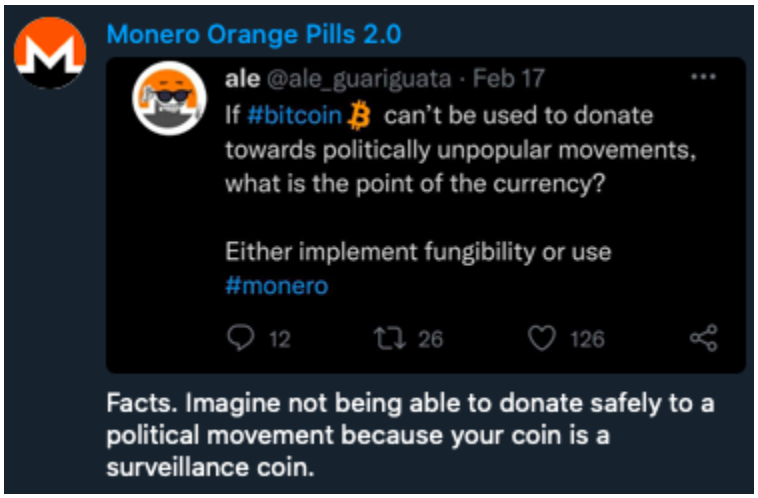
This 'dirty little secret' of Bitcoin has been kept on the hush-hush. Why? Because if it was widely-known, then people would have acted differently and the government *wouldn't have been able* to surveil, censor or control the Trucker Convoy funds.

While there is definitely still a place for Bitcoin and other 'surveillance coins' in the crypto economy of the future, when it comes to defending liberty from tyrants, we need to be brutally honest about their limitations, and focus instead on "what really works". So what does?

There are currently only two primary cryptocurrencies which are truly private, and therefore safe from surveillance, censorship, and seizure - Monero (XMR) and Pirate Chain (ARRR).

Monero and Pirate Chain are fundamentally different from all the others in that they are TRULY PRIVATE. This means that if you use them:

- *No one but YOU will ever know that you sent them to anyone else. In other words, they can keep this from happening to you.*



By using Monero and Pirate Chain, your privacy is protected, even when it comes to the recipient of the funds! They don't see 'who' it came from, unless of course you *want* them to know.

- *It is not possible to 'blacklist' wallets and therefore censor coins*.

When it comes to Monero and Pirate, even speaking about 'blacklisting wallets or coins' is somewhat nonsensical. Since no one but you can see the contents of your wallet, or even know whether or not any coins exist in your control, no one can do anything to block them.

There's so much more to say about Monero and Pirate Chain[1], but for now, it's more important to arm you, the reader, with information you can use today. So here are our key recommendations:

1) **If you want to pay, donate, or receive donations or payments for ANY reason, then you should first and foremost be prepared to send/receive Monero or Pirate Chain.**

Had the Trucker Convoy organizers received Monero or Pirate, then not only would those funds not have been able to be frozen or confiscated, not only would the donor-lists not have been 'doxxable', but there would have been zero record that any fund transfer happened in the first place!

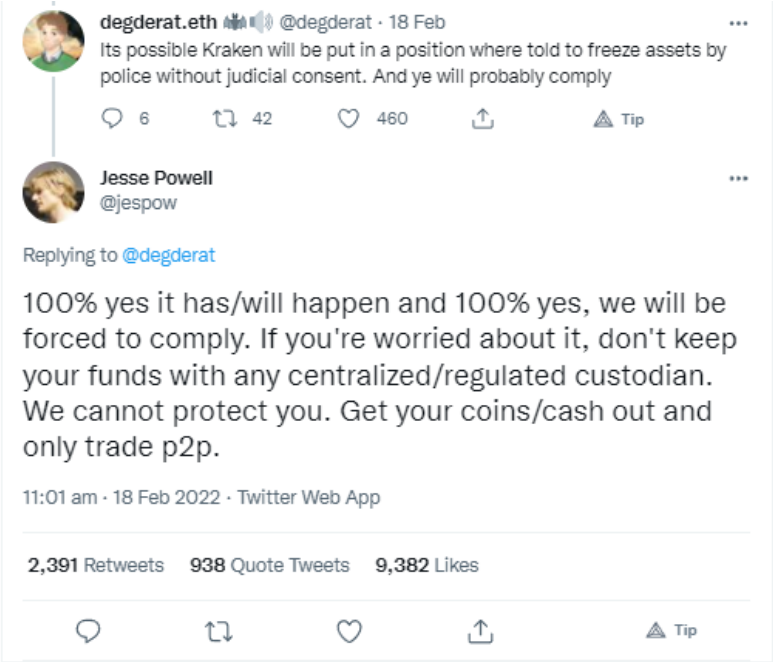
In practice, Monero is easier to obtain than Pirate Chain right now because it's the more developed privacy coin and available on more exchanges. If it's not available on your exchange, don't fret. For Monero, we recommend using Kraken or Binance to buy & sell XMR. If you want extra privacy, you can also use LocalMonero, but be extra careful to carefully read and follow all of the user guides and read the knowledgebase - watch out for scammers and be careful to follow laws in your jurisdiction or risk getting caught by undercover law enforcement. Keep in mind that you can also access LocalMonero via the Tor network here (the Tor Browser is required).

