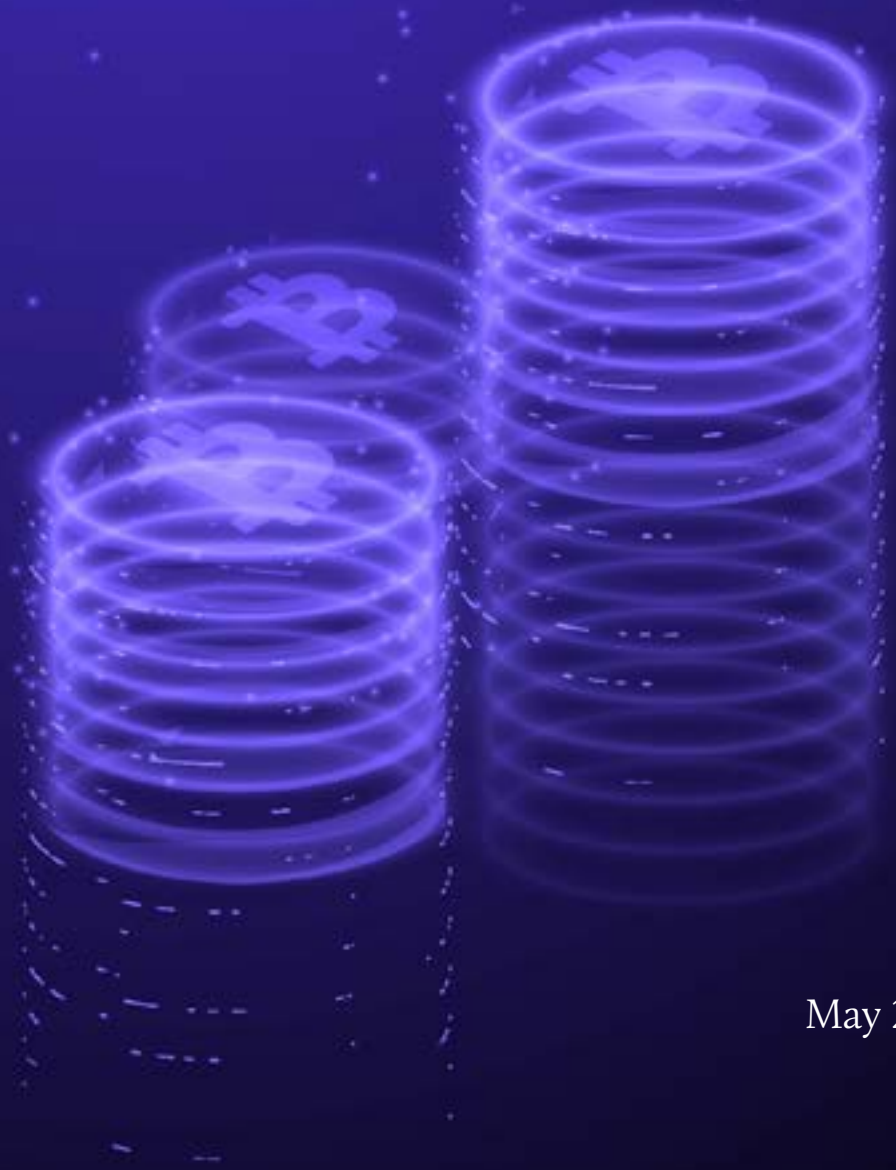
kraken INTELLIGENCE x SECURITY LABS

Wallet Security 101

How to Store Your Coins



May 2021

Table of Contents

1.

Introduction

So you recently bought some crypto and you're ecstatic about it. However, you're new to the space and remain uneasy after hearing horror stories of people losing fortunes just by making mistakes as silly as losing the password to their crypto wallet. Moreover, you can't seem to find any reliable resource that simply explains how to securely store your newly-purchased coins. The truth of the matter is that the crypto space has changed significantly in the past several years and nowadays you don't need to go down the same rabbit hole others had to venture when previously attempting to store their cryptoassets. As such, the leading experts from both Kraken Intelligence and Kraken Security Labs have teamed up to provide you with simple, honest advice on how you might want to store your crypto. Do note that what might work for you may not work for someone else. As such, it's important that you carefully consider the pros and cons of how you ultimately decide to purchase, store and transact with your crypto. After all, if you lose your crypto it is gone forever!

