



How To Get Started With Self-Custody

MASTERING CRYPTO SECURITY

Why NGRAVE

NGRAVE empowers people to master their wealth so they can live the life they want. Founded in 2018, **NGRAVE** is a digital asset security provider offering user-friendly maximum security solutions for blockchain and crypto use cases. Its flagship product — crypto hardware wallet “NGRAVE ZERO” — is the only financial product in the world with a custom operating system featuring the highest security certification: EAL7. NGRAVE partnered with the world’s top tier in nano- and chip technology, cryptography and hardware security. Among its advisors, it counts several blockchain pioneers such as Jean-Jacques Quisquater, famous cryptography professor and second reference of the bitcoin paper.

NGRAVE’s product suite is a 3-tier solution. [ZERO](#), the offline touch-screen hardware wallet allows users to securely store and transact their crypto. [GRAPHENE](#), the stainless steel encrypted backup





solution ensures that users never lose their keys. It is not only made to withstand extreme conditions, but also designed to be recoverable in the event of loss. Last but not least, [LIQUID](#) is the convenient mobile app that connects users real-time to the blockchain without ever exposing their private keys.

We are passionate about making the world of crypto a safer place. We eradicate the chance of loss and malicious hacking of your crypto, giving you complete control of your digital assets. We believe we are all in this together. Join our movement at <https://www.ngrave.io/>



Table Of Content

1	Learning From Satoshi's Take On Self-Custody	1
2	How To Choose The Best Crypto Hardware Wallet?	16
3	How To Store Your Recovery Seed	31
4	Moving Funds From Hot To Cold	42
5	How To Secure Your Nfts	56

1 Learning From Satoshi's Take On Self-Custody

We can use the wisdom of Bitcoin's creator to understand the nuances of self-custody and why many crypto owners choose not to heed crypto's golden rule.

As the list of casualties grows from the sudden and steep descent of crypto markets into bear territory, so does the cry to heed the no.1 rule of crypto - 'not your keys, not your coins'. While NGRAVE wholeheartedly supports self-custody, we also appreciate that the reality isn't quite as simple as that mantra. We can use the wisdom of Bitcoin's creator, Satoshi Nakamoto, to help us understand the nuances of self-custody and why so many crypto owners choose not to heed crypto's golden rule.

In the first two paragraphs of the Bitcoin Whitepaper, Satoshi Nakamoto's blueprint for a new form of peer-to-peer cash, the word 'trust' appears six times. That's because Satoshi viewed the need for trust as the biggest weakness of the traditional financial system.



The genius of Satoshi's creation was to take inspiration from previous attempts at digital cash and then add a crucial missing piece - making it work without the need for trusted central authorities.

*“While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the **trust** based model..... no mechanism exists to make payments over a communications channel without a **trusted** party. What is needed is an electronic payment system based on cryptographic proof instead of **trust**, allowing any two willing parties to transact directly with each other without the need for a **trusted** third party.”* - Bitcoin Whitepaper

What's interesting about this quote from the Bitcoin Whitepaper, and others from Satoshi's digital footprint that we'll use to understand the case for self-custody, is that it both captures their trust-issues with private monetary transactions, as well as their pragmatic acceptance that *‘the system works well enough for most transactions.’*

Satoshi's wisdom around trust might then be summarised to - remove the need for trust as much as possible, but accept that taking a 100% trustless approach to your finances may be impractical.

So let's unpack that wisdom by understanding:

- What Satoshi meant by replacing trust with cryptographic proof
- Why do some people choose not to self-custody?
- The role that trust-based institutions play in accessing crypto
- The risks of not having full custody of your crypto



- What are the alternatives to the trust model?
- The security of cold storage

Trust, self-custody & cryptographic proof

When Satoshi talked about a 'trust based model' for financial transactions, he meant that for you to participate in a financial transaction, say depositing some funds with a bank in order to receive interest or taking out a loan; each has to trust the other to keep their side of the bargain and not simply run off with the money.

Both sides can take action to support that trust. The bank can follow rules and regulations imposed on financial institutions, which require you to trust those entities. At the same time, you must convince the bank to trust you by surrendering a lot of personal information.

This arrangement is sub-optimal because trust is easily broken, so Satoshi replaced trust with cryptographic proof; maths cannot be broken.

Cryptography, self-custody & responsibility

The word cryptocurrency is what is known as a portmanteau, a word that blends the meaning of two other words - cryptography and currency - explaining that it is money secured by cryptographic proof.

The mechanics of cryptographic proof are complicated but they boil down to Bitcoin - and the cryptocurrencies it inspired - functioning like digital vaults controlled by a pair of keys.

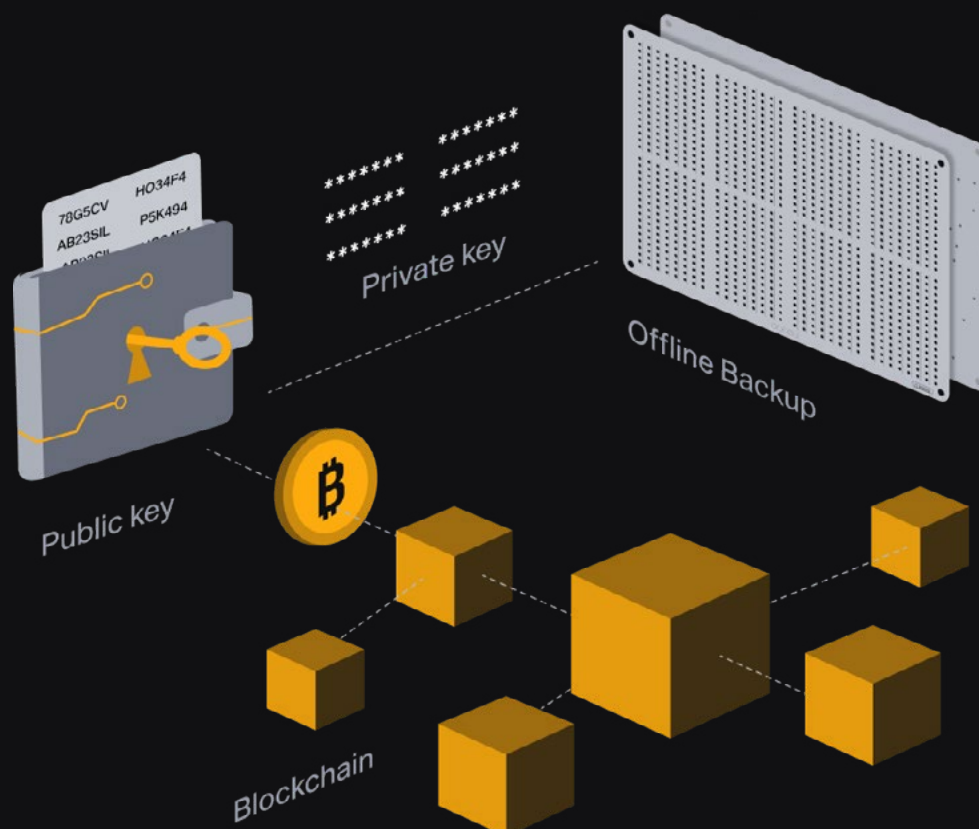


A Public Key specifies the virtual location of the vault on the blockchain - its address. A Private Key enables the vault to be opened and the funds spent.

As the name suggests, a Public Key is intended to be **shared**, while a Private Key - which unlocks the vault - is for your eyes only and must **be protected at all costs**.

How cryptography works

It is nearly impossible to crack the cryptography that generates Private Keys. If they are stolen or lost, there is no way back



You can connect to your vault on the blockchain through a digital wallet, where both the Public and Private Keys are held, and in case you cannot access that wallet, you must store a backup of those keys as a failsafe.

While storing a form of cryptographic proof might sound like a massive headache, wallet innovation has meant that Private Keys - which in raw form amount to strings of 256 ones and zeros - are magically translated into a single collection of unique words or sets of alphanumeric characters. This user-friendly catch-all for Private Keys is commonly referred to as a Seed or in NGRAVE's case, the Perfect Key.

So Satoshi's vision of money without trust requires individuals to store their crypto in a wallet that supports self-custody and to store that Seed securely.

Sounds simple enough but being ultimately responsible for your money via Private Keys presents a paradox.

It is nearly impossible to crack the cryptography used to generate Private Keys/Seeds. Still, if they are stolen or lost, there is no way back, which for many people is a frightening amount of responsibility when we are so used to the trust-based approach for all our online services, which comes with email/chat support.

So the first obstacle to self-custody of cryptocurrency is a behavioural one; we have to get used to taking responsibility and understanding best practices. That, however, is easier said than



done and Satoshi addressed this dilemma directly in another telling quote:!

“May 18, 2010: Creating an account on a website is a lot easier than installing and learning to use software, and a more familiar way of doing it for most people. The only disadvantage is that you have to trust the site, but that’s fine for pocket change amounts for micropayments and misc expenses. It’s an easy way to get started and if you get larger amounts then you can upgrade to the actual bitcoin software.”

