TIPS TO SECURE YOUR CRYPTOCURRENCY WALLET

This document is written exclusively for InvestingHaven's premium crypto members. It is not allowed to distribute this document. On December 14th 2018 we sent an alert to our members inviting them to submit their questions on this topic. **We received 19 questions, and they are all answered in this document**. A big shout-out to the technical blockchain researcher in our team!

Because of the complexity of this topic a simple Q&A might not be sufficient for some members because more context could be required. On the other hand some people just need specific answers. **That's why this document has two parts**:

- Part I from page 2 till page 6: Questions and answers without context
- Part II from page 7 till page 20: Technological context on securing wallets in which we indicate throughout the text the questions that are relevant

Below is the list of questions we are answering in this document.

Hardware wallets:

1. When do we use hot vs cold wallet?
2. Would you recommend using a cold wallet, and what are the pros and cons?
3. Can we store all cryptocurrencies into one hardware wallet?
4. How long we can store in a Hardware wallet?
5. Are hardware wallets only meant for storage?
6. If we lost the Hardware wallet what are the options to recover crypto's or data in wallet?
7. Can we carry a Hardware wallet to different countries and will we be able open it there?
8. How to get the crypto's into a hardware wallet from exchange wallet?
9. What's average cost of quality wallets? Do we need any license or periodic fees to use it?
10. Question: I have a Ledger Nano S or Trezor but can't seem to figure out how to easily use it. It would make sense to use a hardware wallet, but I deal with small amounts of a lot of cryptocurrencies and the Ledger has too many hoops. Any suggestions?
11. Question: I have looked at the Nano S ledger but have trust issues as many stories of people being sold tampered devices. My main question would be could you provide a link to a trusted seller and does it support the top 10 cryptocurrencies of InvestingHaven.

Hot wallets:

12. Are the hot wallets secure (enough)?
13. Any recommendations on (which) hot wallet(s) to consider?
14. What do we do in case we get stolen on hot wallets?

Other questions:

15. I would like to know what is the best way to keep for example XRP?
16. The only 100% safe storage for small investors is an offline cold storage device like a Nano. What is the best way to store altcoins that are not supported by my Hardware wallet?
17. Question: I wonder how safe are some of the trading places such as Iconomi?
18. What are good practices to maintain your exchange account as safe as possible.
19. Can you share a step by step guide on "how to buy and store"?

PART I: QUESTIONS & ANSWERS

(without technological context)

Before starting let's make this principle crystal clear: Crypto funds are as safe as you make them.

This means that using a hardware wallet is a crucial step but certainly not the only measure to take. Where you do the storage, how you do storage, which computer/laptop/device you use, where you store your passwords, doing due diligence when selecting an exchange or hardware wallet provider, etc, are crucial.

HARDWARE WALLETS

When do we use a hot vs. a cold wallet?
The main difference between Hot vs Cold wallet, is that a hot wallet is in one way or another connected to a network. Users of crypto usually prefer a Hot wallet when they look for an easy way to send or receive crypto. Of course, no one prevents you from using a Hot wallet. Using a Hot software wallet for storing big amounts of funds is better than using an online hosted wallet, but still not acceptable and comes with considerable risk.

Would you recommend using a cold wallet, and what are the pros and cons?
We know the majority of our audience is a retail crypto investors with limited to significant exposure. Therefore, as long as you are not managing institutional money or managing others' capital you are good with a tool (wallet) to store crypto funds for long periods. A Cold storage hardware wallet solution is the best option for you at this point in time with current innovation.

Pros

- No direct connection to any network.
- They never expose your precious private keys.
- Support the majority of coins and tokens.
- Small, portable hardware devices.

Cons

- Not easy to use, when compared to a Hot wallet.
- You maybe find some coins or tokens are not supported yet.
- Keeping the device handling private, depends on you (use it in a controlled & secure environment – not in a metro station or coffee places).
- Taking care of the hardware device (keep it in a safe place and do not brake it every time your coins turning red).

A great video about Hardware wallets comes from Mr. Antonopoulos. You can find it here.

Can we store all cryptocurrencies into one hardware wallet?
Cryptocurrencies live on the blockchain, not in any wallet or device. What you store in a hardware wallet is your keys which give you access to your funds (which, as said, are only stored on the blockchain). Different hardware wallets support different cryptocurrencies. There is always an

ongoing work from the hardware manufacturers to support more and more coins, but you have to visit their website and check if a wallet supports all your different cryptos.

How long we can store in a Hardware wallet?
There is no limit on storing your keys on a Hardware wallet, you store them for as long as you wish.

Are hardware wallets only meant for storage?
The only purpose of existence of any Hardware wallet is to let you securely store your keys and give you an "as easy as possible" interface to manage them, in order to spend or receive cryptos. However, some devices can also be used as safe data storage, like USB stick or password manager. Another service that some manufacturers provide is a software embedded crypto exchange bridge which allows you to exchange your cryptos while respecting device and software safety.