2.

Where to Store Cryptoassets?

Because cryptoassets are more decentralized than traditional assets, holders must take precautionary measures to protect against the risk of either loss or theft. Remember, once your crypto is lost, it is gone forever. Common examples of how crypto has either been lost or stolen include the following:

Loss

- Human error
  (e.g., you send your funds to the wrong wallet, you forget your password)
- Natural disaster
  (e.g., your house burns down with your crypto wallet(s) stored inside it)
- Hardware malfunction/loss
  (e.g., your computer hard drive holding your private keys is corrupted)

Theft

- Remote theft
  (e.g., you fall victim to scams, an exchange hack, or a personal hack)
- Physical robbery
  (e.g., your backpack or purse is stolen with your private keys in it)
- Government seizure
  (e.g., law enforcement demands an exchange to freeze your account)

Wallets

Cryptoassets are stored in wallets, which are computer programs that allow crypto to be sent or received. Depending on whether the wallet is connected to the internet, crypto wallets are bucketed into two categories: “hot” (online) or “cold” (offline).

Hot Storage (Online)

Hot storage wallets exist on an internet-connected desktop, laptop, mobile phone or web browser. These wallets are popular because they can be easily created and used instantly. Hot wallets sacrifice some safety for convenience since the wallet is connected to the internet and is therefore readily available for use. Like anything connected to the internet, this also makes the wallet vulnerable to cyberattacks.

Cold Storage (Offline)

Cold storage wallets exist on devices or physical media that are not connected to the internet. Examples include paper/metal with crypto key material written/engraved on it and hardware wallets that look like USB flash drives. Cold wallets are safer than hot wallets because private keys are generated and stored offline where they can't be accessed by cybercriminals – although they can still be stolen in a physical attack or robbery. However, cold wallets usually aren't as readily available for spending as hot wallets.

Exchanges, like Kraken, use both hot and cold wallets. Some funds are always available for immediate use (in hot wallets) to facilitate day-to-day transactions, while the majority are stored offline for safekeeping (cold wallets). You will want to use a reputable exchange that utilizes both hot and cold storage so you can be sure that your assets are properly secured.

There is no perfect solution for storing crypto as there are a series of tradeoffs that may change for each individual at different fund amounts. However, that shouldn't scare you off. In storing your crypto, you should take your own personal financial situation and risk tolerance into account. Kraken Intelligence and Kraken Security Labs suggest that, depending on the purpose behind owning your crypto, you consider one of the following strategies:

Figure 1

The Hodl Matrix[1]

	Tier 1 **Pocket Satoshi**	Tier 2 **Hodl Hobbyist**	Tier 3 **Lifetime Stacker**
Description	First time buyers or those with smaller amounts of crypto.	Market participants that are familiar with the technology and want to store their own crypto.	Those storing generational wealth.
Amount[2]	$1 - $10,000 in crypto, or a small amount of your net worth. Loss of this would be like getting scammed.	$10,000 - $200,000 in crypto, or a modest amount of your net worth. Loss of this would be like a criminal draining your savings account(s).	More than $200,000 in crypto, or a substantial amount of your net worth. Loss of this would be akin to a hurricane destroying your house.
Strategy for Consideration	Leave your crypto on the most trusted, well established exchange(s).	Store your crypto on a hardware wallet, place a backup in a safety deposit box, and put small amounts on a smartphone for daily use.	Securing this amount of wealth is likely to justify bank-grade security by way of a trusted custodian, multisig wallet technology, and/or full nodes. Given the complexity of this strategy, we suggest you consult a professional.

Pocket Satoshi

If you are new to the crypto world and own a relatively small amount, it's okay to keep it simple. It may make most sense for you to simply store your crypto on a major exchange until you become more familiar with the crypto self-custody process. Given the inherent complexities of crypto self-custody, it can be argued that most market participants are *far more likely* to lose funds by simply forgetting their password than to have a hacker steal their funds.

