Casa

A beginner's guide to bitcoin security

Brought to you by Casa, the safest way to store your bitcoin.

https://casa.io

But first, who are we?

We're the Casa team.

We're a distributed team building tools to improve your security and privacy.

There's a lot to learn when you're just getting started down the bitcoin rabbit hole, and security is an important part.

Securing bitcoin is different from any other asset because your wealth is protected with a private key.

You may have heard of the expression "not your keys, not your coins." If your bitcoin is in your exchange account, for example, you don't really own your bitcoin because the exchange has the private key. If something bad happens to the exchange, your bitcoin could be gone forever.

Casa is the world's first personal key manager. We provide a simple, secure way for you to hold your own keys with the peace of mind that your bitcoin is safe. Unlike exchanges or custodians, we give you direct control over your bitcoin keys, making you the true (and only) owner of your bitcoin.

Here's how we do it...

Casa multisig (short for multi-signature) protects your bitcoin with multiple keys, so losing one key doesn't mean losing funds.

Multisig wallets ensure that if anything ever happens to one of your keys, your bitcoin is safe, because you still have remaining keys to move your funds. Plus, Casa holds one key, so if another key is lost or compromised, we can help you recover your bitcoin to a fresh keyset.

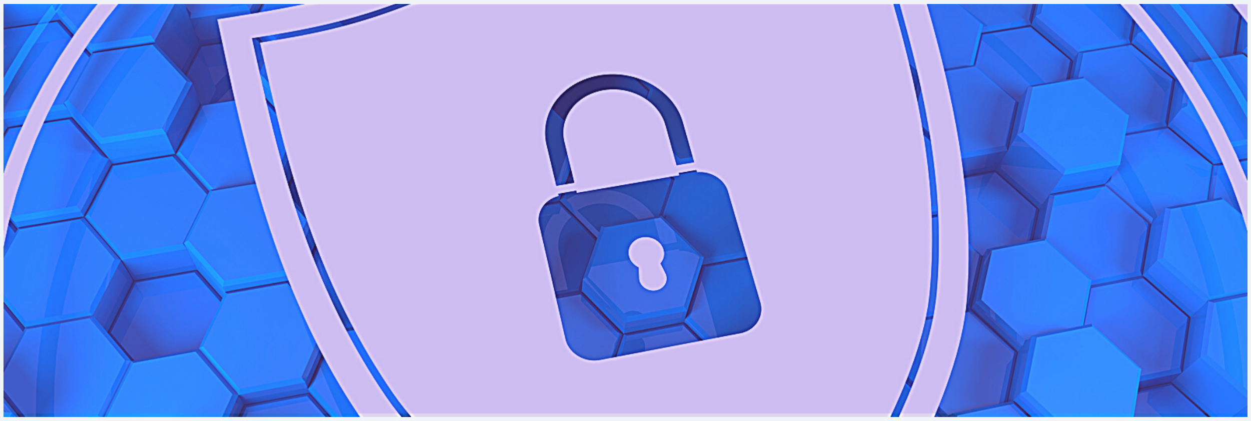
Casa is a non-custodial wallet, which means we're never in control of your bitcoin. We practice self-custody, where you hold most of your keys. We only hold one key, the Casa Recovery Key, as a secure backup. This allows you to distribute the risk of safeguarding your money for peace of mind.

It can be scary to secure bitcoin all on your own. That's why we support our multisig wallet with friendly, polished client service, and we're always here when you need us. With Casa by your side, you can relax knowing your bitcoin is safe and easy to manage.

Table of Contents

Multisig

It's important. We promise.



Part of our mission at Casa is to help teach people about bitcoin and why it's important. Multisig is an important concept for bitcoin security.

"Multisig" is short for multi-signature, and it means that spending money requires more than one approval, or "sign-off."

A real world example

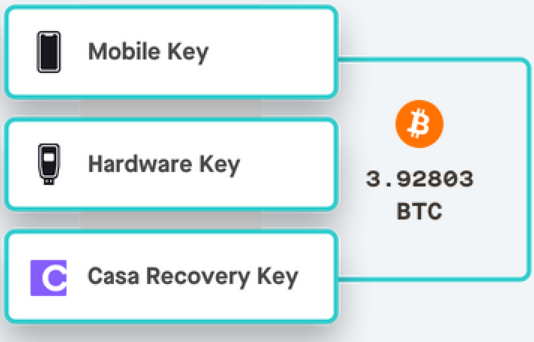
Think about when a married couple sells their house (let's just pick two random names...Bob and Alice). Assume they legally co-own the house. In order for ownership of the house to transfer to the new buyer, both Bob and Alice have to give their approval by writing their signature on separate lines of the contract. Bob couldn't just go and sell the house without telling Alice because he needs Alice's signature to complete the transaction.

