

Forum:[Hack Forums](#)

Thread: [Opsec and wallet addresses](#)

Hackers - January 31, 2025, 5:38 am

When you make a new wallet on an exchange, you are exposing your IP, user agent, real-time browsing behavior, and possibly some trackers.

For opsec, the best way to maintain your privacy is to generate an address completely offline.

From there you can use an open source or otherwise decentralized tool to manage your wallet, on a secure or self hosted RPC. At end of the day all you need is a node and a private key.

Just curious if anyone here has thought through this or not with their wallets.

I made a few tools for this exact purpose:

<https://hackforums.net/showthread.php?tid=6291027>

<https://hackforums.net/showthread.php?tid=6288657>

<https://hackforums.net/showthread.php?tid=6288690>

Hackers - February 1, 2025, 6:51 am

(Feb 1, 2025 01:01 AM)Yung Zel Wrote: [\[CITE\]](#) I barely understand the serverless client address makers, can you clarify?

They use static libraries for the real cryptographic algorithms

This lets you generate your own wallet addresses without any chance of your data being associated with the address, like it is on an exchange or through certain public browser extension wallets.

It's serverless because the programs don't use any networking, and don't notify any backend server about new addresses. It's completely offline on your personal computer. This is different than let's say a GUI wallet which may create an account/profile on a platform/website/app alongside your first new crypto address in their software.

Hackers - February 1, 2025, 10:00 am

(Feb 1, 2025 10:37 AM)SUI-3183372 Wrote: [\[CITE\]](#) The last time (~2020ish) I publicly commented on how to maintain strong levels of anonymity around your crypto, I had law enforcement knock on my door (previous residence, I had already moved out) and received emails from both the FBI and a cyber crime task force out of California asking me what my motivation is to post those. They wanted me to come down to an office to discuss my posts. When I lawyer-ed up (never talk to law enforcement), they started digging into my past, asking questions about LR transactions from a decade prior (law enforcement have the full LR transaction database).

Appreciate you posting this, it's a topic everyone should be passionate about. Wish I could talk about this topic, one that violates no laws, without the headaches associated with it.

Oh wow that's crazy! I hope they wouldn't be upset at this whitehat thread.

If anything I'd imagine an LE could use this type of tool themselves to avoid matters of local or national security being exposed to Coinbase, Binance, random companies, and whoever may be snooping on activities.

This software also is technically "unrelated" to blockchain. It does not connect to any network, node, service, ledger, or anything. It is just a cryptographic algorithm with input output, showing private and public strings on either side of the algo. It is unrelated to cryptocurrency on a technical level. However, the algo is coincidentally used by certain blockchain wallet address formats, and able to be used for those systems outside and separately from the softwares linked in this thread.

StuffSneak - February 1, 2025, 11:07 am

This is an interesting thought. I would love to learn more on these. Any references you can recommend?

Hackers - February 1, 2025, 11:24 am

(Feb 1, 2025 12:07 PM)StuffSneak Wrote: [\[CITE\]](#) This is an interesting thought. I would love to learn more on these. Any references you can recommend?

Well, just in general there is a need for certain people to completely hide their identity. Now, this can be 100% innocent, legal, and for personal privacy alone. However, I'll link this example here: <https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk>

In this case there are a number of crypto addresses being tracked.

If this address, or any other addresses used by the hackers were created on an exchange then that exchange/app/website could be subpoenaed for the data. For example, the sign up email, IP address, etc. From there, this can be traced to another service, which can also be subpoenaed or otherwise coerced into providing information.

Now, it's not always as simple as someone signing up for a KYC exchange.

There are other more obscure ways something can be less private. For example, you could use your wallet to accept funds or send money to someone else. Maybe even if you are using a VPN. But perhaps you used a Chrome extension for your wallet. Or maybe you sent it via a website. Or an app. Somewhere here you most likely ended up being logged. It could be simple - every single CSS file or JS file your browser loads is leaving your IP, timestamp, etc in an access log somewhere. Even just loading in a logo on an extension or software will leave a log. Even a software's auto-update checker is leaving a log. All of these timestamps can be used to be traced back to transaction activity on a wallet address. So, even if you are not signing up for a KYC exchange, you may be leaving traces of yourself across apps and tools. These timestamps, even when using a VPN can be compiled and tracked to find patterns. There are also behavioral patterns for how you move your mouse, type, and click - so you can be profiled online even if you think you are anonymous from a tech standpoint.