Reading Satoshi’s post, you have to appreciate that hardware wallets like the NGRAVE ZERO didn’t even exist. Nevertheless, over a decade later those words still ring true because the path to least resistance for the majority of crypto owners is still to trust someone else with their funds. In the majority of cases, that means a centralised crypto exchange.



A pragmatic view of custody

The most obvious reason crypto users store their funds on an exchange is because that is how they acquired it in the first place. Centralised exchanges are the point of overlap between the existing financial system (aka fiat money) and the new world of decentralised money (cryptocurrency).

Because exchanges have to plug into the banking system, they still operate on the trust model Satoshi wanted to break. So the path to self-custody inevitably starts with trusting an exchange to help you acquire crypto.

How to make crypto really yours

Centralised crypto exchanges are the point of overlap between the existing financial system and the new world of decentralised money.



Once that hurdle has been negotiated, you can exercise self-custody by transferring your funds off the exchange. So why don't more people do just that?

The most obvious reason is that we are psychologically wired to fall back on defaults, given that 99% of crypto users start their journey with a centralised exchange that becomes their default storage system even when they don't intend to trade actively.

Spelling out the risks of custodial services

Any centralised service that has custody of your funds - an exchange or crypto bank - operates as a black box. You cannot know how adequate their security or risk management is, forcing you to trust them to do the right thing. There's that word again!

Though most services will likely live up to their commitments, the opaque nature of trust-based systems inevitably leads to their abuse, often through greed, opportunism, mismanagement, or some combination of all three.

There are countless examples of centralised services being hacked, both from the outside and the inside, or simply going bust. We listed ten of the biggest crypto hacks in this article, but it is worth highlighting a few examples here to show the frailties of the trust model and the dire consequences when trust is broken.



Mt. Gox - The biggest hack

Date: **2014**

Organization: **Mt. Gox**

Sector: **Exchange**

Scale of loss: **840,000 BTC**

Exploit: **Hot wallet hack**

When the Japanese-based exchange went offline in February 2014 it accounted for 70% of all Bitcoin trading worldwide. 850,000 BTC were lost (750k from customers & 100k belonging to the exchange), roughly 7% of the entire supply. Ten years later, customers are still waiting for a restitution plan to be finalised.

The Bitfinex Bail-In

Date: **2016**

Organization: **Bitfinex**

Sector: **Exchange**

Scale of loss: **120,000 BTC**

Exploit: **Exchange hack**

In 2016 the Hong Kong-based exchange Bitfinex lost 120,000 BTC through a hot wallet hack. The exploit accounted for 0.75% of all bitcoin in circulation and caused the price of bitcoin to drop by 23%. To stave off insolvency Bitfinex employed a 'bail in' applying losses to customers with a 36% haircut and compensated with an IOU. This tradeable BFX token eventually ended as net-profitable.



QuadrigaCX - The Most Notorious Exit Scam

Date: 2019

Organization: QuadrigaCX

Sector: Exchange

Scale of loss: \$190million

Exploit: Exit Scam

Though the loss of \$190million of crypto doesn't put Quadriga in the top 10 list of biggest hacks, it has become notorious because of how the exploit was exposed.

Gerald Cotten, the CEO of what was at the time Canada's biggest crypto exchange, died on holiday in India. It soon transpired that he had sole custody of the exchange wallets, which turned out to be empty. Cotten had been trading customer funds on other platforms with disastrous consequences.



Celsius Freezing Withdrawals

Date: **2022**

Organization: **Celsius**

Sector: **Exchange**

Scale of loss: **1.7 million users**

Exploit: **Frozen withdrawals**

The latest event to underline the dangers of custodial crypto services saw the freezing of withdrawals for the 1.7million customers using Celsius Network, a centralised yield generation platform.

Details are still emerging as to why Celsius cannot service withdrawals - suggestions point to a lack of liquidity or insolvency - but whatever the cause, customers have once again had their trust broken and could end up paying a heavy price.

The 2008 financial crisis was the perfect illustration of how significant the consequences can be when risk is obfuscated and becomes systematic. Satoshi gave a hat-tip to this by adding the following reference to the Bitcoin Genesis Block:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”



Over the last few weeks, the crypto industry has witnessed our version of the financial crisis, which is why Twitter is awash with references to Lehman Brothers, as they were the first domino to fall.



The fear now is that the sector might experience an unstoppable chain of liquidations and insolvencies spreading like the sub-prime contagion punishing those that didn't retain control of their keys.

DEFI doesn't have all the answers

Anyone using exchanges as more than an on-ramp can immediately migrate to a DEX (decentralised exchange) that doesn't touch the fiat system and enables you to transact yet retain control over your keys.

This model applies to all DEFI protocols meaning that withdrawals cannot be suspended, and there are no accounts to lock. The bad



news is that this doesn't entirely shield you from risk; it just takes a different form.

Whereas centralised services require trust in people, DEFI requires trust in code, and unfortunately, bad code or bad logic expressed as code can have disastrous consequences.

The recent Terra/Luna collapse is an example of the latter, with a \$40bn platform collapsing like a house of cards in a matter of days, while [DEFI hacks accounted for \\$1.4bn in the first five months of 2022.](#)

So it seems that crypto holders looking to trade or generate yield face risks on both sides - CEFI & DEFI - yet even with these catastrophic events reinforcing the argument for cold storage, the majority won't heed the warning, and we shouldn't expect them to.

People don't always act rationally; to expect them to is unrealistic and ignores basic behavioural psychology. Heuristics aside, we need investors to take some risk; without risk-seekers Bitcoin may have never even gotten off the ground.

The problem is when our judgments are clouded by psychological biases rather than guided by logic. This can lead us to think that hacks are just headlines impacting other people or that Luna's implosion was a one-off.

The best we can expect is that the trauma of recent events acts as a catalyst for more users to adopt the NYK/NYC mantra and actively



move their funds to cold storage rather than leaving them on a CEX by default.

No one should expect or even want all crypto to be sat in cold storage because that would defeat part of its function as a medium of exchange.

June 26, 2010: Like cash, you don't keep your entire net worth in your pocket, (you keep) walking around money for incidental expenses.

Again Satoshi hinted at the idea of striking a balance between funds kept in cold storage (savings) and funds for spending or trading; it's up to you what that balance looks like but consider cold storage as savings and remainder as your current/checking account.

As the Lightning Network develops, it will become easier to spend Bitcoin securely, while [Mastercard and Visa are moving towards integrating crypto into their vast networks.](#)

Moving to the safety of Cold Storage

If you have funds on a centralised service, the good news is that it is easy to move them to the safety of cold storage. Check out the specifications for NGRAVE's ZERO built to provide the highest level of offline protection for your coins.

Once you have a ZERO, we've got an entire article on how to move funds from hot wallets, but the tl'dr is that the process takes just a few minutes and the transaction fees are a price worth paying for



peace of mind in what are turbulent times.

We are an adaptive species, so attitudes around the custody of money will gradually change. Wallet design will play a big part with NGRAVE's mission to produce the safest and easiest way to self-custody:

**No one should
access your
crypto except
you.
Own what is
yours.**

2 How To Choose The Best Crypto Hardware Wallet?

Convenience and usability are important, but there's nothing more inconvenient than losing your hard earned coins.

There are two golden rules for how to choose a cryptocurrency hardware wallet.

Rule number 1 - Security is the most important consideration.

Rule number 2 - Refer to rule number 1

Yes, convenience and usability are important, but there's nothing more inconvenient than losing your hard-earned coins, so design considerations should make using a hardware wallet simpler, without compromising security.

If you think price should be the primary filter when comparing cryptocurrency hardware wallets, then you're probably not ready to buy one. Price matters - and we'll try to help understand how much - but it shouldn't be at the top of your checklist.



If that comes as a surprise to you, take a step back and fully understand what a cryptocurrency hardware wallet is and does. Without that core understanding, much of what follows won't make sense, or be useful to you.

If you're ready to make the jump to financial sovereignty, we can establish four main criteria we can use for comparing cryptocurrency hardware wallets.

Criteria for choosing a crypto hardware wallet

How well they protect you from malicious external threats



How well they protect you from malicious external threats



How well they protect you from yourself



Do they justify their price tag?



- How well they protect you from malicious external threats
- How well they protect you from yourself.
- How tailored they are to your specific user needs, without compromising security
- Do they justify their price tag?

There are a growing number of hardware wallet brands fighting it out to prove they can combine safety and usability, at an affordable price, but for full disclosure, we have a dog in this fight.

We're NGRAVE, makers of the ZERO, the newest, and what we consider to be the most secure, cryptocurrency hardware wallet on the market. But we'll let you be the judge of that. Let the cold war begin.

Protection from malicious external threats

It should be no surprise that security is the key consideration when choosing a cryptocurrency hardware wallet. Though illicit activities represented just 0.34%¹ of all crypto transactions in 2020 according to Chainalysis, that still amounted to a massive \$523million in stolen crypto.

