Bitcoin Privacy: Why You Should Care

CONTRIBUTED BY

Matt Odell
TFTC Co-Host

Twitter

Matt Odell is a bitcoiner who cares deeply about privacy. His current focus is on education, both as cohost of the Tales from the Crypt podcast and as cofounder of the Bitcoin Citadel workshop initiative.

Learn more about Matt here.

For many years there has been a common misconception that bitcoin is private by default. The reality is that many bitcoin users are extremely easy to track. Every transaction is recorded forever in the block chain; publicly visible to all participants. If personal information is linked to a specific transaction - name, email, IP address, mailing address, phone number, twitter account, etc. - that information can then be used to track past and future transactions using publicly available data. As bitcoin has matured, so have the tools used by surveillance companies. Bitcoiners should assume these companies have large datasets which combine information from many disparate sources including public on-chain metadata and private off-chain information used to improve their transaction tracking capabilities across the network as a whole.

Further complicating this situation is the insidious spread of KYC/AML compliance among fiat onramps and offramps. For years the accepted best practice has been to avoid these services as much as possible, but - unfortunately - that has become much more difficult throughout the world and especially if you desire to accumulate large amounts of bitcoin or make frequent regular purchases. There are still non-KYC options such as Bisq and HodlHodl, but they are relatively easy to choke

The issue is the fiat side of the equation since non-cash fiat transactions require trusted third parties which are vulnerable to government pressure.

Cash transactions are more difficult to restrict, but the alarming increase in global cash restrictions should not be underestimated. Global cash usage will probably fall to a negligible level within the next decade due both to state restrictions and to general apathy from individuals. Mining remains an option for private accumulation, but - dependent on local electricity prices - you will most likely have to pay a premium over KYC compliant onramps.

Bitcoiners tend to talk a big game when it comes to avoiding KYC, but I fear the unspoken reality is the majority are purchasing through compliant services. Those services can track past and future transactions linked to deposit and withdrawal addresses. They may share the data with governments. They may share that data with surveillance companies. The data may be leaked or get stolen. At scale - with a majority of users linked to their addresses – companies, governments, and malicious individuals can use these datasets to better track all users in the network through process of elimination, timing analysis, and external surveillance techniques.

Bitcoin Privacy: Why You Should Care

The first step towards a solution is admitting we have a problem. There is a lot of work being done, but too many people are blind to this fundamental concern. What is the goal here? At a fundamental level most people seem to agree that the people you pay and the people that pay you should not know your spending habits or net worth. Furthermore, I think most of us can agree that we would prefer money that cannot be easily tracked by foreign governments and corporations. These are tangible goals we can strive for when it comes to bitcoin privacy guarantees.

As mentioned, the biggest issue is the fiat side of the equation. The bright side is that as bitcoin adoption increases, a circular economy should develop reducing the need to interact with fiat at all. Those who wish to accumulate bitcoin will either earn it or accept it in exchange for goods and services leveraging self sovereign software stacks such as BTCPayServer. Most won't buy bitcoin – they will earn it. Most won't sell bitcoin – they will spend it. This reality will take some time to develop and I think we must be able to provide KYC'd users decent privacy - without losing auditable supply - until we bootstrap a circular bitcoin economy.

WHAT CAN BITCOIN USERS DO TODAY TO IMPROVE THEIR PRIVACY?

1. AVOID KYC
2. USE YOUR OWN NODE SO YOU DON’T HAVE TO TRUST A THIRD PARTY WITH TRANSACTION INFO
3. MAKE EVERY SPEND A COINJOIN
4. PRACTICE PRUDENT COIN CONTROL GOING FORWARD
5. DEMONSTRATE BISQ AT YOUR LOCAL MEETUP TO BOOSTRAP A LOCAL P2P MARKETPLACE IN YOUR CITY

The tools available to us will only get better. Many users are capable of building or purchasing their own dedicated node or using one run by a friend or a family member. We have seen tremendous growth in dedicated node projects such as RaspiBlitz, MyNode, and RoninDojo, which make it cheaper and more accessible to build a node that you can easily use with your own wallet. HWI and PSBT standards should also make it much easier to directly use an external wallet with bitcoin core for users who don't have the need or capability to run a dedicated node.

