COMPASS
MINING

# The OPSEC Manual:

## A Guide For Secure and Private Bitcoin Mining

Operations security best practices for purchasing, hosting, lending, mixing and selling when mining Bitcoin.

# The OPSEC Manual:

## A Guide For Secure and Private Bitcoin Mining

By Lili Rhodes

Compass Mining would like to thank @econoalchemist and Tyler Cohoon for their contributions on Data Protection, @econoalchemist for their input on Online Privacy and Bitcoin QnA for their contributions on Storage.

# Table of Contents:

## Introduction

Disclaimer ---------------------------------------- 4

## Part 1: Setting Up

**Scam Prevention** -------------------------------- 5
**Hardware Shopping** ---------------------------- 6
Communication -------------------------------- 6
Payment Risks -------------------------------- 6
Know Your Customer Information ----------- 7
Shipping Information ------------------------- 7
**Threat Modeling** -------------------------------- 7

## Part 2: Mining Operations

**Security Management** ------------------------- 9
Site Security ----------------------------------- 9
Physical Security ------------------------------ 9
Site Monitoring -------------------------------- 9
**Power Consumption** ---------------------------- 9
**Heat Signatures** --------------------------------- 10
How to conceal heat signatures --------------- 10
*Mining room and backdrop* ------------- 10
*Fluids — immersion cooling* ------------- 10
*Other materials — aluminum* ------------ 10
Other considerations for minimizing ASIC heat - 10
**Noise Pollution** --------------------------------- 10
ASIC placement ------------------------------- 11
Noise-dampening enclosures and materials -- 11
Noise-dampening curtains -------------------- 11
Noise-dampening software ------------------- 11
**Hardware Considerations Summary** -------- 11
**Data Protection** -------------------------------- 11
General Web Traffic --------------------------- 11
Stratum Protocol Data Transfers ------------- 12
Stratum V2 ------------------------------------ 12
Proxies ----------------------------------------- 13
100% Anonymity Is Impossible --------------- 13

## Part 3: Pools and Payout

**Pool Accounts** ----------------------------------14
Login Security ---------------------------------- 14
Address Reuse ---------------------------------- 14
**Storage** ------------------------------------------14
Exchange Wallets ------------------------------- 14
Software Wallets --------------------------------15
Hardware wallets ------------------------------- 15
**CoinJoin Payouts** -------------------------------- 15
**Selling and Lending** ----------------------------- 18
Selling ------------------------------------------- 18
Lending ------------------------------------------19

## Part 4: Online Privacy

**Social Media** --------------------------------------20
**Mining Apps** --------------------------------------21
Downloading Mobile Apps --------------------- 21
Using Mining Apps ------------------------------21
**Web Browsing Privacy** --------------------------21
Browser Alternatives --------------------------- 22
VPNs and Orbot ---------------------------------22

## Part 5: Other Privacy Resources

# Introduction

Operations security (OPSEC) is one of the most important considerations for all bitcoin and cryptocurrency users. But due to the complexity of their operations, cryptocurrency miners face much larger OPSEC considerations than average investors. Nearly all large mining institutions have developed internal protocols and best practices that guide the security of their operations. But small-scale hosted or at-home miners typically have to fend for themselves to develop and maintain proper OPSEC. The only way for most retail miners to learn about threat vectors, best security practices, and general mining security information is by mapping out a model suited for them through countless hours browsing blogs, discussion forums, social media threads, and videos.

The Cryptocurrency Mining Operations Security Manual is intended to serve as a starting point for all retail miners to understand the full scope of mining OPSEC considerations. The information in this manual is not meant to be used as a handbook for how to start mining. Instead, this document should be used only as a mining security and privacy educational resource.

There is no definitive right or wrong way to approach OPSEC. OPSEC is a spectrum, and the precautions required will depend on a miner's risk tolerance and goals. Miners can use any suggestions in this guide as it applies to their individual situations.

Although this guide is meant to be as comprehensive as possible, the security needs and potential attack vectors of the entire cryptocurrency industry can change. Readers who notice missing or outdated information are encouraged to contact media@compassmining.io.

Additional mining education resources can be found in the Compass Mining education archive.

## Disclaimer

This material is not intended to be relied upon as a forecast, research or investment advice, and is not a recommendation, offer or solicitation to buy or sell any investment or to adopt any investment strategy. This information is for educational purposes only and is as of the date of that particular presentation. Compass does not guarantee profits from mining activity. Past performance is not a reliable indicator of current or future results and should not be the sole factor of consideration when selecting a mining product, service or strategy. Changes in the rates of exchange of cryptocurrencies, hashrate, difficulty, network transaction fees, hosting and other fees may cause the efficiency and returns of mining to diminish or increase. Individuals are responsible for their own decisions regarding cryptocurrency mining, including all financial and operational risks.

# Part 1: Setting Up

## Scam Prevention

The mining industry is rife with scams, just like every other sector of the cryptocurrency ecosystem. Identifying and avoiding scams is essential, especially for new miners.

Scam prevention requires being alert and attentive to details. Miners should never be reluctant to double-check information, ask a sales representative to offer alternative identity verification (e.g., a video call, voice chat or communication through another platform) and follow their instincts if a business offer, invoice or promotion seems amiss.

First, any cloud mining operation should be treated with caution. Although some cloud mining providers operate legitimately, it can be difficult to differentiate between legitimate and fraudulent cloud mining services and promotions.

Some of the most basic and prevalent cryptocurrency mining scams involve tricking people into paying for products or services that do not exist. These scams take a variety of forms, including selling cloud mining contracts for hashrate that doesn't exist or creating hardware listings online to sell ASICs owned by someone else.

Other popular mining scams include phishing websites that mirror websites from real companies; mobile mining apps with malware; and fake invoices for mining hardware, hosting or other services with branding from real mining companies. Miners should be careful before clicking shortened website links or visiting websites that are not secured with an HTTPS connection. Most modern web browsers will indicate whether a website is secured.

### Red flags of potential mining scams:

- **Promising free money.** Any mining service that promises free money or outrageously high returns for its customers is likely a scam.

- **Offering heavy discounts**. Any company that promotes mining hardware, hosting services or other products at prices that are heavily discounted from going rates offered by other mining companies is likely a scam.

- **Sending unexpected correspondence.** If a miner receives an invoice, request for payment or other billing that is late, early or otherwise unexpected but includes branding from a company they have previously done business with, the miner should not send any payment before verifying the charges with the company.

- **Imitating real businesses.** Just because a promotion, invoice or other business material contains the branding of a real mining company does not mean that document is legitimate. Also, any suspicious requests for payment should be verified.

- **Inability to provide identity verification.** Real employees from legitimate mining companies are always available to verify their identities to a customer via video calls, voice chats or other means of communication. Miners who suspect a scam can insist on identity verification before doing business and making payments.

- **Immediate payment requests.** Any service that wants urgent payment is likely a scam. Legitimate companies will happily take the time to answer any and all questions about their products and won't rush you into any decisions.

# Hardware Shopping

## Communication

Secure communication is essential for strong operations security. Secure and encrypted email or messenger services are reliably private communication channels. Social media-based direct messaging, for example, are not. Encrypted messaging protects personal information shared in messages and the messenger's identity. It also prevents snooping by third parties and inadvertent leaks.

### *Email*

Email services like Gmail, Yahoo! Mail, Apple Mail and Outlook all collect user data and present heightened risks of compromising a user's personal data. Encrypted email services like ProtonMail, CTemplar and Tutanota offer superior information security and data privacy. CTemplar also features onion addresses, which makes it accessible through the Tor privacy browser.

### *Direct Messengers*

Messaging apps including Whatsapp, Facebook Messenger and iMessage, and messaging via social media DMs, are insecure options for regular mining-related communications that involve sensitive information. These messengers are unencrypted, and all data is stored on corporate servers. Even some messengers that are advertised as being encrypted are known to collect user data, and related data breaches are very common.

Alternative messaging products with better privacy and data security are commonly used by cryptocurrency miners. These options include Threema, Briar, Signal, Keybase, Telegram (secret chats) and Molly, a fork of Signal. Each app offers different features and levels of encryption, but all of them are significantly better communication tools than mainstream messaging products. Miners should note that Signal does not allow them to hide the phone number they use on the app from the people who they communicate with. Phone number databases are widely available online and can be used to identify and even doxx people.