In April 2021 one [Coinbase user alone lost \\$11.6million in just 10 minutes](#) to a fake notification scam.

With so many bad actors on the prowl, the first security consideration of your crypto hardware wallet is **how the device protects you from malicious external threats**, intent on stealing



your cryptocurrency. This should focus on two areas:

- Reducing the attack surface
- Secure Key Generation

Reducing the online attack surface?

Attack surface has nothing to do with soccer tactics. It is a fancy tech security term that describes the sum of entry points where an attacker might try to gain access to systems or data.

Cryptocurrency hardware wallets have to interact with blockchains via the internet to enable you to transact. Most devices rely on a USB connection or BLE - Bluetooth Low Energy - creating a potential attack surface at the point of connection, turning the wallet from cold storage to hot.

The ideal is a hardware wallet that is 100% offline. The only way a cryptocurrency hardware wallet can be 100% offline is if **the method of communication is one-way via QR Code**, rather than USB or BLE, which tends to be the standard. The NGRAVE ZERO is 'air gapped' in this way, offering the coldest of cold storage.

The ZERO has a built-in USB-C port, but this is isolated from the rest of the device - so the device remains offline - and is used for just two things only: charging and firmware updates.

Firmware updates - accessing newer versions of the device's operating system - are another potential attack vector, as operating systems are regularly patched and improved. Look for the highest



level of firmware/OS security known as the **Evaluation Assurance Level (EAL)**. It runs on a scale from 1-7, with EAL7 being the highest.

The NGRAVE ZERO's operating system is rated EAL7 - for comparison banks and governments are typically EAL5 certified - and firmware updates will be cryptographically protected and only available through the NGRAVE website.

Protection from malicious external threats

Reducing online attack surface

The entry points for an attacker to try to gain access.



No Wifi



No USB



No NFC



No Bluetooth



Reducing physical attacks

The risk of someone tampering with your device before or after it is in your possession.



Anti-tampering



Optional Passphrase



Secure Element

Guarding against physical tampering

Attack surface relates to the online threat of unauthorised remote access via the internet. A cryptocurrency hardware wallet should also employ **countermeasures against the threat of physical compromise**. This should cover both the risk of someone tampering with your device before you receive it, as well as once it is in your possession. Measures should include:

Anti-tampering - A comprehensive framework to ensure the device hasn't been compromised before you receive it. Tamper evident package stickers aren't enough.

Optional Passphrase - The option of adding an additional layer of security

Secure Element - A chip that is by design protected from unauthorized access and used to run a limited set of applications, as well as store cryptographic data.

Secure Key Generation

Private Keys/Seeds provide the impenetrable cryptographic wall that enables crypto to work in a trustless way. They are, ultimately, what your cryptocurrency hardware wallet should be protecting, but some devices fall short of best practices in generating them. Here are three things to look out for:

Weak key generation - Some methods for generating keys are completely outdated



TRNG Backdoors - Seeds should be generated randomly, but the chips used for some of the True Random Number Generators (TRNGs) in popular hard wallet manufacturers may be exposed to backdoors, allowing prior knowledge.

Take-it or leave-it Seeds - If you have no choice but to accept a Seed generated by the hard wallet you are at risk if the manufacturer keeps a record. This is considered a feature of BIP-39 where the last part of the wordlist serves as a checksum of the entropy contained in the preceding words. It may actually be more of a bug.

Avoid getting a hardware wallet with weak key generation

Some devices fall short of best practices in generating Private Keys/Seeds.



Outdated methods



TRNG Backdoors



Predetermined Seeds



Protection from yourself

What you may not have previously thought of as security is **how a cryptocurrency hardware wallet protects you from yourself.**

It's an in-joke among tech support that the majority of the cause of a problem is found between the keyword and the computer. So when assessing security criteria for crypto hard wallets you should consider how the design and usability of a hardware wallet help you avoid making mistakes.

This is especially relevant because hardware wallets can be described as a *discontinuous technology*. This means that they scare newbies because they don't look, function or even sound like devices consumers are used to for storing money.

They introduce completely new concepts - like Seeds & Private Keys - so usability is an especially important security consideration in stopping you from shooting yourself in the foot.

One of the common reasons crypto newbies give for being shy of cryptocurrency hardware wallets is not trusting themselves to protect their Seed. This is understandable, as with great power, comes great responsibility.

There is no getting away from the fact your Seed is the only recovery failsafe you have for funds stored in your hard wallet. Securely storing a copy is crucial; use SWOF analysis to judge:



- **Shockproof**
- **Waterproof**
- **Offline**
- **Fireproof**

Too many crypto users think it's okay to store a photo of their Seed on Google Drive or iCloud. This poses a threat from hackers and malware and provides no redundancy if you lose access.

Given how offline Seed protection is such a key point of failure, it is surprising that the default approach from major crypto hardware wallet vendors remains to provide a few flimsy paper recovery sheets that fail on three of the four SWOF criteria.

The best way to secure a Seed is to engrave the phrases onto a metal sheet, but not just any metal, one that is resistant to heat and corrosion, so stainless steel is a good standard.

Punching your Seed into a steel sheet ticks the SWOF box and can mitigate against a lot of self-inflicted errors, but it still represents a single point of failure, lose it and you risk losing your coins forever. If you make a backup, you are doubling the risk of exposure. There is no absolute solution to this problem of infinite regression, but NGRAVE has come up with a unique approach.

When you buy the NGRAVE ZERO you also get a two-part system for Seed storage - GRAPHENE - featuring two stainless steel sheets and an automated punch pen, so you don't need a qualification in



engraving. The top sheet contains 16 columns and 64 hexadecimal values (0-9, A-F) creating 256bit security (16*64).

The automated pen allows you to punch the values associated with the holes on the top sheet into the base. Together they reveal your Seed, but on their own, each part reveals nothing.

If you lose the top sheet, there is a recovery process (via a Unique ID) but the base sheet has to be your responsibility, otherwise, NGRAVE will become a point of weakness and undermine your security.

The **focus on durability should also extend to the device itself**. Most cryptocurrency hardware wallets are the size of a USB memory stick you might get as a freebie at a conference, and just as flimsy, made from plastic and/or brushed stainless steel.

The more durable the device, the less likely you are to damage or break it, which will save you the hassle and cost of a replacement.

Convenience & Usability

Once you've satisfied yourself that a cryptocurrency hardware wallet ticks all the security boxes you can then - and only then - move on to considering convenience and usability.

This might hinge on the kind of crypto user you are because some crypto hardware wallets are designed for infrequent transacting, which is fine if you are a hodler, but far from ideal if you're active in trading, Defi, NFTs or all the above.



The early versions of hardware wallets operated via desktop-only software, but given the ubiquitous nature of mobile usage, **a Mobile App must be considered a standard**, so long as this doesn't create an attack surface (as discussed above) - so again look for a QR Code connection.

So far we've overlooked that we are talking about a wallet, with all the function expectation that entails. How does it handle sending, receiving, account creation, and setting fees? And what about **the range of supported cryptocurrencies** and the support for NFTs?

Hardware Wallet Convenience & Usability

Once you find a crypto hardware wallet that ticks all security boxes, you can start considering convenience and usability.



Mobile app



Range of coins



Compatibility with
web3 wallets



Tax services



User interface



Battery life

More important still, given the growth of Defi, is **compatibility with the standard in web3 browser wallets - MetaMask**, but without any compromise in security. These considerations shouldn't trump security but in a world of ever-increasing chains and coin standards, it's worth considering how future-proof a crypto hardware wallet is.

You might not have expected the cryptocurrency hardware wallet comparison to mention taxes, but like or not, the taxman is paying increasing attention to all the money being made in crypto. There are an increasing number of services that can help calculate your tax liabilities but they rely on support from popular exchanges and wallets; **it's worth checking whether the hardware wallet manufacturer has compatibility with tax services on their radar**, especially if you're likely to be making a few hundred transactions, as without an automated option, the process can be painful.

If you've done some research, and looked at images of some of the popular cryptocurrency hardware wallets, you might be surprised by how small they are and how small the read-out is. Again, this might be a throwback to the days before hard wallets weren't compatible with frequent transactions, but the small screen and buttons mean they are pretty damn fiddly.

Yes, you want things to be discrete, but equally, avoid the need for the manual dexterity of a magician, and the vision of a hawk, so **pay attention to screen size and quality**. How bright is the display and does it feature a touch-screen or support Biometrics? This will not only have a huge impact on how easy the device is to operate but



provide another tick on the security front, as well as minimising fat-finger mistakes.

Though we are talking about a high-end piece of technology, don't overlook the more mundane **consideration of battery life**. Cryptocurrency hardware wallets need a power source, and though you are unlikely to be creating significant aggregate demand, it would be reassuring to know the battery is using ultra-efficient low power.

How important is price?

