

Forum:[Hack Forums](#)

Thread: [Bitcoin privacy, run your own node. You're exposed.](#)

SIM-4831178 - January 21, 2021, 5:05 am

I'll list few things just to help everyone here as I believe 95% of the users have no clue how this network works and what they're doing to themselves.

Choose your case and you'll understand the level of your privacy. I won't talk about online exchanges, obviously you gave them all your info so you're not safe-private at all.

When you don't run your own node, third party broadcasts the transactions for you, so they get info from your devices as you're connected to these servers.

XPUB = is basically a master privacy key, anyone who knows it can view all past and future transactions that wallet created or ever will create, even if each transaction used a different address.

Case 1:

I stored my bitcoins into a non-custodian wallet (pc or phone) like Blockchain.info, Exodus, Electrum, Coinomi, Metamask, TrustWallet, LEDGER, TREZOR(AS YOU RUN THEIR APPS) etc etc.

In that case IF you used VPN as you created and as you use these wallets:
Your IP is stored into VPN's server and in case of a court your IP can be found and will be associated with all your BTC addresses.

In that case IF you DIDN'T use VPN as you created and as you use these wallets:
Servers of all these wallets have your IP and know your xpub so pretty much they know you and all your Bitcoin addresses (if they got your mac address they're able to know even more things about you).

Case 2:

I stored my bitcoins into non custodian wallets that support Tor like Samurai wallet, Blockstream Green etc for Phone and Wasabi Wallet for PC.

In that case your Bitcoin addresses are not likely to be associated with you (obviously if you move these coins to an exchange or into another wallet you're back to case 1.

Case 3 (and the best one):

I run my node and connected my wallet with that.

Subcases:

- I connected Wasabi Wallet which supports Tor with my node -> Your ISP knows you run a node but your Bitcoins can't be associated with you.
- I connected a wallet that doesn't support Tor -> Your ISP knows your node and your ISP knows which server stores your Bitcoin addresses which are obviously connected with you.
- I run node over VPN and connected Wasabi -> You're much safer but still the VPN server knows

you run a node.

- I run a node over Tor (best way is if your Operating System is Tails) and connected Wasabi (or even if you didn't doesn't matter that much) -> Noone knows that you run a node, noone knows your Bitcoin addresses.

After reading this thread I feel exposed, what could I do?

- Run your own node and run it over Tor.
- Use wallets that support Tor.
- Use Coinjoin (it's a coinmix feature of Wasabi). That doesn't make you 100% safe but it's something that helps A LOT, the more you coinmix the better of course. A chainanalysis can be done but doesn't mean they will be able to find your new btc address 100%, they have to find the owners of other 100-200 addresses which were participants to that coinmix so they can be sure that the new address they found is yours. In case of a court if it's not a criminal case that had to do with millions(many not just 1-2) or even billions of dollars worth of bitcoin I doubt that they'll do such analysis. Also imagine if you do 10 or 20 coinmixes.

If everyone uses CoinJoin chainanalysis will be useless, also exchanges will be forced to accept coins that come from coinjoin as they won't have a choice.

In few years you won't be able to deposit coins that used coinjoin feature in the past to online exchanges. If you want to do it, you'll have to do it now, I dream about a community that often uses schnorr, taproot, ricochet and coinjoin but that would be very ideal as people don't know the basics.

In code we trust, Bitcoin is the future.

Capital Bra - January 21, 2021, 5:58 am

I've read a story about a guy who used wasabi's coinjoin. He was never involved in any crimes but just wanted to try coinjoin out. He mixed his coins and ordered something online with bitcoin afterwards. A few days later he got raided by police and they suspected him to be involved in some serious crimes and that he wanted to launder his money on wasabi.

Can this really happen if you use coinjoin's?

I mean you are mixing with other ones bitcoin and obviously there will be some coins from criminals.

?Ñâzg?! - January 21, 2021, 6:03 am

(Jan 21, 2021 06:58 AM)Capital Bra Wrote: [\[CITE\]](#) I've read a story about a guy who used wasabi's coinjoin. He was never involved in any crimes but just wanted to try coinjoin out. He mixed his coins and ordered something online with bitcoin afterwards. A few days later he got raided by police and they suspected him to be involved in some serious crimes and that he wanted to launder his money on wasabi.

