[JTC: Don’t let this writer’s literary eccentricities and internet jargon stop you from absorbing the message! He (or she) has the basic idea of how freedom is to be wrenched from the leviathan state. I am intrigued that the techniques I have been relying on – the TOR Browser and the private web – are not even mentioned. However, there may be more than one way to – *Oh, pardon!* -- skin a cat!]

the road back from serfdom

is a road that leads away from state controlled money

By “bad cattitude”

el gato malo Apr 18, 2024
[First seen on LewRockwell.com]

my article the other day about the **road to serfdom** and the ratchets of inflation and political power providing perverse incentives laid out the problem:

politicians who gain power by wrecking financial and social fabrics and gain revenues by wrecking currencies will run awful playbooks to maximize their perverse incentives and the worse they do, the more they get, which, in turn, makes things worse.

it’s a positive feedback loop and those only end in starvation or explosion.

so what is the solution?

the solution is to take money, commerce, savings, and investment away from not only state control but from state view. in the end, the truly operative phrase is “you cannot tax what you cannot see.”

it’s quite literally the only way to get a durable fix.

even outright rebellion and mass movements and “putting new governments in charge with better rules etc” is not a long term solution. best case, you just reset or move back on the **tytler cycle**. but the cycle will remain as inexorable as the seasons and you’ll be fighting the same wars over and over, probably at higher rates of speed. it’s a lot better than nothing and still a worthwhile undertaking, but i think we can do better. i think we can go our own way.

since time immemorial, governments have controlled currencies and done an awful job of it. we still call money printing “debasement” in reference to rulers mixing other metals into the gold or silver when striking coins. it’s just the classical version of “money printer go BRRRR.”

governments are lousy stewards of currency. always have been. always will be. they debase, devalue, and steal. let them run the banks as well and you are well and truly trapped. this is not some accident of financial evolution, it was done by design: rulers have always sought to control currencies because control of currencies is power and wealth.

you come into gatostan and i make you restrike your gold into “gatitos” the currency of the realm. maybe i mix some lead in when i do. or maybe i just take some of your gold as “seigniorage” and the coins you get back weigh 5% less than the ones you gave me to melt. this basically worked like early sales tax (but at least it only applied to coins once, not every time they were spent). of course “recoinages” were common so this could be repeated.

governments love banking because banks keep records and are easy to co-opt or bully. you bribe or threaten your way into getting them to:

1. let you see what everyone does
2. let you grab whatever anyone has without having to go rooting through the back yard trying to discern where they buried the silver

that second one is REALLY important so let’s delve a bit deeper.

in the age of metallic/physical money, you as an owner of such faced a choice: you could keep it yourself and hide/protect it or you could deposit it with a trusted counterparty. each has risks and costs and the danger of having (and being known or even suspected to have) large amounts of cash on hand are no joke. it attracts brigands and sneak thieves and this is, for most, unreasonable, impossible, or intolerable. very few people are willing/able to keep their life savings under the floorboards.

so you need a bank-like entity to get this money monkey off your back.

we’ve had a number of private currencies that have worked well from private US bank scrip to birmingham buttons. private issuers, especially if they must compete and clear with other private issuers and grant one another audit rights can and have provided systems for very sound money. it’s a market solution that works to create good, useful currencies.

but it’s not government proof.

no currency however sound is safe if leviathan can see it.

no bank that requires licensure from the state to operate or even whose executives and bookkeepers are known to and subject to arrest or intimidation by state actors can truly be trusted and if the IRS or DEA or FBI says “gimmie dat” the bank locks your accounts and your assets are seized faster than you can say:

civil asset forfeiture, liens, garnishments, there must be 50 ways to lose your lucre. (apologies to paul simon who did nothing to deserve that)

at least in the case of the US, this reach is increasingly near perfectly global and even the gaps are not terribly useful as you cannot get that money back into any banking system where it would be useful to you and simply being known to hold or trade assets in “forbidden zones” gets you on a list and KYC (know your customer) rules get more draconian every 5 minutes.

so you’re always, in effect, choosing between forms of thieves to which you’ll be vulnerable. the whole thing is a hobson’s choice.

