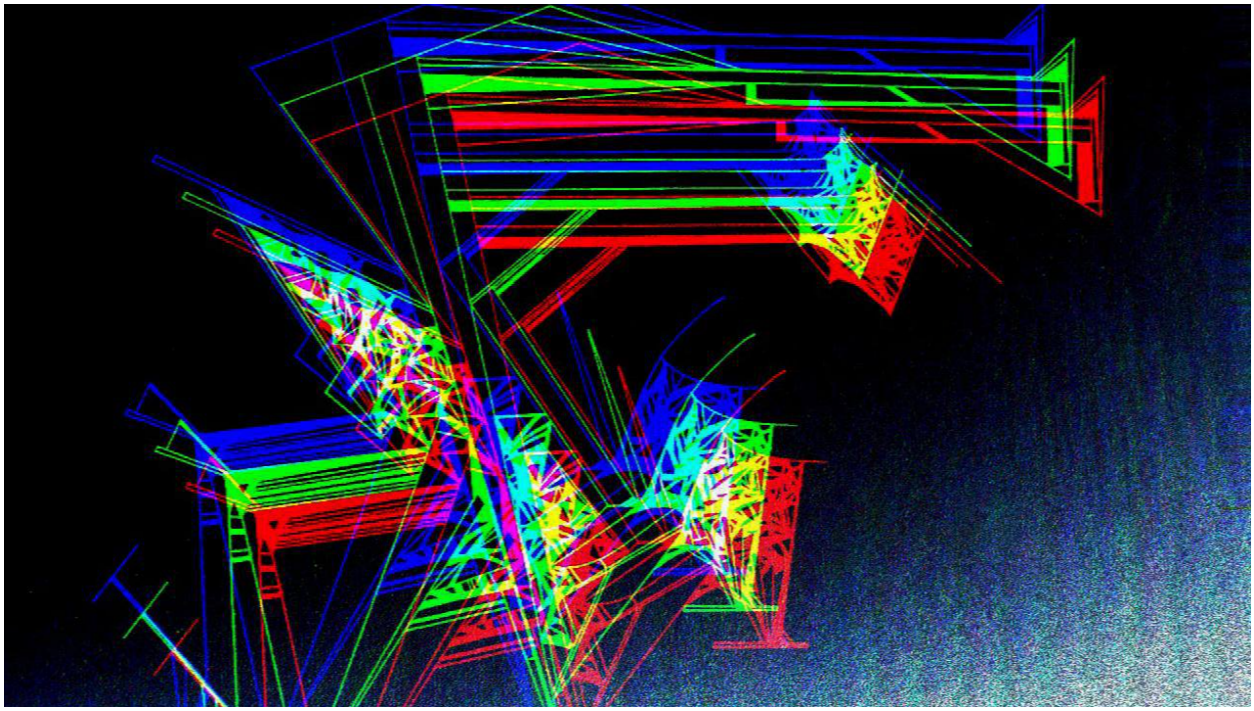
What's The Safest Way to Store Crypto?



Greetings, dear readers! I'm frequently asked what the most dependable way to keep cryptocurrency is, whether it is Bitcoin, Monero, ERC20 tokens, or DOGE.

In this essay, I'd like to offer the solution to that question; regrettably, there are no clear and simple answers!

I'd also like to thank the authors of all of the services that were used as examples in this essay, as well as the authors of all of the resources that I utilized as references; keep up the fantastic job!

#I - Introduction

So, first of all, we have to decide, what do we need it for? Anyone can use Ethereum securely, same with Monero, in which you should keep in mind way less security rules.

If you need a bulletproof anonymity or ultra privacy, then read this awesome ultra hardcore guide. Read my recent article dedicated to a «Timing Attack» or «Attack via a representative sample».

You must remember the main rule:

> ***Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.***

The thing is that if you need a certain crypto-wallet for work, for staking, for paying your employees and so on - it is considered "operational" or "hot", so we will consciously build its protection based on objective threats, you can learn about this from my articles:

- **officercia.mirror.xyz**
- **hackernoon.com/u/officercia**
- **cia.start.me**

But today, I'd like to focus our conversation on the fact that we require a truly secure solution. To help us visualize it, let me phrase the topic of today's essay as follows:

"You suddenly received $1 billion in any cryptocurrency, and you don't want to invest it yet, but you want to securely save the majority of it using cryptocurrencies."