Default Telegram chats are stored in plaintext on Telegram servers. When opting for privacy, use secret chats on Telegram.

### *Voice and Video Calls*

Most commonly used voice and video conference products are unencrypted and can be replaced by safer, more private alternatives. Jitsi, for example, is a free, open-source, encrypted, and private alternative to Zoom. Several of the alternative messaging apps mentioned above also offer voice call features.

## Payment Risks

The market for cryptocurrency mining hardware is still underdeveloped and fragmented, which presents abundant opportunities for scammers to prey on unsuspecting miners. Miners should exercise caution when evaluating options for buying or selling mining hardware. Miners should be particularly wary when asked to share payment information or transfer funds.

Most hardware retailers accept payment in fiat currency or cryptocurrency. Considering the benefits and risks of both options is important. Transferring funds via a credit charge, ACH payment or wire transfer requires sending a customer's legal name and bank information to the retailer, which is undesirable for privacy-conscious miners. These traditional payment methods, however, offer stronger legal recourse than pseudonymous cryptocurrency. Miners who operate under a limited liability corporation (LLC) established through a registered agent rather than tied to their real identities may prefer fiat payment methods.

Buying mining hardware with cryptocurrency is typically more private and sometimes easier than fiat payments. Privacy is not always a native feature for cryptocurrency payments especially when using Bitcoin, so miners should take precautions to protect their identity. When using Bitcoin, miners should transfer funds from a wallet they control that is not connected to any personal information (e.g., an exchange wallet) and mix the coins using CoinJoin tools (discussed later in this manual) to obscure the coin's transaction history for better payment privacy.

The primary risks of cryptocurrency payments are irreversibility and upward price volatility. A customer's ability to receive a refunded cryptocurrency payment is never guaranteed. Unlike paying with fiat money, crypto-paying customers must also decide if the product they're purchasing is more valuable than the potential gains from simply holding the crypto asset if it appreciates.

### Know Your Customer (KYC) Information

Some miners prefer to shop for hardware in chat rooms on Telegram or Discord or by browsing online marketplaces like eBay. However, due to lack of identity verification requirements, using these channels comes with risks of receiving damaged hardware or no hardware at all. Casual hardware markets that operate in chat rooms and require customer identification are highly unusual and should be avoided. Scammers requesting this info could use it to sign up for services, make payments or sell on the dark web without permission. The tradeoff between making a best effort to avoid being scammed and not having to disclose personal information is worth taking for some miners.

Curated marketplaces that verify the existence and quality of machines before listing them are much safer platforms for hardware shopping. Some retailers require identity verification, but not all do, nor are the information requirements applied universally. For example, miners trying to sell mining hardware may be required to verify their identities, but buyers do not always have the same requirements.

Buying hardware directly from manufacturers also typically requires identity verification. Small-scale miners will almost always pay a premium for their hardware when placing these orders compared to institutional miners who receive discounted pricing due to the size of their purchases. Ordering through Bitmain requires a valid name, ID and verified shipping address. MicroBT requires slightly less personal information: a valid name, shipping address and email address. These requirements, however, are always subject to change.

### Shipping Information

Shipping any cryptocurrency-related products, especially mining hardware, to a home or work address presents severe security risks. Customer shipping data is stored in company databases, and data breaches for cryptocurrency customer data are not uncommon. Even trusted retailers are not invulnerable to information leaks. The risks associated with leaks of this information can include spam, theft, robbery and even bodily injury or death.

The simplest way to avoid shipping information risks is to apply for a post office box or personal UPS mailbox. Both options replace the need to hand over personal or work addresses, which will end up in the databases of mining hardware retailers.

## Threat modeling

Before diving into security and privacy for mining operations, it's important to discuss threat modeling. A threat model helps an individual identify the data or equipment they need to protect and who they need to protect it from. Proper threat modeling includes identifying likely threats and attack vectors. Building a threat model will help a miner decide what OPSEC precautions and solutions they should take and implement.

### Miners should ask themselves these questions when defining their threat model:

1. *What assets, physical and digital, do I want to protect?*
   In the context of mining, physical assets include mining hardware and infrastructure, hardware wallets and smartphones. Digital assets include accounts containing personal identifying information and cryptocurrency.

2. *Who do I want to protect them from?*
   Be as specific as possible. This will be situation-dependent, but miners typically want to protect themselves against spying from their neighbors, their ISP and mining pool, and third-party surveillance organizations.

3. *If I fail to protect these assets, what are the consequences and how bad are they?*
   Rate the consequences of having your assets compromised or seized and the long term implications of an occurrence.

4. *How likely is it that I need to protect these assets?*
   If these assets make up a larger portion of a miner's net worth or livelihood, they are more likely to need to protect them.

5. *How many steps or hurdles am I willing to deal with to try to prevent potential consequences?*
   Some privacy strategies will require miners to take extra precautions and do extra work. Each privacy- or security-enhancing practice needs to be evaluated from this perspective: is the added benefit of doing this worth the extra effort?

Spend some time thinking about this before moving on to the next section.

# Part 2: Mining Operations

## Security Management

Mining hardware requires significant power consumption, and as a result emits a lot of heat and noise. This needs to be taken into consideration when managing OPSEC, as improperly managed heat and noise can easily draw attention to a mining operation.

### Site Security

Properly secured mining hardware is necessary for good OPSEC. For most small-scale miners, securing the site of their mining operations includes many basic home security practices. Just like many cryptocurrency users take precautions to protect their stored assets, securing valuable ASIC and computing hardware is a key security consideration for miners.

A collection of 25-pound, $10,000 computers are not secured by mnemonic phrases; protecting these assets is more involved. Whether a thief is likely to know the value of a loud computer running in their neighbor's garage or where to resell it is irrelevant. Electronic hardware is a common enough target for theft even without any known cryptocurrency use.

### Physical Security

Miners should store their hardware in locked rooms. If this room has windows, they should be tinted or covered with curtains. In addition, limiting the entry points into the area where mining equipment is kept can decrease the risk of physical break-ins. Miners can also use trees and other vegetation to block outdoor entry points if necessary.

If a miner decides to keep their equipment underground, they must take extra precautions to use proper cooling methods due to lack of airflow.

### Site Monitoring

In addition to physically securing equipment, miners can purchase cameras to monitor the perimeter of their site while they are away. This may also help them identify any potential threats because it will give them a better visual of the landscape and any passersby.

Additional operations security suggestions for heat, noise and electricity consumption are discussed in the following section.

## Power Consumption

Mining is an energy-intensive process at any scale. While industrial businesses may use large amounts of power intermittently, cryptocurrency mining uses large amounts of power constantly. Utility companies, who can look at energy consumption profiles for each address, may be able to tie mining operations to a customer's account.

First of all, a miner should not operate at more than 80% capacity of their electrical circuit, as is best practice for any electrical application.

Additionally, miners can bring their machines online over time as this will look less suspicious than bringing all the mining hardware online instantaneously. If a miner wants to operate one to two ASICs, they can run these machines in place of their common household appliances. A common adjustment is running an ASIC in place of their clothing dryer or dishwasher.

Another option to protect OPSEC is running miners for part of the day. Using excess power solely in the day time, rather than 24/7, is typically overlooked by power providers. This isn't recommended due to inefficiency but may be appealing in certain situations. Miners can also take advantage of power purchase agreements (PPAs) from their electricity provider in order to secure cheaper rates on excess power usage. When negotiating, there is no need to mention that the excess electricity will be used for bitcoin mining. An overview of these types of agreements can be found here.

# Heat Signatures

Since mining hardware requires such a large amount of power, it puts off a lot of heat. This heat needs to be dissipated and moved away from the mining hardware to prevent damaging the machines. Generally, mining operations run their equipment in one area. This can put off a large heat signature. By using heat mapping or thermal imaging technology, third parties can reveal mining facilities from afar without even entering the facilities. Miners should consider proper air and cooling to avoid damaging their hardware and to reduce the heat signature of their mining operation.

Thermal imaging technology picks up infrared radiation, or heat, and displays the object's temperature versus its surroundings. In the case of bitcoin mining, this heat is radiated by ASICs. It doesn't matter how expertly camouflaged a miner's hardware is – if it's warmer or cooler than its background, the imaging technology will detect it. If a miner is running a small mining operation from their home, they must be mindful of their heat signature and at least partially mask it if they wish to achieve strong OPSEC.