Can this really happen if you use coinjoin's?

I mean you are mixing with other ones bitcoin and obviously there will be some coins from criminals.

FFS guys don't use bitcoin if you want privacy
use monero

SIM-4831178 - January 21, 2021, 6:10 am

(Jan 21, 2021 06:58 AM)Capital Bra Wrote: [\[CITE\]](#) I've read a story about a guy who used wasabi's coinjoin. He was never involved in any crimes but just wanted to try coinjoin out. He mixed his coins and ordered something online with bitcoin afterwards. A few days later he got raided by police and they suspected him to be involved in some serious crimes and that he wanted to launder his money on wasabi.

Can this really happen if you use coinjoin's?

I mean you are mixing with other ones bitcoin and obviously there will be some coins from criminals.

As you're not the criminal you won't have any problem, you could easily prove by sign message or providing xpub (if it's a court case). By that way you'll prove that your previous address has nothing to do with fraud. Using coinjoin isn't illegal and you have the right to use this feature so you can improve your privacy. It's same like using Tor, it's human's right to use such features/services.

(Jan 21, 2021 07:03 AM)?Ñåzg?I Wrote: [\[CITE\]](#) FFS guys don't use bitcoin if you want privacy use monero

I'm a very big fan of monero, although it has other problems to be solved and it is not Bitcoin.

Omniscient - January 21, 2021, 8:08 am

So then how do you get the coins into FIAT under your scenario? Because I'm fairly sure that your BTC will be flagged for all that secrecy. They'll want to know where those Bitcoins came from and if they don't know they might just shut you down.

If you open a bank account and are constantly depositing cash, they will close your account, because they'll consider the activity as suspicious.

Quote:FFS guys don't use bitcoin if you want privacy

Yeah, that's basically it. It's a PUBLIC LEDGER. Consider how similar it is to HF. We are open web site and everyone uses a pseudonym but if you use this site to commit a crime you're at risk. The lesson is don't use something that PUBLIC to commit a crime. You can't escape the fact that Bitcoin is an open ledger and that no matter what you do on it it's a potential that you'll expose yourself.

Quote:As you're not the criminal you won't have any problem, you could easily prove by sign message or providing xpub (if it's a court case). By that way you'll prove that your previous address has nothing to do with fraud. Using coinjoin isn't illegal and you have the right to use this feature so you can improve your privacy. It's same like using Tor, it's human's right to use such features/services.

Meanwhile you're in a jail having your life ruined. Yeah, shit plan right there. And trust me, they'll find a way to get you once they arrest you. The chances of you walking are slim.

Use Monero if you need a privacy blockchain.

btw you didn't really mention that imho you should be changing wallets frequently. Easy to start wallets. Heck you can do a new wallet for every transaction if you're really paranoid about losing your privacy.

SIM-1866423 - January 21, 2021, 8:33 am

Cant you just create new bitcoin wallet for each transaction ? Its pretty easy.

SIM-4831178 - January 21, 2021, 8:44 am

(Jan 21, 2021 09:08 AM)Omniscient Wrote: [\[CITE\]](#) So then how do you get the coins into FIAT under your scenario? Because I'm fairly sure that your BTC will be flagged for all that secrecy. They'll want to know where those Bitcoins came from and if they don't know they might just shut you down.

If you open a bank account and are constantly depositing cash, they will close your account, because they'll consider the activity as suspicious.

Meanwhile you're in a jail having your life ruined. Yeah, shit plan right there. And trust me, they'll find a way to get you once they arrest you. The chances of you walking are slim.

Use Monero if you need a privacy blockchain.

btw you didn't really mention that imho you should be changing wallets frequently. Easy to start wallets. Heck you can do a new wallet for every transaction if you're really paranoid about losing your privacy.