Another way you can break opsec with this is an extension of the last problem I just mentioned. Lets say you have 100% perfect opsec, but you send me crypto. Now your secure address is relying on my opsec. What this means is that if i then use the funds I received from you, for any reason, and then I send it to my KYC wallet, or another system that is subpoenaed ... well, this would mean that they show up for me to try to get info on you. The point is that even if one of these DPRK hackers from the link I shared has 100% opsec on certain addresses, they are also relying on every other person they received crypto from, or sent crypto to - to also have 100% perfect opsec.

So, it all starts with the address you use. If you need wifi to generate your address, you've already failed the first step.

The next steps include:

- private bulletproof blockchain node
- private bulletproof blockchain RPC, for web/IP front-facing API to connect your client and backend
- encrypted static & encrypted runtime client to connect to private RPC, to pull recent TX data and send new TX
- secure storage or memorization of your private key and exact cryptographic algorithm (at least the names & certain variables) for future retrieval/use (offline if needed)

That's essentially the only way you really can have close to full opsec on blockchain. You would also need a mix of VPN or RDP, different forwarders, and methods to obfuscate the timestamps for artificial delays & also fake events. This is the only way to get around ISP & other logs that can still be used to correlate timestamp data to build a behavioral profile on you.

Anything short of that is going to increase the risks a lot by forcing you to rely on a service or company's TOS and data privacy even if a government pressures them for your info. There are only so many VPN / IP chains you can hide behind.

Omniscient - February 1, 2025, 12:05 pm

I don't understand why you're talking about privacy of wallets on an exchange.

Quote:When you make a new wallet on an exchange

Right there ends the discussion. You shouldn't be using exchanges as part of your privacy routine. It's just not gonna work. The moment your funds are in a CEX the privacy is over. And technically the more you attempt to be private the more likely you'll either be red-flagged or even accused of money laundering when using a CEX.

Many of the exchanges appear to label their wallets now for the AML checkers. I've spend a good amount of time this month going through all the AML checkers, they are a growing list, you can't really escape them. What I recommend is that you use them yourself to check your own addresses before sending funds to a CEX. I've accidentally sent "high-risk" funds to exchanges and it gets me shut down. So no more of that shit. Now I check my addresses carefully.

Hackers - February 1, 2025, 12:06 pm

(Feb 1, 2025 01:05 PM)Omniscient Wrote: [CITE](#) I don't understand why you're talking about privacy of wallets on an exchange.

Right there ends the discussion. You shouldn't be using exchanges as part of your privacy routine. It's just not gonna work. The moment your funds are in a CEX the privacy is over. And technically the more you attempt to be private the more likely you'll either be red-flagged or even accused of money laundering when using a CEX.

Many of the exchanges appear to label their wallets now for the AML checkers. I've spend a good amount of time this month going through all the AML checkers, they are a growing list, you can't really escape them. What I recommend is that you use them yourself to check your own addresses before sending funds to a CEX. I've accidentally sent "high-risk" funds to exchanges and it gets me shut down. So no more of that shit. Now I check my addresses carefully.

Yeah sorry I should edit my post.

I really mean any clearnet platform.

Omniscient - February 1, 2025, 12:08 pm

So you're talking about web3 wallet creation? I don't like using those.

btw, did you know HF had a Bip39 generator?

<https://hackforums.net/tools.php?action=bip39>

Sometimes I'll use it for wallet seed.

Hackers - February 1, 2025, 12:14 pm

(Feb 1, 2025 01:08 PM)Omniscient Wrote: [\[CITE\]](#) So you're talking about web3 wallet creation? I don't like using those.

btw, did you know HF had a Bip39 generator?

<https://hackforums.net/tools.php?action=bip39>

Sometimes I'll use it for wallet seed.

That's cool, I didn't know that

Yes, for web3 it's good - but mostly I just mean in general, managing your own keys is great because you can use a backend package in a script with it all pre generated so you can automate anything from any server.