Historically, this was an unpopular strategy because exchanges **regularly had funds stolen by hackers**.[3] Many exchanges these days have market participants that store millions of dollars worth of assets on the platform for extended periods of time. Major exchanges aren't without risk and do not carry the same protections as your bank (i.e. there is no insurance for your crypto holdings), but trusted platforms invest millions of dollars into dedicated professional security teams, utilize a mix of hot and cold wallets, and take other precautions in an effort to ward off attacks. However, exchange users have a responsibility to take the appropriate precautions to prevent their account(s) from being compromised as a result of, for example, a weak password used for your exchange account. Although an exchange may be secure, that doesn't necessarily mean so is your account. Make sure that you're following **security basics** like using strong passwords and securing your sign-in with 2FA to protect your exchange account. [4]

If you want to experiment more with crypto, start transferring smaller amounts onto a smartphone wallet, like Exodus, BlueWallet or BRD, for daily spending. We suggest market participants in this category spend the time to become more knowledgeable of the risks and manage accordingly before moving to a self-custody option. See below for a greater discussion on self-custody.

Hodl Hobbyist

If you hold a good amount of crypto and have a handle on how crypto transactions work, you may wish to take advantage of one of crypto's main benefits: self-custody.

Being in complete control of crypto is liberating, but it comes with a measure of individual responsibility. No one can help you if your crypto is lost or stolen.

How Do Wallets Work?

Crypto wallets function similarly to traditional bank accounts, in that both an "account number" and "password" are required to access the funds held in the wallet. When a user creates a wallet, they generate a unique cryptographic key pair – one public and one private – which allows the user to send or receive crypto.

On most crypto networks, the public key acts as the "account number" and the private key like the "password." In figure 2, we'll describe the three basic components of a Bitcoin wallet. Although there are some exceptions, most cryptoassets, such as ether (ETH), work in pretty much the same way. The following example is for illustrative purposes; please do not send funds to this wallet or claim it as your own – everyone can use it as they have the private key!

Figure 2

Components of a Bitcoin Wallet

Seed Phrase	Any Bitcoin wallet starts by creating a seed phrase. The seed phrase is usually converted into a list of 12-24 words that can be used to back up and restore the wallet. Anyone that knows the seed can drain the wallet, which is why it's critical to **never** type the seed into any computer. **Example of a Bitcoin seed phrase:** valley pulp iron unique pen tired energy crash topic business happy feel
Private Key	From that seed, the Bitcoin wallet generates a public and private key. A Bitcoin private key is a randomly-generated, large number that acts as the password that the wallet requires to **spend** your bitcoin. The wallet automatically keeps track of your private keys. **Example of a Bitcoin private key:** KzJq6FuvJLMDDTRWrkB9RT1JPEDYuFPARrTtsFjr9dVmGFNhWRbY
Public Key	A bitcoin public key is also a large number that is paired with a specific private key. Public keys act as the account number to **receive** bitcoin. **Example of a Bitcoin public key:** 03b859a2b6331328e014e734c889bf99b3c0b92728c13bc5176e8c90780d4487f9
Address	The Bitcoin wallet creates addresses by hashing the public key to shorten it and add some security. A wallet address can then be shared with others to "receive" bitcoin. **Example of a Bitcoin address:** 1GJXxDQAFrQ9LuUj2Y4uSM3J7S8Y7ExKet

Example of a Bitcoin Transaction

1. Alice owes Bob 0.02 bitcoin for remodeling her kitchen
2. Bob sends Alice his public wallet address to receive payment
3. Alice uses her own private key to send 0.02 bitcoin associated with one of her wallets to Bob's public wallet address
4. The 0.02 bitcoin sent by Alice is received in Bob's wallet

What Wallets Should I Use for Self-Custody?

There's a myriad of choices. In making your decision, we suggest that you consider the following:

First and foremost, for most users, it may make sense to use a major hardware wallet (like a Ledger or Trezor). However, note that these hardware wallets aren't perfect. Kraken Security Labs has **hacked multiple hardware wallets in the past**, but we believe they do offer a good mix of security and convenience.[5]

Alternatively, a modern smartphone can be used. Modern smartphones contain security chips designed to keep confidential information private. We believe that regularly-updated versions of Android and iOS are safer than their desktop counterparts. Don't store assets in desktop wallets, brain wallets (i.e., memorized private key), or web wallets (i.e., private key held on a website) as these wallets offer low security in comparison.

Be careful about where you get your hardware or software wallet from. Always order hardware wallets from an authorized retailer and not from second-hand stores, such as eBay, as there have been cases where **bad actors sold infected hardware wallets**.[6] Always confirm you are downloading the official app, as fraudsters have been known to **place imposter apps in the app stores**.[7]

Be sure to also make at least one physical backup of your seed phrase and store it in a secure location, like a personal safe or a safety deposit box. Your seed phrase can be written on paper or engraved into a piece of metal, which can prevent loss due to water damage, fire damage, etc.