If we lost the Hardware wallet what are the options to recover crypto's or data in a wallet?
Always back up your SEED (Master Private Key) and your Passphrase:

- If you have a backup of your keys you can always import these keys to any Hot or Cold wallet, and manage your addresses using it.
- If you do **not** have a backup of your keys you can import your SEED (or Master Private Key) to any HD compatible wallet, and this will generate all of your keys as well as addresses. That's how to gain access to your funds again.

Taking a look at the wallet documentation before bad things happen will help you understand the recovery process and have peace of mind!

Can we carry a Hardware wallet to different countries and will we be able open it there?
A hardware wallet is usually smaller than your smartphone. It's highly portable, and you can have it wherever your wish. But it's always better to keep it at a safe place so you reduce the possibility of losing it. This is a personal choice though, and risk must be considered in this.

In order to use it you'll need a PC. So you can manage your funds by just using a PC in any country. It's best practice to be always updated about the "crypto regulations" and the laws of the country in which you are going manage your funds. For example, we should avoid traveling to Iran with a Trezor device, and try to manage our funds from there because crypto is banned in Iran. Government authorities are allowed to keep your Trezor in case they find it.

How to get the crypto's into a hardware wallet from exchange wallet?
We actually need to know our receiving address which can be found via Hardware wallet interface. Then we have to import this address to the exchange "crypto withdraw" tool, at an empty space asking for our receiving address, usually called "receiving address".
Before any withdrawal you'll have to confirm your actions. You must always check that the receiving address imported in the exchange is the same address depicted on your hardware device display. A compromised PC can change your address while you copy it at the exchange withdrawal toll interface, and send funds to a "hacker". You have to always cross check and trust your Hardware wallet display.

What is the average cost of quality wallets? Do we need to buy any license or pay periodic fees to use it?
A good quality, handy, quite easy to use and well supported Hardware wallet will cost you around 100$, shipping included. After the purchase it belongs to you, and no more fees for license are

required. In some cases, you maybe find some companies providing expert, instant support for a periodic fee or at a "pay as you go" module. This can be extremely useful for critical cases like when you need to recover your keys but you lack knowledge.

Question: I have a Ledger Nano S or Trezor but can't seem to figure out how to easily use it. It would make sense to use a hardware wallet, but I deal with small amounts of a lot of cryptocurrencies and it seems the Ledger has too many hoops. Any suggestions?
Specific information on how to use your device can be found on manufacturers support page site.
Ledger official support site | Trezor official support site | KeepKey official support site

If you deal with small amount of cryptos and you're looking for an easier, cheaper way to manage your keys Hot wallets are always an option. Keep in mind the safest way to manage any amount of crypto is always a Hardware wallet.

A very nice, step by step, video explanation of how to use a Ledger nano S, can be found here. You'll find many similar video tutorials for other hardware wallets as well.

Question: I have looked at the Nano S ledger but have trust issues as many stories of people being sold tampered devices. My main question would be could you provide a link to a trusted seller and does it support the top 10 cryptocurrencies of InvestingHaven.
Every hardware wallet manufacturer provides a list of authorized retailers globally and a list of supported coins/tokens. Some examples: Ledger retailers | Trezor resellers | KeepKey resellers

SOFT WALLETS

Are the hot wallets secure (enough)?
Absolutely not! A lot of knowledge, practice and experimentation is required about software Hot wallets in order to keep your funds safe.

Any recommendations on (which) hot wallet(s) to consider?
Some of the widely used hot wallets include:

- Bitcoin: Bitcoin Core, Copay, Bitpay, Electrum
- Ethereum (including eth tokens): Ethereum Wallet, Mist, Parity, MyEtherWallet or MyCrypto
- Ripple: Toast wallet, GateHub, Exarpy
- Multicurrency Wallets: Exodus, Jaxx, MyCelium, ABRA, Edge and a nice commercial crypto gateway called CoinPayments

What do we do in case we get stolen on hot wallets?
Stolen fund from hot wallet means your machine on which your wallet was hosted and your private & public keys were stored, was hacked. Well, all you can do is the same thing you would do if your physical wallet got stolen: collect as many as possible clues or evidence (log files, network logged traffic, open ledger records etc), report it to the appropriate office (Police, Cyber Crime, Online Fraud) of your country, and pray for a resolution! If your Hot wallet is an online hosted wallet, in addition to the above, stay in contact with the host of the wallet service.

OTHER QUESTIONS

I would like to know what is the best way to keep for example XRP?
Provided that a Hardware is the safest option to store your keys, using a Hardware wallet like Trezor or Ledger is a good idea. Whatever you choose be sure it supports XRP, before you buy it (ledger nano S does support it, while we're not sure about trezor).

The only 100% safe storage for small investors is an offline cold storage device like a Nano. What is the best way to store altcoins that are not supported by my Hardware wallet?
If a coin or altcoin is not supported by any Hardware wallet then you have to create your own cold storage system. That can be an always updated PC with a software wallet, compatible to your altcoin, which will be kept isolated from any networking activity. It will be used to only sign transactions and broadcast them using another networked PC. This way you will not expose your keys to any network related threat.