Multisig in bitcoin

Imagine Bob and Alice share a credit card with their daughter, Mary. If Mary goes out and spends a bunch of money on the credit card, Bob and Alice don't find out about it until after the fact. Mary gets grounded for life, but the money is spent.

With Bitcoin, Bob and Alice have the ability to program restrictions into their money. They could utilize a multisig wallet (think wallet = spending account) to rein in Mary's out-of-control spending. With a 2-of-3 multisig wallet, the family would require any 2 out of the 3 people to approve a transaction before the money can be spent. So the next time Mary wants to buy expensive concert tickets, either Bob or Alice have to sign off too.

How Casa uses multisig



When many people think of multisig, they think of it like the scenario above, where different people manage each signature. With Casa, we've taken a slightly different approach, using multisig to add security to the bitcoin wallet of a single person or a team. Our setup options include a 2-of-3 multisig wallet (at least 2 signatures are required to spend any bitcoin), and a 3-of-5 multisig wallet (at least 3 signatures are required to spend any bitcoin). The signatures come from different devices (hardware devices such as Trezor), which are in different locations, but owned by one person or team. This provides significant security against hackers and in-person attackers who want to steal a user's cryptocurrency because a transaction must be physically approved from multiple different locations or individuals before it can be completed.

Bitcoin transactions

What makes bitcoin different? It's decentralized.

When you use Venmo, all of your transactions go through Venmo's servers, and they have the ability to block, reverse, stall, or even accidentally lose a transaction. Venmo is the single entity responsible for processing your transaction—this system is centralized.

On the other hand, the process of sending a bitcoin transaction was specifically engineered to be trustless, immutable, and censorship resistant. It takes a smart combination of social and technical engineering to create bitcoin's trustless transactions, which is why it's an important concept to grasp before moving on to more complicated concepts in crypto.

At a high level, bitcoin transactions can be broken down into three parts:

1. Creating a transaction and sending it to the bitcoin network
2. Mining blocks of transactions (which creates the blockchain)
3. Validating transactions

Each of these parts is handled by a different party with different incentives:

1. Users (creating and sending transactions)
2. Miners (mining transaction blocks to build the blockchain)
3. Nodes (validating the blockchain)

All of these entities work separately, making the bitcoin network decentralized.

Sending a transaction

In the “normal” (fiat) financial system, when I send a payment, I am sending the transaction details to a bank or credit card processor and asking them to approve it.

In bitcoin, instead of sending the transaction to one entity, I broadcast a transaction to the global bitcoin network. It then goes to a pool of “unconfirmed transactions” that are waiting to be processed. This pool is visible to all miners and validators (aka “nodes”) on the network. My transaction is in limbo at this point, and you have not received the payment.

Mining the transaction

At the most basic level, “miners” are individuals and groups racing each other to create blocks on the blockchain. Their computers run a single calculation (essentially a random number calculator) repeatedly, changing one variable each time to get different outcomes. Eventually it results in a number that is sufficient to fulfill the bitcoin protocol’s requirements.

The first miner to calculate a correct number “mines” that block. That miner then proposes their block, which includes now-confirmed transactions, to the nodes on the network.

Since miners are all competing to win the next block reward, and the calculation is random, no one knows who will add the next block of transactions to the chain. This results in a critical benefit of using bitcoin—it’s nearly impossible for an outside party to control which transactions are processed. In a centralized monetary system, a user could be completely locked out of transferring money by one entity (e.g. Venmo decides you can’t use their app anymore). But in a decentralized system like bitcoin, there is no one party to control, bribe, or threaten in an attempt to affect transactions. This is why bitcoin is said to be highly censorship resistant.

Verifying the transaction

After a miner proposes a new block, the nodes in the network verify that block. A node can actually be run by anyone—it’s just a program that runs on regular laptop or desktop computers that many people have at home.

The nodes have a record of all pending and historical transactions in the chain, so they know if the transactions in the newly proposed block are valid. For example, if I’m sending you 1 BTC, the nodes know whether or not I actually had 1 BTC in my account, because they previously validated a transaction in which someone else sent that 1 BTC to me, and so on.

If the nodes accept the proposed block as true, the miner receives a reward of newly minted bitcoin, plus transaction fees from all the transactions included in the block. A miner could try to cheat and pass a false block, in which they give themselves a bunch of bitcoin they don't own. If this happens, the nodes can reject the block, and the miner loses out on the block reward.

Assume the newly validated block contains my payment to you. Once it's been verified by a sufficient number of nodes, it's considered completed, and you receive the payment. Blocks are continually added by miners and verified by nodes, creating a long chain of transaction records, which is why it's called the "blockchain."

Why it works—incentivization

There's some incredibly interesting game theory involved in making the bitcoin network run correctly. Everyone who participates in the network is incentivized to act in their own self-interest, yet the result is a huge amount of people working together to maintain an immutable public ledger of transactions. Let's run through the various incentives driving each party.

Users

This one is pretty straightforward—users want a safe, reliable way to make transactions and store value. If a blockchain network like bitcoin fails to provide the benefits users want, they will vote with their feet and move on to using a different network. This hurts the network as a whole—there is less liquidity for other users, the value of a bitcoin decreases, which hurts miners' profitability, etc, so network stakeholders should all be working to keep users happy over the long term.

Miners

Instead of Venmo recording transactions to its servers, miners record transactions to the blockchain. They don't do this out of the goodness of their own heart—they do it to make a profit off of block rewards and transaction fees. A block is mined about every ten minutes. There's a lot of money to be made mining BTC—if you can win the race.

While the miners work to calculate the next block, their computers are using lots of electricity, which gets very expensive. This computation cost is what helps secure the blockchain, and the overall arrangement is known as Proof of Work.

See, the problem with a decentralized network where everyone acts in their own self interest is people will inevitably try to cheat the system to increase their profits. As we learned earlier, nodes will reject a proposed block if miners blatantly include transactions that don't match the public balances from previous blocks. However, what if a miner went back and recalculated enough historical blocks to completely rewrite the ledger, thereby tricking nodes into believing their false blocks?

This is where Proof of Work comes to save the day. The nodes on the network will always accept the chain with the most cumulative Proof of Work as the true state of the public ledger. While the cheating miner is going back to recalculate and falsify old blocks, the rest of the miners are still racing forward, creating blocks on the legitimate chain, thereby adding more "work done" to that chain. The cheater would have to spend a massive amount of money on recomputing blocks to catch up and surpass the chain with the most work done. This makes it more profitable for miners to act honestly and simply try to find the next block than to cheat and steal from the network.

Nodes

Nodes have an interesting set of incentives in the bitcoin network. Node operators are not directly rewarded for their services, yet they are crucial to keeping the other actors in the network honest. The more nodes exist, the more decentralized and immutable the network becomes.

Each node has a copy of the entire blockchain ledger, meaning you can't just hack one server and change account balances around in your own favor—you would have to hack thousands of computers around the world all at once. More nodes makes the network safer to store value in because you don't have to worry about your bitcoin suddenly disappearing one day.

This is the indirect incentive for people to run validating nodes: as the network becomes safer, more people are willing to buy bitcoin for storing value or transacting. As more people buy bitcoin, the price increases. Node operators likely hold bitcoin, so over the long term, their investment should increase with the safety of the network.

Bringing it all back together

We highlighted three terms in our opening paragraphs: trustless, immutable, and censorship resistant. These three qualities make bitcoin valuable, and the bitcoin protocol was explicitly engineered to maximize them.

- Transactions are trustless because everyone acts in their own self-interest, yet this results in a thriving network and true historical record of value transfer.
- The blockchain ledger is immutable because of the computational costs it would require to rewrite it and the near impossibility of hacking every node in the world to change it.
- Bitcoin is censorship resistant because no one knows who will process the next batch of transactions, therefore it’s very difficult to control which transactions are completed.

So that’s how bitcoin transactions work, and it’s what makes bitcoin valuable to so many people.

Where are my bitcoin stored?

What's in your bitcoin wallet? If you said "bitcoins," you're wrong.

Bitcoins are simply entries in a publicly viewable database: the blockchain.

Since the blockchain is available online for all to see, you, as a bitcoin owner, don't actually "hold" bitcoin in your wallet. You hold something even more important: private keys.

A bitcoin private key is like a secret passcode that's needed to transfer ownership of bitcoins on the blockchain. With private keys, you have the power to alter the blockchain record by authorizing an ownership transfer from one bitcoin address to another. That transaction gets recorded in the blockchain.

To go a level deeper, bitcoins are, at their root, numbers; monetary amounts that are assigned to bitcoin addresses. For every private key, there is a public key (translated to a "bitcoin address" or a "deposit address").

The private key belonging to that corresponding public key is the secret code needed to "spend" bitcoin.

So my bitcoin wallet just holds private keys — no bitcoins?

That's right — you're holding the private keys needed to move the bitcoin you own on the blockchain.

You can think of your bitcoin wallet like a password manager (which everyone should be using!). Password managers store and secure the secret passwords you need to access websites, rather than the content of the websites themselves.

