Protect your privacy

Bitcoin is often perceived as an anonymous payment network. But in reality, Bitcoin is probably the most transparent payment network in the world. At the same time, Bitcoin can provide acceptable levels of privacy when used correctly. **Always remember that it is your responsibility to adopt good practices in order to protect your privacy**.

Understanding Bitcoin traceability

Bitcoin works with an unprecedented level of transparency that most people are not used to dealing with. All Bitcoin transactions are public, traceable, and permanently stored in the Bitcoin network. Bitcoin addresses are the only information used to define where bitcoins are allocated and where they are sent. These addresses are created privately by each user's wallets. However, once addresses are used, they become tainted by the history of all transactions they are involved with. Anyone can see the balance and all transactions of any address. Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous. For these reasons, Bitcoin addresses should only be used once and users must be careful not to disclose their addresses.

Use new addresses to receive payments

To protect your privacy, you should use a new Bitcoin address each time you receive a new payment. Additionally, you can use multiple wallets for different purposes. Doing so allows you to isolate each of your transactions in such a way that it is not possible to associate them all together. People who send you money cannot see what other Bitcoin addresses you own and what you do with them. This is probably the most important advice you should keep in mind.

Be careful with public spaces

Unless your intention is to receive public donations or payments with full transparency, publishing a Bitcoin address on any public space such as a website or social network is not a good idea when it comes to privacy. If you choose to do so, always remember that if you move any funds with this address to one of your other addresses, they will be publicly tainted by the history of your public address. Additionally, you might also want to be careful not to publish information about your transactions and purchases that could allow someone to identify your Bitcoin addresses.

Your IP address can be logged

Because the Bitcoin network is a peer-to-peer network, it is possible to listen for transactions' relays and log their IP addresses. Full node clients relay all users' transactions just like their own. This means that finding the source of any particular transaction can be difficult and any Bitcoin node can be mistaken as the source of a transaction when they are not. You might want to consider hiding your computer's IP address with a tool like Tor so that it cannot be logged.

Limitations of mixing services

Some online services called mixing services offer to mix traceability between users by receiving and sending back the same amount using independent Bitcoin addresses. It is important to note that the legality of using such services might vary and be subjected to different rules in each jurisdiction. Such services also require you to trust the individuals running them not to lose or steal your funds and not to keep a log of your requests. Even though mixing services can break traceability for small amounts, it becomes increasingly difficult to do the same for larger transactions.

Future improvements

Many improvements can be expected in the future to improve privacy. For instance, some efforts are ongoing with the payment messages API to avoid tainting multiple addresses together during a payment. Bitcoin Core change addresses might be implemented in other wallets over time. Graphical user interfaces might be improved to provide user friendly payment request features and discourage addresses reuse. Various work and research is also being done to develop other potential extended

privacy features like being able to join random users' transactions together.