A beginner's guide to Crypto Security

Seed Phrases – The Basics

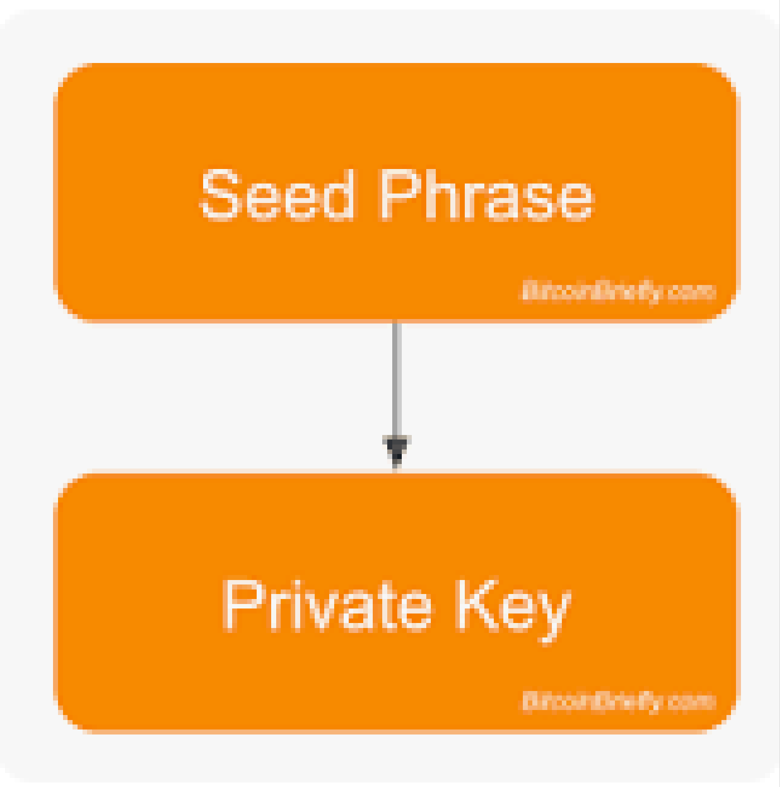
Anytime you set up a new crypto wallet, you will be given a list of words to write down and keep safe.

What is a seed phrase? A seed phrase, also known as a mnemonic code, is a set of (usually 12 or 24) words that represents a very large random number; this random number is used to generate a nearly limitless number of private keys that can be used to secure your bitcoin. The algorithm for generating the private keys is deterministic, meaning that the same seed phrase will always generate the same private keys. As such, you can think of a seed phrase as the "master key" to all of your private keys. It's incredibly important!

If anyone other than you has your seed phrase, it means they can access your wallet and all your funds. PROTECT YOUR SEED PHRASE at all costs!

In the event of a hardware failure, or you lose your phone, etc, the only way to recover your account is to enter your seed phrase. If you do not have it, no one can help you recover the funds…not even the company you chose your wallet with.

Seed Phrase and your Private Key



- A private key allows you to spend your bitcoin, and a seed phrase is a way to derive your private key. Your wallet derives your private key from your seed phrase.

Private Keys

What is it? A private key is a sophisticated form of cryptography that allows a user to access his or her cryptocurrency. A private key is an integral aspect of bitcoin and altcoins, and its security make up helps to protect a user from theft and unauthorized access to funds.

Every Bitcoin wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Bitcoin addresses generated for the wallet.

For example: If your wallet has Bitcoin and Ethereum, you will have a separate private key for each crypto asset you have in your wallet.
Never share your private keys!

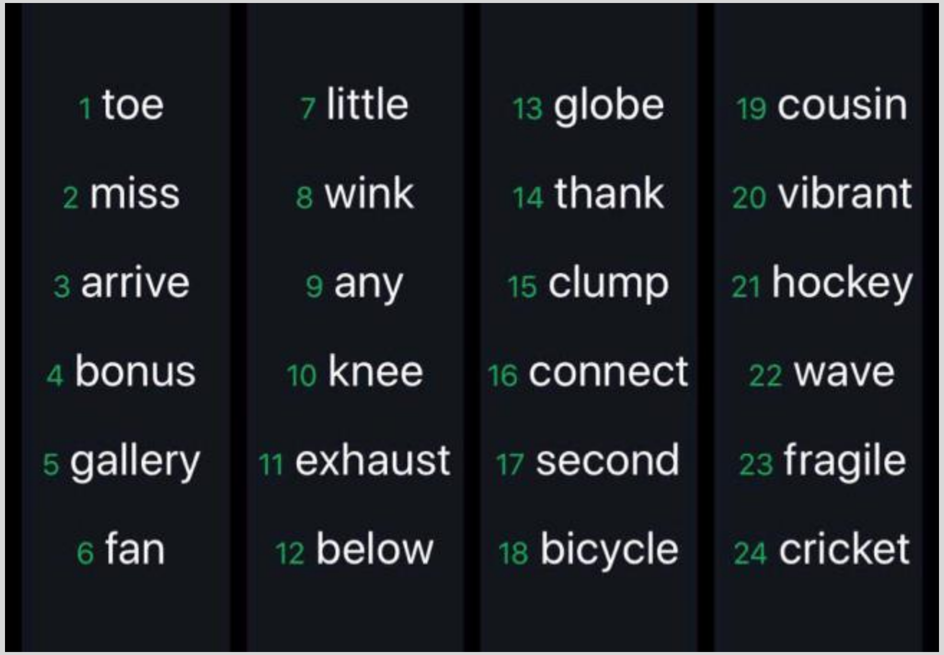
Public Keys

What is it? A public key allows you to receive cryptocurrency transactions. It's a cryptographic code that's paired to a private key. While anyone can send transactions to the public key, you need the private key to “unlock” them and prove that you are the owner of the cryptocurrency received in the transaction.

If you want to receive or move (withdraw) crypto to another wallet or person, you would send them your public key. This is how the funds will be moved/deposited into your account.

Seed Phrase Do’s and Don’t’s

Example Seed Phrase



1 toe
2 miss
3 arrive
4 bonus
5 gallery
6 fan
7 little
8 wink
9 any
10 knee
11 exhaust
12 below
13 globe
14 thank
15 clump
16 connect
17 second
18 bicycle
19 cousin
20 vibrant
21 hockey
22 wave
23 fragile
24 cricket

DO’s and Don’ts

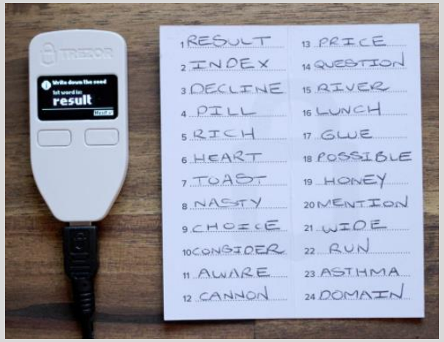
- **Do NOT** ever ever EVER share your seed phrase with anyone.
- **Do NOT** screenshot your seed phrase
- **Do NOT** set up wallets on public wifi or wifi you do not implicitly trust (not even at work)
- **Do NOT** store in plain text (unencrypted) on your computer
- **Do NOT** email your seed phrase
- **Do** get yourself a good VPN
- **Do** physically write down your seed phrase and keep it somewhere safe (and fireproof).
- **Do** always verify the website first before entering your seed phrase for recover. Trezor has been subject to a phishing scam ([PSA] Phishing Alert: Fake Trezor Wallet Website | by SatoshiLabs | Trezor Blog)