Well, at first place you shouldn't commit any crime at all. If someone does this, he'll have to face the consequences of his actions. This thread isn't made for those who are about to commit a crime/or those who committed already a crime. It's for those who want to have their privacy. I don't think you'll be in trouble as you prove that your previous address (before coinjoin) has nothing to do with illegal activities. I mean authorities will understand easily what's going on, at least I hope so, cause signing message or providing xpub is an 100% evidence that you're innocent and your previous address has nothing to do with fraud/crime.

I don't think your btc will be flagged. You could easily just coinjoin then split again and again and again btc till it seems like a normal payment. You could split 1 btc into 100 different addresses of 0.01 btc. Why your btc will be flagged for "secrecy"? I don't get it. I mean you could be a guy who received payment from another guy who received payment from another guy etc and all these with different xpub.

In general, I truly believe that chainanalysis help to avoid crimes and I encourage this but, if Bitcoin turns into a fully KYC only system and noone has his own privacy I'll consider bitcoin as a failure project and I'll be very disappointed.

About what you asked, I don't want to get coins into fiat, I'd rather hodl till everything becomes crypto than selling to get "profit as price goes up". If the profit was the case I'd invest into stocks, no need for cryptos.

It doesn't matter if you make thousands of wallets if you used a third party-server to broadcast transactions for you. They have your xpub and will have every xpub from every wallet you make. The thing is to make wallets that support Tor and run your own node.

MystiKaL - January 21, 2021, 8:50 am

What separates CoinJoin from other cryptocurrency tumblers like Blender.io? I'm not saying one is better than the other, asking because I'm still relatively new to the scene.

WillYoung - January 21, 2021, 10:10 am

(Jan 21, 2021 06:05 AM)SIM-4831178 Wrote: [\[CITE\]](#) - I run node over VPN and connected Wasabi -> You're much safer but still the VPN server knows you run a node.

- I run a node over Tor (best way is if your Operating System is Tails) and connected Wasabi (or even if you didn't doesn't matter that much) -> Noone knows that you run a node, noone knows your Bitcoin addresses. So your saying its safer to use tor directly without VPN? rather then VPN and

connect to Tor?

MystiKaL - January 21, 2021, 3:49 pm

(Jan 21, 2021 04:08 PM)Focus Broken Wrote: [\[CITE\]](#) Coinjoin is better than a tumbler because you never have to trust anyone else with your funds or privacy. A tumbler service can just steal your coins or leak your privacy, you trust them completely.

You can use a VPN to connect to Tor if you want to hide the fact you are using Tor from your ISP.. but then your ISP knows you are using a VPN, so it's not much difference.

Ah, I see. Thanks for the clarification!

Mortician - January 21, 2021, 5:00 pm

great post , a lot of people I know use coinbase... as their main storage of crypto and they never understand me when I explain the risks that come with that they think coinbase is untouchable.

Omniscient - January 21, 2021, 6:19 pm

You can use a private dedicated server instead of a well known VPN or even Tor. You tunnel to that then use Tor from it. Your ISP won't know. The big mistake most people do with a VPN is use their ISP's DNS still.

Hopsin - January 22, 2021, 6:37 am

This OP is actually useful, appreciated for sharing.

WillYoung - February 22, 2021, 7:09 am

Is it possible to run the node on a vps also? and then connect from the wallet to it? also will it be open for others to use it so u wont be the only one?

Omniscient - February 22, 2021, 7:43 am

(Feb 22, 2021 08:09 AM)WillYoung Wrote: [\[CITE\]](#) Is it possible to run the node on a vps also? and then connect from the wallet to it? also will it be open for others to use it so u wont be the only one? Yes, you'd probably want an ElectrumX server setup.

<https://freedomnode.com/blog/how-to-install-an-electrum-server-using-full-bitcoin-node-and-electrumx/>

I recommend using Lunanode for a full BTC node.

<https://docs.btcpayserver.org/LunaNodeWebDeployment/>

A BTCpay node is a full BTC node and it's easy to setup.

<https://launchbtcpay.lunanode.com/>

They also accept crypto as payment.

aude - February 22, 2021, 8:05 am

You should read about the way XMR (monero) is done for privacy. This is pretty great.

BTC is ok for speculating, XMR best for everything else.