In this way, your bitcoin wallet is essentially a key manager.

Private keys empower you to take full control over the bitcoin you own

Part of the beauty and elegance of the bitcoin network is that it allows one to have total sovereign control over a digital monetary asset — a simple but powerful tool of self-empowerment.

With that power comes the responsibility of keeping those private keys secure. If an attacker is able to obtain your private key, they can claim ownership of the bitcoin. Likewise, if the private key to a bitcoin address is lost, the bitcoins will not be able to move on the blockchain at all.

There is no password reset button you can press in bitcoin.

Private keys seem important...

They are. Anyone who holds the private key to a bitcoin address can spend that bitcoin. Because of this, it's vitally important that not only are your keys secure, but that you have full control over those keys.

With centralized entities (like bitcoin exchanges), you're trusting someone else to keep your private keys secure and give you access to those keys when you request it. Unfortunately, third-party custodians have been notoriously poor keepers of private keys.

Maximum security, minimal risk

For greatest security and resilience, you can generate multiple private keys, with a customizable quorum of keys needed to spend funds. This type of wallet is called a multisignature (or "multisig" for short) wallet.

Multisig allows you to create, as an example, 5 private keys to a bitcoin wallet, with at least 3 keys needed in order to move funds on the blockchain. To picture this, imagine a safe with 5 keyholes. If there are at least 3 keys in any of the 3 keyholes, the safe can be opened.

Multisig offers the greatest resilience against both theft and user error. In such a setup, 2 keys could be compromised, and the attacker would not be able to move the bitcoin. Likewise, you can lose up to 2 keys, and still be able to access funds using your remaining 3 keys.

Storing your bitcoin

The main types of storage and the pros and cons of each.

Before we discuss each storage method, it’s important to understand the concepts of public keys and private keys.

Similarly to how many store cash, your bitcoin is stored in a digital “wallet.” These wallets contain a public key for receiving funds and a private key for spending funds—you’ll often hear them referred to as a key pair. Each key is represented by a long, cryptographically generated sequence of numbers and letters.

You can think of a public key as similar to a bank account number, and a private key like the PIN for that bank account.

For any given transaction, the public key generates an address for a recipient. Each new transaction will create a unique public key, and there’s no need to remember it in order to use it because it can simply be scanned or copied and pasted.

The private key acts like a password and allows someone access to transfer or spend their currency. Due to the cryptography used in key generation, it is not possible to reverse engineer a public key to ascertain a private key. However, anyone who knows your private key has access to your funds; therefore, the security of your funds is only as strong as the protection of your private keys. The harder it is for anyone but you to obtain your private keys, the more secure the storage.

The main differences between storage types, discussed below, are usability and security—most notably in how private keys are stored.

Storage

Now that we've got a basic understanding of how public and private keys work, let's dive into the methods for bitcoin safekeeping. There are two primary types of storage: hot and cold. Hot storage is generally considered easier to use, but far less secure because it relies upon a device that is connected to the internet. This makes hot storage more vulnerable to hackers and malware. Cold storage does not use a connection to the internet, and is thus considered the safer of the two.

Among hot and cold storage, the three most prominent classifications are: software, hardware, and paper.

Software

Software storage can be divided into three sub-categories: Desktop, Mobile, and Web.

Desktop

This type of storage can be installed on your computer. Once installed, your funds are only accessible from that single device. This means you can't borrow a friend's computer to access your own desktop device. Private keys are stored on the computer's hard drive.

Pros	Cons
• Ease of access • Generally simplistic UX/UI	• If someone gains access to your device (whether directly or via exploitation), your funds are compromised. • If your device breaks or you otherwise lose access to it, you may lose all of your funds.

Mobile

This type runs on an app on your phone and is available on most operating systems. As with desktop storage, private keys are stored directly on your mobile device.

Pros	Cons
• Accessible anywhere your phone is • Generally simplistic UX/UI • Easy to update software	• Similar to desktop wallets, if your device is somehow lost, damaged, or otherwise compromised, so are your funds* • If an app doesn't store your private key in phone's secure element, your key could be exposed to the internet.

*You should keep a paper backup and a secure PIN to prevent unauthorized access in the event that your mobile device is lost.

Web

Web storage is often run on the cloud and managed via web browser or browser extension. This makes it accessible from any computing device and at any location, provided there is an internet connection. However, web wallets are generally more of a black box than other types. Many are custodial and managed by a third party, so you can't be sure of what goes on behind the scenes.

Pros	Cons
• Universal access • Minimal learning curve	• Service is controlled by a third party. As such, of the three types of software wallets, web wallets are the most susceptible to theft.

