

Forum: [Hack Forums](#)

Thread: [Who Here Runs Their Own Bitcoin Full Node?](#)

Kaleb - July 15, 2025, 3:03 pm

? I was doing some reading today on the safest methods of storing your funds. And by that I mean I just asked Gemini out of curiosity, a friend of mine took a decently large position in Bitcoin about a year ago, and I learned he's still holding it on Coinbase...

Needless to say I was a lazy bitch and just sent him basic instructions from ChatGPT on how hardware wallets work and how to set them up, how they keep your private key offline while giving you your public key etc.

But one part of the prompt sparked my interest.

AI Quote:

Run Your Own Full Node (Advanced): For the highest level of privacy and verification, consider running your own Bitcoin full node. This allows your wallet software to verify transactions independently, rather than relying on third-party servers.

So I did some Googling on how feasible that is, as I remember some other coins had "nodes" which required you to hold very large amounts of coin, I assumed bitcoins would be in the millions but I found a reddit thread claiming:

https://www.reddit.com/r/Bitcoin/comments/1exrd8z/how_much_bitcoin_justifies_running_your_own_node/

castorfromtheva from Reddit.com Wrote: The whole point of bitcoin is to cut off 3rd parties/middlemen and be your own bank.

Running a bitcoin fullnode costs around 150 to 200 bucks one time payment and around 2 bucks per month of energy usage.

Imho if you own less than 500 bucks in BTC running an own fullnode might not be worth it. For any other amount in BTC you'd be stupid to not to.

Because the truth is only if you do run your own fullnode you can use the bitcoin network completely sovereign and in a private and censorship-resistant way and don't have to trust, rely and make public your holdings to another entity.

Does he have a point? Is this true? Or is it overkill? Does anyone here run their own node, and if so, what is its purpose: security, contributing to decentralization, or both?

Mewtwo - July 15, 2025, 3:23 pm

I would run my own nodes for Monero, but for Bitcoin among other crypto currency, it's kind of pointless since the transactions are traceable anyways. Bitcoin doesn't have dandelion like XMR

does, so you can potentially disclose your IP address when you broadcast a transaction (unless you are using TOR/VPN) I run it via tor nodes which is still safe.

AI Quote:

If you run your own Bitcoin node and broadcast your own transaction, then yes, your IP address can potentially be exposed—but the extent and risk depend on how you're connected and what privacy protections you're using.

? Here's how it works:

When you post a transaction via your node:

- The node sends the transaction to its peers.
- The first IPs seen broadcasting a new transaction can be linked to the originator by a network observer (like surveillance nodes or chain analysis companies).
- If you're broadcasting directly without privacy tools, your IP address can be associated with the transaction.

?

? Ways your IP can be leaked:

1. No Tor or VPN:

- Your real IP address is exposed to the first peers your node connects to.
- This includes ISPs, chain surveillance nodes, or even government monitors.

2. Your node uses the default P2P connection setup:

- Peers can tell when you're the first to send a transaction. That can indicate you're the originator.

?

? How to protect yourself:

Method Protection Level Notes

Tor High Hides IP, can be configured for Bitcoin Core with `-proxy=127.0.0.1:9050` `-onlynet=onion`

VPN Medium Hides IP from peers, but trust in VPN is required

Broadcast via other nodes Medium to High Use another node to send transactions (e.g. via Electrum, or a hardware wallet with a backend)

Dandelion++ (not in Bitcoin Core yet) Theoretical High Designed to obfuscate origin by relaying transactions in a "stem" phase first (used in Monero)

?

? Summary:

- Yes, if you post a transaction directly from your node without protections, your IP address can be linked to that transaction.
- To maintain privacy, you should:
 - Run your node over Tor or a trusted VPN
 - Avoid posting sensitive transactions from your home IP
 - Consider using wallets or clients that support remote broadcast or privacy-enhancing techniques.

(Jul 15, 2025 03:23 PM)Mewtwo Wrote: [\[CITE\]](#) I would run my own nodes for Monero, but for Bitcoin among other crypto currency, it's kind of pointless since the transactions are traceable anyways. Bitcoin doesn't have dandelion like XMR does, so you can potentially disclose your IP address when you broadcast a transaction (unless you are using TOR/VPN) I run it via tor nodes which is still safe.

AI Quote:

If you run your own Bitcoin node and broadcast your own transaction, then yes, your IP address can potentially be exposed—but the extent and risk depend on how you're connected and what privacy protections you're using.

? Here's how it works:

When you post a transaction via your node:

- The node sends the transaction to its peers.
- The first IPs seen broadcasting a new transaction can be linked to the originator by a network observer (like surveillance nodes or chain analysis companies).
- If you're broadcasting directly without privacy tools, your IP address can be associated with the transaction.

?

? Ways your IP can be leaked:

1. No Tor or VPN:
 - Your real IP address is exposed to the first peers your node connects to.
 - This includes ISPs, chain surveillance nodes, or even government monitors.
2. Your node uses the default P2P connection setup:
 - Peers can tell when you're the first to send a transaction. That can indicate you're the originator.

?

? How to protect yourself:

Method Protection Level Notes

Tor High Hides IP, can be configured for Bitcoin Core with -proxy=127.0.0.1:9050 -onlynet=onion

VPN Medium Hides IP from peers, but trust in VPN is required

Broadcast via other nodes Medium to High Use another node to send transactions (e.g. via Electrum, or a hardware wallet with a backend)

Dandelion++ (not in Bitcoin Core yet) Theoretical High Designed to obfuscate origin by relaying transactions in a "stem" phase first (used in Monero)

?

? Summary:

- Yes, if you post a transaction directly from your node without protections, your IP address can be linked to that transaction.
- To maintain privacy, you should:
 - Run your node over Tor or a trusted VPN
 - Avoid posting sensitive transactions from your home IP
 - Consider using wallets or clients that support remote broadcast or privacy-enhancing techniques.

I see. It seems the argument for running your own Bitcoin node in this case though is its the safest way to handle your coins, nothing to do with privacy, but that's an interesting application too.

So you run your own node over Tor so your transactions broadcasted are more private?

Mewtwo - July 15, 2025, 4:25 pm

(Jul 15, 2025 03:38 PM)Kaleb Wrote: [\[CITE\]](#) I see. It seems the argument for running your own Bitcoin node in this case though is its the safest way to handle your coins, nothing to do with privacy, but that's an interesting application too.

So you run your own node over Tor so your transactions broadcasted are more private?

It really just depends what wallet you are using. There's some bad wallets that can expose your private key to the public node. Or if the public node is signing your transactions, of course they have your private keys as well. But if you're using local wallets like Electrum, Trezor, Ledger etc, and you sign your transactions yourself before broadcasting it to a node, you should be totally fine. A huge plus to use Tor/VPN so you obfuscate your IP address.

The only problem with Trezor / ledger is they can see all your X PUB addresses ever linked to that device. It's really just a private risk unless as you stated, you run your own node via bitcoin/electrum/sparrow