Lifetime Stacker

Long-time holders looking to store generational wealth should custody their cryptoassets via more complex strategies, including running a full node to verify transactions, storing funds with a trusted custodian, utilizing multi-signature technology (multisig) to split private keys between trusted third parties, and/or splitting funds between multiple hardware wallets, among others. Therefore, market participants that fall under this tier should consult a professional for an appropriate strategy relative to their financial situation. A solution in this realm probably requires multiple keys to unlock funds (i.e. multisig) in a wallet and might look like:

1. Your own Rube Goldberg-esque system with separate devices on different continents, custom-written applications and laser-etched backup plates buried under your home.
2. A professional company storing your crypto (known as a custodian).
3. The middle-ground - a company that helps you to self-custody your assets (e.g., Casa custody and Unchained Capital).

Don't Let Your Coins Die With You

Regardless of the tier, every market participant must have a plan for their crypto when they pass away. If no plan is put in place, the cryptoassets will die along with its owner. It's essential that every crypto owner take time to include their cryptoasset holdings in their will and to teach one or more trusted individuals (i.e. family members) how to access their crypto funds in the case of severe injury or death. In addition to teaching your trusted heir(s) how to access your cryptoassets in your absence, step-by-step instructions on the process should also be documented and stored safely with your paper/metal wallet backup(s). If you custody funds on a trusted exchange, it's worthwhile to see if they have a process for handling cryptoassets in the case of its owner's passing. Some exchanges, **such as Kraken**, are willing to assist your legal successors in retrieving the funds provided they can produce certain legal documents (e.g. death certificate, government ID, etc).[8]

3.

Key Takeaways

Though more complexity can be added to the crypto self-custody process, we find it more effective to emphasize simplicity:

- Most market participants are arguably more prone to crypto loss than theft.
- Securing your cryptoassets is contingent on your personal needs. Store small amounts of crypto on well-established exchanges that utilize a combination of hot and cold storage, store moderate amounts of crypto in a hardware wallet with a seed phrase backup held in a personal safe or safety deposit box, and seek professional guidance on multisig solutions and the like for storing generational crypto wealth.
- Always have a contingency plan in place in case of death.

Footnotes

1. HODL is a term derived from a misspelling of "hold" that refers to buy-and-hold strategies for bitcoin and other cryptoassets.
2. Financial considerations vary greatly between individuals. Consider what amounts are correct for you.
3. https://www.wired.com/2014/03/bitcoin-exchange/
4. https://support.kraken.com/hc/en-us/articles/360000426923-Secure-your-account-with-two-factor-authentication-2FA-
5. https://blog.kraken.com/security-labs/
6. https://medium.com/@briananderson_99612/scam-alert-a-cautionary-tale-on-the-purchase-of-cryptocurrency-wallets-from-third-party-vendors-5c300acd7d0e
7. https://blog.kraken.com/post/4237/inside-kraken-security-labs-analyzing-android-malware/
8. https://support.kraken.com/hc/en-us/articles/360031279771-Is-it-possible-to-set-a-beneficiary-or-nominee-

We appreciate your feedback! Please visit https://surveys.kraken.com/jfe/form/SV_2lBbVeVVjWEYmpo to participate in a brief survey. For all future Kraken Intelligence content, sign up here. For comments, suggestions, or questions related to this article or future topics you'd like to learn more about, you may also direct your communication to intel@kraken.com or to your account manager.

Kraken provides access to 57 cryptocurrencies spanning more than 280 markets with advanced trading features, industry leading security, and on-demand client service. With the acquisition of Crypto Facilities, Kraken now offers seamless access to regulated derivatives on 5 cryptocurrencies with up to 50x leverage. Sign up for a free account in minutes at www.kraken.com/sign-up. We look forward to welcoming you.

For multi-exchange charting, trading, portfolio tracking, and high resolution historical data, please visit https://cryptowat.ch. Create a free Cryptowatch account today at https://cryptowat.ch/account/create.

For OTC-related execution services or inquiries, please direct your communication to otc@kraken.com or to your account manager.

Disclaimer