## How to conceal heat signature

### *Mining room and backdrop*

Different materials radiate heat in different ways. Therefore, a miner can place their ASICs in a room with a backdrop that naturally balances infrared radiation. Stud partitions or drywall won't reliably block heat. Glass, concrete and brick, however, are known to help conceal infrared radiation. The room that ASICs are placed in should also have good ventilation and a low ambient temperature.

### *Fluids – Immersion cooling*

Immersion cooling can be used to better manage heat and mask an operation's heat signature. Fluids have a higher heat capacity than air, often requiring four times as much energy to raise or lower the temperature. This means that objects are harder to differentiate via thermal imaging technologies when they are submerged. An example of an immersion cooling setup can be found here.

Miners wishing to pursue an immersion cooling setup will need to use dielectric coolant to avoid damage to their machines. This article offers an overview of immersion cooling and breaks down terminology, cooling methods (single and double phase) and setup components.

### *Other materials – Aluminum*

Any electrically conductive material will block some infrared radiation. The greater the conductivity, the greater the blocking. Aluminum foil can serve as a possible radiation deflection tool for a cheap DIY project.

## Other considerations for minimizing ASIC heat

Regular dust removal is very important. This will prevent the machines from getting clogged with dust and overheating. Dust removal can be done using a high-pressure blower to blow the dust out of the machines. This should be done monthly. A miner can also replace a machine's lower-speed fans with higher-speed versions for better cooling, which will contribute to reducing the overall heat signature.

# Noise Pollution

Mining machines are loud and easily heard. By design miners come with attached fans that draw new air in past the mining chips and expel hot air. While these fans contribute to solving heat issues, they also run constantly and put off a lot of noise that could draw attention to a mining operation.

### ASIC placement

It's recommended to place miners in remote areas or areas with less human traffic, such as a garage, basement, storage room or warehouse.

### Noise-dampening enclosures and materials

Noise can be dampened with containers and NVH (noise, vibration, and harshness) material, but airflow must be maintained, otherwise heat may damage the hardware. For example, a miner can place their ASIC in a styrofoam box with flexible vent pipes running in and out from both ends. This allows air to flow freely through the machine. Immersion cooling, discussed above, also significantly reduces the noise pollution from mining.

Additionally, noise can be reduced through the use of aftermarket fans, noise dampening foam or nozzles. Home miners can also put up acoustic foam or acoustic felt on the walls in the room their machines are in to reduce some of the noise heard elsewhere in their house. Thicker egg-shaped foam tends to work best for this purpose.

Miners can also have rooms where they plan to place their machines sound-proofed by professionals, but this option can cost over $5000.

### Nose-dampening curtains

If ASICs are placed in a room with windows, installing noise-dampening curtains is an easy way to control excess noise. These curtains can be purchased online. Windows should also be covered to prevent snooping from neighbors regardless, so these curtains offer a two-for-one solution.

### Noise-dampening software

Miners can use software meant to reduce noise. For example, custom firmware such as Braiins OS+ works by reducing fan noise. More information on this software's functionality can be found here.

# Hardware Considerations Summary

Power, heat and sound all go hand in hand in a mining operation.
In most cases, reducing the power draw per miner will reduce the noise and heat of the device, but this will also reduce the profitability. Each of these should be considered when planning a mining operation because they may draw unwanted attention that could affect user OPSEC. Climate, location and utility provider are all things to consider when evaluating these risks.

# Data Protection

The noise and heat outputs of ASICs are not the only way that miners can be identified. In fact, the easiest way for a miner to lose their OPSEC is via their web activity. Whether accessing mining pool websites or sending shares to a pool's stratum server, if miners don't take extra measures to protect the privacy and security of their data, they can easily expose their mining operations.

### General Web Traffic

An internet service provider (ISP) can see pretty much everything someone does online if they don't use a VPN, Tor or a similar solution to privately route their web traffic. This includes visiting a mining pool's website.

Latency is not a concern when checking a pool account, so it's recommended to use a VPN or Tor to hide the sites visited from ISPs and hide IP addresses from mining pools. Please see part 4 of this manual for details on private web browsing, browser and VPN recommendations and mobile privacy usage.

## Stratum Protocol Data Transfers

Privacy and security are a bit more complicated when it comes to the mining data transfers themselves. As miners understand, every second counts in the race to find blocks. While the latency of a high quality VPN isn't significant for general web browsing, it can impact the profitability of mining by increasing a miner's stale shares (i.e. shares submitted for a block height which has already been mined), which they don't receive payouts for.

One common-sense approach presented by @econoalchemist in his Home Mining Network Privacy guide is to utilize multiple VPN tunnels in a failover fashion to automatically route mining traffic to the tunnel with the least latency. This affords the user privacy from the ISP, privacy from the mining pool, and no material-added latency. In fact, based on a 5-day test conducted in the guide, econoalchemist found that mining with multiple VPN tunnels actually introduced less latency than mining over clearnet.

The downsides of not using a VPN are also significant. With a basic networking setup, a miner's ISP will see that they have a connection with a pool's stratum server and the pool will see their IP address. Not only that, but a miner's hashrate is actually at risk of being stolen if an eavesdropper is sophisticated enough. This is because data transfers via stratum protocol are unencrypted and in human-readable JSON format.

This is comparable to visiting HTTP websites without security certificates (i.e. not HTTPS). When someone visits an HTTPS web url, their ISP can see that they visited it but not any of the activity that they actually do there, such as inputting login credentials or credit card details. With HTTP, they can see everything. Mining today is similar to HTTP, where all that data being between a miner and their chosen mining pool is out in the open to see.

Fortunately, there are some solutions that don't introduce significant latency and impact mining profitability.

## Stratum V2

The most straightforward and simple solution to protecting stratum data transfers is upgrading to Stratum V2. Unlike in Stratum V1, data transfers in V2 are encrypted and in binary format rather than JSON. The encryption means that Stratum V2 is like the HTTPS to Stratum V1's HTTP, keeping all of a miner's actual mining activity private and hidden from potentially malicious onlookers and preventing them from being able to steal any of their hashrate.

The binary format reduces the size of data transfers, such that an encrypted Stratum V2 data transfer is actually about 2x lighter than an unencrypted Stratum V1 data transfer. Stratum V2 will prevent the ISP from seeing what information is contained in the data on the miner's network traffic routes but Stratum V2 will not prevent an ISP from seeing where that data is going to. Also, the mining pool can still see the miner's IP address.

As of November 2021, Stratum V2 is only natively supported in the Braiins OS+ firmware and the pool operated by Braiins, Slush Pool. Other pools have expressed their intention of implementing Stratum V2 but could be waiting for the specification to be finalized and turned into an official BIP (Bitcoin Improvement Proposal). This is currently being independently worked on by developers funded through Spiral's (formerly Square Crypto) grant program.

For miners who aren't able to use Stratum V2 yet, there are some other solid options to improve privacy and security of Stratum V1 connections.

## Proxies

A great option that doesn't significantly increase latency is a DNS proxy such as dnsscrypt-proxy, which can be used to encrypt and authenticate requests using the DNSCrypt protocol and pass them to upstream servers (i.e. mining pools).

This makes it so that ISPs won't see details about the communication between a miner and a mining pool, only that there is a connection. In other words, itslike changing from HTTP to HTTPS, similar to Stratum V2. The difference is that a DNS proxy isn't native, so it will take some work to set it up. The exact steps will vary depending on the operating system used, but general instructions and OS-specific guides can be found here.

Even with this solution, it would still be possible for a miner's pool to know their IP address and for an ISP to see that they're communicating with a pool. If a miner wants to go the extra mile to improve anonymity, another solution is to route their hashrate through a TCP proxy or a SOCKS proxy that can be set up on a cloud server. This should be combined either with Stratum V2 (if possible) or a DNS proxy so that the data transfers are still encrypted.

## 100% Anonymity Is Impossible

Lastly, it's best to be aware that all of these solutions mentioned above –while far better than nothing – do not guarantee anonymity. If some powerful 3-letter organization or an extremely persistent hacker really wants to find a specific person, they might be able to piece together enough info to do so. However, if a miner implements these solutions, doxxing by these bad actors will become an order of magnitude more difficult.