So, what are our options?

Cold hardware wallets, brain wallets, and paper wallets are the most common. I feel that "designed" techniques have earned the right to exist as well, but let's concentrate on the first one, which is a cold hardware wallet.

Following that, I will tell you about the ways that I deem safe and recommend to my clients!

#II - Cold Wallets

I am often asked why in my recent articles: about secure cryptocurrency storage, about an attack on old-and-forgotten hard-drives and on how hackers are caught I do not recommend using Trezor or Ledger devices for a main cold storage.

> ***…in space no-one can hear you scream…***

So I chose the two most popular devices and had no previous assumptions about them.

I believe that no technology is inherently harmful; rather, diverse conditions for safe use and reasons for using it exist.

So, let's get back on track and examine these two examples through two separate technical lenses. I can get info from your Trezor or Ledger if you have one.

But there will only be a couple of attempts. That's why I've never recommended Trezor or Ledger... If the device falls into someone's hands, you're screwed.

They have different approaches, you can read more about them here and here, but the gist is basically the same. There's a great fresh video on this topic:

> *Check out wallet rating: walletscrutiny.com*

If you own something like this device, it is unlikely that it will be possible to restore anything without his participation. Because there are all sorts of cool, bulletproof features.

> *Check out these rather interesting hardware wallets gridplus.io/products/grid-lattice1 (2) & this BitLox device*

In essence, cold wallet is just a pseudo-AirGap system (100% AirGap is impossible to achieve on Earth by definition, that's why CubeSat topic is so interesting) and it can be cracked.

And you can make a cold wallet out of a regular phone, for example via airgap.it - there will be almost no difference from Trezor or Ledger!

Trezor is and serves as the basis for many hardware wallet clones out there, but it also has no physical security which is why there are numerous "key recovery" services you can reach out to for extraction if you own one.

It is important to add that not a single hardware cold wallet at the moment is fully Open-Sourced - not even Trezor, Ledger and the ones I cited above.

Also, if you go to their websites you can see that they are one of these companies does not consider the bug-bounty report "in scope" if you have physical access to the device…

Needless to say, with the increase in physical attacks, it is very important to take this into account?

#III - Brain Wallet

It is often chosen because it is easier to remember than the seed or the private key, it is easier to put there some poem that you made up.

Or make up your own seed out of the nicknames of all the pets you've had in your life.

> *BrainWallets are basically instantly crackable since the range is tiny github.com/ryancdotorg/brainflayer*

But the problem was that people didn't want to be creative and just took some lyrics from songs or simple words like "Bitcoin"...

But there are dozens of bots with huge tables, where all these options are already turned into private keys and public keys and mempool is constantly monitored in case one of these wallets is refilled:

- badkeys.info
- playxo.com

- keys.lol

At the same time, in my opinion, we should not bury this technology - we just need to collect such a wallet, using natural Entropy, for example, weather data or atmospheric noise to determine words from the dictionary, but that is another issue.

With all said, this technology looks old in 2022.

#IV - Paper Wallet

The most secure option would be to use a cold card or a "paper wallet."

It's also preferable to store a private key rather than a seed phrase on the paper wallet. In case you're wondering what the distinction is between a Private Key and a Seed Phrase.

A private key grants access to a single address (account), whereas a seed phrase grants access to the entire wallet, which can contain multiple addresses and private keys.

In general, paper wallets are the most secure item you can imagine. When storing the private key, do not store the seed. Different machines, separate wallets, and correct multi-sig...