Keep in mind that many altcoins are created by ETH blockchain, like ERC20 tokens. That means you can store them at any ETH address, even the ETH address of your Hardware wallet. The problem is that you cannot manage them using the Hardware wallet if it does not support it. You can use another wallet to manage it.

Question: I wonder how safe are some of the trading places such as Iconomi?
While we cannot to know every exchange out there we can give you some points which you can use yourself as reference before selecting an exchange.

- Search the internet and forums like Reddit, Medium, Dsquare or any other valuable information sharing platform. Gather info on past users experience and use it wisely to choose your exchange.
- Visit their website and collect information about: Country of operation, users support gates, language support, Coins and/or tokens supported, wallet storage methods and funds insurance.
- Make a collection of "red flags" and figure out if they are able to compromise your funds safety, or user experience.
- Avoid exchanges with a bad reputation, bad past behavior and events (like a hacked exchange).
- Always keep an eye on maker/taker, storing, deposit/withdrawal fees, and liquidity.
- Remember: Storing cryptos in any exchange means you're using someone else's online hot wallet, which is the most vulnerable kind of wallet and method to store any kind of cryptos. The best practice is to immediately transfer all funds to your own wallet, preferably a cold storage wallet.

Some widely used exchanges with quite good reputation are:

- Coinbase: no serious damaging events were reported so far, they claim to use cold storage and funds insurance. They provide the "pro" trading platform-formerly GDAX. They provide you with many account security measures and features. Not many coins are offered though.
- Kraken: no serious damaging events were reported so far. Users were facing difficulties on trades time of execution, due to network congestion, but that was in 2017. They provide a quite nice trading platform with plenty of trading tools. They provide you with many account security measures and features. Not many coins are offered.
- Bitstamp: They have been hacked in the past. After this they claim they use cold storage and funds insurance. They provide an easy to use interface. They provide you with many account security measures and features. Not many coins are offered.

What are good practices to maintain your exchange account as safe as possible.
Most exchanges provide safety measures and security tools. You must always use:

- Strong passwords.
- Strong master passwords.
- Login 2FA which is 2 Factor Authentication through SMS, hardware or software.
- Withdrawal 2FA which is 2 Factor Authentication through SMS, hardware or software.
- Crypto addresses whitelisting (restricts withdrawals to only whitelisted addresses).
- E-mail login, trading, deposits and withdrawal confirmations.
- IP whitelisting/ you will only be able to access your account from a specific IP address. Be careful! If your IP changes you will have to contact support in order to regain access to your account.

Can you share a step by step guide on "how to buy and store"?
The most complete, step by step, guide we've found is this one. If you visit the page, you'll be able to learn how to buy and store XRP, based on your preferences by selecting between multiple ways of buying and a wide list of storing options. You'll also be notified about the pros and cons between the options you can follow.

Take your time to test everything before you actually buy and store. Always keep an eye on scam links and sites, use a safe PC, a safe network and take all necessary precaution measures.

PART II: TECHNOLOGY OF BLOCKCHAIN AND HOW IT RELATES TO SECURING WALLETS (questions mentioned inside)

Before starting let's make this principle crystal clear: Crypto funds are as safe as you make them.

This means that using a hardware wallet is a crucial step but certainly not the only measure to take. Where you do the storage, how you do storage, which computer/laptop/device you use, where you store your passwords, doing due diligence when selecting an exchange or hardware wallet provider, etc, are crucial.

Blockchain

What it is and how it works-Basics

As explained on Wikipedia, a blockchain, originally 'block chain', is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". Here you can find a nice video explanation of blockchain and distributed ledger basic principles.

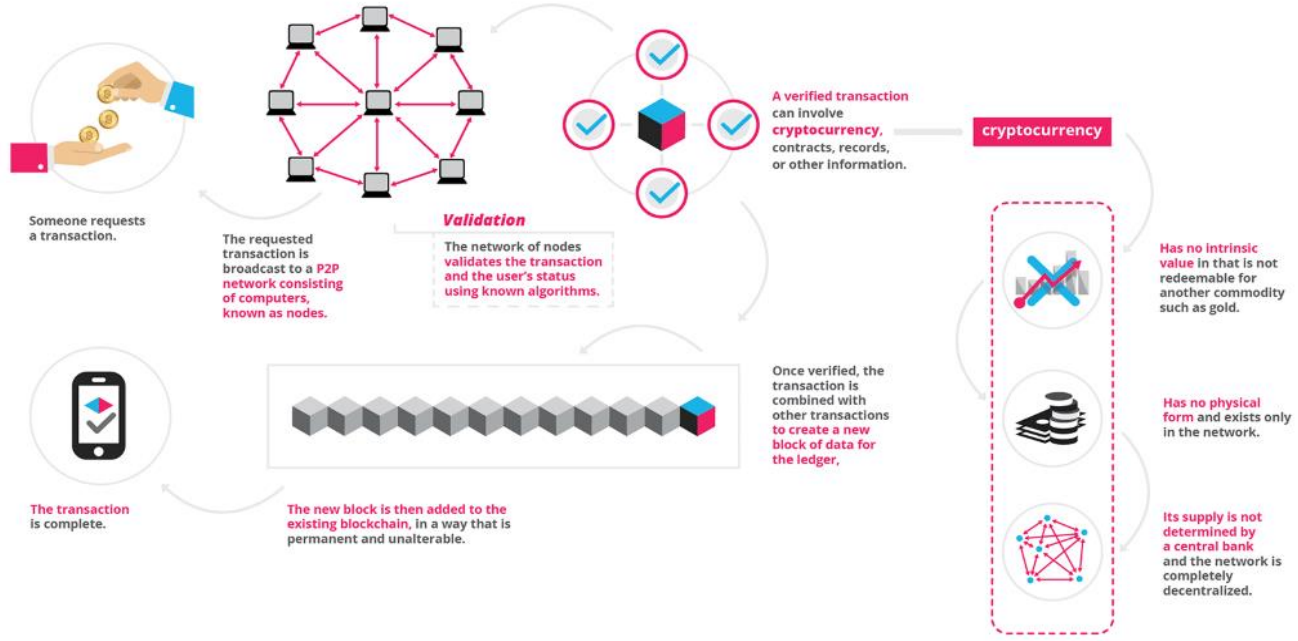


Image Source

This leads us to the conclusion that cryptocurrencies are "stored" on the blockchain as a set of data. In other words the amount of cryptocurrency referred to a specific address can be found in the public ledger. Change of any of the ledger's records regarding a specific address requires the keys of that address (Public & Private keys). That means your private keys will give you access and absolute control of the respected address(es). It is simple but also strict as follows:

No keys → No records change!

Addresses

What it is, how it is generated, how and why it's used

During the early stages of Bitcoin someone could use an IP address to send and receive Bitcoins but this system was proven to be vulnerable to attacks. Developers soon implemented a new system based on cryptography (Public & Private keys) in which sending and receiving was made to addresses derived from a set of Private and Public keys. Without getting too technical here the basic model is based on the use of a Private Key which is used to create a Public Key which is used to create a Public Address. **It's a one-way process**:

Private Key → Public Key → Public Address

The public address is used to spend and receive funds. It was a matter of time to realize that this method of deriving an address was lacking privacy. That's because a private key will generate max two public keys which will generate a max of two public addresses. If you use these addresses multiple times for spending someone can check their balance (using public ledger explorer) and connect it to you as a physical person. It's like publishing your savings account balance.

A solution to that problem came from using a Master Private Key which did generate a near infite number of Private Keys, at the same order every time:

Master Private Key → Private Key (1), Private Key (2), …, Private Key(n)

This results in max two Public Keys and max two Public Addresses for each Private Key generated above. Actually we solve the privacy problem by using a different address for every transaction, so no one can connect the dots and trace transactions back to us. The only thing we have to remember is the Master Private Key, everything else will be generated at the same order every time using this Master Private Key, also called **SEED**.

Private Key(1) → Public Key(1a, 1b) → Public Address(1a,1b)
Private Key(2) → Public Key(2a,2b) → Public Address(2a,2b)
.
.
.
Private Key(n) → Public Key(na,nb) → Public Address(na,nb)

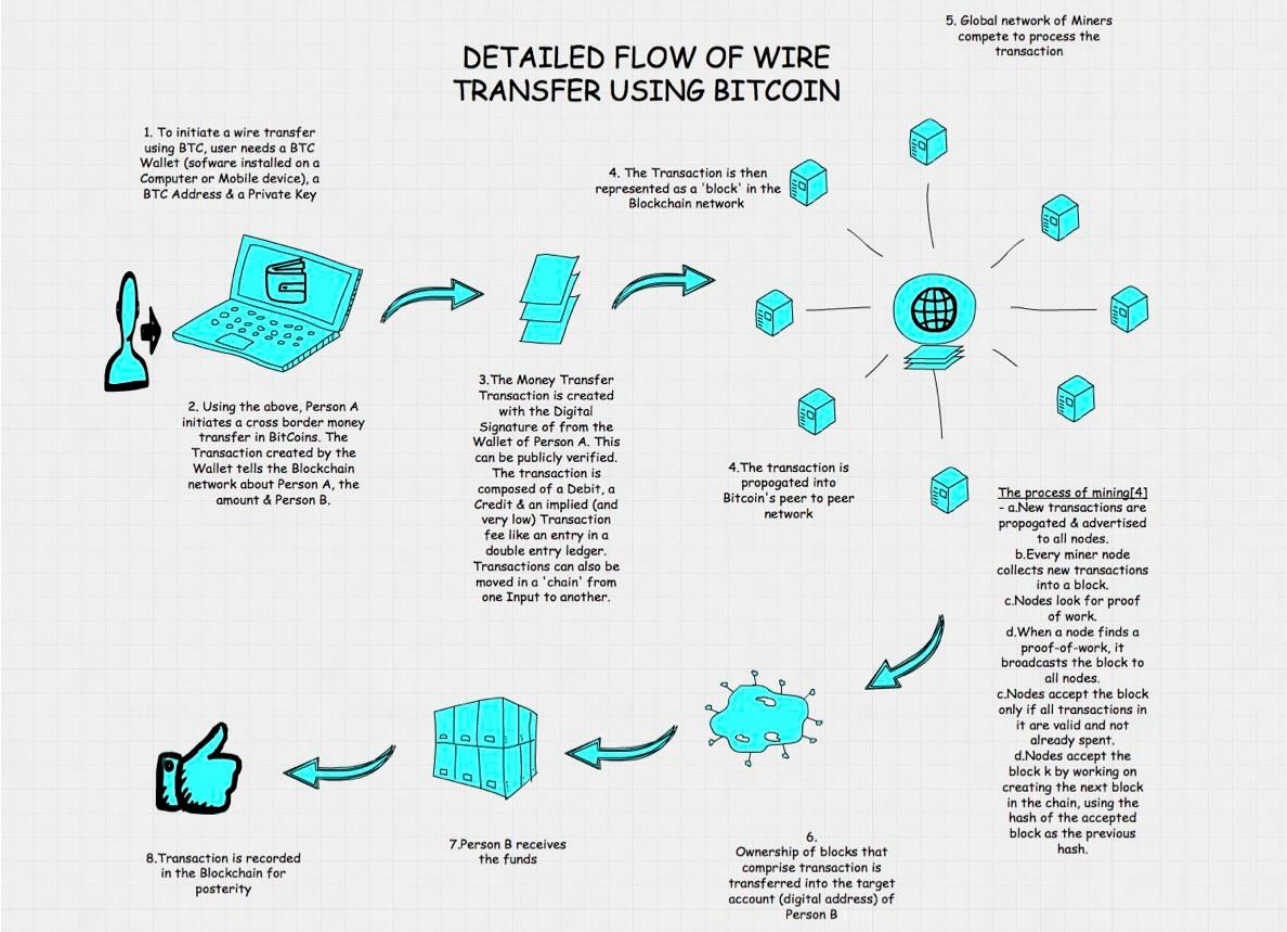
This process of generating or recovering an address (its Public & Private keys associated), is using a **Hierarchical Deterministic (HD)** system (a Standarization). Not to get too technical, it's way to transform a series of 12 or 24 human readable words, to a 512bit hexadecimal seed which is used to create 3 alphanumeric strings, one master key, a private key, a public key and an address (more can be found here). These 12 or 24 words, are your **SEED (Master Private Key)**. As an extra layer of security, you can use an extra word, a Passphrase, as additive to the 12 or 24 words. It's all done by your HD wallet. Any **multicurrency** HD wallet will use one SEED (or SEED+Passphrase), to derive addresses for all the types of coins you use (and it's compatible). That's the magic of storing near any cryptocurrency you wish, while all you have to remember is a **SEED and a Passphrase**.

How funds are Transferred

The "under the hood" process logic of a transfer, what we do and how to track it-Basics

The logic behind a transfer is very simple:

1. You need to own an account (Private & Public keys and Public Address);
2. Prove that you are the owner of the account (Sign a transaction with your Private key);
3. Define a destination Address;
4. Prove the account has the required funds (you broadcast the signed transaction and your address is been audited using the public ledger);
5. Wait for the transfer to take place, the public ledger to refresh the respective addresses balance entries.



The image above will give you a bit more detailed view of how things actually work.

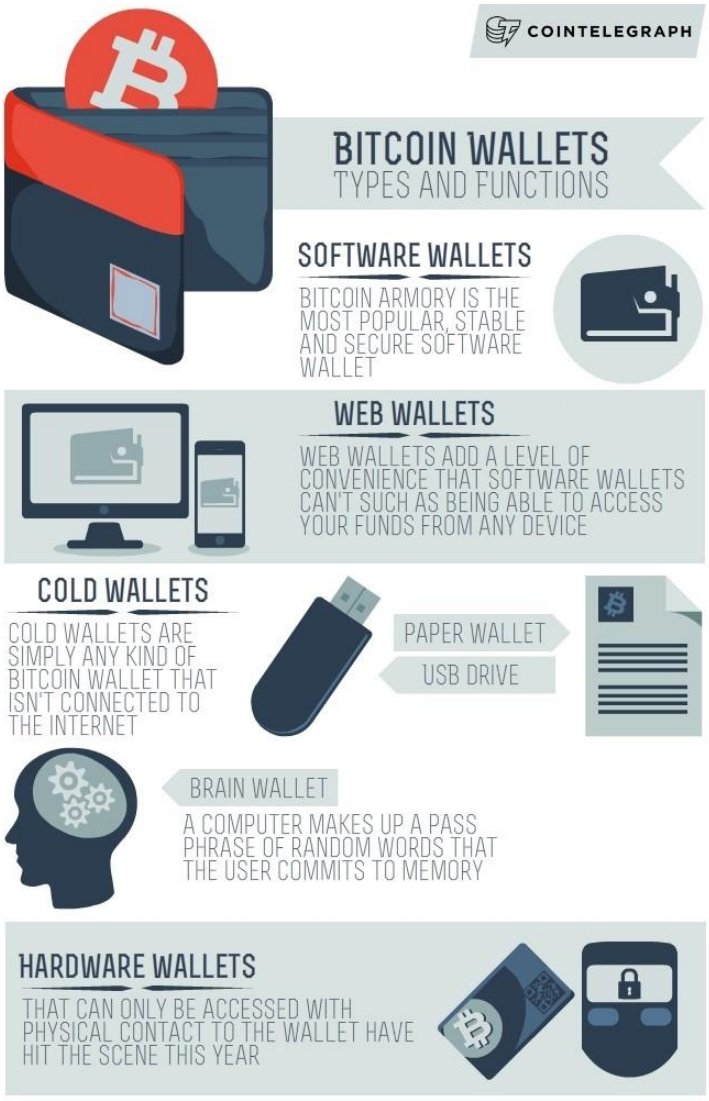
Even if you don't have access to your wallet you can always use a blockchain explorer to watch your balance, by searching for your address. BTC explorer, ETH explorer, XRP explorer

Wallet

What it is, type of wallets, how it's used, main differences hot vs cold

A wallet is simply a tool to use (and sometimes store), when you need to send or receive funds, your public and private keys. The main difference between a Cold and Hot wallet is that a Hot wallet is directly connected to a network (Internet) while a Cold wallet is not. Metamask or Bitcoin Core are Hot Wallets while Ledger Nano S and a simple Paper wallet are Cold Wallets.

To be clear: a PC connected to the internet which runns Bitcoin core is a Hot wallet. The same PC offline running Bitcoin Core can be used as a Cold wallet.



**** QUESTIONS BY INVESTINGHAVEN MEMBERS ****

When do we use hot vs cold wallet?
Would you recommend using a cold wallet, and what are the pros and cons?

A Hot wallet will give you the simplicity and ease-of-use for everyday spending while it's always online in return at the expense of security. A Cold wallet will give you the most Security at the

expense of ease-of-use which is why it is the recommended way to store the keys of addresses used for investment in cryptos.

Assuming an attacker or hacker is trying to compromise the safety of your funds he will first need to get connected to your machine in order to access your files, and using your network (internet connection) is the most obvious way to do it. Therefore, we can easily understand that maintaining funds in a Hot wallet hosted on a networked machine is not safe.

On the other hand a Cold wallet (or Cold storage) is not directly connected to any network. The most famous (for its security precautions and measures) type of Cold wallet is what's called a Hardware wallet. This kind of wallets is usually a small piece of hardware built to store and manage public and private keys. Depending on the design of each of them most can be connected to your computer machine (using a USB port) and sign transactions online or offline. They can indirectly be connected to the internet when you need to make a transaction and go off it in order to preserve security. That means when the attacker attempts to find your keys, using your network (internet), he will not be successful because your keys are kept offline.

A wallet is only a tool which will help you manage an address or multiple addresses (like checking your balance or spend coins) provided you have the right keys. A user **can store the keys** (Public & Private) on a cold storage (paper) or hot storage (smartphone), and use them to manage an address using a cold wallet (hardware wallet) or a hot wallet (software wallet). **No cryptocurrency is stored in any kind of wallet. All cryptocurrencies live on the Blockchain!**

In the end the security of any wallet is a combination of **good habits** (how you use and maintain your computer machine, OS & network) and wallet **software code security** (opensource, widely audited code, well maintained and **up to date** software).

Most people engaged in crypto investing recommend a **combined use** of hot and cold wallet while the funds are divided (everyday spending, investments, HODLing) and scattered under different "accounts" (public & private keys). This way you can maintain small amounts in hot wallets (choose the most secure), for every day use, and big amounts, like investments, in cold wallets.

Hot Wallets

What it is, security, hot wallets recommendations and "expecting the unexpected"

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

Are hot wallets secure (enough)?

As mentioned before a wallet is called Hot if, and only if, it is connected to any kind of network (home, company, public networks, Internet, etc). Networks are vulnerable, and so is your wallet (and your funds) as long as it is attached to a network. Although most developers are implying security measures in their software, and they often prefer to keep it open source, so to be widely audited and tested in order to not let it be compromised. But there is much left for the users to do, for example using the safest software on a PC full of malware is not a good practice, and it will inevitably lead to loss of funds.

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

Any recommendations on (which) hot wallet(s) to consider?

Some of the most used hot wallets are:

- Bitcoin: Bitcoin Core, Copay, Bitpay, Electrum
- Ethereum (including eth tokens): Ethereum Wallet, Mist, Parity, MyEtherWallet or MyCrypto
- Ripple: Toast wallet, GateHub, Exarpy
- Multicurrency Wallets: Exodus, Jaxx, MyCelium, ABRA, Edge and a nice commercial crypto gateway called CoinPayments

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

What do we do in case we get stolen on hot wallets?

Many will ask “what to do if I got hacked, my hot wallet with funds stolen”. Funds that are stolen from a hot wallet means that the machine on which your wallet was hosted and your private & public keys were stored were hacked. Well, all you can do is the same thing you would do if your physical wallet got stolen: collect as many as possible clue or evidence (log files, network logged traffic, open ledger records etc), report it to the appropriate office (Police, Cyber Crime, Online Fraud) of your country, and pray that the thief will be found!