# Part 3: Pools and Payout

## Pool Accounts

### Login Security

Protecting a mining pool account means protecting login information that gives access to critical details on a miner's operation, including determining which addresses receive payouts from the pool. Miners with an improperly secured account are putting their data at risk of being compromised, this involves a third party accessing the miner's pool information and changing payout addresses and other important settings.

Enabling two-factor or multi-factor authentication (2FA or MFA) for mining pool accounts is a critical step in preventing unauthorized account access. In addition to a username and account password, 2FA or MFA introduces an additional layer of security to ensure that only authenticated users can access an account online.

Mining pools typically offer 2FA for added user account security, and these pools encourage their miners to activate it. Miners should not use text message 2FA or Google Authenticator; these methods are not secure. Privacy-focused 2FA tools include but are not limited to andOTP, Authy and Aegis Authenticator.

### Address Reuse

Miners should avoid address reuse. All address balances are visible to anyone with a block explorer. Reused addresses are also more easily linked to real-world identities, which could result in doxxing, address blacklisting and other risks. Mining pool balances and payout transactions are some of the most closely watched types of on-chain data by everyone from amateur data analysts to government officials and corporate chainalysis companies.

Risks associated with address reuse increase exponentially if the address has a large balance and can be traced from a mining pool to any service that stores personal information (e.g., names, addresses) like a third-party wallet or a cryptocurrency exchange.

Miners can mitigate address reuse risks by reducing the frequency of their payouts from the pool so addresses are reused less often, or by supplying the pool operator with a new receive address after every payout. The second suggestion completely eliminates address reuse. The first comes with increased third-party risk because the miner leaves more of their funds in the control of the pool operator while the second is more inconvenient, especially if the miner prefers to receive smaller, more frequent payouts from the pool.

Switching payout addresses is a simple process. The user account settings for most pools allow a miner to easily replace their current payout address with a new one at any time.

## Storage

Creating a strong and safe storage setup starts with choosing a secure cryptocurrency wallet. Wallet products are broken into two categories, hot (software) wallets and cold (hardware) wallets, meaning wallets connected to the internet and those that are not. The software wallet market is saturated with hundreds of products that are built for web browsers, desktops and mobile devices. Custodial (exchange) wallets are also classified as software wallets.

### Exchange Wallets

Exchange wallets are addresses controlled by an exchange that a user can deposit to and request withdrawals from through their exchange account.

Mining directly to a custodial exchange's online wallet presents a high level of security risks.

In the event that an exchange temporarily disables withdrawals or completely goes offline, a miner will lose access to their funds. Troubleshooting or resetting custodial exchange wallets is a difficult process. And because most exchanges require full Know Your Customer (KYC) information, sending payouts to these exchange wallets doxxes the pool a miner uses and their payout address, in addition to the personal identifying KYC information they gave the exchange while initially signing up. In the event of a data leak or hack, all of this information collected by the exchange can become public.

### Software Wallets

Software wallets are applications that run on a user's computer and typically give the user full control over managing the wallet's addresses. Mining to a desktop or mobile software wallet carries fewer risks than mining directly to an exchange wallet.

Software wallets are only as secure as the devices they run on. Miners should make sure that their devices are free of malware and viruses. Most software wallets are connected to the internet. This connection presents the owner with the theoretical risk that their wallet can be accessed by other internet users. By taking proper precautions, software wallets can be used safely as temporary storage for smaller amounts of cryptocurrency, and for CoinJoin payouts prior to transferring to a hardware wallet.

### Hardware wallets

Hardware wallets (HWWs) are secure physical devices for storing cryptocurrency. These devices secure bitcoin private keys offline. Accumulating payouts to a hardware wallet in full control of the miner is the best storage strategy.

Not all hardware wallets are created equal. The most secure hardware wallets are developed with open-source software and air-gapped hardware, meaning the device communicates with a software wallet without needing to be physically connected to the computer running the wallet. Miners can use their HWW connected to a watch-only (mobile or desktop) wallet and generate receiving addresses. This makes receiving payouts to a hardware wallet as easy as receiving to a software wallet. This guide walks users through how to set up and use a hardware wallet.

To further minimize risks, miners can also consider distributing payouts across multiple hardware wallets, including a variety of makes and models into their storage plans. Miners should also safeguard their wallets' seed phrases, whether the wallet is a software or hardware product. Seed phrase storage can be done in numerous ways as well. For instance, some users place seed phrases on storage devices like microSD cards. Others opt for durability and longevity by carving seed phrases into physical objects like steel or titanium. Lastly, some miners can also use multi-signature wallets (multi-sig) in order to provide a different type of security.

# CoinJoin payouts

Transaction histories on all public blockchains are easily auditable. CoinJoins, or mixing, is a simple way for miners to protect their financial privacy by obscuring the history of their holdings. Sometimes referred to as "cleaning" by privacy advocates, the mixing process prevents blockchain data watchers from following where coins originated and accessing their full transaction history. Users should note that mixing is often used interchangeably with "tumbling" and "CoinJoin." "Tumbling" is an older technique where users give up custody of their coins and hopefully receive coins with a different history. In this article, we will use the term "mixing" in reference to "CoinJoin" transactions.

Users should also be aware of the term "unspent transaction output," or "UTXO," which refers to a discrete piece of Bitcoin. When mixing coins, UTXOs are swapped among participants in equal value, similarly to swapping pocket change with multiple strangers.

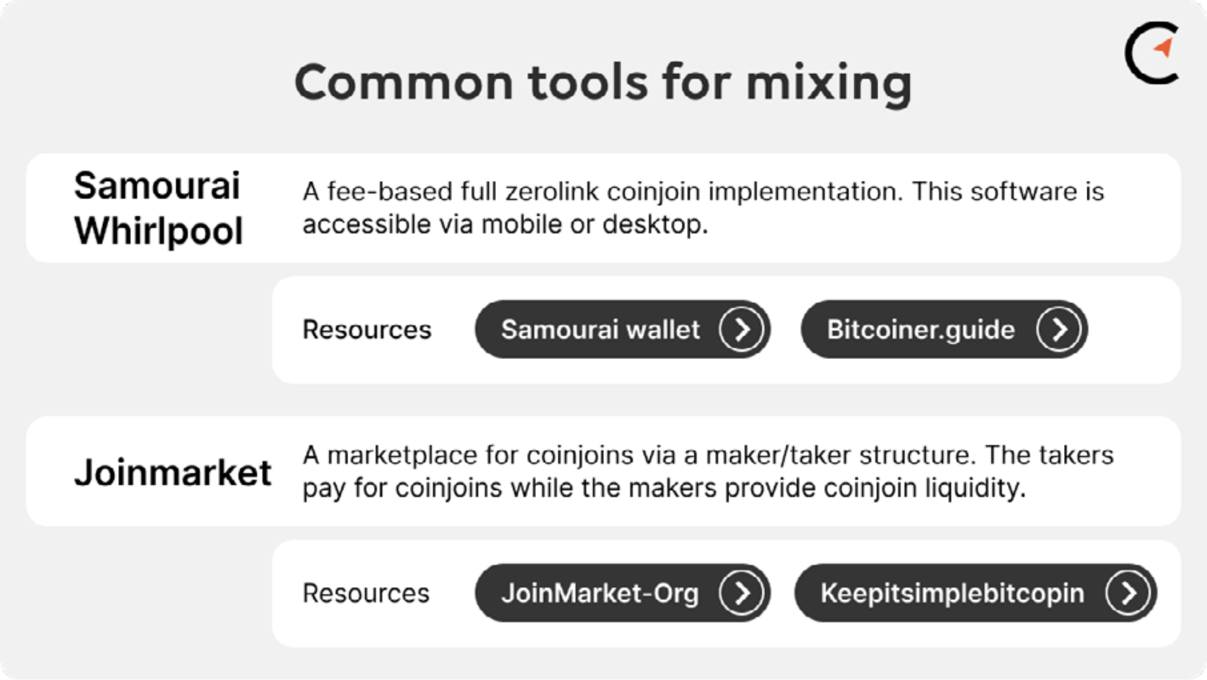
A CoinJoin is a multi-party transaction where several senders contribute UTXOs to a transaction ("mix") and receive the same amount of bitcoin back to complete the transaction. After a mix has completed, a blockchain watcher cannot know which transaction output is linked to an input. CoinJoin transactions are non-custodial and do not require trust or handing over keys like tumbling.

For optimal privacy, consistent and multiple remixes are ideal. Why does this matter? One round of a CoinJoin breaks deterministic links (separates the coins from its history), but, remixes increase a user's anonymity (anon) set.