THE REACTION FROM THE IRS WHEN YOU CHEAT ON YOUR TAXES.
YOU'RE TRYING TO KIDNAP WHAT I'VE RIGHTFULLY STOLEN.

and now i’m going to upset a bunch of people: sorry, but bitcoin does not fix this.

i wish it did, but it doesn’t and i’ve been tracking and digging around in it for ages and bought my first coins in 2011, so while i do not ask that anyone ultimately agree with me, i would appreciate people actually listening to my take on this first before the flood of “yOu dON’t GEt bITcoIN!” comments start. i do. and the plumbing. and the math. it’s a marvel. it’s fascinating. it was an astounding achievement and innovation. so was netscape. and like netscape, BTS is a version 1.0 product that’s not gonna make the cut.

bitcoin constitutes an exceedingly vulnerable system (often in ways people are not considering) that is highly compromised by state actors to the point of being more honeypot than hidey hole.

and you’d rather be chased by ring wraiths than these people.

BTC is certainly not a currency in any meaningful sense.

it is not a minimally viable product as either a means of exchange or as a means or escape.

and that latter one is the real doozie.

i came grudgingly to this viewpoint having been in and around BTC since it was in the single digits. i came to bitcoin through cryptography and early public key crypto projects like PGP that were so seminal in the whole idea of open source.

let me be clear: i am a huge believer in crypto-currency.

i think it’s probably the most important idea in the world right now.

but i also think it’s been stuck in an that ends in a brick wall as the early promise and purpose was lost among ponzi games, “coin have dog,” and lost vision and execution to the point where i was having a conversation with the founder of one of the major exchanges and he literally could not describe his order matching algo in even rudimentary terms, the primary purpose of ETH is ponzi casino games, and the best argument for BTC right now is “publicly traded ETF’s gotta buy it!”

this last one, of course, only makes the problem worse by generating not just greater fiat links but massive KYC systems. it’s all an increasingly curated garden of surveillance.

BTC was the AOL of crypto, a good start but unable to move forward out of early days; but now, BTC is predominantly spyware. and that’s not going to work out for people who want to leave governments behind.

when one looks at a currency there are a number of features that are needed:

1. sound
2. secure
3. scalable
4. widely accepted
5. stable
6. private
7. anonymous

BTC is 1 for 7, maybe 2 for 7, but probably not in the long run. it is sound. but it is not secure in the sense you really want it to be and the security around block integrity and ability to spam empty or altered ones inherently stands in opposition to “scalable” because its security lies in processing power and that makes scale expensive/prohibitive.

simple fact: until 100 million of us can buy lunch with it tomorrow, it’s not even in the discussion as a currency.

the argument that “this is fixable with layer 2” has been “2 years away” for a decade and yet we’re no materially closer to buying burgers mañana. this seems unlikely to change but even if it did and we got sound, secure, scalable, and widely accepted and those then led to “stable” as the tie to goods based transactions made BTC value a function of what it can buy as opposed to bubble baby beachball trading, it is STILL not a minimally viable currency. these would be neat technical feats and a cool monetary study in alt systems, but as a vehicle to “go our own way and leave leviathan behind?” nope. it’s loaded with GPS trackers, bugs, cameras, and every off and on ramp into currencies and markets is a stasi checkpoint.