Long story short: do everything you can in order to prevent a situation like a hot wallet hack. Ask yourself “what should I do to protect my fund” instead of asking “what to do now my funds are stolen”. This space is a modern ‘wild wild west’. Prevention is imperative!

Hardware Wallets

Why and where to buy one, recommendations and tips

In most cases a hardware wallet acts as a cold storage and cold wallet, and you’ll be able to store and/or manage your addresses using the same piece of hardware. You will find many Hardware wallets in the market. Some of them are dedicated to store Bitcoin keys only which is not that practical for investors like (y)ourselves. The good news is that the majority of hardware wallets are compatible with a lot of different blockchains, which means you will easily find a hardware wallet to store your keys of different blockchains (BTC, XRP, XLM, ETH and its tokens like POLY and BAT, etc).

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

Can we store all cryptocurrencies into one hardware wallet?

It’s good to notice here that not all tokens are supported by any hardware wallet. For example, you can find a wallet supports ETH but does not support DOE Erc20 token. What actually happens is that the wallet is not (yet) capable of “reading” the balance related to DOE token recorder under your ETH address nor of using DOE token for transactions. The good news is that you can use the ETH address to send your DOE, and you will also be able to check the balance on the blockchain explorer so your coins will continue to live on blockchain and under your address. If you wish to make transactions of your DOE token you’ll be able to do it using another cold or hot compatible. Remember, coins live on blockchain, not in any wallet.

Hardware wallets are designed and constructed by companies like Trezor, Ledger, or Keepkey. Each of them has a similar approach on deriving addresses and security methods. Their main use is to safely store your Private keys. Some of the companies provide software which is specifically designed to cooperate with their piece of hardware in order for you to check the status of your addresses, sign transactions, watch your portfolio, and even buy or sell crypto

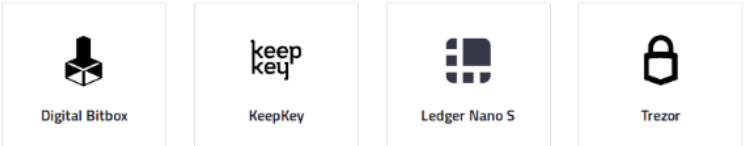
while still enjoying the security they provide you. For example, trezor.io decided to cooperate with exchanges like Shapeshift and Changelly so their users don't have to look for an exchange, and trade directly using trezor wallet software accompanied by a Trezor hardware wallet.

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

Are hardware wallets only meant for storage?

Another utility that some hardware wallets serve is using them as password manager and/or a safe storage for your data (like a sophisticated USB stick). Some of the recent implementations include the "pairing" of a hardware wallet with the software of a hot wallet. This allows you to store your keys into the hardware machine, and use them with your favorite software wallet (which can be a hot wallet) without exposing them to any network. We currently don't know the state of security and/or privacy of this kind of operation.

If you 'duck' it you'll find Trezor, Ledger, Keepkey, CoolWallet, Digital Bitbox, OpenDime, as the most famous hardware wallets. We think there is a good reason for this: they all are well established companies, supporting a variety of OS. They also provide customer support while maintaining easily accessible support pages (like on reddit). Their hardware has been tested by many users and the feedback can be easily found out there (youtube, reddit, forums).



**** QUESTIONS BY INVESTINGHAVEN MEMBERS ****

What is average cost of best quality wallet?
Do we need to buy any license , pay periodic fees to use it?

A good quality, multi-currency, well tested and supported cold wallet would cost around 90$. You'll find prices as low as 40$ up to 400$ (ultimate packages). The most used and famous multi-currency Trezor and Ledger Nano S cost you around 100$ incl shipping. Once you buy it, you will never be asked to pay for it again: no license renewal or periodic fees are required.

An important thing to remember when you buy a hardware wallet is to use official resellers (Trezor, Ledger) and even better buy it directly from the manufacturer. When you receive it confirm the good-looking condition of the package, and make sure there are no signs of bad package handling. Most of the companies have taken measures in order to help you find signs of compromise (like this one). In any case, do not hesitate to contact the company support! Whatever wallet you choose it is mandatory to follow the manufacturers best practices notes.

Coins live on the blockchain. In case a wallet is not displaying its balance it **does not** mean they are not held by the wallet's address. It just means the wallet you use does "recognize" or "support" the specific token yet.

When your wallet does not support your token you can still hold funds in the address. You cannot manage funds that are not supported by a wallet. You can still use another wallet to complete your transactions.

You can always check the balance of your addresses on blockchain explorer.

Stay away from scams!
Don't follow ads. Use official web stores to buy anything crypto related.

Don't forget to back up your SEED (12-24 words & **passphrase** & Device PIN) and learn how to use it safely.

**** QUESTIONS BY INVESTINGHAVEN MEMBERS ****

How long we can store in a Hardware wallet?
Can we carry it to different countries and will we be able open it there?

Other than that, you can store your keys into a hardware wallet for as long you wish (HODL), take it wherever you wish (this is a borderless world), and use it at any time. But always ensure to use a safe place, network, PC, OS, hardware (USB). It's also recommended to stay up-to-date about the laws of the country you live in or visit because there are countries which forbid cryptocurrency buying or transactions (one of the many examples include Iran).