It is also possible to mix directly into cold storage. Please see the Sparrow guide linked above, or if you prefer using the full Samourai stack, please see this guide written by @Diverter_noKYC.

CoinJoins are not risk-free. Past transaction histories are not erased per se; only forward-looking privacy is achieved for mixed coins. Similarly, mixing does not undo a KYC event, meaning that an owner's name is still recorded as belonging to past transaction history from when coins were used or purchased or spent. But mixing provides a sort of clean slate for users wishing to disconnect future use from past transaction histories.

Centralized cryptocurrency exchanges also represent another barrier for using mixed coins. Most exchanges flag deposits made from external addresses with mixed transaction outputs that can occur during mixing. Transferring or selling coins through peer-to-peer (P2P) markets or other KYC-free platforms, however, is rarely restricted. Setting aside some amount of non-mixed bitcoins is a good practice to have the option of using services that reject mixed coins if necessary.



Common tools for mixing

**Samourai Whirlpool**

A fee-based full zerolink coinjoin implementation. This software is accessible via mobile or desktop.

Resources: Samourai wallet › Bitcoiner.guide ›

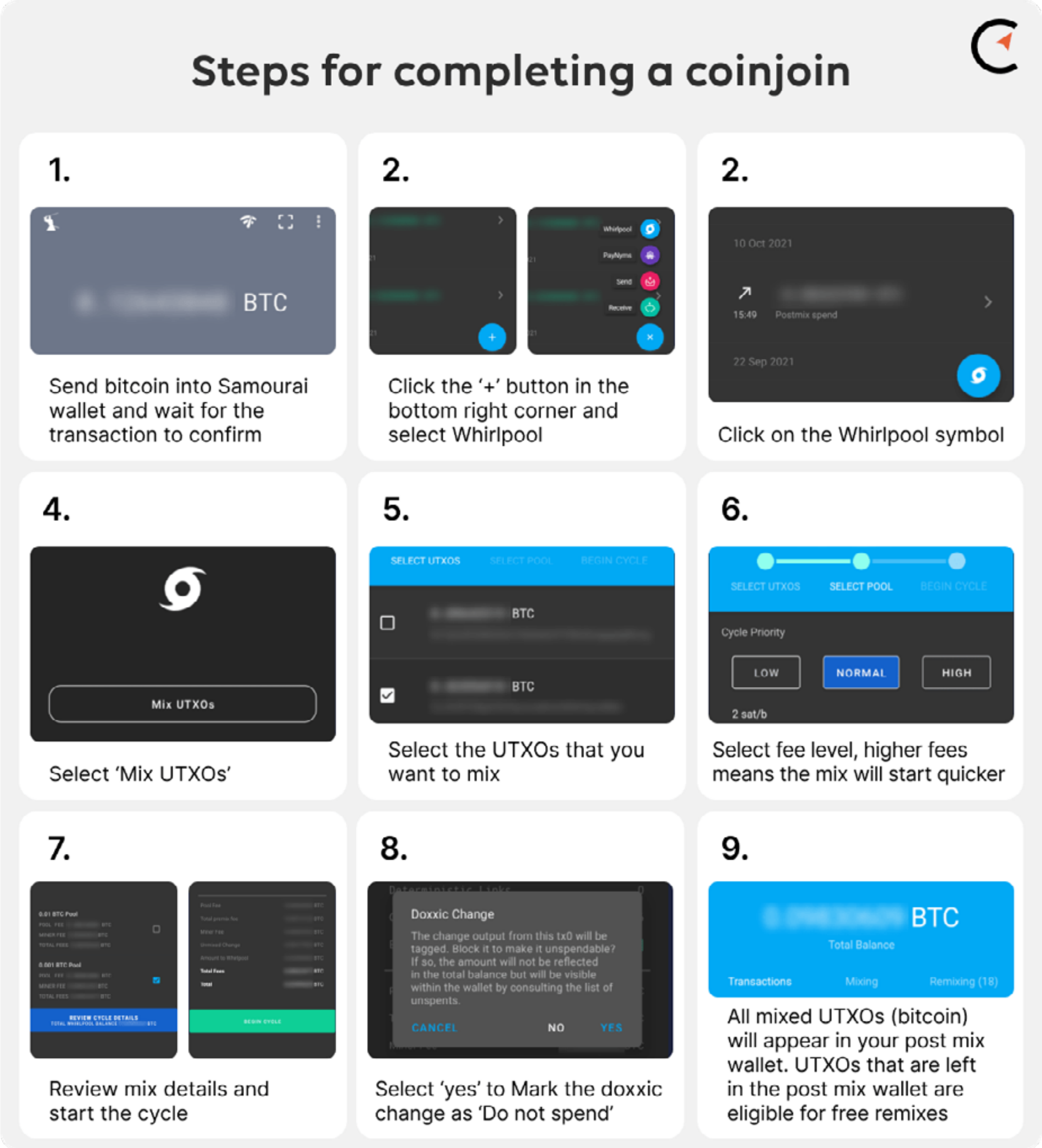
**Joinmarket**

A marketplace for coinjoins via a maker/taker structure. The takers pay for coinjoins while the makers provide coinjoin liquidity.

Resources: JoinMarket-Org › Keepitsimplebitcopin ›

CoinJoins are not as complex and intimidating as they look. Whirlpool makes it possible to mix from your smartphone. Simply download the Samourai wallet app from the Google Play Store (Samourai wallet is only available on Android) and follow the steps below.

## Examples: How to Coinjoin



### Steps for completing a coinjoin

1. Send bitcoin into Samourai wallet and wait for the transaction to confirm

2. Click the '+' button in the bottom right corner and select Whirlpool

2. Click on the Whirlpool symbol

4. Select 'Mix UTXOs'

5. Select the UTXOs that you want to mix

6. Select fee level, higher fees means the mix will start quicker

7. Review mix details and start the cycle

8. Doxxic Change

   The change output from this tx0 will be tagged. Block it to make it unspendable? If so, the amount will not be reflected in the total balance but will be visible within the wallet by consulting the list of unspents.

   CANCEL NO YES

   Select 'yes' to Mark the doxxic change as 'Do not spend'

9. All mixed UTXOs (bitcoin) will appear in your post mix wallet. UTXOs that are left in the post mix wallet are eligible for free remixes