Another thing to watch is growing payjoin adoption among wallets, users, and merchants. BTCPay Server recently joined Joinmarket and Samourai Wallet in adding support for payjoin and we see more wallets prioritizing support due to demand. Payjoins are coinjoin transactions where the sender and receiver each contribute an input and the result often looks the same as any ordinary transaction. PayJoin adoption could make all transactions more private by breaking a common heuristic used by surveillance companies; that all inputs belong to the same user.

Node	Build It Yourself?	Signed Releases	Electrum	Dojo	Whirlpool	Lightning	Joinmarket	BTCPay	Block Explorer	Mempool Visualizer	LNDHub
RoninDojo	☑	☐	☑	☑	☑	☐	☐	☐	☑	☐	☐
MyNode	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
RaspiBlitz	☑	☑	☑	☐	☐	☑	☑	☑	☑	☐	☐
Nodl	☐	☑	☑	☑	☑	☑	☐	☑	☑	☐	☐

Bitcoin Privacy: Why You Should Care

Self sovereign software stacks such as BTCPay Server, Samourai Dojo, and MyNode help to automate best practices at the app level without adding unnecessary third parties.

BTCPay Server

Easily enable merchants to accept bitcoin privately

Samourai Dojo

Easily link your node to a mobile wallet to CoinJoin and spend

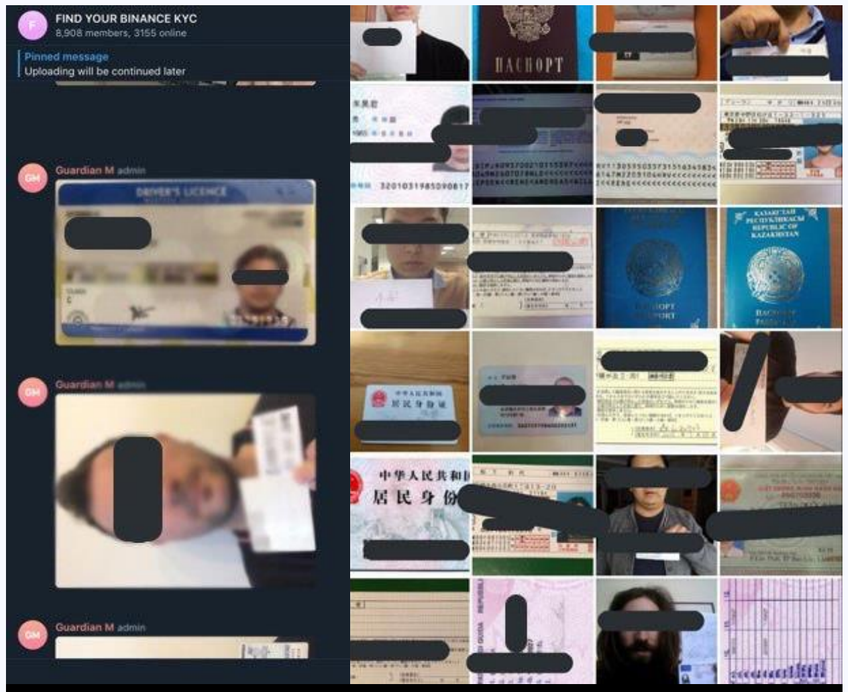
MyNode

Easily run a dedicated full node and link with a variety of wallets/tools

I am also cautiously optimistic about the lightning network - although much work still needs to be done, it has multiple properties that seem to improve the privacy situation substantially. At a fundamental level lightning improves privacy by not including transaction data on chain, so surveillance must be active and/or rely on surveilling channel opens and closes. Lightning routing improvements, such as the recent support for multi-path payments, should make active lightning surveillance more difficult and expensive. Furthermore, potential bitcoin protocol improvements such as Taproot and cross input signature aggregation could be really powerful when combined with lightning. Together they would make it cheaper for multiple parties to collaborate when opening and closing channels, obfuscating chain data from outside observers. One important stat to watch is the percent of public lightning capacity that is being run through Tor - currently sitting at ~43%. If lightning centralizes around a few KYC compliant hubs run by known actors then it will fail as a privacy tool.

The amount of nuance surrounding private bitcoin usage is a perfect example of why we must support tools and protocol improvements that help improve privacy guarantees for all users. You will know we are on the right track when it doesn't take 1100 words to have a basic discussion on it...

If you wish to dive further into this topic, I recommend the extensive resources curated by 6102bitcoin at btcprivacy.org.



KYC requirements are both dangerous and ineffective. Criminals can simply use leaked, stolen, or purchased data while honest users suffer increased risk of theft & extortion.