Protect Your Financial Privacy With Bitcoin: A Comprehensive Guide

This comprehensive manual will explain how you can use Bitcoin to protect your financial privacy.

After you’ve read this manual, be sure to check out our step-by-step guide: How to Make Anonymous Payments With Bitcoin.

Jump to...

Why It Is Important to Keep Your Funds Private

As a financial system, Bitcoin functions completely differently from the established banking network. Bitcoin allows you to store funds yourself, without the need for a third party, and it places the burden of keeping said funds secure and accessible on you.

While opening an account with a traditional bank or other financial institution requires significant cost and effort, creating a Bitcoin account is quick and easy to do on your home computer. This speedy process makes it possible to create millions of separate accounts if you wish.

Two aspects in particular—privacy and identity—function very differently with Bitcoin than in the legacy financial system.

Pseudonyms Protect Your Identity in Bitcoin

A bank account, PayPal account, or credit card is always tied to a real identity, making it difficult for many people to open them. Bitcoin allows you to use any persona or online identity you wish.

Being able to use the Internet anonymously or pseudonymously is the only way for many people to truly be themselves. Hundreds of millions of people around the globe are not accepted in their societies for reasons they cannot control.

Pseudonyms are used by women who speak up for their rights, atheists born into religious societies, and people critical of their governments to spread their thought, empower their causes, and encourage those around them to do the same.

These courageous men and women threaten their own safety and wellbeing to defend who they are and what they believe in. Technology empowers them to be leaders in social change more efficiently than they could have ever been before. Technology also connects like-minded individuals so they can together form the communities for which they strive.

Maintaining an identity with a large following might require paid services such as blogs, logo designs, stock photos, VPNs, or translations. Without the ability to pay for these services anonymously, you would be forced to reveal your true identity in order to maintain your pseudonym. A situation which clearly makes no sense, and one with potentially dangerous ramifications.

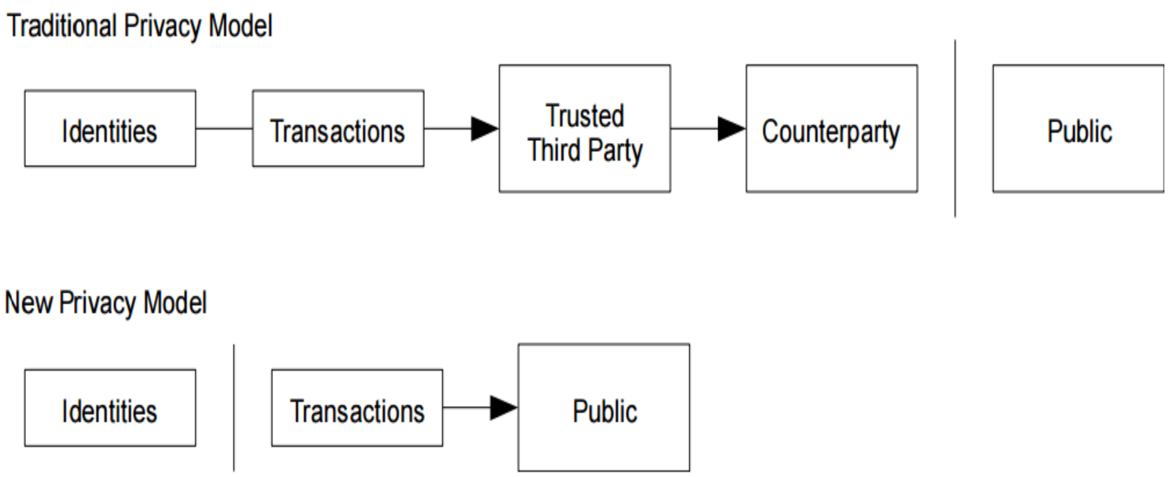
How Bitcoin Empowers Anonymity

Bitcoin is an important, empowering technology. Using a Bitcoin account with a pseudonym protects your right to remain anonymous on the Internet. It allows anonymous or pseudonymous fundraising. Groups can collectively control Bitcoin accounts, and choose to either hide or reveal financial information at will.

There are many positive reasons for a private and secure banking system like Bitcoin:

A workers’ rights group could, for example, raise funds with Bitcoin. The money could be used for servers, flyers, remote helpers… and all without tying any transaction to the real identities of the volunteers.

Perhaps a domestic abuse victim might use Bitcoin to securely stack away funds to prepare for an independent life.



The traditional privacy model and the new privacy model as explained by Satoshi Nakamoto in the original Bitcoin Whitepaper.

Privacy Through Pseudonymous Accounts

Privacy in traditional banking is guaranteed by the institutions that make up the system, such as banks, credit card companies, and governments. They (try to) ensure that your bank balance stays a secret. This puts them in a delicate position, where only they have complete oversight as to what is going on.

In the Bitcoin ecosystem, everyone can see the history of every account balance, but they cannot see who controls an account. All addresses and transactions are recorded in Bitcoin’s publicly distributed database, the Blockchain. The addresses do not have names or IP addresses attached to them, so it is not always possible to know which transaction belongs to which individual.

Transparency Requires Protection

Bitcoin is by default a transparent system, in which every piece of information is available to the public. As such, every Bitcoin user requires some level of protection. Anyone with substantial wealth in Bitcoin would not want to advertise their funds to every person they transact with, for obvious reasons. But every time you spend just a tiny portion of your Bitcoin wallet, you reveal your wealth to the other party. Doing that on the Internet is like flashing large stacks of cash in a dark back alley. It is not advisable! A criminal might see how much you have, and decide to come after it. Distributing your wealth between several wallets and using a different address for each transaction is a common practice that prevents others from knowing how much Bitcoin you have.

How You Can Be De-anonymized Using Bitcoin

Sadly, there are hundreds of ways a Bitcoin transaction can be linked to someone's real identity. True pseudonymity against a resourceful adversary is very difficult to achieve. Any sincere approach to anonymity in Bitcoin requires a holistic use of encryption and communication tools (see our guides on PGP, OTR and Tor).

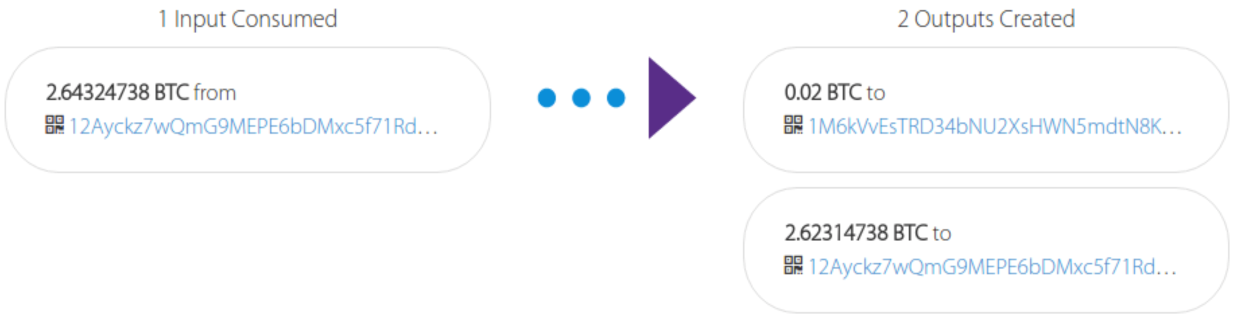
Over the course of just a few months, you could come into contact with hundreds of Bitcoin addresses. It is often only necessary to associate just one of these addresses with your real identity to work out your real identity.

Bitcoins Are Traceable On The Blockchain

Each Bitcoin transaction contains at least one input (where the Bitcoins are from) and at least one output (where the Bitcoins are being sent). This means that once a single address is known, there is a trail to follow the Bitcoins.

Another characteristic of Bitcoin transactions is that they always need to match the previous transaction. If 1 Bitcoin is received, but you only want to spend 0.4 Bitcoin, you will need to make a transaction where 1 Bitcoin will leave your account. 0.4 Bitcoin will go as payment, then 0.6 Bitcoin will return to you as change. Your Bitcoin wallet will handle this process automatically, but it is important to understand the principle in order to use it anonymously.

The owner of the original Bitcoin doesn't know what you did with the money, but they can see the amounts involved. They can see two transactions on your account: one for 0.4 Bitcoin and one for 0.6 Bitcoin. They cannot see which was the purchase and which is the "change", but it's a 50% guess. The next time you make a transaction, it's a 25% guess, and so on.



1 Input Consumed

2.64324738 BTC from
12Ayckz7wQmG9MEPE6bDMxc5f71Rd...

2 Outputs Created

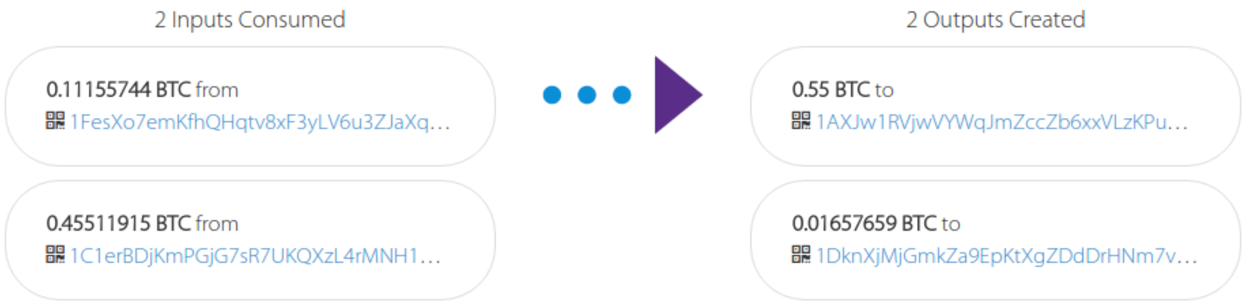
0.02 BTC to
1M6kVvEsTRD34bNU2XsHWN5mdtN8K...

2.62314738 BTC to
12Ayckz7wQmG9MEPE6bDMxc5f71Rd...

1 input consumed, 2 outputs created.

This is why making lots of transactions, even between yourself, increases your anonymity in the Bitcoin network (as long as your wallet software does not reuse addresses!).

Similarly, if you receive 0.5 Bitcoin but want to spend 1 Bitcoin, you need to own additional Bitcoin addresses with a combined value of at least 0.5 Bitcoins in them. Again it's a 50% guess, but now you have one extra publicly visible Bitcoin address. Having publicly visible Bitcoin addresses could make it easier to find out your identity.



2 Inputs Consumed

0.11155744 BTC from
1FesXo7emKfhQHqtv8xF3yLV6u3ZJaXq…

0.45511915 BTC from
1C1erBDjKmPGjG7sR7UKQXzL4rMNH1…

2 Outputs Created

0.55 BTC to
1AXJw1RVjwVYWqJmZccZb6xxVLzKPu…

0.01657659 BTC to
1DknXjMjGmkZa9EpKtXgZDdDrHNm7v…

2 inputs consumed, 2 outputs created.

Your Name Might Be Linked to Your Bitcoin Address

Your real name might be connected to a Bitcoin transaction when you make transactions with Bitcoin, for example, if you buy goods online and have them shipped to your real address. Bitcoin exchanges and even some ATMs often require you to show identification before making a purchase. When you buy bitcoins from someone in person, they might know who you are and keep a record of the transaction. This record could fall into the hands of your adversary, or maybe even be made public

Your country's anti-money laundering laws might require you to reveal your identity when buying or selling Bitcoin, making it necessary to obfuscate their trail on the blockchain.

Your IP Address Might Be Linked to Your Bitcoin Address

When you make a Bitcoin transaction, you are essentially creating a message on your phone or computer and sending it to the Bitcoin network. Someone operating a large number of nodes in the Bitcoin network might be able to match some of your transactions to your IP address, then deanonymize your entire stack of Bitcoins.

It is relatively easy to avoid this on a computer by relaying all transactions through the Tor network. Most Bitcoin clients and wallets support Tor's Socks5 proxy.

Revealing Your Bitcoin Address Before It Goes Into the Blockchain Could Let Others Track You

As soon as a Bitcoin address is entered into the Blockchain, it is publicly recorded in an immutable global database. But before that happens it's likely that only two parties—the recipient and sender—had knowledge of this address. If you are making a search for an address that has not yet appeared on the Blockchain, either you are the owner of this address, or someone is requesting a payment from you.

To avoid being tracked in this way, it is important to make all payment requests and other mentions of addresses via encrypted channels:

- make sure the website you are visiting has HTTPS enabled when you search for Bitcoin addresses;

- use VPNs and Tor when possible;
- and encrypt your communications with PGP and OTR.

Possessing a Wallet File Might Be Enough Proof That You Control Bitcoins

A signed message is the only strong proof that you own a Bitcoin address without revealing the private key. Be careful when signing messages using your Bitcoin keys, though. Signed messages are a great feature (we'll talk more about why later), but they allow anybody to know that you control the Bitcoin address you signed from.

If someone is trying to deanonymize you, they might be satisfied with a weaker form of proof than a signed message: knowing that you keep records of public addresses is enough evidence for someone to draw the conclusion that you are involved in Bitcoin transactions and the Bitcoin Blockchain will point them exactly to which transactions. All they have to do is search for the address you recorded.

Most wallet software store public addresses without encryption, only encrypting the private keys. This is good for user experience, since you don't have to type in a password every time you want to see your balance or check transactions.

You can safely store your wallet in an external USB drive, a cloud storage service, or even your email account if the private keys are sufficiently encrypted. But anybody with access to these mediums could estimate what addresses you control and the transactions you make.

To protect yourself, you should encrypt all backups with a second password or PGP.

Encrypt EVERYTHING to stay truly anonymous!

How to Be Transparent

The concept of privacy is best defined as the amount of control you have over your information. This control not only includes the power to hide or conceal your personal information, but also the power to reveal it to the public. Transparency is useful if you need to gain legitimacy in the eyes of your audience or backers. Bitcoin allows you to be transparent to any degree you like. You can use it to prove single transactions or ownership of a Bitcoin address. Transparency also allows you to audit your organization down to the last satoshi (the smallest unit of a Bitcoin), without revealing your real identity or location.

When compared to traditional financial systems, Bitcoin’s transparency is an important and empowering innovation because it allows you to prove beyond doubt that you made a transaction of funds. The blockchain does not lie, and it cannot be bribed.

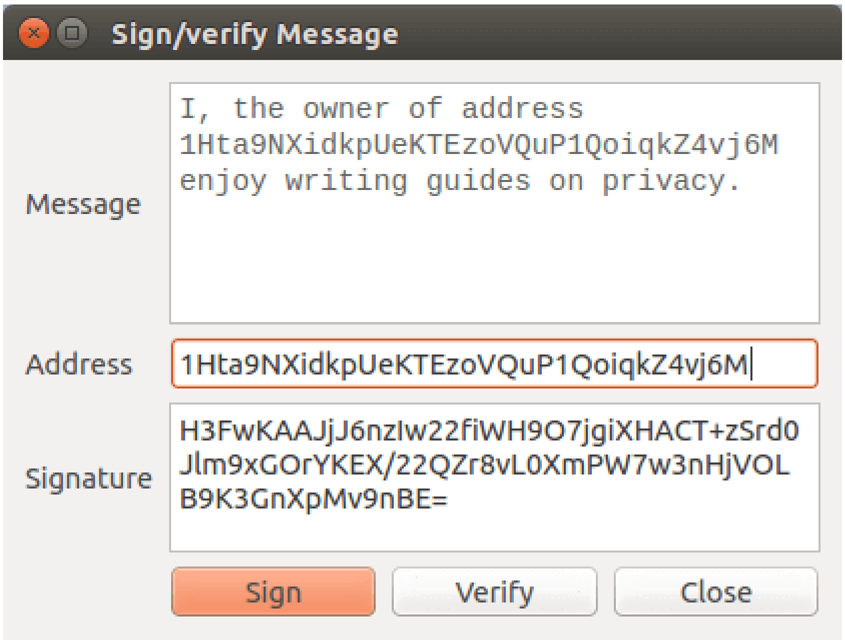
Transparency via Signatures

The simplest form of Bitcoin transparency is to link two identities by signing statements. How you do this depends on your specific wallet software, but the principle is always the same. You write up a verbal statement then sign it digitally, with your private key. This will not necessarily prove that the statement is true; it only proves that the owner of the address made the statement.

For example, if the operator of a website claims they control a Bitcoin address in their statement, and the owner of the Bitcoin address claims they are the operator of the website in their statement, you can reliably conclude the two are the same entity. You can then send funds to the Bitcoin address, safe in the knowledge that it is going to the right website.

You can also use these signatures to make statements about some of your transactions. For example, you might need to prove to auditors that you made a transaction, or that you control a certain amount of funds.

This is very useful for unforgeable, digital receipts. With just a few clicks you can prove to an art dealer that you are in possession of enough funds to purchase a painting, or maybe show your investors that you are still in control of their money.



I, the owner of address
1Hta9NXidkpUeKTEzoVQuP1QoiqkZ4vj6M
enjoy writing guides on privacy.

1Hta9NXidkpUeKTEzoVQuP1QoiqkZ4vj6M

H3FwKAAJjJ6nzIw22fiWH9O7jgiXHACT+zSrd0
Jlm9xGOrYKEX/22QZr8vL0XmPW7w3nHjVOL
B9K3GnXpMv9nBE=

Sign and verify your message to prove you control the funds.

I, the owner of address 1Hta9NXidkpUeKTEzoVQuP1QoiqkZ4vj6M enjoy writing guides on privacy.

```
H3FwKAAJjJ6nzIw22fiWH9O7jgiXHACT+zSrd0Jlm9xGOrYKEX/22QZr8vL0XmPW7w3nHjVOLB9K3GnXpMv9nBE=
```

Transparency via Reused Addresses

The official [Edward Snowden Defense Fund] uses a static Bitcoin address for its Bitcoin donations. This shows how many Bitcoins they have raised, and gives backers assurance that they are not being duped into donating to someone claiming to be collecting money on behalf of the defense of Snowden.

This level of transparency can be used anywhere, to prove that funds are not being embezzled and money is being spent responsibly.

How to Protect Yourself from Being De-anonymized

Be conscious of What Information You Reveal About Yourself

The first rule is to be conscious about what you are doing, and what you are revealing about yourself. Question your actions. Are you on a VPN? What have you previously done on this IP address? Which tabs do you currently have open in your browser? Which Bitcoin wallet are you using? Where does the money in that wallet come from, and what have you previously bought with it? Who have you recently communicated about what you are about to do, and was that information encrypted?

All of this information is important if you want to protect yourself. There are many little things which reveal a bit about you online. The following points will explain how you can best protect yourself. Always be vigilant, and remember to stay conscious of what data you submit to whom, and to think about how it could be used to identify you.

Never Reuse Addresses

Choose Bitcoin wallets that respect your privacy by never reusing addresses. HD wallets (Hierarchical Deterministic) generate a theoretically infinite number of addresses from a single seed. HD

Wallets make it easy to use a new address for each transaction and also provide a safe backup mechanism.

Be cautious of services where your withdrawal address is fixed. Change your Bitcoin address manually after each withdrawal to an unused address. Encourage others to change their addresses after each use too, as their practices will affect your privacy as you interact with them.

Use Tor

To maintain your anonymity, use the Tor Browser or the TAILS operating system, which comes pre-installed with the Electrum Bitcoin wallet. Route everything through Tor by default.

Configure your wallets to connect to the Bitcoin network via the Tor network. You can do so by installing the Tor Browser and configuring the proxy under Preferences > Advanced > Network > Settings. Keep the default setting of Socks v5 at 127.0.0.1 on Port 9050, then enter these values in the connection settings of your Bitcoin wallet.

It is also good practice to route your chats through the Tor network, with that same proxy settings. You can also configure many cloud storage providers in this way.

Encrypt Your Browsing, Chats, Emails, Backups

Secure Your Browsing

Always use HTTPS when viewing websites with any information related to your identity or Bitcoin transactions. This simple protocol is used to encrypt the traffic between the site you are viewing and your computer. A green lock icon in your browser’s address bar indicates that the website you are on is using HTTPS.

Another way to secure your browsing is with a VPN. When you use a VPN, the VPN hides your real IP from the sites you are interacting with. Be careful when choosing a VPN provider. Carefully read their privacy policies, specifically with regard to the information they log.

Use the Tor Browser to further hide your location from the sites you access. Services using an .onion address allow for the most secure end-to-end encrypted and anonymous connections on the Internet.

Encrypt Your Chats

For maximum protection, create at least one jabber account (also referred to as XMPP) for each of your online identities. There are plenty of free services available for you to choose from. Sign up through Tor and route all your chats through the Tor network, using the inbuilt Socks v5 proxy for extra security.

To ensure that your chats cannot be intercepted and read by anyone other than the intended recipient, use OTR as a reliable and robust encryption protocol. Note that you can only use OTR if the person you are communicating with is using it, too.

Make Your Emails Private

Of all online services, email is most vulnerable to snooping and hacking. While a good email provider will make it very difficult for attackers to access your system, the provider could still voluntarily hand over your data to governments, when asked. Unfortunately for people seeking privacy, many email providers make it difficult, if not impossible, to access your email via Tor. Some even require you tie your email address to a phone number or real identity.

Use PGP to encrypt your emails, although you will only be able to do so with people who also use PGP. If you are super concerned about your privacy, avoid communicating via email all together.

Secure and Encrypt Your Back Ups

How you back up your bitcoins depends on the software you are using. HD Wallets give you a string of random words that can be used to recreate your wallet. All you need to do is write those words down and lock them securely away. Be careful, though! Bad guys need only to know your words to steal your Bitcoins. It is generally considered unwise to store these words on any electronic device for that reason, but in the absence of secure physical space, it might be unavoidable.

The easiest way to encrypt the random words from your HD wallet (or any other text) is with PGP, though this will require you to also think about how to backup the PGP key. If you encrypt your PGP key with a very good password (it needs to be long and memorable: a combination human minds are notoriously bad at), you only need to remember one master password to access all your files. Check out our blog post about Diceware to find out how to create such a master password. Use the password to encrypt your PGP key, then back up all other files by encrypting them with the encrypted PGP key.

Use Separate Wallets for Each identity

It is easy to maintain a different Bitcoin wallet for each of your online identities. You could have a wallet for every need. For example, you could have:

- a wallet for incoming donations
- a wallet for your real identity
- a wallet for your advertisement revenue
- a wallet for your savings… etc.

You are going to need a lot of wallets!

You don’t need to download separate software for each of your identities. All you have to do is keep separate wallet files (files that contain your public and private keys). Just make sure not to confuse the separate files, and not to mix their funds.

Whenever you need to move funds between your identities, you will need to obfuscate the trail to make it difficult for anyone to link your identities together.

Obfuscate Transfers Between Identities

When thinking about the traditional financial system the synonyms “obfuscate”, “tumble”, or “mix” sound like activities for criminals.

Due to the transparent nature of Bitcoin, business transactions might require some form of obfuscation to protect trade secrets and business practices. A wire transfer from a person to a regular bank account should not be revealed to another party. Nor should the customer or competitors find out how revenue is used. Without obfuscation we inevitably reveal a lot more than we have to, so it’s a good practice to ensure your Bitcoin wallet is as private as you need it to be.

How to Obfuscate Transfers Between Identities

Individual Exchange

There are many ways to obfuscate transfers. You could exchange Bitcoins with someone else at a 1:1 exchange rate, though this requires great trust in the other party. You could also use an external escrow service. This option is rarely used, as the escrow company could possibly record compromizing information about the transaction.

Online Wallets

You can also protect your privacy by using an online wallet that doesn’t assign unique addresses to each user. An example of this are online exchanges. When depositing your Bitcoins into such a wallet, your coins might end up in the hands of someone else. Conversely, you might receive coins previously owned by someone else. These services are called Tumblers. It’s important to note that you won’t gain or lose any Bitcoins during this process.

A common Bitcoin exchange very likely abides to strict anti-money laundering regulation. They will keep records of all your transactions, possibly indefinitely, which they may hand over to a law enforcement agency. They might also ask for proof of your identity before they let you withdraw coins, a practice that might affect your privacy more than simply tracing your Bitcoin.

No online wallet that exists for the purpose of tumbling coins would be able to give you a guarantee that you will receive Bitcoins that were not already held by you. Doing so would require them to keep track of the entire process (rather than just deposits and withdrawals), which would defeat the point of the system. Another significant risk of a Bitcoin Exchange is that you trust your Bitcoins with a third party that likely operates anonymously themselves. You will have no recourse if the exchange or wallet provider disappears with your funds, as has happened several times.

Altcoins

Another way to disconnect yourself from your Bitcoins is just to sell them. You could exchange your Bitcoins for cash or gold, but a better option is to exchange them for altcoins. That way the transaction is cheaper, safer and easier to execute anonymously online. You could even sell your Bitcoins in exchange for another cryptocurrency with high volume and market cap, then buy them back on a second exchange shortly after.

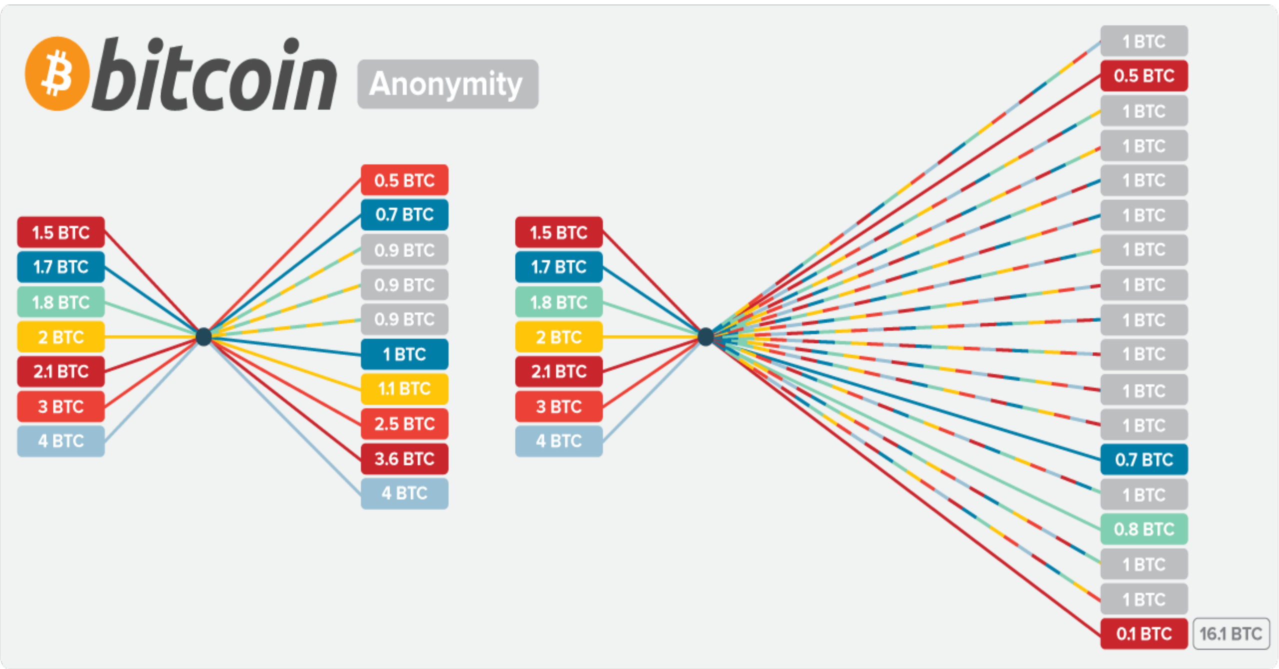
You will have to find multiple exchanges, with low KYC (Know Your Customer) requirements, that can be trusted with your coins. This can prove to be quite a challenge.

Coinjoin

Coinjoin is the most promising way to maintain your financial privacy with Bitcoin. It works by combining many transactions into one, so that it is not clear which inputs and outputs are correlated.

This can be done with software that eliminates the risk of funds disappearing or being stolen. Each of the signatures are created on the participants' computers, so anyone trying to connect the signatures is unable to alter the transaction, or redirect the funds. The funds will always be in a Bitcoin address that you control.

It's possible to do this in a decentralized way, so that the service does not rely on external parties or centralized servers. It just needs the participants of the transaction.



Services like Coinjoin scramble the Bitcoin inputs and outputs to maintain everyone's anonymity.

The biggest problem with Coinjoin is that it might still be possible to correlate the inputs and outputs, as there are often mathematically too few possible combinations of inputs and outputs, which allows a computer to determine which inputs correspond to which output.

To mitigate the possibility of someone figuring out which inputs and outputs belong to each other, the protocol has to be standardized in some way. As the inputs cannot easily be standardized, the outputs may be predefined. For example, you might limit the outputs to exactly one Bitcoin. Limiting the outputs to exactly one Bitcoin would make it impossible to match the account to the transaction, as every output will be for 1 Bitcoin. However, your inputs will likely be more than one Bitcoin each, so the difference will be returned to you untumbled. This is because the spare amount can be matched to a transaction.

Coinjoin can be applied multiple times, and as many transactions are grouped together, participants may save on transaction fees. Coinjoin is the preferred method of gaining privacy in the Bitcoin network. It is even possible that this functionality might one day be included directly on the protocol level as standard, as some altcoins already do.

Don’t forget to check out our step-by-step guide: How to Make Anonymous Payments With Bitcoin.

Featured images: (1) allapen / Dollar Photo Club, (2) Sergey Nivens / Dollar Photo Club, (3)pitrs / Dollar Photo Club.