## Sparrow Wallet's Whirlpool Client

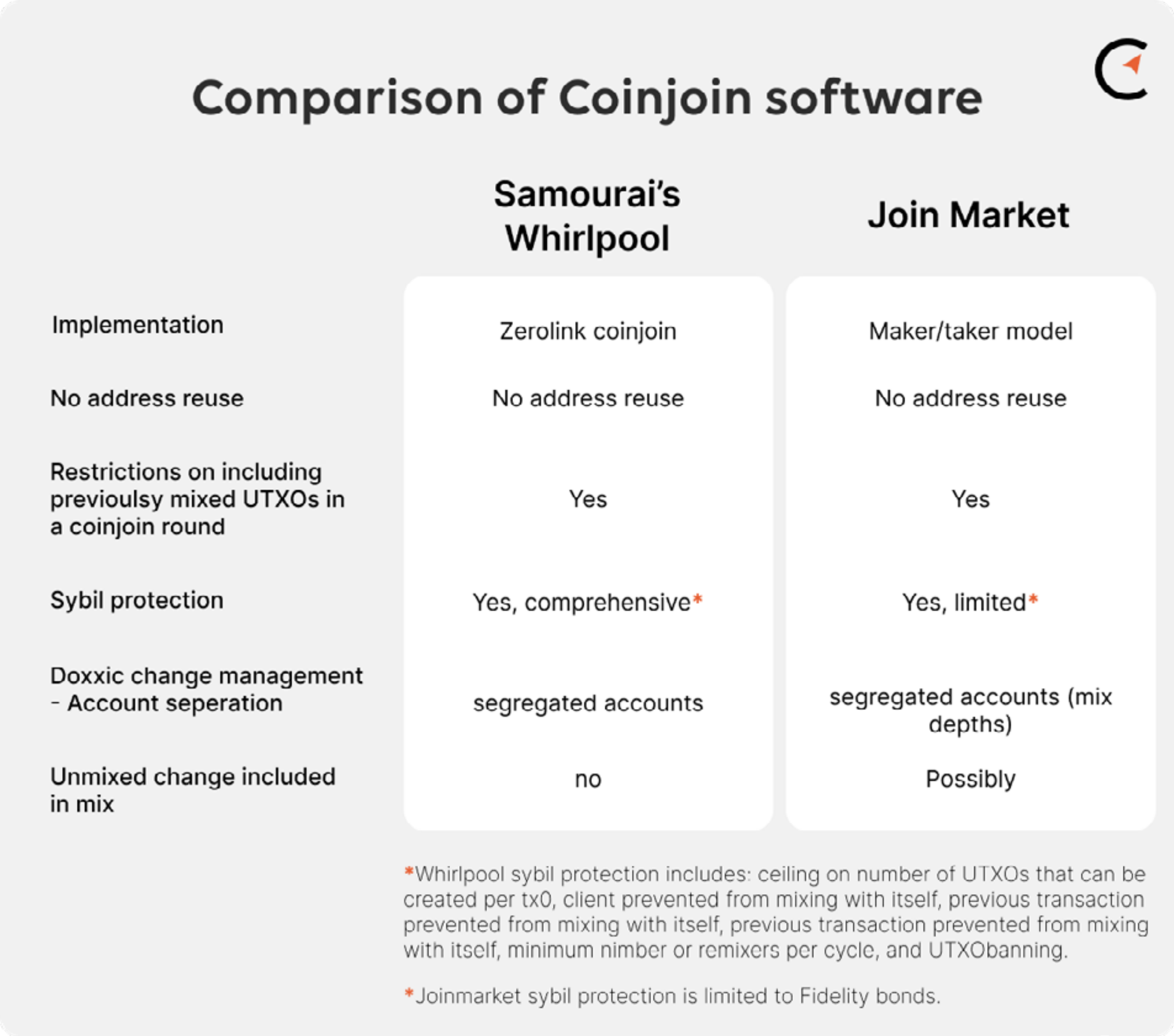
In order to use Sparrow's implementation of Whirlpool, the user will need to download and install Sparrow and set up a wallet (quick start guide). After this is done, the user can start mixing in Sparrow. Like RoninDojo's Whirlpool CLI, Sparrow wallet should be left open in the background for 24/7 remixing.

## Coin control, labeling and doxxic change

After mixing your coins, it is important to label them and segregate them from unmixed coins. Proper coin control involves selecting which UTXOs are spent in a transaction and avoiding spending mixed and unmixed UTXOs together. If this is not done, it will compromise user privacy and undo the anonymization benefits from mixing.

Doxxic change is the leftover amount of bitcoin after the UTXOs selected for a CoinJoin are divided into equal amounts (determined by the size of the mixing pool), e.g. if you selected a total of 0.056 bitcoin and the 0.05 coinjoin pool, that leaves 0.006 in doxxic change. Users should also not combine this with mixed bitcoin.

Each implementation deals with doxxic change differently. Samourai wallet's Whirlpool allows users to mark this change as "do not spend." Sparrow wallet's implementation of Whirlpool completely separates this change into a separate wallet (Badbank). If using Joinmarket, takers can propose a mix that consumes an entire UTXO. Best practices for dealing with doxxic change.



Comparison of Coinjoin software

| | Samourai's Whirlpool | Join Market |
|---|---|---|
| Implementation | Zerolink coinjoin | Maker/taker model |
| No address reuse | No address reuse | No address reuse |
| Restrictions on including previoulsy mixed UTXOs in a coinjoin round | Yes | Yes |
| Sybil protection | Yes, comprehensive* | Yes, limited* |
| Doxxic change management - Account seperation | segregated accounts | segregated accounts (mix depths) |
| Unmixed change included in mix | no | Possibly |

*Whirlpool sybil protection includes: ceiling on number of UTXOs that can be created per tx0, client prevented from mixing with itself, previous transaction prevented from mixing with itself, previous transaction prevented from mixing with itself, minimum nimber or remixers per cycle, and UTXObanning.

*Joinmarket sybil protection is limited to Fidelity bonds.

## Selling and Lending

Instead of only holding their payouts in cold storage, many miners choose to lend or sell some of their holdings. Lending and selling are easy ways for miners to generate extra revenue or liquidate their cryptocurrency to cover operating costs. Miners should carefully evaluate selling and lending products because often the easiest ways to sell or lend present the highest OPSEC risks.

### Selling

Mining directly to an exchange wallet is not secure for the reasons explained in the previous section. But even mining to a hardware wallet and later transferring funds to a centralized exchange doxxes sensitive data. Consequently, data – including the address used and its complete transaction history – become known to that exchange and any party with whom the exchange shares the data with.

Although managing funds is always a matter of personal preference, miners should be aware of the risks involved with sending funds from a securely stored payout address to a fully KYC-ed exchange account.

Depending on a miner's security practices, some assets will be harder to sell than others. Depositing and selling bitcoin that was previously mixed in a coinjoin transaction, for example, could be difficult to sell because many top exchanges follow internal guidelines that limit or prohibit deposits from addresses with a history of receiving mixed coins. Miners wishing to sell mixed bitcoin should use a decentralized non-KYC exchange or P2P markets.

Decentralized or P2P exchanges like Bisq and Hodl Hodl do not screen deposited coins based on their address history. Lastly, their software's decentralized design and minimal customer information requirements reduces the risks of data leaks, address doxxing, and other mining privacy concerns.

## Lending

Some miners prefer lending to selling since it allows them to generate profits from their cryptocurrency without liquidating their holdings. However, most cryptocurrency lending services are fully centralized platforms that require full user identification information. As a result, most lending options inherently carry data protection and miner privacy risks that have been discussed elsewhere in this manual.

To be clear, lending with these platforms is not entirely insecure, but the nature of the service introduces OPSEC risks that miners should carefully consider. Miners can also use decentralized lending options. For example, Hodl Hodl allows lenders and borrowers to remain anonymous and transfer their funds to their counterparty without relying on a third party. The terms of the loan are agreed upon by the lender and borrower, not Hodl Hodl.

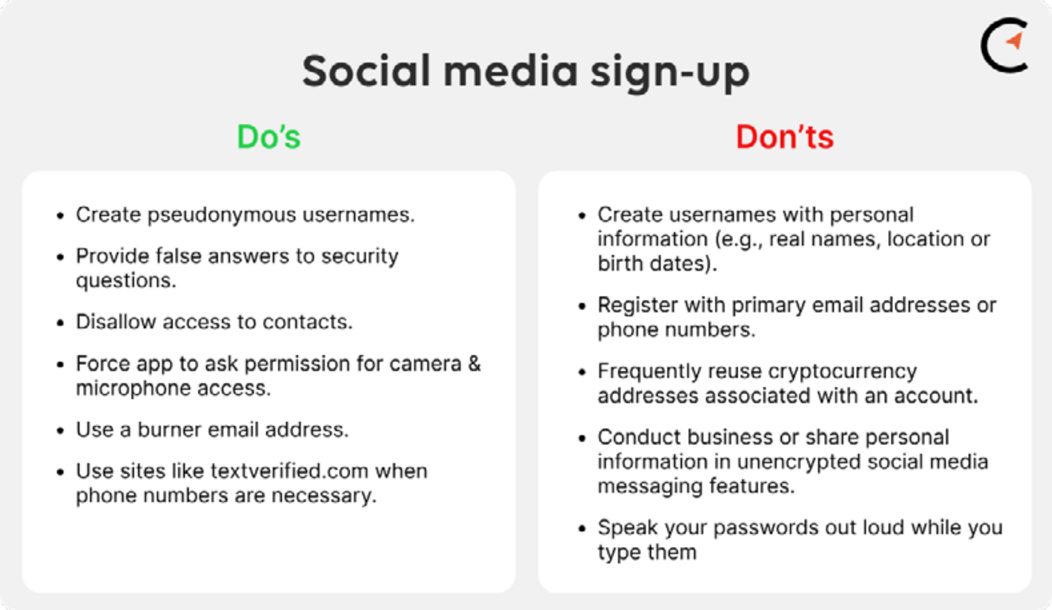
Other lending options include exchanging cryptocurrency the miner earns for a tokenized form of that same asset, like swapping Bitcoin (BTC) for the bitcoin-backed ERC-20 token Wrapped Bitcoin (WBTC) from BitGo. Miners can then stake or lend this bitcoin-backed token through various protocols in the decentralized finance (DeFi) ecosystem. But the token swapping process generally requires complete KYC information even if the DeFi lending platforms do not.

