HOW TO STORE & TRADE CRYPTO LIKE A PRO

faa.st

CONTENTS

INTRODUCTION

All cryptocurrency wallets come with a public key (or “public address”) and a private key (or “private address”). Your public key is the address you use to send/receive cryptocurrency to/from your wallet. Your *private key* however is the key to ownership and control of the cryptocurrency in that wallet.

The terms “address” and “key” can be used interchangeably, and this lends itself to a simple metaphor that will help you understand how the public and private ones differ:

Your public wallet address is like your home address. It is public information, referencing a specific place (your home), and it’s how the postal service knows where to deliver your mail.

Your private wallet key however is like the keys to your mailbox. Only you have access to it, and only you can open it. You *want* everyone to know your public address, so you can send/receive mail. But you would *never* want everyone to have copies of your private key.

If they did, they could open your mailbox and can take your mail. Similarly, when someone gets ahold of your wallet’s private keys, they can open up your wallet and take your cryptocurrency.

This is a very real risk, but it’s one that this guide will help you avoid.

WALLET EXAMPLES

The format of public and private keys will vary from one mainnet cryptocurrency to another.

With a Bitcoin wallet, for example, the public key will look like this:

1MzuwVXVnsXa5qZ2gqdUPDnLGUsUKijRWS

While the private key is longer, and will look like this:

L234skiBruPTrTVSBvGUfkH1YSWhnJ9cXFg54udd4k2YQeES174s

With an Ethereum/ERC20 token wallet, the public key will look as follows:

0x0469f7a9f791f9759d75d9b4f080257074c58338

While the private key will look like this:

0x355157ad1fb16875bd3e56f0914d67008b2698c172650a59ca605b1ac314bae3

Etc...(Note: these keys were randomly generated for the purposes of this book. Do not attempt to use them)

The #1 rule of cryptocurrency is that the private key should never be shared with anyone. Every wallet has one, whether it is a personally owned hardware wallet, or a hot wallet provided by a crypto exchange.

While it may be convenient to keep your funds on an exchange hot wallet, it comes with a risk: If someone else gains access to your wallet's private key, they can take your cryptocurrency anytime they want. This is what happened in the many thefts of crypto exchanges by hackers: the perpetrators got into the exchange customers' private keys, and began draining their wallets. Customers do not control those wallets, because they don't hold the private keys- the exchange does.

Whenever you trust someone else to take custody of your cryptocurrency (like a centralized exchange or some other service) you are trusting them to keep your private keys safe.

It's a risky assumption to make, and too many folks have learned the hard way that if you don't control your wallet's private keys, your cryptocurrency isn't really "yours".

This is why cryptocurrency pros store their keys themselves, and keep their holdings much more secure. Now you can too! It's simpler and easier than you might think.

In this guide we'll cover best practices and methods for keeping your cryptocurrency safe, and how to ensure you can regain access to your funds in case you lose access to your personal wallets.

PART 1: CRYPTOCURRENCY STORAGE BEST PRACTICES, AND KEEPING YOUR PRIVATE KEYS SAFE

1. BACK UP EVERYTHING.

This is the first and most common-sense rule of crypto safety. As with all data, the best way to avoid losing it is to create back up copies.

Save copies of your public and private keys for all your wallets, as well as seed phrases (which we'll cover in Part 2), and exchange usernames and passwords.

Store them in multiple secure electronic devices, such as thumb drives, CDs, external hard drives, or even a dedicated computer that is not connected to the internet. Consider encrypting the files afterward for an added layer of protection.

Old school, analog backups are also a good idea. Once you have saved it digitally, write the information down on paper and store it in a secure place like a safe or a safe deposit box.

If you want an actual method to follow, the **3–2–1 Backup Rule** is great for securing your sensitive crypto data. This means storing 3 different copies of your data on 2 different types of storage media, and have at least one of the copies stored off-site in a secure location.

This next part is very important: NEVER store your keys, recovery seed phrases or anything else related to your cryptocurrency holdings online in Dropbox, Evernote or anything like that. You are basically *begging* to eventually get your funds taken if you are so careless with this information.