Securing your seed phrase & Crypto

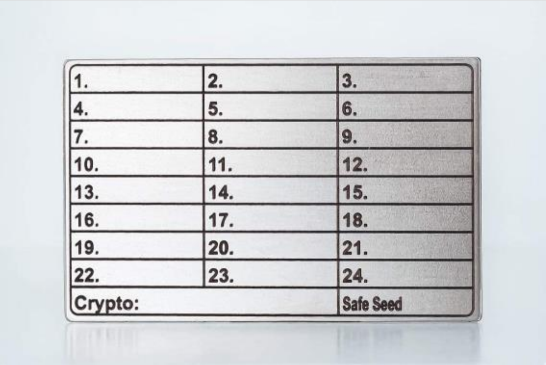
There are several options to storing your seed phrase securely

Cold Wallets
A cryptocurrency wallet that cannot be compromised because it is not connected to the Internet. Also called a "hardware wallet" and "offline wallet," the cold wallet stores the user's address and private key and works in conjunction with compatible software in the computer.

Paper options – write down on paper and store securely (and hopefully fire proof)
Metal options –Ways of storing your seed phrase on metal
Hardware Wallets – Offline hardware used to store your private keys
Watch-only accounts-Watch-only wallets allows you to keep an eye on your cold storage or paper wallet without touching your private key. Easily import your public address, xpub or ypub and watch it from your app without moving anything.



1 RESULT
2 INDEX
3 DECLINE
4 PILL
5 RICH
6 HEART
7 TOAST
8 NASTY
9 CHOICE
10 CONSIDER
11 AWARE
12 CANNON
13 PRICE
14 QUESTION
15 RIVER
16 LUNCH
17 GLUE
18 POSSIBLE
19 HONEY
20 MENTION
21 WIDE
22 RUN
23 ASTHMA
24 DOMAIN



1.	2.	3.
4.	5.	6.
7.	8.	9.
10.	11.	12.
13.	14.	15.
16.	17.	18.
19.	20.	21.
22.	23.	24.
Crypto:		Safe Seed

Hot Wallets vs Cold Wallets

Hot wallets: Hot wallets are wallets that are always connected to the internet. EX: Crypto exchanges, mobile wallets, some hot wallets below:

Your hot wallet should behave in the same way as a real-world wallet.

You use it to carry a small amount of cash for ease of access. That is all.

While transacting with hot wallets is very simple, there is a huge drawback when it comes to them.

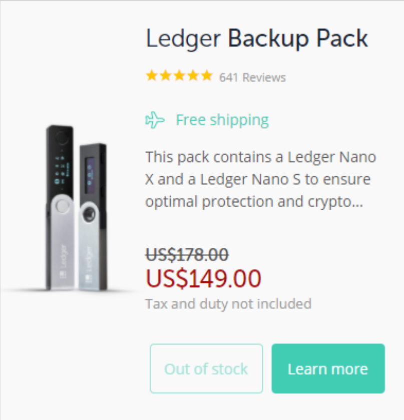
They are easily hackable. The whole crypto-space has been gaining a lot of value recently and where there’s value, crime is never far behind.

Hot Wallets vs Cold Wallets

Cold wallets: cold wallets are hardware devices that store your cryptos offline. Safety-wise, cold wallets are considered the best option - since they are always offline, you don't need to worry about some sort of a hacker stealing all your cryptocurrency assets.

These are best suited to long-term holders, who don't require access to their coins for months, or years at a time.

They aren't without their own set of risks but if you follow the instructions correctly, and take every precaution possible, these are greatly minimized.



Ledger Backup Pack

★★★★★ 641 Reviews

Free shipping

This pack contains a Ledger Nano X and a Ledger Nano S to ensure optimal protection and crypto...

~~US$178.00~~

US$149.00

Tax and duty not included

Its also a very good idea to have more than one cold wallet. One to use and one to use as a backup (in case anything happens to the first one)

Pros and Cons

While paper wallets substantially decrease the threat of compromise from the virtual world, they aren’t without their own set of risks.

- **Coercion:** There are always going to be people willing to break the law to get at something valuable. Just as crooks tear off in Lamborghinis after raiding a property, so too might they stumble upon your safe. They don’t know what’s in there but presumably, it’s valuable. Anyway, you get where this is going, and the moral of the story is simple: don’t go bragging about your crypto investments. It doesn’t matter if it’s online, or in person, it’s never a clever idea. Don’t make yourself a target.