# Part 4: Online Privacy

## Social Media

Most mining discussion and education materials are accessible from a variety of public online forums and social media platforms. Miners naturally gravitate toward these resources to learn from other miners and share their own experiences. But privacy-conscious miners should exercise caution when engaging with these online communities to avoid sharing any sensitive geographic, financial or other personal information.

Below are some primary dos and don'ts for creating accounts on any popular online forums. Although perfect anonymity is unachievable, miners can remain mostly pseudonymous by avoiding use of personal information when registering for these platforms and protecting that information while interacting on them.



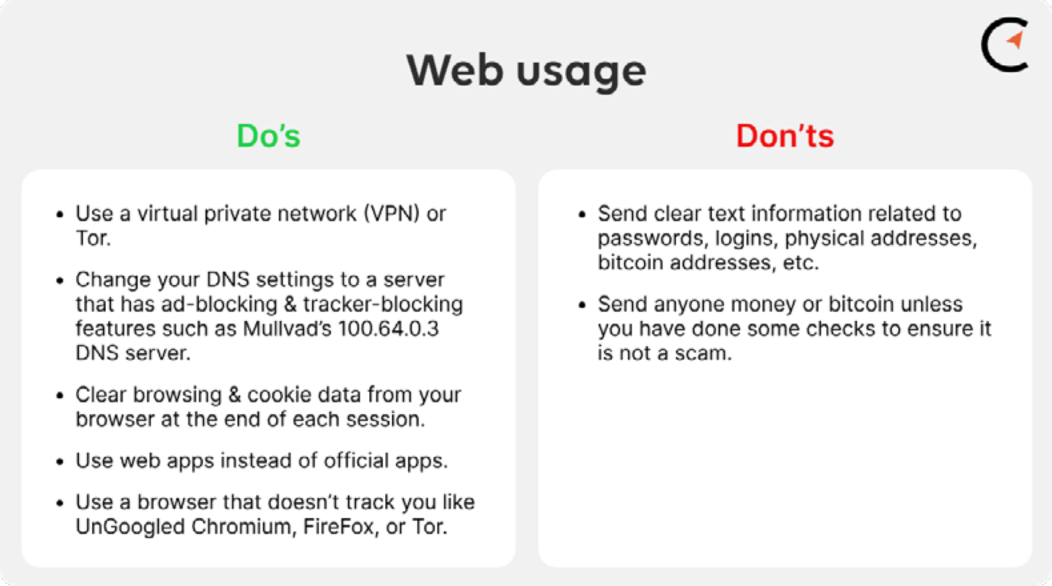
### Social media sign-up

**Do's**

- Create pseudonymous usernames.
- Provide false answers to security questions.
- Disallow access to contacts.
- Force app to ask permission for camera & microphone access.
- Use a burner email address.
- Use sites like textverified.com when phone numbers are necessary.

**Don'ts**

- Create usernames with personal information (e.g., real names, location or birth dates).
- Register with primary email addresses or phone numbers.
- Frequently reuse cryptocurrency addresses associated with an account.
- Conduct business or share personal information in unencrypted social media messaging features.
- Speak your passwords out loud while you type them



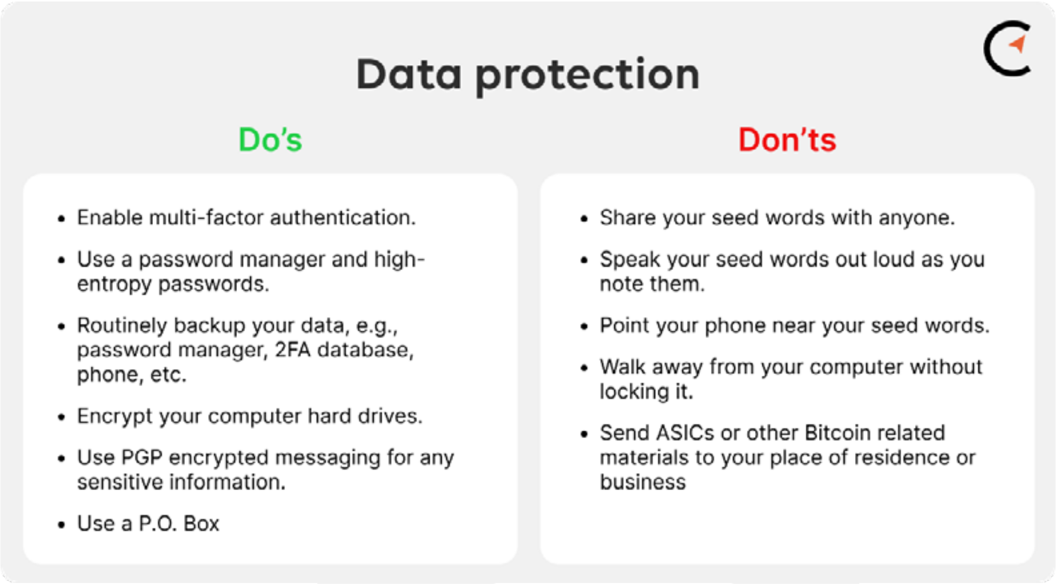
### Web usage

**Do's**

- Use a virtual private network (VPN) or Tor.
- Change your DNS settings to a server that has ad-blocking & tracker-blocking features such as Mullvad's 100.64.0.3 DNS server.
- Clear browsing & cookie data from your browser at the end of each session.
- Use web apps instead of official apps.
- Use a browser that doesn't track you like UnGoogled Chromium, FireFox, or Tor.

**Don'ts**

- Send clear text information related to passwords, logins, physical addresses, bitcoin addresses, etc.
- Send anyone money or bitcoin unless you have done some checks to ensure it is not a scam.



Data protection

Do's

- Enable multi-factor authentication.
- Use a password manager and high-entropy passwords.
- Routinely backup your data, e.g., password manager, 2FA database, phone, etc.
- Encrypt your computer hard drives.
- Use PGP encrypted messaging for any sensitive information.
- Use a P.O. Box

Don'ts

- Share your seed words with anyone.
- Speak your seed words out loud as you note them.
- Point your phone near your seed words.
- Walk away from your computer without locking it.
- Send ASICs or other Bitcoin related materials to your place of residence or business

Online mining-related conversations routinely involve sharing pictures of video clips of a miner's mining setup. A primary concern for pseudonymous miners posting this content is doxxing their location and identities. Avoiding content that contains visual or auditory identifiers is a simple way to protect this information.

# Mining Apps

## Downloading Mobile Apps

Before downloading mining apps, making a strong effort to verify their legitimacy is essential for avoiding phishing or scam apps. Downloading new software always carries some risk, however, and no security measure is completely invulnerable.

Following direct links to apps for mining pools or other service providers provided by these companies on their websites or verified social profiles also helps avoid downloading harmful software. Consider first downloading an app to a separate, blank device with no other compromisable information.

Understand what the app does before downloading it. Check the developer's name, review the app's privacy policy and query Google or another search engine for the app's name with "scam" or "fake." If the software is malicious, reviews and discussions about the problem will likely surface.

Verify downloads with the developer's PGP public key and signature when possible.