You could theoretically use unreleased IPFS content for future hash matching and have software awaiting the hash's data to become public to trigger automatic blockchain actions from a server

All in all I hope this thread sparks more ideas.

There's lots I don't know about and I actually use BTC the least.

Sec13B - February 7, 2025, 3:46 am

can share more about :

- private bulletproof blockchain node
- private bulletproof blockchain RPC, for web/IP front-facing API to connect your client and backend

Mewtwo - February 7, 2025, 6:34 am

(Feb 1, 2025 12:24 PM)nodes Wrote: [\[CITE\]](#) Well, just in general there is a need for certain people to completely hide their identity. Now, this can be 100% innocent, legal, and for personal privacy alone. However, I'll link this example here:

<https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk>

In this case there are a number of crypto addresses being tracked.

If this address, or any other addresses used by the hackers were created on an exchange then that exchange/app/website could be subpoenaed for the data. For example, the sign up email, IP address, etc. From there, this can be traced to another service, which can also be subpoenaed or otherwise coerced into providing information.

Now, it's not always as simple as someone signing up for a KYC exchange.

There are other more obscure ways something can be less private. For example, you could use your wallet to accept funds or send money to someone else. Maybe even if you are using a VPN. But perhaps you used a Chrome extension for your wallet. Or maybe you sent it via a website. Or an app. Somewhere here you most likely ended up being logged. It could be simple - every single CSS file or JS file your browser loads is leaving your IP, timestamp, etc in an access log somewhere.

Even just loading in a logo on an extension or software will leave a log. Even a software's auto-update checker is leaving a log. All of these timestamps can be used to be traced back to transaction activity on a wallet address. So, even if you are not signing up for a KYC exchange, you may be leaving traces of yourself across apps and tools. These timestamps, even when using a VPN can be compiled and tracked to find patterns. There are also behavioral patterns for how you move your mouse, type, and click - so you can be profiled online even if you think you are anonymous from a tech standpoint.

Another way you can break opsec with this is an extension of the last problem I just mentioned. Lets say you have 100% perfect opsec, but you send me crypto. Now your secure address is relying on my opsec. What this means is that if i then use the funds I received from you, for any reason, and then I send it to my KYC wallet, or another system that is subpoenaed ... well, this would mean that they show up for me to try to get info on you. The point is that even if one of these DPRK hackers from the link I shared has 100% opsec on certain addresses, they are also relying on every other person they received crypto from, or sent crypto to - to also have 100% perfect opsec.

So, it all starts with the address you use. If you need wifi to generate your address, you've already failed the first step.

The next steps include:

- private bulletproof blockchain node
- private bulletproof blockchain RPC, for web/IP front-facing API to connect your client and backend
- encrypted static & encrypted runtime client to connect to private RPC, to pull recent TX data and send new TX
- secure storage or memorization of your private key and exact cryptographic algorithm (at least the names & certain variables) for future retrieval/use (offline if needed)

That's essentially the only way you really can have close to full opsec on blockchain. You would also need a mix of VPN or RDP, different forwarders, and methods to obfuscate the timestamps for artificial delays & also fake events. This is the only way to get around ISP & other logs that can still be used to correlate timestamp data to build a behavioral profile on you.

Anything short of that is going to increase the risks a lot by forcing you to rely on a service or company's TOS and data privacy even if a government pressures them for your info. There are only so many VPN / IP chains you can hide behind.

At this point, it's really being paranoid. There's a lot of scammers and crypto thieves that rely on wallets like Trust Wallet, meta mask, or even Trezor / Ledger. All these website can simply keep logs of the crypto addresses and send it to law enforcement. But I haven't seen any case of this. And if there were any cases like these, for sure those crypto wallets would have bad publicity and no one would want to use them.

Sec13B - February 7, 2025, 8:33 am

(Feb 1, 2025 01:05 PM)Omniscient Wrote: [\[CITE\]](#) What I recommend is that you use them yourself to check your own addresses before sending funds to a CEX.

"What I recommend is that you use them yourself to check your own addresses before sending funds to a CEX."

What you recommend?