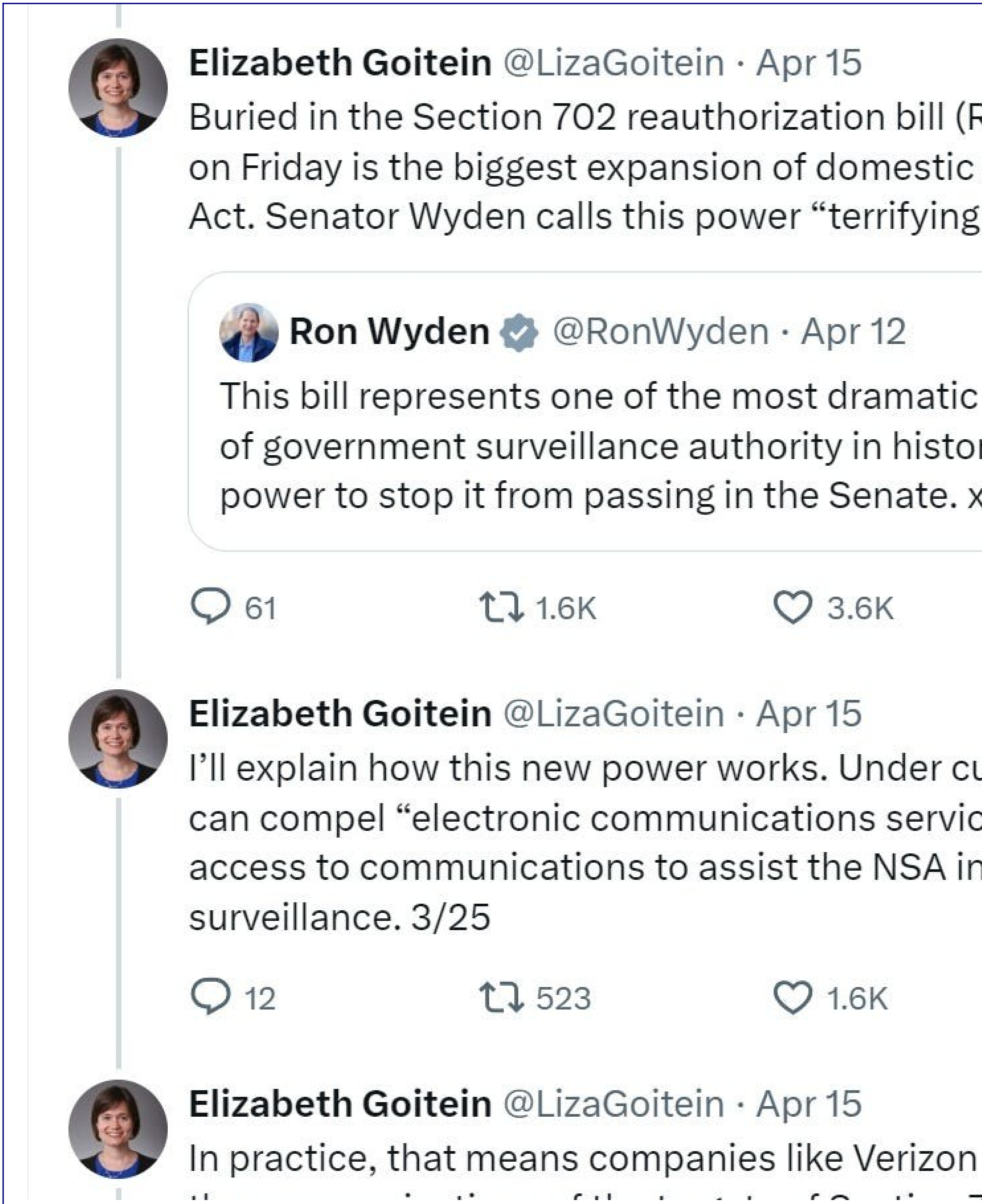
get this thing off me
Tractive GPS Tracker for Cats and Dogs with Activity Monitoring | Tractive
Visit ›

private and anonymous matter and BTC is neither. tumblers do not really work and it’s easy to flag tumbled coins as they hit chains and bar them from many kinds of commerce. they can create “tainted money” lists and make merchants adhere. they are just waiting for you to set up patterns that let them lock into your public keys and get a picture of everything you have done. maybe (but quite probably not) a few utter obsessives might manage to accomplish a sort of “one time pad” for BTC, but doing this every day, every trade, every transaction is monstrously expensive and difficult. “works for the most OCD 0.001%.” is not a basis for currency and certainly not for shopping or vendors.