## Using Mining Apps

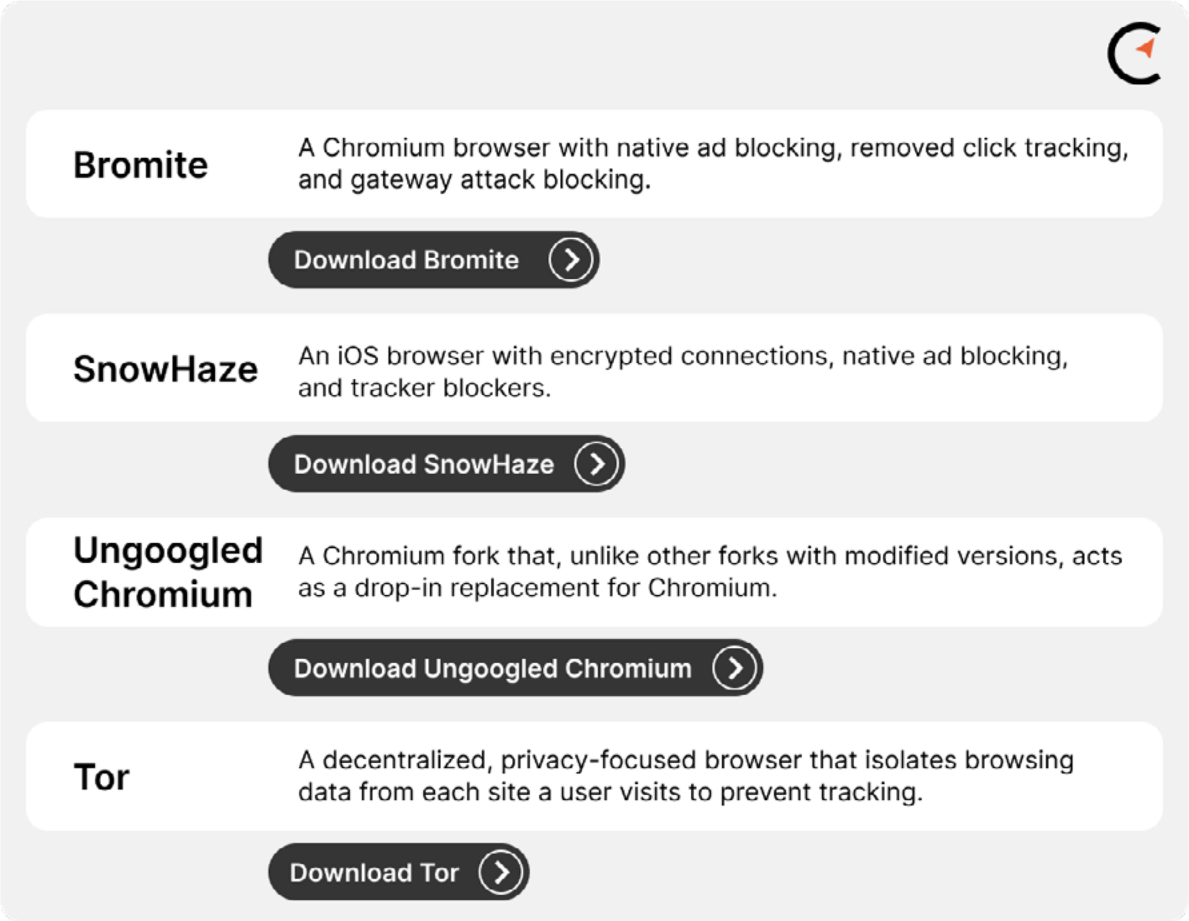
Secure use of mining apps borrows from the same practices for secure internet use mentioned earlier in this document. Enabling a VPN while using a mining app helps to obscure a miner's location and activity. Other internet proxy services like the Orbot app discussed later in this document also offer increased privacy.

# Web Browsing Privacy

Most internet browsers offer alarmingly weak data security and user privacy. Avoiding commonly used browsers like Google Chrome, Microsoft Edge and Apple Safari is an essential basic step toward enhanced online operation security. Regular VPN use is also a key step for safer internet use.

## Browser Alternatives

Here's a short list of some alternative internet browsers to supplement or replace using Google Chrome and other popular browsing software.



**Bromite** A Chromium browser with native ad blocking, removed click tracking, and gateway attack blocking.

**SnowHaze** An iOS browser with encrypted connections, native ad blocking, and tracker blockers.

**Ungoogled Chromium** A Chromium fork that, unlike other forks with modified versions, acts as a drop-in replacement for Chromium.

**Tor** A decentralized, privacy-focused browser that isolates browsing data from each site a user visits to prevent tracking.

## VPNs and Orbot

Browsing the internet with a VPN helps obscure an individual's online footprint. VPNs encrypt browsing data and hide IP addresses by redirecting network activity to different servers. VPNs can be used on both mobile and desktop devices, and miners should use VPNs for any online activity, from posting on social media accounts to using a mining pool app.

Choosing the right VPN should not be a random decision because not all VPNs are engineered equally. Some VPNs collect user data, which compromises privacy. Some VPNs accept subscription payments in Bitcoin, Monero and a variety of other cryptocurrencies, however, as an added user privacy measure.

Some VPN alternatives are designed to be trust-minimized proxies that users can be sure are not keeping logs of personal data or browsing activity. Orbot, for example, is an internet proxy that routes user traffic through the Tor network and offers a built-in VPN feature that cannot be blocked as easily as other VPNs. Unlike other VPN apps, Orbot doesn't render any advertisements in its interface. Orbot is slower than other alternatives though due to its privacy features.

# Part 5: Other Privacy Resources

Operational security does not exist in a vacuum, which makes holistic security and privacy beneficial for any particular application of these practices (e.g. bitcoin mining). This section offers a short list of additional products and services that miners may find useful for enhanced privacy and security in mining-related activities and beyond.

***andOTP*** - An app for two factor authentication (2FA). andOTP generates Time-based One Time Passwords (TOTP) from QR codes. Read more

***Aegis Authenticator*** - A secure, free and open source 2FA app for Android. Read more

***Azteco*** - Buy bitcoin vouchers without KYC from a local distributor. Read more

***Bisq*** - A P2P platform for buying or selling bitcoin privately. Bisq requires no identity verification or KYC information from its users. There is no KYC centralized database; however, some payment methods will require a user to share some information with their trade counterparty. Read more

***Briar messenger*** - Unlike traditional messaging apps, Briar is a peer-to-peer encrypted messenger with no central server to relay info or store users' messages. Messages are stored on the devices of the sender and receiver only. Briar uses the Tor network to send and receive messages and all communications are free of metadata. Read more

***Threema*** - A secure and open source end-to-end encrypted (E2EE) messaging app that also enables voice calls. Users do need to pay a small one-time fee (~$5 USD), but the payments can be made with bitcoin, no identifying information is collected, and instead of a phone number, each user receives a unique Threema ID. Plus there is a desktop extension that runs off of the users phone if wanted. Read more

***Clipboard Cleaner*** - An app for emptying Android clipboards. Any Android app can access a user's clipboard contents. This app clears clipboards to remove all information, including sensitive data like copied Bitcoin addresses. Read more

***Cryptpad*** - A private alternative to Microsoft Office and Google Drive. Cryptpad is a browser-based word processing and file creation service with client-side encryption, meaning the server doesn't know the contents of a user's files. Users can chat and edit documents together, take private notes, create passwords for files and control access permissions before sharing with other users. Read more

***Jitsi*** - An encrypted conferencing app. Jitsi is an open-source platform for audio and video calls that's available for iOS and Android mobile devices and desktop computers. Read more

***CalyxOS and GrapheneOS*** - Private Android mobile operating systems that prioritize security and privacy. CalyxOS offers a firewall that allows users to control network access on a per app basis. It also offers a built-in VPN, encrypted calls and messages, Tor browsing and more. CalyxOS also offers an option to enable microG, which replaces some functions of Google Play Services while maintaining more anonymity and privacy. GrapheneOS does not include any Google replacements (microG). Read more: CalyxOS, GrapheneOS

***Samourai Wallet*** - Available on Android, Samourai Wallet features a CoinJoin implementation called Whirlpool that breaks deterministic links to prior on-chain activity. Additionally, there are a variety of post-mix spending tools to help the user maintain anonymity. All communications in Samourai Wallet are carried out over Tor and the mobile wallet can be connected to the user's own RoninDojo full node. Read more

***Searx* -** An internet metasearch engine which aggregates results from more than 70 search services. Users are neither tracked nor profiled. Searx can also be used over Tor.

***Sparrow Wallet* -** A desktop Bitcoin wallet that is free and open source. Sparrow Wallet features an intuitive user interface and is easy for beginners to start understanding the basics but also has many advanced features for more technical users. Sparrow Wallet also implemented Whirlpool CoinJoin. *Read more*

***Standard Notes* -** A simple mobile and desktop encrypted note taking application. Standard Notes users can manually download a backup of their files and other data or enable automatic backups by having files sent to an email inbox daily or through real-time backups synced to your Dropbox or Google Drive folders. *Read more*

***Tutanota* -** An ad-free, encrypted and open-source email service. Users can register for an email account without providing personal information, including a phone number. *Read more*

***YunoHost* -** A platform for self-hosted email and web domains. YunoHost simplifies self-hosting by allowing users to manage their own internet server through the service's web interface. Users can deploy apps, self-host email, send messages and manage domain names. *Read more*

COMPASS
MINING