#Multi-Sig Best Practices & Attack Vectors:

- safehodl.github.io/multisig
- help.gnosis-safe.io/en/articles/4772567-what-safe-setup-should-i-use
- blog.gnosis.pm/how-to-securely-manage-company-crypto-funds-with-gnosis-safe-multisig-8b3f67485985
- polygon.technology/blog/multsig-best-practices-to-maximize-transaction-security
- blog.logrocket.com/build-treasury-wallet-multisignature-gnosis-safe
- medium.com/gauntlet-networks/multisig-transactions-with-gnosis-safe-f5dbe67c1c2d
- blog.openzeppelin.com/backdooring-gnosis-safe-multisig-wallets/amp/
- blog.gnosis.pm/the-0xhabitat-multisig-got-drained-an-analysis-16ab74ddf42
- slowmist.medium.com/gnosis-safe-multisig-user-incident-analysis-9a270b8e1452

Would also suggest key segregation and key cycling as well. Meaning, don't use the same keys as your hot wallets for multi-sig management, and don't use the same keys forever.

Get in the habit of maybe quarterly or yearly audits of these keys (and their backups) because it's surprisingly easy to lose track of them!

You should RSA-encrypt it or use Steganography, also hide it like pirates hide treasures. You can read about it here!

I also want to remind you about one scam service, which nevertheless occupies the first position in the Google search for "paper wallet generator" and even "paper wallet generator".

The name is not printed intentionally, just look at the screenshot.

In any case, any such service has only one goal - to steal your cryptocurrencies by giving you pre-generated key pairs from the service owner:

As a result, never utilize an online service to generate private keys.

> **Only Bitcoin Core and Electrum can be trusted if they were downloaded from an approved source.**

And that condition might alter at any time: someone could hack the core engineers' GitHub accounts or simply pay them for a "damaging" commit. For Ethereum, you can check out something like this script.

Also, bitcoincore.org is the official website of the Bitcoin Core project while bitcoin.org is a separate website and project which aims to provide general information about Bitcoin! Keep that in mind!

Last but not least, there is such a thing as hierarchical determination (HD) in the settings of some wallets.

It sounds scary, but it means that every time you get money to an address, a new clean address will be generated from the same private key. And you can accidentally send money to an already inactive wallet.

It is better to turn this function off (if it will be enabled), because it is easy to get confused with it.

Lastly, here is my special compilation of four crypto services aimed to help you when you are already a dead man:

- **safient.io**
- **sarcophagus.io**
- **safehaven.io**
- **killcord.io**

Check out this article for more info on this sensitive topic.

#V - What's for EVM-based Blockchains?

For Ethereum, you can check out something like this script. In any case, the variations will be insignificant if we are talking about the level of protection that we have specified in the article.

The main difference is that hot or "operational" Ethereum wallets must adhere to stricter security guidelines, as I detailed in my blog.

However, if we have the amount of money we need to store on hand and it is in tokens or ETH, or for example in BSC, Avalanche, or Polygon - the differences with the ones outlined before in the paper wallet section will be minor.

It is important to say that cryptography and natural entropy is a reliable protection. By no means try to make yourself some "vanity" address - no matter what network. You can use Profanity2, but don't forget about the history with Profanity1, let me remind you about it.

If you go for a larger form factor, you could use QR code swapping for the ultimate air-gap solution, but keep in mind:

If you are looking for something web3 or GameFi-specific like a EVM (or Non-EVM) smart-contract wallet, check out frame or Argent.xyz and some web3-ethos aligned non-custodial wallets.

Remember that an average smart wallet is an Ethereum wallet that is governed by a smart contract rather than a private key.

At the same time, many multi-cig solutions are inherently such wallets. Account abstraction is one of their key features, so make sure to double-check everything on their website!

To summarize, I do not recommend adopting any of the above smart-wallet or smart contract wallet techniques for cold storage.

Metamask (alternatives: myetherwallet.com or this list), which is a non-custodial wallet, combined with Airgap.it would be a way better solution! Here is a nice manual on this topic. Check out this guide as well.

Don’t forget to set up a secure RPC provider!

- **securerpc.com**
- **www-securerpc.netlify.app**

Check out this manual for a MetaMask wallet. Always use a reliable VPN provider - mullvad.net is a perfect choice.

I am also not asking you to comply with all of this, but you must remember the main rule in this particular case:

- **Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.**

If we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defenses.

Only knowledge can defeat criminals' knowledge. In this intellectual boxing match the most prepared wins, and we want that to be you!

Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

I don't have as much money as the fictional character in our essay, but your support helps me to exist 🙂

If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**