If you must store private keys and other sensitive crypto information online, use a secure service like LastPass, and be sure to set up 2-Factor Authentication (2FA) for your account.

2) DON'T LEAVE FUNDS IN EXCHANGE HOT WALLETS INDEFINITELY; KEEP THEM IN A PERSONAL WALLET FOR LONG-TERM STORAGE.

This is one of the most important things you can do to protect your cryptocurrency holdings.

The wallets on a centralized exchange are generated for you by the exchange, and they have the private keys to those wallets. This is how they are able to freeze access to your wallets when performing system maintenance.

While having a wallet set up for you is convenient, it can be dangerous. If the exchange gets hacked, the hackers can gain access to those keys and can drain your wallets. All exchanges have cyber security measures in place, but that has not stopped hackers from getting in anyway and stealing well over $2 *billion* of cryptocurrency directly from those hot wallets to date.

Keeping your money in an exchange hot wallet is roughly analogous to walking around with thousands of dollars of cash in your pocket. Would anyone agree that this is a smart thing to do? Of course not. But millions of people essentially do the same thing every day with their cryptocurrency.

So where should you keep your crypto assets instead?

3) USE MULTIPLE HARDWARE, SOFTWARE, DESKTOP OR MOBILE WALLETS THAT YOU OWN AND CONTROL.

By keeping your funds in your own wallet, only YOU have access to the private keys.

Software wallets offer an excellent compromise between security and ease of access. Browser-based wallets like MetaMask or MyEtherWallet are very popular, and allow you to quickly access your funds from any computer (provided you have the login credentials). Always make sure the wallet app or website URL is correct (save the real URL to your bookmarks). Fake phishing apps/websites have been created by criminals to steal users' wallet info.

Hardware wallets are a form of "cold" (meaning offline) storage, and are probably the safest way to store your holdings short of engraving your keys in metal and placing it in a nuclear fallout shelter. The user experience is not quite as frictionless, but you get an added layer of security due to the fact that it remains offline unless you connect it. We recommend using either a Trezor or Ledger wallet.

There are also desktop wallet products like Exodus, or mobile wallets like EdgeWallet which allow you to store funds directly on your phone or home computer. The same principles described above for storing private keys and login information would apply to these wallets as well.

4) SPREAD THE WEALTH AROUND!

It's best not to keep all or even most of your funds in only one wallet. Set up multiple wallets, some that you use for long term HODLing, and others for smaller, more frequent transactions. Spread your assets around to avoid having a single failure point.