WillYoung - February 22, 2021, 8:32 am

(Feb 22, 2021 08:43 AM)Omniscient Wrote: [\[CITE\]](#) Yes, you'd probably want an ElectrumX server setup.

<https://freedomnode.com/blog/how-to-install-an-electrum-server-using-full-bitcoin-node-and-electrumx/>

I recommend using Lunanode for a full BTC node.

<https://docs.btcpayserver.org/LunaNodeWebDeployment/>

A BTCPay node is a full BTC node and it's easy to setup.

<https://launchbtcpay.lunanode.com/>

They also accept crypto as payment.

Simply doing with bitcoin core isnt as good as electrumX?

Also this BTCPay does all the work like runes the node and everything ready? also how secure it is instead of using a vps

Omniscient - February 22, 2021, 9:06 am

Quote:Simply doing with bitcoin core isnt as good as electrumX?

You asked about connecting your wallet to the Bitcoin Core. Not 100% sure what's the best way to do that but with Electrum it's a light wallet. You'd be able to set a private server up connecting to the ElectrumX Server thus broadcasting your transactions more privately. And you'd not really use the BTCPay server but it's just part of the deal with Lunanode. I don't really know too many VPS companies that do cheap full BTC nodes. Lunanode gonna cost you about \$10-\$12 a month. They'll maintain it for you too with updates. They have a wizard that sets up the node and btcpay. You'd follow the instructions I sent to add ElectrumX and customize your node too.

I found this too which might be cheaper in the long run because you'd buy the hardware and just run it from home. But with home setup your IP is going to get exposed potentially unless you run it through TOR but not sure your ISP will be secure.

WillYoung - February 22, 2021, 10:52 am

(Feb 22, 2021 10:06 AM)Omniscient Wrote: [\[CITE\]](#) You asked about connecting your wallet to the Bitcoin Core. Not 100% sure what's the best way to do that but with Electrum it's a light wallet. You'd be able to set a private server up connecting to the ElectrumX Server thus broadcasting your transactions more privately. And you'd not really use the BTCPay server but it's just part of the deal with Lunanode. I don't really know too many VPS companies that do cheap full BTC nodes. Lunanode gonna cost you about \$10-\$12 a month. They'll maintain it for you too with updates. They have a wizard that sets up the node and btcpay. You'd follow the instructions I sent to add ElectrumX and customize your node too.

I found this too which might be cheaper in the long run because you'd buy the hardware and just run it from home. But with home setup your IP is going to get exposed potentially unless you run it through TOR but not sure your ISP will be secure.

And on the electrum server u can connect with any wallet electrum and wasabi also?

Omniscient - February 22, 2021, 11:07 am

(Feb 22, 2021 11:52 AM)WillYoung Wrote: [\[CITE\]](#) And on the electrum server u can connect with any wallet electrum and wasabi also?

I am not sure about Wasabi. One of the few wallets I have not used.

Tommie R - September 19, 2021, 8:12 am

I started running my own Bitcoin node recently - shoutout to [mention=3209658] for referring me to <https://getumbrel.com/>

Ordered a Raspberry PI 4 kit and an SSD which cost about \$400 in total.

The process is very straightforward and Umbrel has an App Store for various other use-cases besides running a Bitcoin / Lightning node. Everything happens over Tor as well which is great. All in all took an hour.

SIM-4831178 - September 19, 2021, 8:47 am

(Sep 19, 2021 08:12 AM)Tommie R Wrote: [\[CITE\]](#) I started running my own Bitcoin node recently - shoutout to @@Focus Broken@@ for referring me to <https://getumbrel.com/>

Ordered a Raspberry PI 4 kit and an SSD which cost about \$400 in total.

The process is very straightforward and Umbrel has an App Store for various other use-cases besides running a Bitcoin / Lightning node. Everything happens over Tor as well which is great. All in all took an hour.

Very glad to hear it [mention=3209658] indeed helps a lot and we thank him as community.

Keep stacking sats. We're all Satoshi.

Stanley - September 22, 2021, 4:40 am

I'm Stanley HF's helper bot. This OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley