Bitcoin Anonymity Guide 2019: How to use BTC like a straight up G

In the last few years, many people have realized that Bitcoin is not anonymous, and some of them have realized it with dire, life-destroying consequences.

Bitcoin is pseudonymous and some have learned this lesson on the bitter end of a long prison sentence. The Bitcoin blockchain while remarkable and revolutionary, is at it’s core, an immutable public ledger.

This means that every single transaction is unchangeably recorded and verifiable by every other participant in the network as long as electricity and the internet exist.

This is not an optimal state of affairs for those who require privacy.

I am not going to delve into who needs privacy and why because it is a commonly accepted give in that privacy is a fundamental human right that everyone needs, among civilized peoples.

This guide will show you the reality of using Bitcoin anonymously in 2019.

This post may express views you don’t agree with, I don’t care. Go read another blog if it bothers you.

Our foes are state-level attackers. That means governments, militaries, intelligence agencies, tax collectors, law enforcement, and other jackboot thugs of the world banking cartel.

Our foes will use the tired but common excuses of drug trafficking, money laundering and terror financing as the age-old boogeyman to scare you into submission allowing them to strip you of your privacy and freedom, but we know better.

So how can we tell these rent-seeking parasites to suck it, and flip them a giant middle-finger?

How can we spread financial freedom and privacy in the name of a truly free market?

How can we promote economic liberation from the yoke of a debt-based economy, ensuring a better and more prosperous future for every man, woman, and child worldwide?

I thought you’d never ask.

Step 1. Always use cash to get in and out of BTC

Never, ever use any service that requires AML/KYC. This is how law enforcement ties your real name to your Bitcoin address, exchanges are more than happy to cooperate.

Bisq is the best alternative for buying and selling Bitcoin without AML/KYC. It's a decentralized peer to peer Bitcoin exchange that lets you buy/sell Bitcoin with a variety of payment methods.

AML/KYC or more precisely known as Anti-Money Laundering/Know Your Customer laws *(Assholes Monitoring Life/Killing Your Creativity)* are completely idiotic.

It doesn't prevent any money laundering or terrorist financing and creates an onerous regulatory burden on businesses who have to comply with extortionary so-called "regulatory agencies" in order to operate.

AML/KYC regulations are designed to create an unnecessary paper trail, instead of actually stopping crime from occuring.

It's nothing but a slightly more polished presentation of common "mob-style" racketeering with suits and ties and licenses.

Contrary to popular belief, Terrorists are funded by governments and money-laundering is a non-crime.

Even if you believe money-laundering is a criminal act, banks are the biggest perpetrators of this crime.

If you buy or sell Bitcoin from an exchange which has all your AML/KYC information you must anonymize your coins.

The disruption and innovation that Bitcoin offers us, is to get rid of these middlemen interfering with the market, the money supply, and the economy overall.

We can now transact directly peer to peer with nobody taking a cut, or trying to interfere.

This is the actual end result of AML/KYC:

No personal freedom and total financial surveillance for everyone, while terrorists and criminals operate with impunity regardless.

In other words, ***AML/KYC is garbage***.

This conclusion does not even consider the higher costs of these financial services for customers who manage to jump through all the hoops of providing an intrusive level of personal information in order to be approved.

This added cost is the blood that the parasites are consuming.

It is a direct consequence of the regulatory compliance costs these businesses face. After all, a tick needs to suck blood from its host.

Step 2. Never reuse Bitcoin addresses

Not even once!

Re-using a Bitcoin address is a massive privacy and security risk.

It makes it easier for blockchain analysis agencies to use heuristics to deanonymize you, as well as others who may have transacted with you.

Reusing addresses is the virtual version of spreading an STD.

The best practice is to use a new Bitcoin address for every single payment you receive, and never send money twice to the same exact Bitcoin address.

Luckily many of the newer wallets are Hierarchical Deterministic, which means that you can generate an unlimited number of public addresses from a single seed, as well as recover the wallet completely, from the very same seed.

Most newer wallets are still SPV wallets, however, and are vulnerable to a wide variety of security vulnerabilities.

The only wallets I can even feel comfortable recommending to others, are the wallets I really use in my day to day.

I use Wasabi on my laptop, Samourai on my phone, Electrum for my BTCPay server, and a Cold Card as my offline cold storage solution. Cold Card and Electrum allow you to sign transactions offline, for added privacy and security. Signing transactions offline also the door to utilizing a Bitcoin satellite node and the Gotenna mesh network, for next level privacy.

Step 3. Never use a wallet that uses Bloom Filters (BIP 37)

Bloom filters are defined as:
A filter used primarily by SPV clients to request only matching transactions and blocks from full nodes.

Ok, now that we have established that, why does it matter if you use an SPV wallet that utilizes Bloom Filters? Bloom filters were introduced for security, right? Yes, but the implementation has lots of systemic flaws.

Without getting too technical and boring you to tears, I will refer to the Breaking Bitcoin SPV security PDF. In this document it states that an attacker could possibly:

- spoof full-nodes
- block SPV requests
- spoof SPV requests

- sniff out SPV requests
- block SPV answers.

These vulnerabilities come from the fact that SPV wallets do not verify the entire blockchain in all its immutable glory, they only verify headers, which leaves them open to these avenues of attack.

Electrum, a wallet I recommended above, is a thin-client SPV wallet that uses Bloom Filters, which could be risky to your privacy.

If you use Electrum with your own Bitcoin full or an Electrum personal server, you can mitigate a lot of these risks, especially if your is run as a Tor hidden service.

Step 4. Use an anonymity network or VPN like Torguard

Shameless plug: Torguard Anonymous VPN works against the great firewall of China & internet crackdowns in Iran, the link is a special offer from our partners at Torguard, which supports our site, Coincache.net.

Contrary to popular belief Tor is not the only anonymity network. There are others like I2P, Bitmessage, Zeronet, and Freenet that are engineered towards privacy security and anonymity, although at varying degrees of accessibility to the non-technologically inclined.

Always connect to the internet through a network like those listed above or a and use a privacy optimized version of Firefox, or the Tor browser.

How do the attackers actually attack our privacy?

In this section, I will address some of the techniques an attacker might use to deanonymize you and compromise your security.

I will heavily rely my upon my layman’s understanding from firsthand experience and reading a bunch of blog posts about online anonymity and the presentation by Jonas Nick of Blockstream linked above “Bitcoin Privacy in Theory and Practice” which was given in Zurich in March of 2016.

I want to take a moment to say free Ross Ulbricht!

You can donate to his cause here: https://freeross.org/donate/

Blockchain Forensic Analysis in a nutshell

Blockchain forensic analysis has been marketed as a surefire way to stop crime and people trying to use Bitcoin for evil and nefarious reasons like buying weed from the Mujahadeen off of the dark web.

Blockchain analysis has become a billion dollar industry with blockchain forensic services charging top dollar for their analysis to law enforcement governments, banks, and major Bitcoin exchanges worldwide.

I don’t want to pick on Chainalysis (or Bitfury) but they are hands down, the most famous such firms, although many others exist. Chainalysis will give you a good idea of the services these types of firms offer: activity monitoring reports, cyber-threat intel, and enhanced due-diligence tools.

These kinds of forensic blockchain analysts use a method of guessing what is actually taking place on the blockchain, in the sense of monitoring movement of funds. They do this with a technique called heuristics.

Jonas Nick claims a 70% recall rate with his blockchain analysis, which means that ***with one single , (public bitcoin address) he can discover 70% of your wallet.***

While this is concerning, we can use tools which attack these heuristic assumptions and make them invalid, allowing us to take back our privacy.

OK, so what are heuristics?

Heuristics are basically imprecise assumptions that are precise enough for the job at hand.

In Bitcoin, this means using software and algorithms to monitor the blockchain and movement of UTXOs to try and deanonymize users.

According to Jonas Nick, there are various heuristics utilized by blockchain forensic analysis companies like .

I am not qualified to speak on the specifics but the simplified summary sounds something like this:

Bitcoin Blockchain Analysis Heuristics Types

(from: Bitcoin Privacy in Theory and Practice, presented by Jonas Nick of Blockstream in Zurich 2016)

Multi input Heuristic, assumes all inputs are from the same wallet

Shadow change Heuristic, analyzes change addresses that have never before been on the blockchain, lets blockchain analysis experts know who is the sender and who is receiving funds

Consumer change Heuristic, transaction from consumer wallets have two or outputs, identifies people using services like exchanges, , etc**.**

Optimal Change uses the assumption that wallets don't send unnecessary outputs, if there is a unique output with a smaller value than any of the inputs then this is the change

These different techniques are used by themselves or in varying combinations in an analysis technique called "clustering".

Clustering allows analysts to follow the movement of funds from wallet to wallet, identify senders and receivers, and deanonymize and identify users themselves by linking addresses to a real-world identity.

Clustering is used on individual wallets (or), as well as to track complete transaction chains.

Since heuristics are just assumptions about what's actually happening, they can be attacked by making those assumptions fundamentally unreliable.

Privacy-conscious wallets like Wasabi & Samourai have incorporated such features into the wallets themselves as countermeasures to blockchain analysis.

For example, Samourai has Stonewall, Ricochet, and Paynyms, which make transactions in such a way that many of these heuristic techniques become invalid and uncertain.

Wasabi has so many privacy-protecting features, that I will cover them in its own section.

What can we do to minimize risk?

- Run and use a Bitcoin full-node, so you can broadcast and verify your own transactions.
- Run your Bitcoin full-node as a Tor hidden service.
- Use Wasabi as your desktop wallet and Samourai on your mobile. Learn to use the privacy features.
- Use a Cold Card as your cold storage hardware wallet.
- Never use any exchange or service that has your AML/KYC info. Buy and Sell Bitcoin with cash.
- Don't tell people you own Bitcoin and never talk about our Bitcoin on social media profiles with your real identity or information.

- Practice good general computer security habits.
- Use Coinjoin or a mixing service to breaking heuristic links to ownership of UTXOs, and maintaining a sufficient anonymity set.
- There are various types of Coinjoin implementations that can’t deanonymize you or steal your funds.
- Zerolink, , , and Coinshuffle are all different types of Coinjoins which can’t steal your funds or deanonymize you.
- Practice Coin Control like a champ.

Why you should stay away from centralized online mixing services.

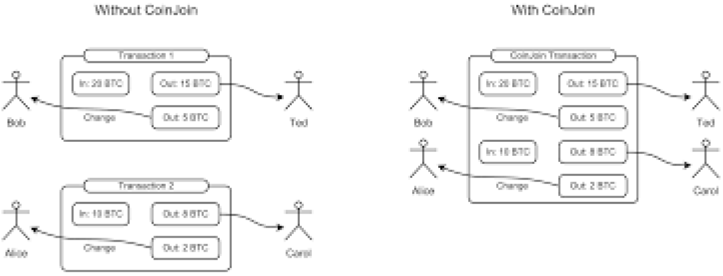
There are various Bitcoin mixers or tumblers that are in use by denizens of the dark web. Some are complete scams, others are legit and charge a fee, and still, others selectively scam their customers.

You cannot trust these services

Even if they don’t rip you off, you have no idea how they are actually mixing your coins, if they are providing sufficient anonymity, and you have no guarantees they are not deanonymizing everyone themselves. Using a mixing service is extremely risky.

There are now safer, more secure options called Coinjoins.

What are Coinjoins?



Coinjoins are a method of obscuring ownership of UTXOs by joining the inputs and outputs of many people into a single transaction. If the inputs are all the same size, it makes it impossibe for blockchain analysis to tell whos coins are whos. It was first proposed by Bitcoin core developer Greg Maxwell in 2013.

There have been various styles of Coinjoins which have been developed. They all follow the basic framework laid out by Maxwell, each with their unique approach and techniques.

I will take a look at a couple different implementations and give you a quick overview of each, so you can decide which one is the best for your privacy needs.

Joinmarket

Battle tested, dark web approved.

Joinmarket is a trustless Coinjoin implementation that uses a Maker/Taker model to incentivize users and provide liquidity.

matches users who want to anonymize their coins, (Takers) with users who wish to provide liquidity for Coinjoins (Makers) while earning a fee.

With , it is impossible for your coins to be stolen (your keys are never broadcast outside your computer) and the right amount is always sent to the correct wallet.

As a maker providing liquidity, you can help Bitcoin privacy and fungibility while earning a passive income in fees for doing so. The income in fees is low, but it is also very low risk.

A single will not give you very strong anonymity, however, there is a tumbler script which allows you to run many chained together to give an exponentially higher anonymity set. This will give you the privacy you need to overcome a motivated attacker.

The Yield Generator is a bot that performs the market maker duties in . It links to the trading pit IRC channel and offers the to takers for a fee.

is one of the most popular implementations. It has been in use for a couple years already, although since it is written in Python it does have a substantial learning curve.

An anecdotal testament to Joinmarket's effectiveness is this guy's offer to reward 220 Bitcoins to anyone who could help him recover his 440 stolen Bitcoins. He was able to watch the thief send the coins to Joinmarket, and then sadly, the trail was lost forever. Nobody was able to help him or claim any reward.

is open source and contributions are welcome.

Tumblebit

was first proposed in 2016, by a team of Bitcoin privacy researchers led by Ethan Heilman. is another trustless implementation of and provides users with anonymity by obscuring the ownership of UTXOs.

It is more than just a , it is also an anonymous payment hub which would help increase Bitcoin's overall scalability as well as privacy and fungibility.

has a classic tumbler mode which is the part of the protocol. It has another mode for payment hub which allows users to make anonymous payments through the trustless tumbler that can't steal your funds.

Tumblebit's payment channels are different than the payment channels employed by the Lightning Network, so it is unclear if the two protocols would be integrated at this time.

Tumblebit's anonymous payment hub would require users to open a payment channel with the payment hub, similar to how channels must be opened to use the Lightning Network.

Tumblebit's payment hub would also be second layer scaling solution that could make payments in seconds, similar to the lightning network but it would exist as its own layer 2 . (unless major work is done to integrate the two).

Additionally, payment hubs would pool Bitcoin, creating upward price pressure while ensuring anonymity, fungibility, privacy, and scaling.

is a pretty new project, so It only has one working proof-of-concept implementation which is not ready for production yet.

It is called NTumblebit and was written by Nicolas Dorier, Bitcoin core developer and creator of BTCPay server.

is open source so anyone can contribute.

Coinshuffle++

Coinshuffle++ is yet another trustless implementation of , and this one also takes a unique approach to how your coins are mixed/tumbled.

Coinshuffle was first by a team of Bitcoin security researchers from Saarland University in Germany.

Coinshuffle is more decentralized than other implementations. (It doesn't rely on a centralized coordinator.) It may be possible to build Coinshuffle in a fully trustless and decentralized way. This would give it more censorship resistance and resilience to attackers.

Coinshuffle++ is the successor of the original Coinshuffle project. Coinshuffle has had a couple of implementations like Shufflepuff, and CashShuffle, but a fully decentralized implementation of Coinshuffle++ has not yet been implemented.

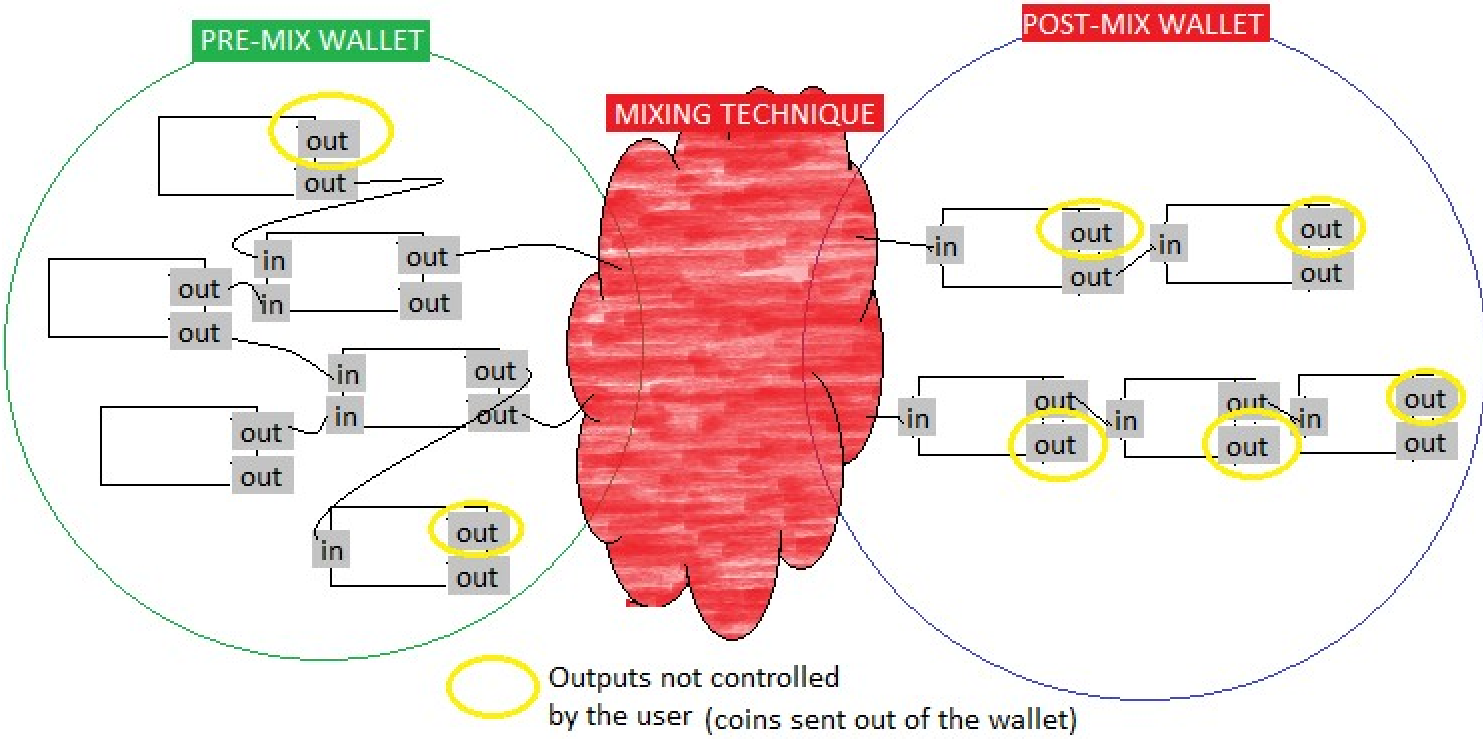
This is for two reasons, the first being that Coinshuffle++ utilizes its own mixing network called DiceMix (DM). DiceMix would need to be integrated with TOR/I2P which would require a lot of development work.

The second is that building a decentralized/distributed network is very challenging. It is hard to fix bugs, everything must be done nearly perfect the first time. It is akin to working on the engines of an airplane while it is still in flight.

Decentralized systems are much more complex to create than a standard implementation.

Coinshuffle is also open source, so feel free to contribute.

Zerolink


PRE-MIX WALLET
MIXING TECHNIQUE
POST-MIX WALLET
in
out
Outputs not controlled by the user (coins sent out of the wallet)

Zerolink has been called the Bitcoin fungibility framework. It is another unique and interesting implementation of .

Zerolink utilizes a new technique called Chaumian Coinjoin which is a faster and less expensive method of conducting .

Zerolink is billed as being the first implementation to:

> “offer protections against all the different ways a user’s privacy can be breached. The scope of ZeroLink is not limited to a single transaction, it extends to transaction chains and it addresses various network layer deanonymizations”

Nopara73

Zerolink at its core is a 3 part system. It consists of a pre-mix wallet, a post-mix wallet, and a method of mixing coins which known as Chaumian Coinjoin. Chaumian is based up David Chaum's Chaumian Blind Signatures.

Chaumian can be immediately implemented by existing and has already been implemented into Wasabi wallet, and work is underway on a Samourai implementation as well.

Chaumian utilizes a simple round-based mixing technique. Its tumbler cannot deanonymize users or steal funds, and its simplicity makes it much faster than other implementations with much lower fees.

Zerolink provides mathematically provable anonymity to users.

It is also open source and contributions are encouraged.

My experience using Wasabi Wallet

Wasabi wallet is a complete gamechanger for Bitcoin privacy, anonymity and fungibility. It is brand new and has just released version 1.0.5 which you can download here.

Wasabi wallet was created by Adam Ficsor, aka Nopara73. Adam worked on before he began to work on Zerolink, he also worked on Stratis' Breeze wallet, and then Hiddenwallet before it morphed into Wasabi.

Wasabi wallet is completely redesigned (from the ground up) version of Adam's earlier project . It has several privacy/security improvements and utilizes Chaumian Coinjoin as it's mixing technique.

Wasabi is the first-ever Zerolink compliant wallet and it's now live on Bitcoin's main net.

Wasabi is hands down my favorite Bitcoin wallet. It has forever raised the bar in what a Bitcoin wallet should be, and which features it should incorporate.

Let's take a look at Wasabi's features to protect your privacy and anonymity:

- It's open source, you can audit its code.
- Cross-platform (Linux, Windows, OSX).
- Zerolink Compliant.
- BIP 84 Wallet (only Bech32 Native Segwit Addresses).
- Only light wallet which does not fail against Blockchain Forensic Analysis.
- Built-in high volume mixer/tumbler based on Chaumian Coinjoin.
- Built-in Blockchain analysis tool to help you keep your anonymity intact.

- Built-in advanced coin control feature to help you manage your UTXOs with precision.
- Tumbler cannot deanonymize you or steal your coins.
- Extremely minimal fees of only 0.03%
- Wasabi has made over 2417 BTC fungible since August 1, 2018.

Wasabi is super easy to use and makes coin control simple and easy to understand and use effectively.

It is commonly said that an anonymity set of 50 is sufficient to evade blockchain forensics analysis. With Wasabi this can be achieved in a matter of hours (or minutes if there are lots of other users).

I have been able to achieve much higher anonymity sets than this with my coins. I think the highest anonymity set I have reached is 360, which is extremely high. If I continue tumbling these coins I could keep getting a higher and higher anonymity set.

Coin Control is essential to maintain this level of anonymity, which means using the tools in Wasabi to never mix UTXOs which could deanonymize you. (It’s much easier than it sounds.)

Wasabi utilizes the Zerolink framework of a pre-mix wallet, post-mix wallet . It also allows you even more control of your UTXOs by having multiple wallets in the Wasabi app itself.

This means after you mix your coins, you can send them to a completely new Wasabi wallet with no heuristic links to your other wallets.

It also allows you to have a wallet for each subsector of your spending, (e.g. Healthcare, Monthly expenses, Discretionary spending, Cold storage, etc.).

This allows you to practice coin control across all your wallets and to control your UTXOs with surgical precision.

You can also send anonymized UTXOs to another wallet or a hardware wallet (send the UTXOs one by one so you don’t deanonymize yourself) for offline cold storage.

All in all, Wasabi has changed the dynamics of Blockchain forensic analysis by making their heuristic assumptions unreliable and gives power back to the Bitcoin user by giving them mathematically provable privacy and anonymity sets.

Samourai Wallet will be the second wallet to be Zerolink compliant and will share many of the same groundbreaking features as Wasabi, but for mobile wallets and spending Bitcoin anonymously on the go.

In Conclusion

Privacy is more important than scaling for mass adoption of Bitcoin. It is also the main reason that the mainstream finance and business words have not fully embraced Bitcoin yet. They need to protect their business' financial confidentiality from competitors, and Bitcoin's public ledger is not conducive to this need, yet.

This post is an overview of existing privacy techniques and how you can utilize them yourself.

To actually use these techniques, this blog post should be viewed as a starting point for further research. Make sure you understand all these concepts before attempting to use them in the wild.

Be very careful when using these anonymity techniques, especially if your life depends on it. There are very real consequences to engaging in controversial behavior that may benefit from the techniques reviewed here.

Every single Bitcoin user that cares about personal freedom and financial privacy should be utilizing , Wasabi, or another trustless mixing technique. Privacy is a team effort, it is much easier to hide in a large crowd.

The more people who use these techniques the more fungible every Bitcoin becomes, making it more and more like digital cash.

If this article was useful to you or informative and entertaining, you can donate to our site (microdonations via lightning network accepted), or visit our shop and purchase one of the special offers from our site partners.