- **Fragility:** At the end of the day, it is still paper. Paper can be easily damaged or it can get worn out over time. This is why you should always make multiple backups.

- **Stealing:** Since it is written on a piece of paper, anyone who can read it or take a photograph of it can steal your money.

- **Not immune to disasters:** It is just a piece of paper, it is not immune to natural disasters and can easily be destroyed if you have not taken any backups.

- **Type of printer used:** The quality of printer used can also have a detrimental effect. Non-laser printers may cause the ink to run if the paper gets wet.

- **Human Errors:** Humans are prone to mistakes and you can simply forget the location of your paper or accidentally tear it.

Paper Wallets

What is it? paper wallets are an offline cold storage method of saving cryptocurrency. It includes printing out your public and private keys on a piece of paper which you then store and save in a secure place. The keys are printed in the form of QR codes which you can scan in the future for all your transactions. The reason why it is so safe is that it gives complete control to you, the user. You do not need to worry about the well-being of a piece of hardware, nor do you have to worry about hackers or any piece of malware. You just need to take care of a piece of paper.

Setting up a paper wallet:
Paper wallets are formed by using a program to randomly generate a public and private key. The keys will be unique, and the program that generates them is open source.
What's more, we'll be generating our keys offline. This eradicates the exposure to online threats, and deleting the simple program after use will destroy any trace of them.

Paper wallet generator: Walletgenerator.net
MyEtherWallet.com (for Etherium)

NOTE: Before setting up a paper wallet on your PC, ensure there is no malware or viruses on your machine, and use a VPN. A brand new PC is best but often not practical

Paper Wallet Risks

While paper wallets substantially decrease the threat of compromise from the virtual world, they aren’t without their own set of risks.

•Coercion: There are always going to be people willing to break the law to get at something valuable. Just as crooks tear off in Lamborghinis after raiding a property, so too might they stumble upon your safe. They don’t know what’s in there but presumably, it’s valuable. Anyway, you get where this is going, and the moral of the story is simple: don’t go bragging about your crypto investments. It doesn’t matter if it’s online, or in person, it’s never a clever idea. Don’t make yourself a target.

•Fragility: At the end of the day, it is still paper. Paper can be easily damaged or it can get worn out over time. This is why you should always make multiple backups.

•Stealing: Since it is written on a piece of paper, anyone who can read it or take a photograph of it can steal your money.

•Not immune to disasters: It is just a piece of paper, it is not immune to natural disasters and can easily be destroyed if you have not taken any backups.

Paper Wallet Risks Continued..

- Type of printer used: The quality of printer used can also have a detrimental effect. Non-laser printers may cause the ink to run if the paper gets wet.

- Human Errors: Humans are prone to mistakes and you can simply forget the location of your paper or accidentally tear it.

Conclusion

The security of your funds is completely up to you. Use a combination of the methods discussed to secure your crypto assets in the best manner for you.

Setting up a cold wallet is a straightforward way to help alleviate third-party risks associated with most other cryptocurrency storage methods. While no method is entirely free from threat, storing coins offline drastically reduces the chances of losing your investment through digital means – exchange compromise, exchange insolvency, ransomware attacks, other cybercriminal operations.

It is still as important as ever to remain vigilant of real-world threats such as loss, theft, or damage of private keys. Always protect your private keys, and ensure to replace them (setup new cold storage) immediately if there is any indication that their privacy may have become compromised.

The best solution is diversification. As the old saying goes, “Do not keep all your eggs in one basket.” Always diversify. Keep a portion of your currency (a major portion), in paper wallets and have lots of backups to ensure that you are not going to get screwed. Keep some in hardware wallets and if you really must, keep a few in a hot wallet as well so that you can do quick transactions. Having said that, make sure that most of your money is in cold storage.

Thank you – Stay Safe