Paper

At the opposite end of the hot and cold spectrum lies paper storage— which is, quite literally, paper. Keeping paper storage means printing out both your private and public keys onto a piece of paper, which should then be kept in a safe or other very secure place. Paper storage should not be confused with a paper backup, which is a means of recovery for all storage types.

Pros	Cons
• Easy to carry with you • Easy to make and receive payments without relying upon a charged battery or wifi connection	• Without proper precautions in place, paper wallets are highly susceptible to theft, damage, and loss. • Not conducive to making frequent transactions.

Hardware

Hardware storage is a physical device that generates and holds your private keys offline. To make a transaction, users connect their hardware device to any computer with internet access, enter a security PIN, and confirm.

Pros	Cons
• Can support multiple accounts, addresses, and coin types • Can be backed up for restoration, should the device break or become lost • Small and easy to carry or hide	• Susceptible to damage and loss • Requires users to trust that a device manufacturer has not installed any back doors on a device*

*You should not trust pre-owned hardware storage, as previous users may have tampered with it in some fashion. Although many devices are open source (and thus do not require you to trust a manufacturer), some are not.

Well? Which should I use?

The answer is different for every person, and really depends on the trade-offs you want to make. What's more certain, however, is that the more you rely upon a third party for management of your private keys, the more security risks you take on. Cold storage offers the greatest opportunity for management of your own keys. The catch is that you take on the added responsibility of understanding the security risks associated with self-management of keys. On the other hand, hot storage solutions may force you to sacrifice some degree of control of your private keys in exchange for less personal responsibility.

- For a casual bitcoin user with small investments and high risk-tolerance, desktop or mobile storage will probably suffice.
- As your bitcoin holdings increase, you should look to more secure solutions like hardware storage (we specifically recommend Ledger or Trezor).
- The plainness of paper storage may be alluring, but we recommend against it because it is highly prone to damage, loss, and hacking during the process of importing private keys.
- For the greatest of security needs, Casa's multi-signature, multi-location, multi-device key management solution gives you ultimate control of your keys, and a world-class support system to back you up.

At the end of the day, it's a matter of preference. The solution you choose should reflect your specific needs, but the bottom line is this: the greater control over your keys you have, the better.

Should you trust a third party for bitcoin security?

Here’s a quick overview of third parties and how to best protect your money.

Can you count on someone else to keep your bitcoin safe? That’s the million-satoshi question.

In a world where we’re used to banks securing our money, assuming total custody over your wealth can seem intimidating. Many bitcoiners wonder if they’re better off letting someone else secure their bitcoin, such as a custodian or exchange, but this is often riskier than it appears.

What’s a third party?

In finance, third parties are organizations who facilitate transactions in some way, such as processing payments, brokering deals, or protecting assets.

The most common example of a third party is a bank. When you earn money, you usually don’t spend it right away, so you might deposit it into a bank account for safekeeping. Then when it’s time to spend money, you could use a credit card, which is a service from another third party.

Even when you choose to transact in cash, you’re still dealing with a third party because cash is generally produced and monitored by central banks. Third parties are everywhere in the legacy financial system.

Third party risk: Closer than it appears

People trust third parties because third parties appear to be safer. For instance, if you’re carrying around a lot of cash, you could lose your wallet or get robbed at any time, in which case a bank account may seem more secure.

But in reality, third parties actually present a different set of risks. Banks store a lot of money, which makes them a frequent target of robberies. The U.S. experienced more than 1,700 bank robberies in 2020 alone, according to the FBI.

There's also systemic risks to consider. Banks make money by lending it out and taking on investment risk. If account holders go to withdraw their money all at once — as often happens in an economic crisis — it's possible the bank won't have it on hand, due to fractional reserve policies. And third parties can go bankrupt, too. More than 500 banks have failed in the U.S. since 2000.

So, third parties come with some risk. Most of us are just not used to thinking about it.

Bitcoin: Money without third parties

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"

Bitcoin is a totally different kind of money. It lets you transact peer-to-peer without having to rely on a third party, such as a bank, government, or credit card company. This independence is part of what makes bitcoin special — you don't have to trust a third party. You can be your own bank.

Owning bitcoin, however, comes with a challenge: protecting your money is up to you. It's a double-edged sword at first. If you assume custody over your bitcoin, you become responsible for protecting your bitcoin from hackers, burglars, accidents, and any number of disaster scenarios. On the other hand, if you leave your bitcoin with a custodian or exchange, there's no guarantee they will keep it safe either.