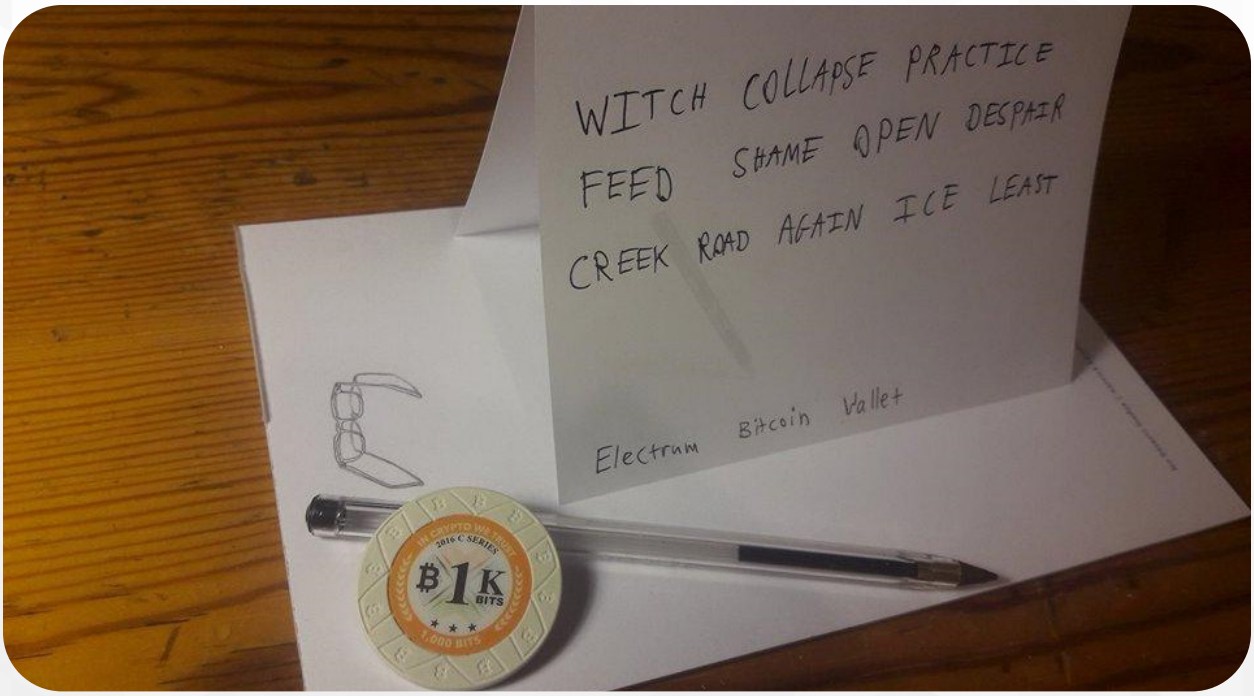
PART 2: PROTECTING YOUR CRYPTO RECOVERY SEED PHRASES

One of the most important features of cryptocurrency is recovery seed phrases. Knowing how to protect your recovery seeds is an essential skill for anyone who wants to trade and hodl crypto. Here's how to do it right.

WHAT'S A RECOVERY SEED?

Recovery seeds are known by many names. They are also called a "recovery keys", "backup seed" or, "crypto seed" or "keystore phrase", and these terms can all be used interchangeably. Whatever you choose to call them, they all serve the same purpose: **they provide a safe and secure way to regain access to your funds should you ever lose access to your wallet.**

A recovery seed is typically a series of random words that must be entered in the right order to access the wallet it corresponds with. Here is an example of recovery seed for a bitcoin wallet, written down on paper:



Example recovery seed. (source: en.bitcoin.it)

The number of words in a recovery seed will vary depending on the type of wallet. A BTC wallet like the one pictured above will have 12 words. Some hardware wallets like those made by Trezor or Ledger have 24 word recovery seeds.

Sometimes a recovery seed can be paired with one extra word that acts as a "password" for an additional layer of security. So a 12 word seed would not work until the 13th word had been added, and the 24 word phrase one would not work unless you also enter the 25th word.

HOW TO STORE YOUR RECOVERY SEEDS SAFELY

As with your keys and passwords, a combination of physical and digital backups for your recovery seeds is a good option.

For physical options, the simplest way is to just write down your recovery seeds on paper, and store them in a secure location like a lockbox or safe deposit box at a bank. You can also get your recovery seed engraved in steel cards, which are obviously more durable than paper.

For digital backups, use external hard drives and thumb drives to store your recovery seeds in Word docs. They should be kept offline and preferably used only for this purpose. You might want to consider encrypting them. If you go with a hard drive, go with a solid-state design since they are more durable.

One thing to keep in mind is that hard drives and thumb drives are typically only good for about 5-10 years. So while they are a perfectly good short to medium-term option for backing up recovery seeds, they should not be your only option.

Another popular option is to simply keep an extra computer which is solely used for storing sensitive data like recovery seeds. This computer should be kept offline at all times to eliminate the risk of cyber theft.