And now, we can get to the **price**. It may be your favourite filter on Amazon, and a natural consideration in most product comparisons, but we'll do our best to argue that you should make an exception when choosing a crypto hardware wallet because focusing on thrift is a false economy.

How Important Is The Price?

When buying a cryptocurrency hardware wallet, consider the following:



Your current portfolio and its future value



Stress of knowing your crypto is not safe



It is an infrequent purchase



Price-to-portfolio ratio

A focus on thrift suggests that you may not fully buy into the underlying value of decentralised money, reading this article on what a cryptocurrency hardware wallet represents might help. If convenience and price are still overriding factors, then a hot wallet might be more appropriate for you.

It might help to use a more relatable example, again focused on security, like buying a lock for a bicycle.

The replacement value of your bike isn't the only consideration. If it is crucial for work and getting around, you will also consider the opportunity cost of not having a bike and the stress you'll experience constantly thinking your bike is at risk.

Applying that logic, you won't buy the cheapest lock on the market, as you're thinking about the cost of the lock as a proportion of the overall value the bike represents to you - not just sale price. It will also govern how much care you take in looking after the lock key or code.

Now apply this concept to crypto. The cost base today of your crypto, isn't the only consideration - given the huge upside that many cryptocurrencies can have over very short timeframes - you have to consider the potential future value.

Not only that, it's the security risk to any other crypto you might buy and store on the device and its future value, as well as the ongoing stress of feeling your stash isn't as secure as it could be.



Like a bike lock, a cryptocurrency hardware wallet should be considered an infrequent purchase, its value derives from longevity, unless you go cheap, in which case, a hard lesson may force you to reconsider.

If you really want to put a figure on when your portfolio value justifies buying a cryptocurrency hardware wallet, a sensible price-to-portfolio ratio is around 10% which - given the average price of a hardware wallet - generally means shopping around once your portfolio hits around \$1,000 in value.

But in all honesty, if you value security and control - the two key elements of storing money - it is never too soon to consider getting a cryptocurrency hardware wallet. At the risk of straying into broken record territory, your choice should always be guided by how well the device deals with security. Choosing the best cryptocurrency hardware wallet isn't like buying a toaster on Amazon; your financial independence and future are at stake.



3 How To Store Your Recovery Seed?

Owning crypto is often described as being your own bank because you get total control over your funds. To do so, you need to know what a Seed is and how to protect it.

What is a recovery Seed?

A recovery Seed is a failsafe for recovering all the funds stored in a cryptocurrency wallet. It is generally a collection of 12-24 ordered words (mnemonics). Think of it as a complex password.

Recovery Seeds are only generated by a specific type of crypto wallet, known as non-custodial, where you fully control the funds. This is the power of true decentralised money, but with great power comes great responsibility.

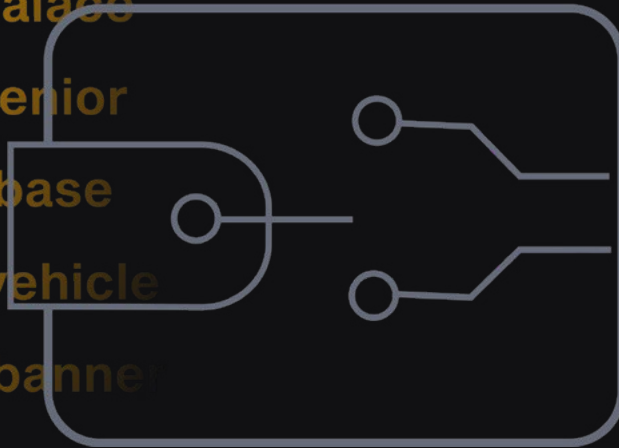
It is near mathematically impossible for someone to guess your Seed, giving it immense security, but being your own bank means there is no password reset function or 24/7 chat support.



What Is A Recovery Seed?

Recovery seeds are a complex password that can recover all the funds you store in a cryptocurrency wallet.

1 tool	7 jealous
2 settle	8 palace
3 shy	9 senior
4 race	10 base
5 zebra	11 vehicle
6 fluid	12 banner



If your Seed is lost, destroyed or stolen, there is no way back, so you need to think very carefully about how and where you store your recovery Seed.

Why you need to protect your recovery Seed

Now you understand what the function your recovery Seed serves, it should hopefully make it clear why you need to safely store it. If you lose access to your custodial wallet, your Seed is your only recovery path. It represents the entire value of the funds stored in the wallet.



How might you lose access to your crypto wallet?

Non-custodial wallets can come in many forms - Browser Wallets, Mobile Wallets or Hardware Wallets. Each of them has similar vulnerabilities which can mean you lose access to your crypto funds.

- You might delete the App/Software/Extension by accident.
- Your phone/laptop/device, might break, be lost or be stolen.

Don't think it won't happen to you

In each of those scenarios, your funds might be lost forever without your recovery Seed. You might be reading this and thinking, “that won't happen to me”. That is what is known in behavioural psychology as ‘normalcy bias’ - the tendency to underestimate threat warnings.

Unfortunately, normalcy bias extends to attitudes toward information security. In late 2021 Google started enforcing the use of two-factor authentication because its own data suggested only 10% of users had activated 2FA despite its effectiveness in reducing the most common threats to your personal data.

“A [joint study](#) by Google, New York University, and University of California San Diego found that MFA can thwart up to 100% of attacks coming from automated bots, 99% of bulk phishing attacks, and around 66% of targeted attacks.” From [Bleeping Computer](#).

Normalcy bias can explain the reluctance to use sunscreen or wear a cycling helmet. It is also one of the main reasons why cybercrime is so rampant, and why newcomers to crypto ignore the importance



of safely storing their recovery Seed.

Some estimates suggest that [up to 20% of Bitcoin's Total Supply are lost forever](#) amounting to almost 4 million of 19 million coins that have now been mined, with a staggering value of over \$160bn at current values.

The fear of losing a recovery Seed pushes many crypto investors to opt for the custodial wallet option, though that puts their funds in someone else's control and opens up a bigger list of potential threats.

The challenge, therefore, is to provide **a practical and secure way for you to take ultimate responsibility for the list and order of the words that make up your recovery Seed.**

To help you decide how best to store your Recovery Seed we'll walk through the process of how you access it.

How do you access your Recovery Seed?

Let's start by understanding how you access your Recovery Seed in the first place. Remember, not all cryptocurrency wallets allow self-custody, many act like your banking App, giving you access, but retaining ultimate control. Those that do are known as HD Wallets - Hierarchically Deterministic.

HD wallets simplify crypto security for the end-user because they present the complex cryptography that protects your cryptocurrency



in the user-friendly form of the Seed.

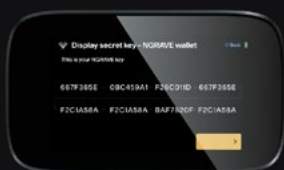
So when you set up/install a new HD wallet it will generate the Recovery Seed as part of the process. This is generally in the form of 12-24 unique ordered words, though NGRAVE use our own special Perfect Key, combining letters and numbers with a high level of entropy (randomness) by incorporating inputs specific to the user and their environment - fingerprint and local light. Read about that process [here](#).

When the Seed is generated you'll be prompted to make a record of it, then confirm this by entering a few of the Seed words based on their position in the order i.e. *'Please enter words 4, 7 and 9 from your Seed'*.

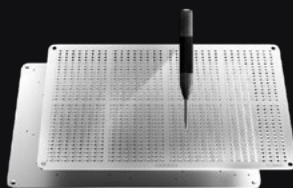
How do you access your recovery seed?

1. Generate a recovery seed in your non-custodial wallet
2. Make an offline record of it
3. Store securely and use when your wallet is lost or broken

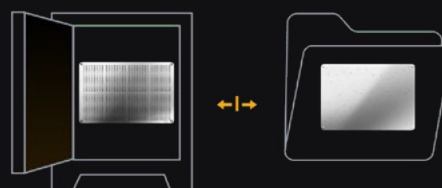
1.



2.



3.



Your wallet will automatically derive all your crypto addresses from that recovery Seed. It means you don't have to care about storing the individual Private Keys which protect each address on the blockchain, just the Seed, which unlocks all of them.

Hierarchically Deterministic wallets were first introduced in 2011 in Bitcoin Improvement Proposal ([BIP 0032](#)), and later applied to other cryptocurrencies through [BIP0044](#), three years later. Seeds are drawn from a standardised list of 2,048 words determined in another Bitcoin Improvement Proposal ([BIP 0039](#)).

Having generated the Recovery Seed there are some obvious ways you might initially consider storing it, which on reflection turn out to be bad ideas.

How Not To Store Your Recovery Seed

Don't store your recovery Seed on a device that is connected to the internet as that could be compromised. That includes Password Managers, Google docs, Text files, Digital photos, Emails or USB Sticks.

Don't even type your recovery Seed out on a connected device as key tracking software could compromise it.



Don't print your recovery Seed, or take a photo of your recovery Seed, as that creates a copy in the device memory which might be compromised.

Don't split your recovery Seed up into two or more sections, and separately store those. This will just double your chances of losing it.

Don't travel with your recovery Seed, this will increase the risk of loss or theft.

Don't try and memorise your recovery Seed, our brains are only optimised to remember seven pieces of information, which is why car registration plates and telephone numbers use seven characters.

Don't jumble the order of the words; a Seed has to be recovered in the order it was created.

Don't add decoy words to your recovery Seed, or store a partial list online. Recovery Seeds are generated from standardised dictionaries so decoys would be easy to spot and partial lists broken by brute force.

Don't write your recovery Seed on a standard piece of paper. Paper is easily lost or destroyed by fire, water, insects or heat.

Having read the list above you might be wondering what options could possibly be left. There aren't many options, which actually make your life easier.



How to store a recovery Seed

Imprint your recovery Seed on a material that is resistant to fire, water and the elements. The most popular option is a stainless steel sheet combined with a punch pen or embossing tool. Store the sheet in a safe place and don't tell anyone.

Write it on special paper that is water-resistant and non-shreddable; ideally, store that paper in a fire-proof strongbox.

The reality of generating a Seed means that it might not be practical to do this straight away. In that case, you might use a standard piece of paper as an initial record, which you then burn once you've transferred it to something more resilient.

The NGRAVE approach to storing your Seed

As part of our focus on security, the NGRAVE ZERO hardware wallet comes as standard with our waterproof, non-shreddable, paper, but we've developed a far better solution to Seed storage if you're prepared to invest a little more for peace of mind.

NGRAVE's backup solution is GRAPHENE, consisting of two stainless steel plates - resistant to temperatures up to 1375°C (2507°F), water, corrosion damage and shocks. The steel sheets are used



to physically imprint a 64 character pattern - the equivalent of the Recovery Seed list - generated from a combination of numbers and letters. We call this **the NGRAVE Perfect Key**.

One plate is a blank piece of stainless steel, while the other is a grid consisting of 64 columns, each with 16 character options (0-9 & A-F) and holes, for a total of 1,024 positions.

The grid plate fits exactly onto the blank sheet, and the user punches the Seed generated by the ZERO during set-up, through the corresponding holes in the upper plate, embossing the Seed onto the lower plate.

A pen is provided featuring a click mechanism that automates the physical power exertion required to “punch” the hole in the lower GRAPHENE plate without damaging the upper one.

Given the user interaction in the Seed generation (mentioned above) NGRAVE has no way of knowing what the key is or might be, as the difficulty of guessing it by brute force becomes too high. The order of hexadecimal characters within the columns is unique to each plate so there is no way to have prior knowledge of the upper GRAPHENE template.

The use of two plates enables the Seed to be split into two parts, which on their own are agnostic and reveal no detail of the Seed, but still allow for an ingenious recovery mechanism in case the user loses the upper template.



Even with the unique approach to Seed storage that we have taken with the GRAPHENE, there will always be an element of personal responsibility. Security comes down to how seriously you take that role. Your crypto is worth far more than the flimsy piece of paper your Seed might be written on, so it is definitely worth considering an alternative for the safe storage of your funds.

If you're worried that your Seed security would mean your funds die with you, NGRAVE's GRAPHENE provides options to handle inheritance. You could, for example, disclose the separate locations of the upper and lower plate in a will, managed either by a traditional notary, a blockchain notary system (e.g. upon death certificate, the blockchain can release the locations).

No inheritance option for a Recovery Seed is simple or without some counterparty risk, because the reality of taking full control of your crypto means responsibility stops with you.

Now you know how to store your recovery Seed you should see this as a feature and not a bug and can embrace the opportunity to be in control of your wealth, acting accordingly.

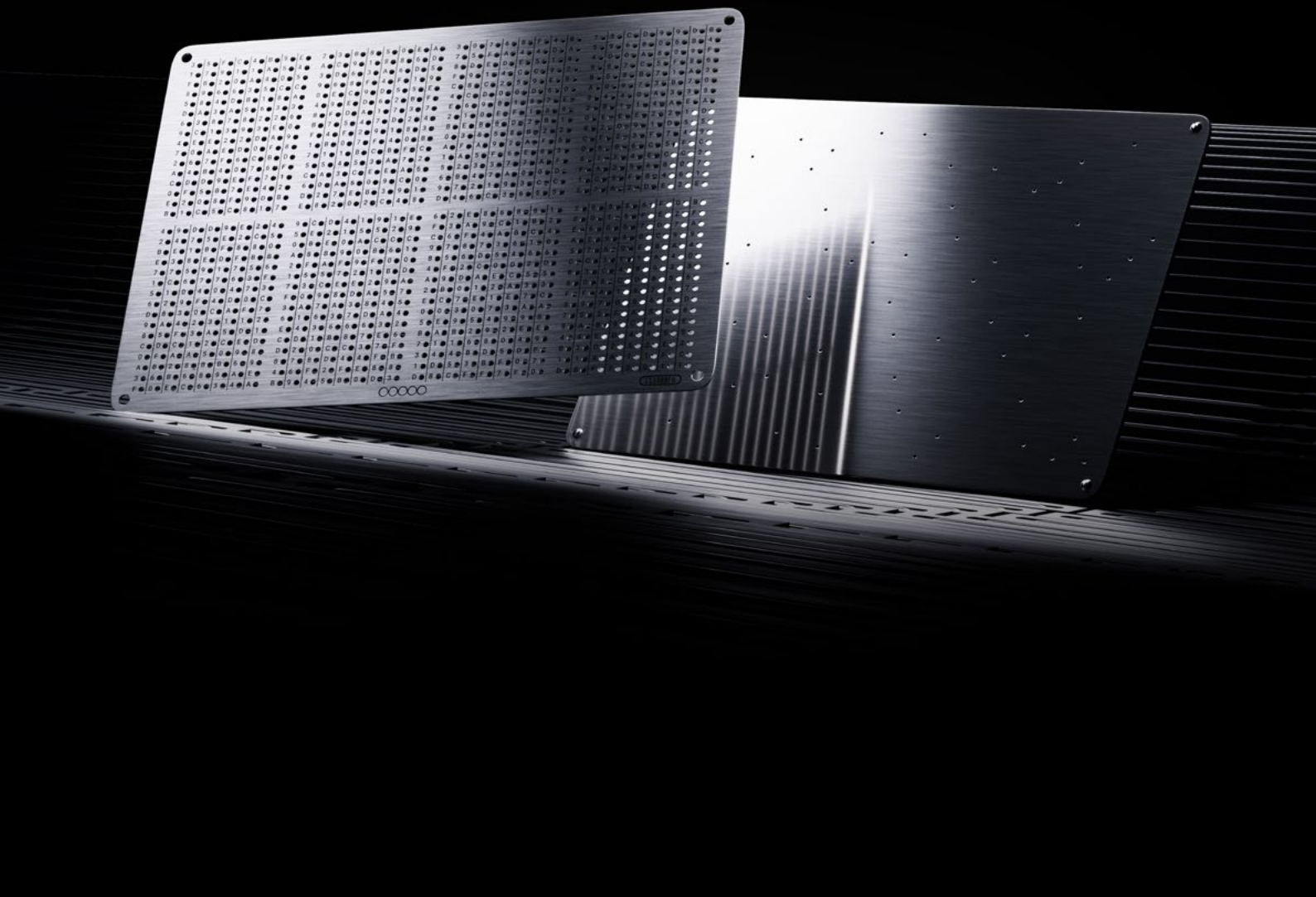
Great overview, but how do I explain it to a friend?

A recovery Seed is the ultimate failsafe for funds stored in a crypto wallet. As it is in the form of a list of 12-24 short words the most popular storage options are within an online document or written on a piece



of paper. Both are insecure. If you're serious about protecting your crypto think about more secure solutions such as the GRAPHENE steel plate option offered by NGRAVE.

The Ultimate Backup



4 Moving Funds From A Hot To A Cold Wallet

Having absorbed all the advice in the NGRAVE Academy, you decided to take the plunge and move your crypto from a hot wallet to cold storage. Your brand-new hardware wallet has landed on the welcome mat. Now what?

A primer on Hot & Cold Wallets

If you're interested in knowing how to move your crypto funds from a hot to the safety of a cold wallet you should be clear on what those terms mean, and why it makes good sense, so we're going to start with a quick primer. You can always jump to step 1 of the actual process if you feel this is overkill.

A wallet is a tool for managing your crypto but doesn't actually store any digital funds, just as your banking App doesn't store any money.

It is an interface to public cryptocurrency blockchains; ledgers of addresses of spendable cryptocurrency. Think of an address like



a bank account. A wallet will create new addresses for free, and display an associated balance of spendable crypto that has been sent to that address.

What makes the funds spendable, is the control of a Private Key that is created for every address generated by the wallet.

Given Private Keys give complete control over funds, they are encrypted by the wallet, but to make their management easier, are aggregated into one piece of information - like a master key/ password - called a recovery Seed. This is normally in the form of a collection of 12-24 mnemonics - unique words.

A recovery Seed is an ultimate fail-safe. It proves you have the right to spend the funds associated with all addresses created by a wallet; the wallet is just a medium for providing that access, so it doesn't matter if you lose access to the wallet, so long as you have the recovery Seed.

Most new crypto users start their journey by purchasing crypto via exchanges using their desktop browser or a mobile app which features wallets that control those Private Keys on the user's behalf - the term used in *custody*.

Crypto's most important mantra is 'not your keys, not your coins' because of the risks of those custodial services losing control of Private Keys to hackers. There is, unfortunately, plenty of evidence of that happening.



So moving from a custodial wallet to one you control will give true ownership over your crypto, but it will also make it more secure, because you have to be online to access a custodial service, providing convenience at the expense of security. This is what the term Hot Wallet describes, a service that is online by default.

Hot wallets are software-based and accessed through a mobile app or website, while a cold wallet is a small, physical piece of hardware.

Hot wallets can be non-custodial, giving you control of your keys, but you are still online and therefore face constant threats.

The alternative is a Cold Wallet - also described as Cold Storage - which is offline by default, and therefore stores all Private Keys locally, so not only puts you in control but provides the security of being offline.

If you're still not entirely clear on custody and the distinction between hot/cold wallets, take the time to read these articles first.

Though cold storage can theoretically include Paper Wallets, we're going to assume that what we're discussing here is a physical hardware device. Head over to this separate article if you want to hear a convincing argument against Paper Wallets.

We'd hope that you've chosen to invest in the NGRIVE ZERO, as we believe it is the most advanced and secure cold storage device on the market, but our advice can apply regardless of your preferred vendor.



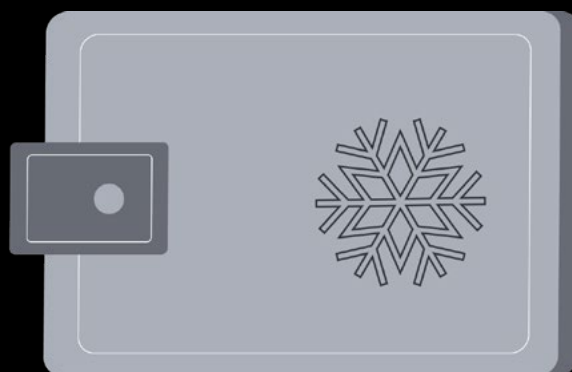
We will, however, highlight features that the ZERO offers that might not be available elsewhere, simply because we've followed what we believe is the best practice for offline storage in making it, and want to share our thinking.

Step 1

Make sure your Cold Wallet hasn't been tampered with



**Verified
Hardware**



The process of safely sending funds from a hot wallet to cold storage for the first time begins before you have even unboxed your new hardware device, by ensuring it hasn't been tampered with.

This may seem like scaremongering, but not only are there cases of devices being tampered with, there are even [examples of users being sent so-called 'replacement' devices](#), which have been doctored, in order to steal funds.



If you have purchased an NGRAVE ZERO there are three levels of tamper protection and a separate cryptographic attestation - a key, verified by NGRAVE, that must be entered by the user to prove the device's authenticity:

- **Tamper Proofing** - The design of the device makes tampering practically impossible
- **Tamper Evidence** - If tampering is attempted it will become obvious
- **Tamper Response** - If someone tries to tamper the device will wipe itself

It isn't enough to check the seal hasn't been broken on the package, as in some countries this can sometimes happen for legitimate reasons, depending on how postal security operates.

Step 2

Make sure your Cold Wallet hasn't been tampered with



It is natural with any new piece of technology to want to skim through the setup process, and just begin using it, with the vague intention of doing the full set-up, and a proper read of the instructions at a later date.

The setup process for a crypto hardware wallet is so important that you cannot afford to do that.

When you use your hardware wallet for the first time the device will prompt you to set the appropriate language and set a standard access pin, similar to accessing your phone.

Make sure to remember the pin, but avoid keeping a digital record of it ([NGRAVE's ZERO](#) requires two-factor access and biometrics, which add extra security). Repeat failed attempts of your pinfall under the 'emergency' category for which you'll need your recovery Seed, the critically important part of the set-up process that follows.

Should you lose your device, or it stops working safely, the recovery Seed is the fail-safe for accessing funds, so storing safely is of paramount importance. This is why the NGRAVE Academy dedicates a lot of attention to Seed Storage best practices.

The most common approach is to write a Seed on a piece of paper, then find somewhere safe to store it, but as paper isn't the most resilient material, the ZERO ships by default with a non-shreddable, water-resistant, Seed recovery sheet.

This is still far from optimal, given how important your Seed is,



so NGRAVE recommends using our [GRAPHENE](#) solution. It is a combination of two stainless steel plates and a punch pen, that will enable you to emboss what we call our Perfect Key, because of the additional efforts to ensure that it is randomly generated.

Whatever approach you decide to take to storing your recovery Seed, be aware that the security of any funds stored using the device will ultimately rely on how and where your Seed is stored.

Once you've established a safe way to store your recovery Seed it should only be needed in an emergency, or if you forget the standard access details required to access the device and companion software, which is the next step.

Step 3

Downloading the companion software



A hardware wallet is purposely small and discrete, and not intended for extended online use as a dedicated interface/wallet dashboard. Though the ZERO features a large high pixel density colour LCD screen, it's designed that way simply to make device set-up easier and to simply confirm transactions, which along with all-over wallet functions, take place via a connected companion software running on your mobile or computer.

You'll need to download the appropriate companion software for your device now. Pay very close attention to downloading the genuine software, either by using the QR codes provided with the device for the Mobile App or for desktop by visiting the official website - double checking the URL and ensuring its security .

The companion software will allow personalisation, the most obvious being the language setting and fiat currency that you want your wallet balances to be displayed in.

Be aware that because using and updating your companion software requires you to be online, this may put your funds at risk. The NGRAVE ZERO has gone to great lengths to ensure Private Keys are never shared by using a companion software - [LIQUID](#) - that uses QR codes to share address details.

The ZERO is also manufactured to ensure that updates to the companion software [cannot introduce malware to the device operating system](#). It is worth looking into how your device guards against infections during software updates.



Step 4

Organising your wallet ready to receive funds



Most crypto hardware wallets will support all popular coins as standard, you simply need to open the companion software and select the relevant coins you want to store on the device and confirm the addition. If your coin isn't supported, you may need to follow manual steps.

Be careful to add the correct coin/network combination for the funds being sent, as many coins function across multiple distinct chains.

When you add coins, you may want to establish multiple accounts for certain coins, separating funds for trading, saving, family members or tax, depending on how active you are.



We are going to assume this is the first time you are moving funds from an exchange, crypto banking provider or App, so will cover all steps from scratch. Depending on the service used, and their policy around withdrawals, this might take a little longer than expected.

In order to move funds from your Hot Wallet to the safety of your Cold Storage device you need to find the destination address for the appropriate coin in your Cold Wallet - this is where funds are being sent.

If you are sending from a desktop Hot Wallet you'll need to use the copy/paste function for the destination address (usually an icon next to it).

If you are sending from a mobile Hot Wallet you scan a QR code.

Once you've added the destination address to your Hot Wallet give it an appropriate label e.g NGRAVE hardware wallet.

If you are using the copy/paste approach take care, as it is easy to make an error. Never rely on manually typing the address. Given certain viruses try to target clipboard modules, run a full virus scan before making the transaction.

Once you have added the destination address to your Hot Wallet, visually compare the first/last few characters to ensure it is correct, then save it.

This is the part that may take longer than expected because some



Hot Wallet services enforce a 24-hour cooling-off period before a new withdrawal address can be used. It is a security feature, generally described as *Whitelisting*, ensuring that withdrawals only go to safe addresses, so plan ahead.

If/when you repeat the process of sending funds you should use a new address each time, as this is good security/privacy practice. Your Cold Wallet should create unique addresses automatically for you, and it won't impact your account set-up because a wallet can generate an unlimited number of individual public addresses from something called an *xPub key*.

Those public addresses can be shared and considered as single-use destinations for funds, which will appear as one balance in your wallet, by reference to the xPub Key.

Sharing your xPub key is inadvisable simply because it allows someone to know the value of all your funds, whereas a single address provides details of just one transaction.

An xPub key is different to a Private Key, and cannot spend funds. It is available within your wallet settings and may be needed when, for example, you use an online service to calculate crypto taxes but otherwise should be rarely needed.



Step 5

Moving Your Funds From Hot to Cold



Once your withdrawal address is active you are ready to create a transaction to move funds from your Hot Wallet. Here are a few things to bear in mind when filling in the actual details of the transaction itself:

- Make sure the address format is the same for the sending/destination address; Bitcoin has different formats for example related to Segwit.
- Some coins such as XRP, XLM, EOS & Cosmos require a piece of information in addition to the address called a Tag or Memo. Make sure to copy this from your destination address.



- Be aware of minimum withdrawal fees charged by the Hot Wallet as this determines the smallest amount that is economical to move.
- If you are sending from a non-custodial wallet you'll generally have three speed/cost options for Ethereum and Bitcoin. Make sure you have enough funds to cover the required transaction fee.

If you are moving a significant amount, and this is your first time moving off an exchange, it is good practice to make a small test transaction first. You will pay more in fees but it will at least reassure you that the funds aren't being sent randomly into the ether.

Enter the required amount to withdraw, double-check all the details twice and then hit Send. You will likely be asked to confirm a further security step which may differ depending on how your Hot Wallet is set up, such as:

- Input your password
- Add a 2FA code
- Click a link sent to the email address registered to your account

Once you have added the required security detail, your withdrawal will be in a pending state as the network validates the transaction. If this is your first time moving funds to Cold Storage you may feel a little nervous. The time it takes to reach the destination address will vary depending on various factors:



- The Hot Wallet service
- The coin being moved as block speeds vary, Bitcoin being the slowest
- The level of fee you paid

If you want reassurance, there will be details available for the withdrawal which usually includes a link to a [block explorer](#), which can show you how the blockchain is validating your transaction.

If there isn't a link, there should be a transaction ID which you can manually paste into a free block explorer, and visually confirm that your transaction is being confirmed.

Your destination Cold Wallet dashboard should also show you that a transaction is incoming, but pending full confirmation, at which point you can let out a sigh of relief.

Once the transaction is fully confirmed, double check the amount is correct, accounting for the transaction fee, and then you can repeat the process or simply disconnect the device.

Congratulations, you have successfully moved funds from your Hot Wallet to a Cold Wallet, and can now sit back and relax with the knowledge that they are safely offline and in your complete control.



5 How to Secure Your NFTs

If all the threats posed to storing your NFTs on hot wallets or exchange accounts leave you in a cold sweat, this is the unfortunate reality of the internet, and in particular, the allure that crypto has for hackers.

The explosion of interest in NFTs has brought a whole new cohort of users into the crypto space. That interest is often driven by FOMO which when combined with inexperience provides fertile ground for scammers and hackers. Given NGRAVE's focus on crypto security, we've summarised the best ways to protect your NFTs.

Investing in NFTs is a risky business as the valuations aren't really grounded in fundamentals. So even before you get to the point of worrying about how to safely store the NFTs you own, you should ensure you've done enough due diligence in the buying process.

Plagiarism, fake provenance, uncanceled listings and Rug Pulls are just a few of the risks posed during the buying process, which we've covered in a separate article in the NGRAVE Academy.



Understanding NFT Storage

Once you have negotiated the minefield of buying an NFT you cannot drop your guard because depending on how you store your newly purchased digital asset can expose it to the risk of loss and theft.

When we talk about the risks of how you store an NFT there are two distinct components:

- The physical location of the asset itself e.g a JPEG, Song or Document
- The token recorded within a blockchain that proves ownership of an asset

The asset itself is very rarely stored within the blockchain because of the storage issues that would create in bloating the blockchain. Instead, the token points to its actual location on the web, so it is important to check how robust and decentralised that storage process is. If it sits on a single server outside of your control that NFT could simply be moved or deleted.

The most common decentralised approach is to use IPFS (InterPlanetary File System) but even this doesn't guarantee that your NFT is hosted across a network of server nodes.

[This Coindesk article](#) does a good job of explaining why that is, but the bottom line is that before buying NFTs you check how and where the file of an NFT reference is actually stored.



From here on, when this article talks about safe NFT storage we are referring to the storage of the token; the digital record of ownership within a blockchain protected by a Private Key.

Storing NFTs On Marketplaces & Exchanges

The most common way to acquire NFTs is through marketplaces like [Opensea](#) or [Rarible](#). They facilitate the minting and exchange of NFTs charging a fee for the service, functioning like centralised crypto exchanges but with one key difference.

Storing NFTs On Marketplaces & Exchanges

When buying an NFT on a marketplace, you are transacting directly with the underlying blockchain. The marketplace only facilitates the transaction and never takes possession of the NFTs.



When you buy an NFT on a marketplace you are transacting directly with the underlying blockchain. The marketplace simply facilitates the transaction and never takes possession of the NFTs. Instead of creating an account directly with the marketplace, you connect to it using a crypto wallet like MetaMask.

This means that hot wallets like MetaMask are the single point of failure once you've bought an NFT on a marketplace because that is where they will be stored after purchase.

Though you access MetaMask on a day-to-day basis through the normal security features of your browser/device, such as a password and/or biometrics, the ultimate failsafe against loss or theft is a single piece of information, called a Seed.

Your MetaMask Recovery Seed is a collection of 12 mnemonics, memorable phrases, that when recorded in a specific order, are a convenient way to represent the much longer random string of numbers and letters called Private Keys associated with individual assets.

In the event of losing regular access to either the app or your device, your Seed is your only fallback. If your Seed ends up in the hands of thieves you can kiss everything in your wallet goodbye.

So if you store your NFTs on a hot wallet, you have to learn how to **protect your Seed**.

Given the explosion in interest in NFTs, exchanges like Coinbase,



Binance and Crypto.com are increasingly offering marketplace functions but their centralised model means they directly custody your assets. This means the risks to your NFTs on exchanges are twofold; you have to trust that exchange won't get hacked, which is unfortunately common, and you also have to **protect your login credentials from hackers.**

In both cases - protecting your Seed and login credentials - you are at risk simply for being online and the safety of your NFTs is, therefore, only as good as your general OpSec - Operations Security.

The threat from poor OpSec

[The subreddit](#) dedicated to the subject of OpSec does a great job of defining what that means: “*OPSEC is the process and practice of Operations Security...[it] is a mindset of critical thinking and safe habits.*”

Critical thinking requires you to constantly consider how your information might be at risk thinking from the perspective of a hacker, which is quite a steep learning curve. Safe habits are a bit easier to summarise:



Crypto-Safety Best Practices

Always enable 2FA for account-based services and not text messages



Use strong passwords unique to each site and a specific email just for crypto activities



Automatically update your browser & operating system



Use a wifi-only mobile phone just for crypto activity at home.



Bookmark the official websites and services you regularly use



Don't identify yourself as an NFT owner on social media



Don't click on random links or attachments



Use reliable anti-virus software



Automatically update your browser & operating system

Browsers and operating systems aren't foolproof. They are constantly updating and patching to improve both user experience and security. Given wallets like MetaMask work through your browser, that can create a direct threat.

Make sure to set both to update automatically. Chrome announced [three zero-day exploits in the first four months of 2022 alone](#). Zero-day means a vulnerability hasn't been communicated or is public knowledge but with no fix.



Always enable 2FA for account-based services using an App or hardware device, not text messages

If you store your NFTs on a centralised service be certain to use two-factor authentication and don't use text-based services. Scammers have become unbelievably sophisticated in the ways in which they can replicate your SIM, in order to intercept the verification code - known as SIM Swapping.

You can mitigate that risk by using App-based 2FA services like Google Authenticator or Authy, better still use 2FA hardware devices like Google Titan or Yubico.

Use strong passwords that are unique to each site and a specific email address just for crypto activities. Not only will this reduce the risk of unauthorised access, but also make SIM Swapping harder. Getting hold of a copy of your SIM is just one part of the process of gaining access to a centralised account storing your NFTs. The attackers also need your account and email credentials.

There is a huge underground market for login credentials that have been harvested from data hacks. You may not even be aware that your details were exposed - go check on <https://haveibeenpwned.com/>.

You might not care if some crummy forum you once used years ago got hacked but hackers will use that information and assume that it might also work elsewhere. They will also harvest anything that data tells them about you in order to more successfully impersonate you.



As Reddit says, security is a mindset. You have to think like a hacker.

Consider using a second wifi only mobile just for crypto activity at home. This will limit the risk that your phone is lost or stolen and can minimise the online threats because the only activity you'll be doing is specific to crypto.

Don't identify yourself as an NFT owner on social media. Flexing might be part of the attraction of owning NFTs but you are putting a target on your back.

Use reliable anti-virus software, schedule regular scans & make sure the virus library automatically updates. Most virus software will guard against unsafe downloads and attachments and fake sites, as well as scan your wi-fi but don't assume that your virus software will make you bulletproof.

Bookmark the official websites and services you regularly use to minimise the chance that you can be tricked into using a spoofed site, or downloading a fake app that will harvest your credentials or sweep your wallet.

Don't click on random links or attachments. Assume that every click or tap you make could be opening the door to an online attack and exposing your NFTs to risk.



Man In the Middle Attacks

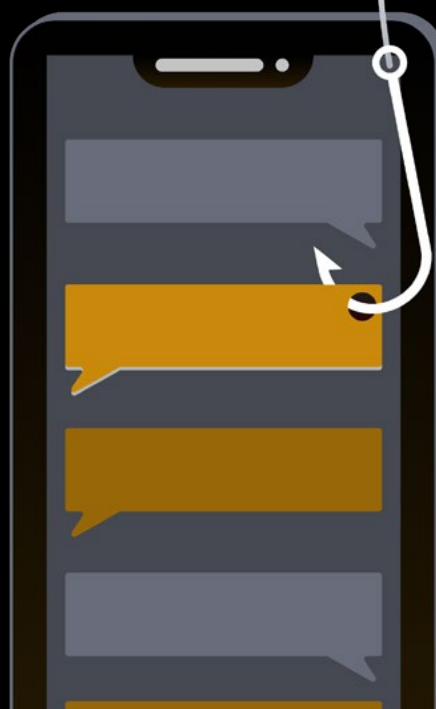
By being online you are constantly exposed to malware with a wide range of intents but one that is of specific danger to NFT transactions is the *Man In The Middle Attack*.

Man In The Middle Attacks

Definition: A cyber exploit where a hacker intercepts or manipulates information, as it passes between two parties.



If your Hot Wallet allows it, use address Whitelisting.



In order to send or receive wallet transactions, you need to share address details, often using chat services and/or your device clipboard. The Man In the Middle attack relies on compromising the clipboard module - on a laptop or smartphone - and using the remote access to intercept/replace the shared address details with details of their own choosing. A Trojan called [Cryptoshuffler was doing the rounds in 2017](#), to achieve precisely this.



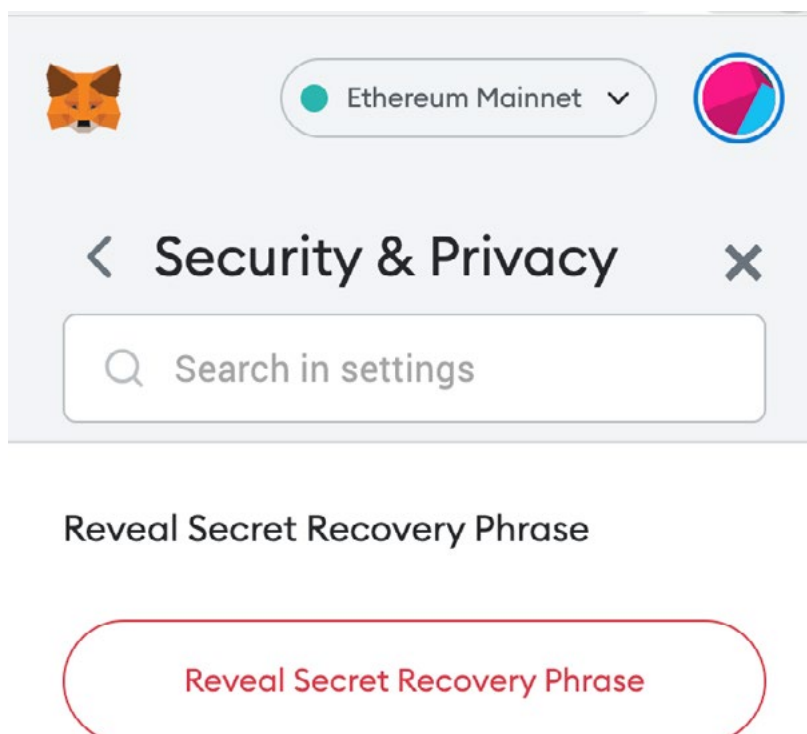
Mitigating the threat

Always double-check the recipient address to ensure it is correct by scanning the first/last few characters.

If your hot wallet allows it, use address Whitelisting, which puts a 24hr restriction on using newly added withdrawal addresses; note MetaMask doesn't enable this feature.

The risks of Social Engineering

Finding your way around the NFT space and understanding how to transact can be confusing for a beginner. It is frighteningly easy to expose your Metamask Seed requiring just three clicks, Settings > Security & Privacy > Reveal Secret Recovery Phrase and your password.



Scammers will try and exploit inexperienced users through what is known as Social Engineering; using psychological manipulation to trick you into revealing your Seed.

One of the most common approaches is listening for requests for help from NFT holders - whether within a Metaverse platform, official Discord or external Social Media.

Scammers will pretend to be part of the official support team, and engineer a reason for you to expose your Seed under the pretence of fixing the issue.

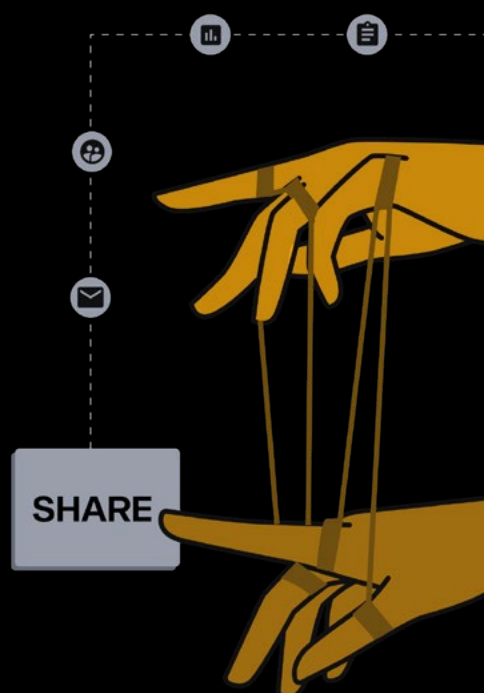
They may go as far as creating fake Discord servers and using what looks like official support accounts, to coerce users into sharing their Seed to help resolve their issue.

Social Engineering

Techniques using direct interaction, not software, to trick an individual or an organisation into providing sensitive information (i.e. Seed phrase).



There is no legitimate reason to ever share your Seed phrase.



Social Engineering works because of well-rehearsed manipulation. Several scammers will work together trying to disarm the target with friendliness then suddenly change pace and create a sense of urgency which is designed to push users to act without thinking.

The scammers will try and convince you that sharing your screen will speed things up and within moments your NFTs will be gone.



Even experienced users can be convinced to act against their best instincts because making money from investing in NFTs can often come down to speed and scammers know this.

OpenSea, the largest NFT marketplace, had its Discord server hacked in May 2022 allowing the intruders to promote a fake Youtube partnership in a series of posts that ramped up the FOMO claiming that 70% of the supply of the fake project had already gone.



OpenSea is just one of several high-profile NFT marketplaces and projects to have had their Discord or Social Media hacked, including [Bored Ape Yacht Club](#), Doodles and KaijuKings.

With access to your Seed a scammer can drain all the funds already in your wallet, but if there is little value, they might try and use a malicious script to intercept transactions.



If they can successfully infect your wallet with the so-called Sweeper Script without you knowing, they will patiently wait to divert future transactions to their address, rather than the genuine recipient.

Other forms of Social Engineering may try and convince you to transfer NFTs as part of some promised exchange, before disappearing or offering a wallet recovery service for anyone who loses their Seed.

Mitigating the threat

There is no legitimate reason why any person, or service, should ever ask you to reveal your Seed. Knowing this should make it easy to detect scams, but here are some things to be aware of:

- Only ever use official support channels - double-check account details
- Be very suspicious of anyone approaching you out of the blue, especially via DM
- Unprofessional language is another red flag
- Scammers may create dApps that look harmless enough but will ask for your Seed

How to have convenience & offline security

If all the threats posed to storing your NFTs on hot wallets or exchange accounts leave you in a cold sweat, this is the unfortunate reality of the internet, and in particular, the allure that crypto has for hackers.



You have to balance the convenience against the risks. Fortunately, there is a middle ground, because a crypto hardware wallet like the [NGRAVE ZERO provides cutting-edge offline security](#) AND the ability to store, send and receive NFTs without exposing your Seed.

The clever use of QR codes, and a companion mobile App - LIQUID - give you the best of both worlds: the convenience of online transactions but with the security of offline storage.

Like MetaMask, hardware wallets are non-custodial so one of the most important security steps to add to your list of best practices is to store your **Seed offline somewhere safe**.

It might seem like a natural thing to do but storing your Seed online ramps the security threat to your NFTs right up. If hackers get access to your devices from any of the methods listed above, they know where to look to find Seeds and what to look for in terms of file names and formats.

Unfortunately, there is a steady flow of people who don't store their Seed offline, lose access to their wallets and then become victims of the Social Engineering mentioned above. Scammers will monitor via social media for targets, using multiple stooge accounts to create an air of credibility, then request upfront payment, and disappear without delivering any service.

No Hot Wallet or crypto exchange can ever be 100% safe because being online automatically means you are vulnerable. You can mitigate the risk through due diligence, security best practices and



simply being vigilant, but the simple truth is that there is no better way to protect your NFTs than cold storage.

The Coldest Wallet



Get the latest crypto-security tips

Subscribe to the
NGRAVE [Blog](#) & [Academy](#) newsletter