In fact, custodians and exchanges have been notoriously bad at keeping bitcoin safe. All of the following have happened in bitcoin's history:

- Exchanges have been hacked
- Governments have seized assets from exchanges
- Accounts have been compromised
- Exchanges have folded

The answer to these security challenges is simple — don't trust third parties. Instead, practice self-reliance and take custody of your bitcoin, beginning with your own private keys.

The dos and don'ts of bitcoin key management

The internet is a dangerous place, but we have the tools to protect ourselves.

Bitcoin provides users with an incredibly high level of sovereignty over their money. The phrase "be your own bank" does a good job describing the power that bitcoin enables its users to wield. The flip side is that being your own bank comes with a lot of responsibility. The same features that make bitcoin so valuable (permissionlessness, censorship resistance, seizure resistance, etc.) also make it attractive to malicious actors. These malicious actors have come up with a wide variety of traps to fool bitcoin users into parting with their money, making bitcoin more challenging to use safely.

Do take control

If you don't take possession of your own private keys, there's no way for you to truly know if they are secure. Any trusted third party such as an exchange is a black box to you.

When you entrust your keys to someone else, you might feel like you're ridding yourself of the risks that come with securing private keys. This is not the case — all of those threats still exist, but now you no longer have control over putting measures in place to stop them. Furthermore, your threat model actually expands because now there are additional risks to your money:

- Collusion against you by the custodian
- Internal attacks within the custodial organization
- External attacks incentivized by the custodian holding funds of many people

The following tips on this topic may feel daunting, but knowledge is power!

Do protect yourself

Practice strong cyber hygiene on all your online accounts. Assume that your usernames and passwords to every service will get leaked. Use a password manager (preferably one secured by hardware second factor authentication [2FA] such as a Yubikey), to generate unique passwords for every service. Similarly, add 2FA to every online account that supports it, preferably hardware-based 2FA. If a service only supports TOTP, then you can secure those secrets on hardware (a Yubikey) via Yubico Authenticator.

Understand the trade-offs between convenience and security when it comes to your private keys. A single-signature hot wallet on your phone is great for "carrying around" spending money but should not be used to store your life savings. On the other hand, a geographically-distributed multisig setup should be inconvenient enough to access that you only spend from it on a monthly or yearly basis.

Use dedicated hardware devices to store your private keys. Verify send addresses on dedicated hardware devices; don't trust addresses displayed in browsers or desktop software.

Be sure to check the entire destination address when sending, not just the first few characters. There are many types of malware that will try to swap out your intended address for a similar-looking one owned by the malware authors.

Develop a solid plan for how to recover from disaster scenarios. This may involve a seed phrase backup scheme for which there are a variety of cold-storage guides. We're not a fan of users having to manage seed phrase data.

If you choose to store your seed phrase backups on metal devices, make sure you buy one that has been stress tested and shown to survive extreme environments.

Verify that the software you install is authentic and not a malicious lookalike. Unfortunately, verifiability is different for every platform. For desktop software, you can verify GPG signatures if you're comfortable with command line use. Mobile apps are generally cryptographically signed, but that signature is only verified by the app store. To prevent installing an imposter mobile app, go to the web site of the company and click on a link to install the mobile app from their site.

Don't get phished

Don't type your seed phrase into any computer that is connected to the internet! Especially not into a web browser! Now that many bitcoin users are protecting their keys with dedicated hardware devices, we're seeing attackers go after the biggest remaining weakness: the human operator.

Typosquatting is a lesser-known attack vector where malicious actors will buy domains that are close misspellings of common bitcoin web services. You should only visit financial websites via bookmarks to ensure that you don't accidentally end up on a typosquatter's malicious site.

Similar to typosquatting is an issue where malicious sites pay for search engine advertisements, thus bumping up their sites before the normal search results. This is another reason to bookmark the sites you use rather than using a search engine to visit them; you might accidentally click on a malicious link.

Don't install malware

Avoid installing many browser extensions; they can easily be malicious and see all of your browsing activity.

Don't use wallets that are browser extensions; they may be outright scams.

Don't run software wallets on a desktop machine that has lots of other software installed. You increase the risk of other software being compromised via dependency injection that will install clipboard malware and trojans that scan your computer for private keys.

Don't fall victim to ransomware that hijacks your hard drive. Only install authentic software and make sure you back up your hard drive regularly so that you can recover data in the event that you lose access to your data.

Don't use web-based QR code generators — especially not "bitcoin QR code generators" — since they may replace your address with their own.

Do verify the authenticity of any software you install, if at all possible. This means checking file hashes and GPG signatures on any binaries that you download. Do not install software to hold your private keys if you can't verify what it's doing. This includes things like running AWS images that are maintained by third parties.