NSA, DEA, and who knows who else track BTC in real time and use public keys to find all your instances on the chain. they can say “yup, that’s actor 27B421R right there” and based on what you bought, triangulating on who you are and where in meatspace you reside from any even rudimentarily common consumption pattern is kindergarten trivial for tax, intelligence, or law enforcement agencies in modern america and it’s about to get 1,000 times worse as the new RISSA rules that just passed in truly shameful fashion come into effect.

in essence, any company that touches communications or has access to communications can be suborned and dragooned by NSA to help them spy on you. every cable guy, IT staff, internet company, store with wifi, or computer repair shop can, without warrant and under gag order that prevents them from revealing that this has occurred, be required to help spy on you.

this is the dark future snowden warned about.



Elizabeth Goitein @LizaGoitein · Apr 15

Buried in the Section 702 reauthorization bill (R
on Friday is the biggest expansion of domestic
Act. Senator Wyden calls this power "terrifying

> **Ron Wyden** @RonWyden · Apr 12
>
> This bill represents one of the most dramatic
> of government surveillance authority in histo
> power to stop it from passing in the Senate. x

61 1.6K 3.6K

Elizabeth Goitein @LizaGoitein · Apr 15

I'll explain how this new power works. Under cu
can compel "electronic communications servic
access to communications to assist the NSA in
surveillance. 3/25

12 523 1.6K

Elizabeth Goitein @LizaGoitein · Apr 15

In practice, that means companies like Verizon the lack of privacy and anonymity in BTC will make it a wide open book here. if the state wants you, they get you. and it’s only going to get worse.

i spoke to a good friend of mine about this. he’s deep into these matters and comes from “the community.”

his take:

“I am moving our data repos to Iceland where they will not enforce a data custody subpoena. Go long on Iceland based and owned data centers.”

he’s the opposite of a worrywart.

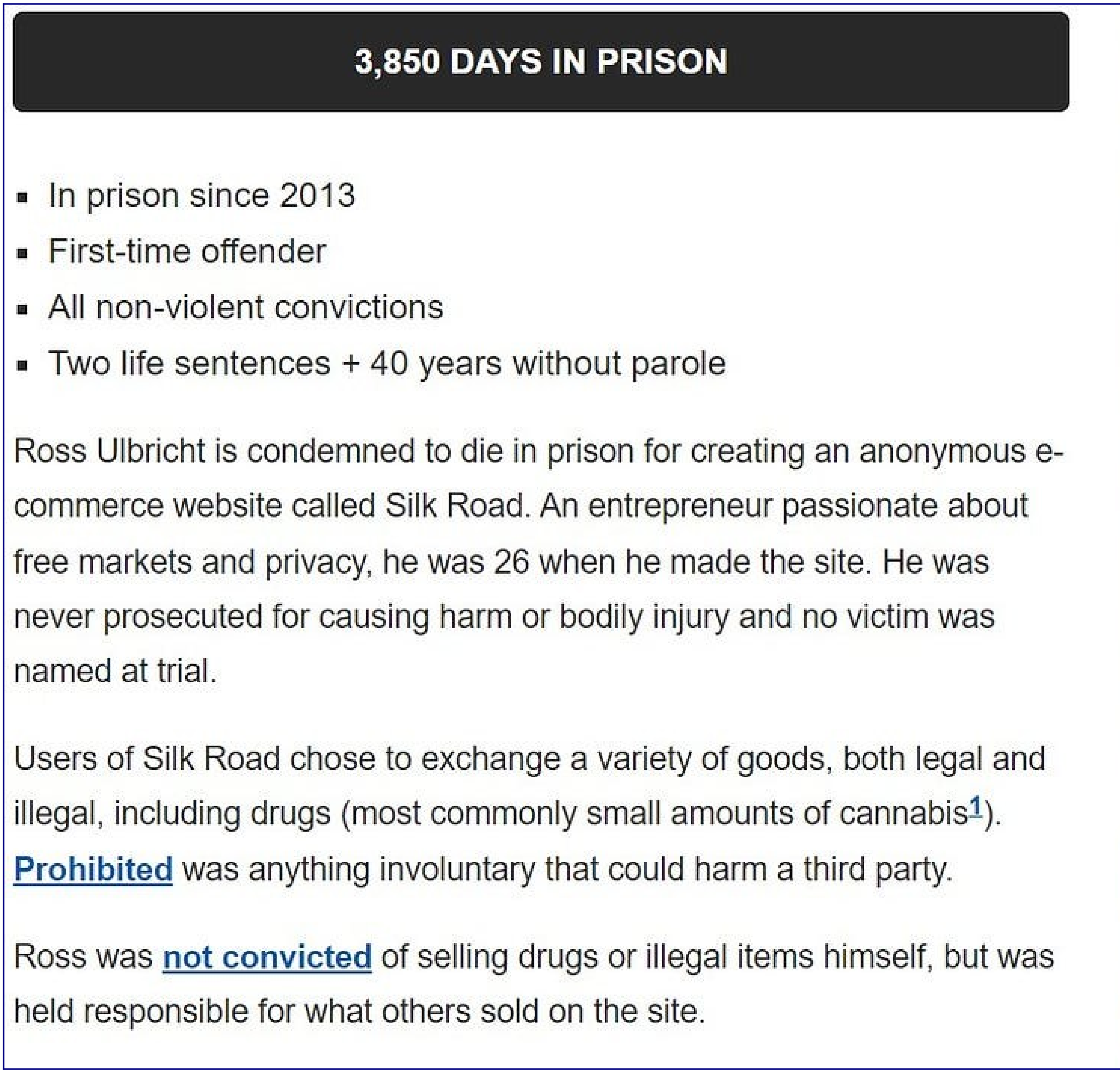
this is likely sound advice.

it’s also the start of the solution.

even “my keys, my coins, no one knows my seed phrase” is not going to save you from greedy grabby government because the mere fact of being known, seen, or suspected of transacting is enough.

they come with guns and they take.

ask ross ulbricht (aka the dread pirate roberts, founder of the silk road marketplace) how “your keys, your coins” worked out for him. (they claim to have busted him based on using internet at a library. this has always seemed like an awfully rookie slip for a guy like this. one wonders about story and cover story. but i doubt we ever know.)



3,850 DAYS IN PRISON

- In prison since 2013
- First-time offender
- All non-violent convictions
- Two life sentences + 40 years without parole

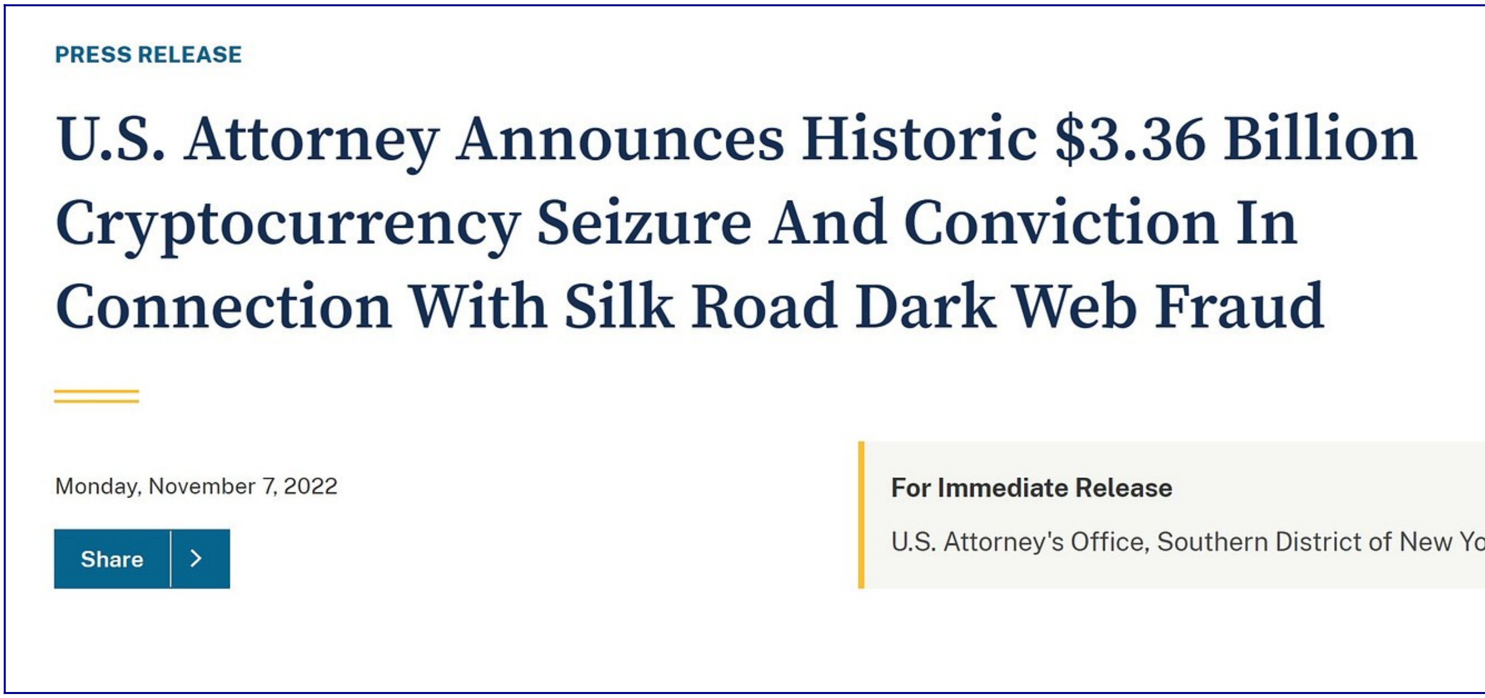
Ross Ulbricht is condemned to die in prison for creating an anonymous e-commerce website called Silk Road. An entrepreneur passionate about free markets and privacy, he was 26 when he made the site. He was never prosecuted for causing harm or bodily injury and no victim was named at trial.

Users of Silk Road chose to exchange a variety of goods, both legal and illegal, including drugs (most commonly small amounts of cannabis[1]). **Prohibited** was anything involuntary that could harm a third party.

Ross was **not convicted** of selling drugs or illegal items himself, but was held responsible for what others sold on the site.

sam bankman fraud gets 25 years (and will not serve 10) for a massive theft, ross gets life for “trying to step outside the system.”

and yes, they did take his coins.


PRESS RELEASE

U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud

Monday, November 7, 2022

For Immediate Release

U.S. Attorney's Office, Southern District of New Yo

there is also a large “**coin blacklist**” to keep specific ones off exchanges, keep them from being turned to other currencies, and to track users. not hard to add “any business accepting them is complicit in money laundering” as an affirmative obligation of doing business. it locks down pretty tight pretty fast. you really want to dance in that minefield?

the whole ecosystem is now mostly spyware. you wanna know why governments don’t shut it down? because it’s a key part of their intelligence gathering. they WANT you on the open network broadcasting your moves while thinking they’re stealthy. you think you’re hiding your cards. but the cards are marked on both sides.

and so here is where we start to get down to the real nub of the matter:

like burying gold in the backyard, simply being known to have a large pile of BTC attracts thieves and many of them may have badges and the modern version of “gimmie dat” far exceeds the dreams of erstwhile sheriffs of nottingham frogmarching you to sherwood to dig up the loot.

and to avoid this, there is only one real feature that matters: invisibility.

if they decide to come and get you, they can probably have you, at least your freedom and your hard assets, home, car, etc. and cryptography is not great for invisibility. secrecy, sure. you cannot read it. but you can see it. it pops like a flare. it invites investigation. secrecy requires stealth. but how can a billion transactions a day be stealthy?

that answer is twofold: they need to mostly be “off network” and take place behind firewalls. this helps (a lot) but it still places the transactional centers as bright strobes in the data ocean and they’ll get monitored and so will all the traffic going to them and from them. that means you. and if they have your network, they have you anyway. and if they don’t have your network, this is how they will know to come and get it. and this is why we need the second half of the answer: deep, omnipresent steganography.

no message

drinks at 9?

steganography is hiding messages against a background so that observers not looking for them do not notice that they are there. if cryptography is making the color of a grain of sand impossible to a viewer to discern, steganography is placing that grain of sand on a beach so a would be crypto-cracker has no idea which one to crack or, indeed, if there is any message here at all.

so how do we build this?

streams of encrypted data packets pop in normal networks. it’s like putting a flashing light on the users governments might be interested in. there are a hundred ways to sort them with data and network analysis, DPI, header analysis, and various forms of interception.

but only if you can see it.

if we want currency taken away from states, first we must take the internet. and this is going to be a helluva arms race. but i like our chances.

foremost, we need new structure. peer to peer mesh network structure with swarm sourced data, storage, and routing all using end to end encryption. this needs to include protocols (like IPFS) [“InterPlanetary File System”] and routing, DNS, all of it. for real safety, it may well need to include layer 1 (the physical fibers and wires and wavelengths of communication) but even the creation of massive meshes of constant encrypted traffic where no outside observer can tell a cat meme from a stock transaction or a picture of your kids from the deed to your house and where senders, sendings, and pathways are all opaque gets us a lot of the way there.

this literally turns the essentially infinite resource of idiots arguing with idiots on social media into the basis to protect the privacy of the internet. (talk about an allegory for the ages)

we need a whole system that’s analysis resistant as a core design premise.

you could hide anything in that.

and THAT is how we get away.

where is the data? who knows? not even the users know. who owns it? no one you can grab. it’s not on any one server. or maybe it’s backed up in iceland or some other safe place. business models around it will proliferate. “privacy purveyor” is a great biz model for small states that are not over the barrel of US regulators holding their banks hostage (as the swiss wound up being).

maybe BTC survives as a sort of ur unit, but i think the advantages of “no one can see the chains” is going to swamp any sort of residual metcalf network value, especially if there is not a large base of actual transactions for coffee and rent and subscriptions to cat memes underpinning it.

this is a truly radical change in networks and in systems. there likely will not be a non-open source operating system you can trust and “audit and checksum for PC and phone” is going to be a big deal as the threat surface shifts to “entry and viewing.” we need new routing, new domain naming, and whole new informational topologies.

it’s a massive undertaking, but the prize is the greatest shift in power between governments and we the people in the history of the species.

a starving leviathan will have to learn to do tricks to please the people in exchange for food. we can become customers, not the captured crops of tax farmers. it’s a helluva thing to imagine.

folks are working on it and parts of it. getting it to coalesce at scale and have the heft to expand is going to be the hard trick. it’s a “minimum energy to start the reaction” sort of equation and as many stunted networks like mastadon can attest, initial energy to get critical mass is high. bittorrent has had some success.

the initial motion will be the hardest part.

if only there were a huge network, some sort of social media, owned by a guy with near infinite resources and a longstanding interest in privacy and payment systems.

if only that guy had ownership of not just to an internet network out of the reach of governments because it was in space, but had actual rockets to launch more and a US government dependency upon him for their own launches that makes him a bit untouchable.

hey, wait a minute…

turning twitter into a hybrid social media and payment system that was end to end encrypted and had a mesh topology would be a helluva beginning. start moving it to the new internet protocols. commence the vast steganographic substrate and the holy mess of traffic that defies analysis as nodes ping each other and swap data payloads just as a matter of course and no single connection can ever be said to mean anything. musk may need to do it from mars for fear of arrest, but he seems like like mars, so…

is he playing 8d chess or is this just a truly wild example of a self-assembling clowncar about to drive into a gold mine? (or might we miss this opportunity altogether?)

bottom line is that this could be the start, the critical mass that leads to a self proliferating set of open source protocols that radically decentralizes everything and takes the whole of social media and commerce out of the hands and view of government, companies, and individuals. this system is too important to be run by anyone so it must become something that is run by no one.

layer one, the actual data connections, will be the hardest part and a final “this is owned by a company” risk. i can imagine systems that do not need this, but they are difficult when countries can grab fibers. the answer may lie in open airwaves to allow peer to peer wireless mesh with satellite/fiber backhaul.

time will tell how this shakes out, but we need to start somewhere and get the ball rolling with enough mass to matter. elon, if you need a cat to come consult on this, you know where to find me.

what a future that could be.