[1] Like for instance, how Satoshi, the inventor of Bitcoin went on record saying that he wished he could have made Bitcoin private like these, but he didn't yet know how (the technology came together only several years after Bitcoin launched and Satoshi had long since ghosted).

If all of those exchanges are unavailable, another option is to use Bisq (a peer-to-peer decentralized exchange) to purchase BTC and convert your BTC to XMR, and back again. *Warning: Since Bisq is a decentralized exchange that doesn't require know-your-customer (KYC) information, BTC going to & from that exchange is often likely to be classified as "dirty" by major blockchain analytics firms, KYC exchanges, major crypto payment processors, and other centralized services. Therefore you must be careful to ONLY send/receive BTC (or any other surveillance coin) from anonymous/decentralized crypto exchanges such as Bisq that are not connected to your real-world identity (i.e., obtained via a KYC exchange), otherwise KYC exchanges may freeze your BTC or even shut down your crypto exchange account entirely. If this concept is too complicated to understand, an even better solution is to avoid this problem altogether, and* ***never send or receive BTC, or any other transparent/surveillance coin to/from an anonymous/decentralized crypto exchange****. You will avoid a lot of problems this way.*

2) **Get your crypto OFF of exchanges and into wallets that only you control.**

We can't emphasize this point enough. As the saying goes, "not your keys, not your crypto." As things stand, the pace of asset seizures on exchanges is looking to accelerate, and you don't want to become a casualty of it. Just look at what the CEO of Kraken has to say about it in the twitter snapshot below.



If you think you are 'safe' and want to use a centralized exchange, you can take that risk - but be smart about it. Treat it like a cold-shower: quick in and out. Every second you leave your assets on a regulated exchange, you run the risk of the funds being stolen by these kleptocratic maniacs.

3) **If you are a liberty-minded vendor of goods and services, then you should acquaint yourself with Monero and Pirate Chain so that you are comfortable receiving these as payment for your goods and services.**

A functional cryptocurrency in a parallel economy is only useful insofar as it can be used to acquire goods and services. If you are a business person or vendor, you will help the cause by being part of that economy.

4) **If you are in Canada and want to 'Cash out' to Fiat (of your Bitcoin, which hopefully was only the last step after using Monero or Pirate Chain) here's how you can do it:**
    a) Get Wasabi desktop wallet for your Bitcoin, and put them through its built-in coinjoin (this is an anonymizing function)
    b) Use maximum coinjoin value of 50
    c) Be patient. The coinjoins can take a while.
    d) Send your post-coinjoin Bitcoin to your account at Bull Bitcoin, which enables you to exit by selling your Bitcoin to Canadian dollars (CAD) and into bank / credit card / billers

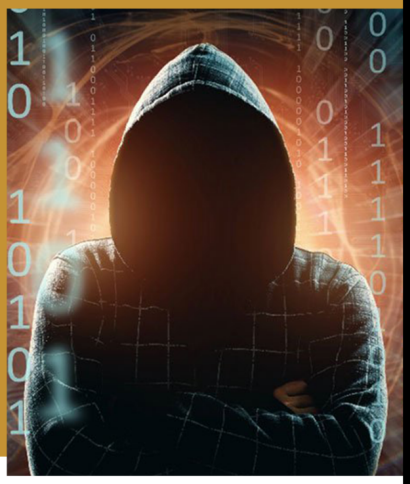
While these tips only scratch the surface of things you can do to protect yourself (and support freedom for yourself and others), they offer a solid start.

As the Canadian trucker freedom convoy movement spreads to the US and other countries, the importance of understanding and practicing these crypto privacy skills and embracing true "freedom coins" like Monero and Pirate Chain will only grow.

If you are not already a TCV subscriber, we invite you to subscribe to our monthly crypto newsletter, which also includes access to our more detailed coin control reports, Featured Crypto Asset Reports, technical analysis trading alerts, videos, & updates (published several times a week), and all our archived newsletter issues since launching in 2019.

We believe that the 'bad guys' have massively overplayed their hand, and it's now only a matter of time before the true power of blockchain - fueled by real privacy - shows the world what it can do. Not only will it enable us to all cast off the shackles of oppression, but for early adopters, it will result in extraordinary wealth creation. We invite you to join us on this journey.