Don't create technical weaknesses

Most users should not store private key backups digitally; especially not in an online service. While it is possible to create secure digital backups, you need to be an advanced user in order to so safely.

We recommend against using browser-based wallets, even if it's just a browser interface to a hardware wallet; the attack surface for browsers is huge.

Similarly, if you're using Tor browser to access a web service that displays bitcoin addresses for deposits, you should be aware that malicious Tor relays could swap out addresses for their own.

Don't use brain wallets — humans are terrible at generating entropy! If you send funds to a brain wallet composed of common English words, it will likely be stolen in seconds.

Don't manually split up your seed phrases; it drastically reduces their security against being brute forced.

Don't get creative and try to obfuscate your seed backups. You'll likely degrade the security and run the risk of data loss.

Along a similar vein, don't bother randomizing your backed-up seed phrases; depending upon the seed phrase length it would be trivial to detect and brute force given that seed phrases have built-in checksums. For example, a 12-word phrase only has 500 million combinations, of which perhaps 50,000 would be valid; a sophisticated attacker would be able to check them all for funds in a matter of minutes.

Don't use paper wallets. They're very hard to use securely and it's easy to accidentally lose funds if you don't understand all the risks.

One common theme we've seen with new Casa clients is that they have split up their funds across a variety of single-signature hardware devices or paper wallets. While this does decrease your risk of catastrophic loss, it actually increases your risk of partial loss. Don't believe that distributing your keys across many single points of failure is safe.

Don't get scammed

Don't believe scareware/blackmail messages, even if they include your username and password to various services — those are taken from database leaks that get sold on the dark web. At time of writing, the latest variant of these are "sextortion scams" that will claim that they installed malware on your computer and recorded embarrassing images of you.

Steer clear of "bitcoin doubling" scams. Nobody is going to take your bitcoin and then give even more back to you for the pleasure of holding onto your money for a matter of minutes. The time value of money simply isn't that high.

Don't try to collect airdrops; they may be fake. Some may try to phish for your credentials to online wallets/services. More sophisticated scams will be malware wallets that steal your bitcoin. The only safe way to collect airdropped forkcoins from a wallet is after you have moved your bitcoin to a completely new wallet.

Avoid the temptation to send bitcoin to mixer websites; most are scams. Mixing can only be done safely by running your own mixing software so that you retain control of your private keys. JoinMarket, Wasabi, and Whirlpool are several such examples.

Don't invest in Initial Coin Offerings without performing plenty of due diligence. Many ICOs are fraudulent.

Similarly, don't fall victim to greed and participate in "pump-and-dump" groups. The most likely outcome of such activity will be that a few insiders end up profiting and you end up losing your money.

Don't buy hardware wallets from resellers. Similarly, don't initialize hardware wallets with seed phrases supplied to you by a third party.

Don't get hacked

Don't install remote-access software like Teamviewer on any of your computers.

Don't be a target

Don't make yourself a target by talking or posting about your bitcoin.

Along the same vein of phone security, avoid connecting your phone number to any online accounts; an attacker could SIM swap your phone number and use it to break into those accounts via password resets.

Bitcoin security tips to help you while traveling

Bitcoin travel requires a little extra precaution.

Cryptocurrency events are a great opportunity to learn more about bitcoin and make industry connections. If you own bitcoin, however, it’s important to be mindful of your surroundings and take proactive steps to protect yourself and your wealth.

As we often say, there are no vacations in security. Bitcoin travel requires a little extra precaution.

Travel hubs

Getting to the destination safely is the part of your trip where some quick preparation can help you avoid bitcoin security issues.

Power down your electronic devices fully before going through the security checkpoint. Once a device is outside of your control, anyone can do anything with it. It is much harder to unlock and decrypt a computing device when it is in a powered-off state versus a powered-on state where the device was previously unlocked (PIN code, biometrics). It is generally safer to turn on devices once passengers have boarded the plane and the plane doors have been locked. The risk of device seizure is much lower once a plane is boarded and moving.

Never take the majority of your Casa keyset with you. Your keyset is designed for geographical distribution and security. If you need to transact in bitcoin at the conference, it is better to use the mobile single key wallet with a limited amount of funds. Having a majority of keys in your possession makes YOU the single point of failure and puts your funds at risk.

Don’t advertise the goods. The first layer of security is privacy, and privacy is about flying under the radar. Every time I am in a travel hub, I take note of who is wearing a cryptocurrency shirt or who has a bitcoin sticker on the lid of their laptop. Criminals and thieves take note of this as well. Don’t broadcast to everyone you’re traveling with bitcoin.