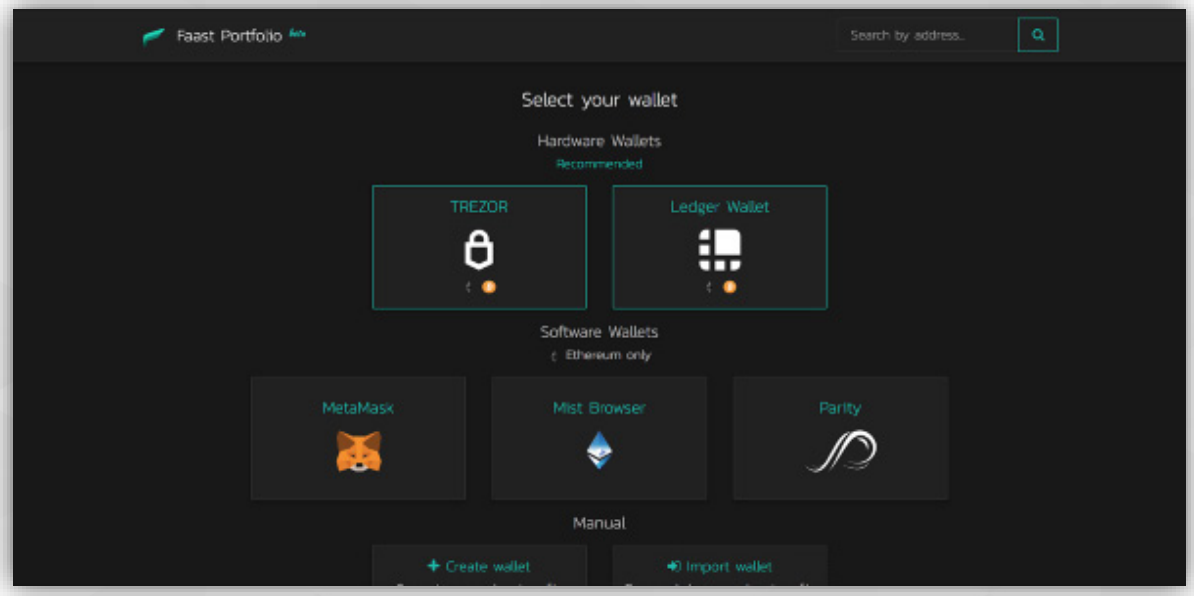
No matter what you choose, you should be regularly backing up the files onto new devices for added redundancy, and store those devices in different, safe locations.

As with your keys, you should NEVER write down your recovery seeds using online, cloud-based storage products like Evernote, Google Docs or Dropbox. While these are fine products, they are by definition much more open and less secure than offline storage. You should also not keep them in word processor files or notepads on your computer if it is connected to the internet. Offline is the best way to go, but if you use an online method, stick with services like Lastpass and again, remember to set up 2FA for your account.

PART 3: TRADING CRYPTOCURRENCY SAFELY & CONVENIENTLY

There are many people who follow the steps described above, and everything is fine and good. But when they want to actually *trade* cryptocurrency, they have to send it back to an exchange first. Whenever they do this, the vulnerabilities we described in the introduction are now reintroduced into the equation. For years, this was simply accepted as an unavoidable risk. But what if there was a way to maintain custody of your funds while still being able to trade effortlessly like with an exchange hot wallet?

Now there is! You can use Faast, a non-custodial, P2P tool for swapping cryptocurrencies *directly from your own wallets*. You simply go to https://faa.st/portfolio/connect, connect the wallet of your choice, and begin trading with our easy and intuitive user interface.



There is no point at which a hacker can take your funds. Even if WE got hacked, they couldn't get to them, because we never see your private keys. The accountless nature of the product also means that you don't have to worry about your login credentials being compromised either.

Using Faast with your wallet allows you to bypass most of the risks associated with trading cryptocurrency, while still enjoying all the benefits. You now have the power to build the swap coins, rebalance your portfolio, and view all your holdings in one place.

Faast allows you to connect multiple wallets and make multiple swaps at once using our rebalancing tool. It also allows you to generate charts and get a complete visual representation of your crypto portfolio by percentage, weight, and $ amount. It's a simple and secure crypto swapping and portfolio management tool. Everything you need- all in one place.

A tool like Faast, combined with the best practices in this guide, brings cryptocurrency back to its roots: a P2P, decentralized network where value can be securely exchanged without the need to go through a centralized intermediary.

Visit the Faast website now to connect your wallet and start trading in seconds.

Thank you, and happy swapping!

The Faast Team

Don't forget to follow us on Twitter @gofaast