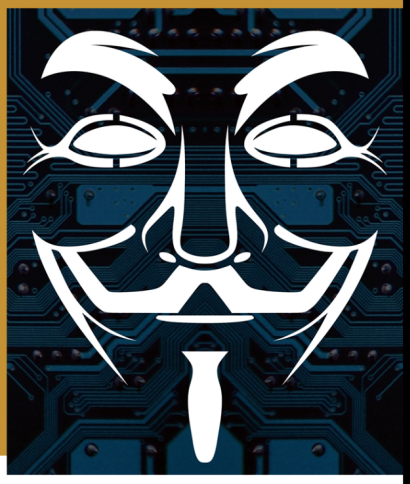
Mr. X, Mr. A, & Mr. Z



Mr. X

Technical Crypto Analyst

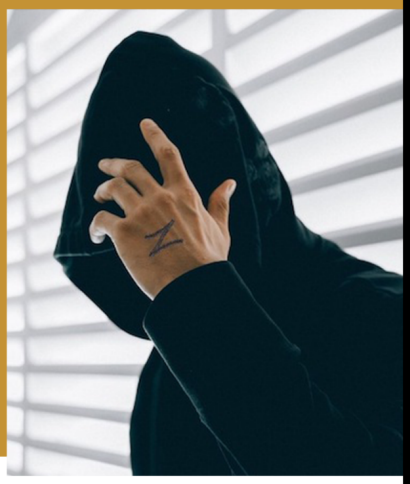
Mr. X is a former IT & information security consultant, and equities trader. He is an early Bitcoin adopter, investor, miner, and trader (since early 2011 when it was under $1), early Monero adopter, investor, miner & trader (since 2015 when it was under 50 cents), and has experience as a crypto asset fund manager, consultant, & analyst, helping his clients generate over $10 million in crypto asset trading profits. His university degree is in business IT systems, with additional studies & certifications in the areas of computer science, information security, networks, & programming. He is passionate about sound money, cryptocurrency, finance, economics, technology, security, liberty, and privacy, and enjoys helping others grow in their knowledge in these areas.



Mr. A

Crypto Market Technician

Mr. A is a former network and security consultant. He was a crypto miner, investor, trader since 2012, and an early Monero and Pirate Chain adopter too. He has consulted for medium and large sized mining operations and hedge funds who need Bitcoin custody solutions. His university degree is in molecular biology with many other certifications in IT, security, networks and audio engineering. He is an accomplished music producer and DJ who has played large festivals around the world and engineers music tracks with the most advanced hardware and software technologies available. He is passionate about biohacking, mountain biking, and generally being outdoors while enjoying life to the fullest in the most epic natural settings.



Mr. Z

Crypto Asset Analyst

Mr. Z is a former Wall Street trader, investment analyst and consultant. Over his career in the corporate world, he awakened to just how broken many of our economic and social systems are. By the mid-2010s, when he had all but completely walked away from financial markets, he stumbled upon Bitcoin in the comments section of ZeroHedge. Here he saw a path which could help bring honesty and equity back to world systems – not to mention offer incredible opportunity for adopters. He was instantly hooked. By early 2017 he was providing fundamental blockchain analysis and advisory to numerous influential crypto investors and enthusiasts. Mr. Z's passion for how blockchain can re-shape the world for the better is influenced by his extensive study in not only world history, economics and finance, but mythology, religion and spiritual traditions of both the East and West.

The CRYPTO VIGILANTE

CryptoVigilante.io

Disclaimer: The Crypto Vigilante needs no disclaimer. Everything we say here is what we believe. Furthermore we need no disclaimer because we believe that all nation states, governments, securities agencies or other legislative bodies are illegitimate and we do not recognize them nor believe we need their permission to say what we feel about any topic and frankly think it is hilarious that people think a government body should be there to protect them.

However, because we know that all manner of government agencies will come after us just for showing such disdain for them we are going to include a standard, cookie-cutter disclaimer below just to keep them off our backs.

Enjoy reading it, bureaucrats at the SEC. Information contained in The Crypto Vigilante emails or on The Crypto Vigilante website (www.cryptovigilante.io) is obtained from sources believed to be reliable, but its accuracy cannot be guaranteed. The information contained in such publications is not intended to constitute individual investment advice and is not designed to meet your personal financial situation. The opinions expressed in such publications are those of the publisher and are subject to change without notice. The information in such publications may become outdated and there is no obligation to update any such information, such as cryptographic advice. Jeff Berwick, Ed Bugos, Rafael LaVerde, Mr. X, and other analysts or employees of The Crypto Vigilante may from time to time have positions in the crypto assets, securities or commodities covered in these publications or website. Any Crypto Vigilante publication or web site and its content and images, as well as all copyright, trademark and other rights therein, are owned by The Crypto Vigilante (TCV). No portion of any TCV publication or web site may be extracted or reproduced without permission of The Crypto Vigilante. Unauthorized use, reproduction or rebroadcast of any content of any TCV publication or web site, including communicating investment recommendations in such publication or website to non-subscribers in any manner, is prohibited and shall be considered an infringement and/or misappropriation of the proprietary rights of TCV. TCV reserves the right to cancel any subscription at any time, and if it does so it will promptly refund to the subscriber the amount of the subscription payment previously received relating to the remaining subscription period. Cancellation of a subscription may result from any unauthorized use or reproduction or rebroadcast of any TCV publication or website, any infringement or misappropriation of TCV proprietary rights, or any other reason determined in the sole discretion of TCV.