Omniscient - February 7, 2025, 8:46 am

(Feb 7, 2025 09:33 AM)Sec13B Wrote: [\[CITE\]](#) "What I recommend is that you use them yourself to check your own addresses before sending funds to a CEX."

What you recommend?

I found ChangeNow has an AML checker. It's not comprehensive in reports but it does have a long list of supported crypto and is only \$15 a month for 40 checks.

<https://changenow.io/pro/aml-check>

Hackers - February 7, 2025, 8:48 am

(Feb 7, 2025 04:46 AM)Sec13B Wrote: [\[CITE\]](#) can share more about :

- private bulletproof blockchain node
 - private bulletproof blockchain RPC, for web/IP front-facing API to connect your client and backend
- It's basically just software running on a private server.
You would host it in a place that's secure, making sure it protects your personal privacy.

A blockchain node is responsible for retrieving data off the chain, or sending new transactions basically.

The RPC is your communication layer, which relays info to your client/wallet app/etc , and from your backend node.

(Feb 7, 2025 07:34 AM)Mewtwo Wrote: [\[CITE\]](#) At this point, it's really being paranoid. There's a lot of scammers and crypto thieves that rely on wallets like Trust Wallet, meta mask, or even Trezor / Ledger. All these website can simply keep logs of the crypto addresses and send it to law enforcement. But I haven't seen any case of this. And if there were any cases like these, for sure those crypto wallets would have bad publicity and no one would want to use them.

This is true, it is super paranoid.

However, I think many people are way too lax and it's surprising how many people get away with things on a transparent & public ledger.

Omniscient - February 7, 2025, 9:12 am

(Feb 7, 2025 07:34 AM)Mewtwo Wrote: [\[CITE\]](#) At this point, it's really being paranoid. There's a lot of scammers and crypto thieves that rely on wallets like Trust Wallet, meta mask, or even Trezor / Ledger. All these website can simply keep logs of the crypto addresses and send it to law enforcement. But I haven't seen any case of this. And if there were any cases like these, for sure those crypto wallets would have bad publicity and no one would want to use them.

I'm positive they share data with AML companies which are used by Law Enforcement. Absolutely they do, I have no doubt.

Hackers - February 7, 2025, 10:32 am

(Feb 7, 2025 10:12 AM)Omniscient Wrote: [\[CITE\]](#) I'm positive they share data with AML companies which are used by Law Enforcement. Absolutely they do, I have no doubt.

Yeah I would rather be paranoid if I were doing something shady... rather than just trust MetaMask and TrustWallet to voluntarily keep all of my data secure. It also relies on every government's laws for data privacy staying in place.

A lot of companies that don't share data would share it in a heartbeat under new legal pressures.

The only correct form of opsec is to treat every single human and company on the internet as a potential informant.

That random guy in the middle of nowhere that saw your face and accepted your BH crypto? That's prison!

I am treating this thread as:

- if any single person, or any single log in a computer has your data, you failed the opsec.

----> for IP, email, MAC address, user agent & timezone & correlation data, etc.

I also want to come back to this thought:

---> Your ISP most likely complies with the government (dependent on where you are)

I think people forget about ISPs.

They think they are connecting to a VPN without using their own network for it or something, who knows.

Your PC -> Your Router/Modem & Your IP -> Your ISP -> Your "private VPN"

^^^ Damn, I probably should've just started with this.

Omniscient - February 7, 2025, 4:13 pm

(Feb 7, 2025 11:32 AM)nodes Wrote: [\[CITE\]](#) I think people forget about ISPs.

They think they are connecting to a VPN without using their own network for it or something, who knows.

Your PC -> Your Router/Modem & Your IP -> Your ISP -> Your "private VPN"

^^^ Damn, I probably should've just started with this.

Encrypted DNS helps.

<https://blog.cloudflare.com/dns-encryption-explained/>

Sec13B - February 20, 2025, 1:10 am

<https://github.com/BtcAutoNode/BtcAutoNode>

Omniscient - February 20, 2025, 11:29 am

(Feb 20, 2025 02:10 AM)Sec13B Wrote: [\[CITE\]](#) <https://github.com/BtcAutoNode/BtcAutoNode>

That's a nice share. Could definitely come in handy. Thank you.