Always use a VPN when on a shared network, including hotels, airports, and individual rental locations. Public networks are often unencrypted, which can put your transmitted data at risk.

Only use your own device power chargers and cables. Attackers have been known to set up impromptu “charging stations” in travel hubs in the hopes that someone with an unpatched device will connect to it for charging purposes. Your device may charge, but it will also now be infected by a process known as juice jacking.

Lodging and accommodations

Hotel safes are not to be trusted for keeping bitcoin and high-value items safe. These safes are easily accessible to hotel staff and cleaning services using bypass codes. These safes are even more easily accessible to attacks using things such as a room key, screwdriver, or ball-point pen cap. When in doubt, don’t bring high-value items with you.

Some hotels and suites have a double door connecting rooms or bathrooms directly. If your room has a double access door, ensure it is locked from your side. You can move or brace a piece of furniture against the door to stop an inquiring neighbor.

Consider using a portable, non-intrusive door brace or deadbolt strap for your hotel door. These devices can vary in effectiveness, ease of use, and known flaws, but they can help prevent an unwanted visitor from gaining entry while you are in your room.

Lodging through vacation rental websites can be great for cost but not as much for security. These accommodations are offered by individual owners rather than a company, and they may not have the same level of physical and network security controls as a hotel. Your personal property may not be protected or covered by insurance in the instance of a break-in or robbery.

At times, it can be dangerous to use your real name everywhere, especially if you're well-known. We live in an age where bad actors can search your name online and instantly find out who you are. When ordering delivery, food, or car rental services, use only a first or fake name if possible. If you decide to do this, make sure the hotel and clerk know as well, otherwise your pizza delivery for "Satoshi Nakamoto" may go to the wrong person.

If you are using rideshare transportation, ensure the driver is who they say they are and work for the company they are representing. This does not need to be a full-blown interrogation but more of a verification ("Are you Kevin with Uber? Oh, your name is Pete. My mistake, my app does show that.") Simple checks like this can work well as a false pretext verification.

Before the event

Consider using the buddy system. Physical attackers are more likely to target individuals traveling alone to conferences and satellite events. Traveling with a trusted companion is a smart practice for venturing into unfamiliar and potentially unsafe areas, and it has the bonus of allowing you to split transportation costs.

Ensure you have an emergency contact (or notify your Casa Emergency Contact) who knows you will be traveling to a remote location. This person does not need to know all of your whereabouts but should be aware of your general plans and location.

Update any computers, tablets, or mobile devices you may be bringing with you prior to the event. This ensures the latest security updates are applied and minimizes the risk of known attacks against the device.

At the event

Once you've checked into your event, the coast isn't necessarily clear. Malicious actors are often present at large crypto gatherings, so don't let your guard down completely.

Turn off all unneeded network communications including Bluetooth, WiFi (in certain areas), and the MacOSX/iOS Airdrop file sharing utility. This stops random connections and scanners from picking up your devices for further analysis and potential attack.

Just like when you're traveling, make sure to use your own power chargers for your mobile and computing devices. A portable battery is a great and cheap option to charge while you're on the move.

Avoid giving out your phone number to strangers. If attackers have your number, they can target you in a SIM swap, port your number to their phone, and drain financial accounts that rely on that number for two-factor authentication. If you would like to keep in touch with someone, consider using encrypted messaging apps or a “sock puppet” social media account.

Do not share any pictures of a location on social media while you are still in that location. It's better to post pictures after you have left the location, or sometime thereafter. This stops a bad actor from finding your physical location in real time. One should also be aware of what is in the background of the photograph, who is in it, and if they are okay with the picture being posted online.

Altering small things about your appearance can greatly help to obfuscate your identity. While there may be some conflicting opinions regarding wearing a mask, it’s a great excuse to hide your identity and blend into the crowd.

Be conscious of what you disclose about yourself at crypto events. As we like to say at Casa, feel free to talk about bitcoin, but don’t talk about your bitcoin. Try not to self-identify as someone who owns a lot of bitcoin. The more data points you reveal, the more of a target you become. There are some subjects that are best left untouched, such as how much bitcoin you have, when you started buying, and the exchanges you use.

Be aware of those in attendance at afterparties, bars, and shared party locations. These patrons may not be attending the conference, but they are now extremely interested in your “bitcoin citadel retirement plan” they overheard you discussing. Limiting alcohol intake will also help to keep one’s senses sharp (but make sure to still have some fun).

While most attendees should feel safe and not be targeted, “An ounce of prevention is worth a pound of cure.” Have fun at the conference and beyond!

Casa

Questions? Contact us.

https://casa.io

+1 (267) 369-0365

help@team.casa