Exchanges

How to choose one, DEX vs Usual recommendations, buy, sell, transfer and HODL

Signing up for an exchange account is usually the first step to get exposure to Crypto investing. Choosing the right one is important because if you read the history of Crypto almost every major fraud happened on or through an exchange. Keep in mind that as an investor there are some points like liquidity or customer support and trading pairs that also matter.

Some questions you should answer before you make a choise:

1. Security: Is it safe? What does a security record look like? Are the website, tools and servers safe? Do they use Cold or Hot wallets for your funds? Are your funds insured? What about 2FA (2 Factor Authentication)?
2. Is the graphical user interface good for you, easy to use?
3. How about the users and customers support?
4. What about the liquidity? What trading pairs does it provide?
5. What about the fees?
6. Is KYC-AML required?

Some of the most famous online exchanges are:

1. Coinbase
2. Bitstamp
3. Kraken
4. Gemini

When you choose an exchange, the next step is to register for an account. Most exchanges let you use your account within certain limits. In order to deposit, withdraw, trade or transfer bigger amounts of fiat currency or Crypto you should pass through a verification process. After you're verified you can continue using your account with less, or no, restrictions.

Depositing or withdrawing funds (FIAT) to/from an exchange happens through a traditional wire transfer, SEPA (E.U.), Credit Card, etc. These operations require KYC-AML: you have to provide your personal information. Always take note of the fees which can vary from 0$ to several hundreds of $ depending on the amount or type of transfer.

Trading usually takes place in a dedicated page in which you'll find options to buy, sell, margin trade, or go short on several assets. This page will also provide you with tools and charts to watch and analyze the markets.

The exchange's interface will let you manage the security options of your account. For example, manage username & password, configure withdrawal address whitelisting, set 2FA (which is highly recommended), lock or unlock your account's activities, etc.

It's also good to know that most exchanges maintain their funds in online HOT wallets. Best case they use a combination of hot and cold wallets. Most people involved in crypto space recommend using a crypto exchange only as a medium to buy or sell crypto. They strongly recommend not to use an exchange as crypto funds storage or wallet.

There are also P2P Decentralized exchanges, but they usually are not user friendly (at all), and safely transacting requires a fairly high affinity with technology:

1. LocalBitcoins
2. LocalEthereum
3. Bitsquare
4. IDEX

Decentralized exchanges are a very interesting model and most of the tokens can be found there! No FIAT trades can be made there which means you'll have to find another way to obtain your first crypto funds. They usually do not require KYC-AML. No private keys are used by DEX platform applications: you connect your address by using a wallet to the exchange protocol, the trades and transfers live on the blockchain and the funds are transferred directly between the maker's and taker's addresses (without a middleman). But you need to be cautious about your transactions and know what you're doing. Using a DEX you don't have to warry for the exchange security, but for the 'safety of your actions'.

If you decide to use any decentralized, P2P exchange, make sure you know what you're doing. **Your actions are irreversible**, you will not find "Undo" button for your actions, and it may cost your funds!

Always use a safe PC and guarded network when trading!

Transfer of funds (exchange → personal address)

Transfer of funds can happen between blockchain addresses. Transferring funds from an exchange is transferring funds from the exchange wallet address to your wallet address.

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

How to get the crypto's into a hardware wallet from exchange wallet?

Let's say you bought crypto using an exchange and now you wish to send an amount or all of your funds from your exchange account to your personal hardware wallet address. All exchanges will give you the option to withdraw your funds from it and send them to the address of your choice. All you need to do is login into your account, navigate to the withdrawals section, choose the appropriate coin and amount to send, read acknowledge and accept the warnings, fill in your public address (or receiving address) into the appropriate space, cross-check that it's the right address and the correct amount, and finally procced with the withdrawal.

A **good habit** is to make a small (experimental) amount withdrawal before you send any major amounts of any coin. For example, you can send 3 XRP to our address, take note of the TxHash which you can use to check the transaction status, and when it's marked as Confirmed/Delivered or Unconfirmed, go to your wallet, let it read the ledger (refresh), and confirm the funds have been transferred. If the funds are missing, TxHash will usually help you find what's wrong.

Always be sure you enter the correct receiving address. Don't forget to notice and calculate the exchange withdrawal fees.

Always use 2FA
(2 factor authentication)

Funds Recovery

**** QUESTION BY INVESTINGHAVEN MEMBERS ****

If we lost the Hardware wallet what are the options to recover crypto's or data in wallet?

What to do when bad things happen? For instance, you lost your hardware wallet (which you were using as a crypto wallet), a password manager and storage device. Needless to say that any passwords and storage data are lost with your wallet. However your crypto coins are NOT stored inside the device. So in order to gain access to your crypto all you have to do is find an HD wallet (Hot or Cold), import your **SEED** (or **SEED + Passphrase**), and let it derive all the relevant addresses. You'll have access, full control and be able to manage your funds again. Deterministic wallets will give you an unlimited number of addresses, derived from a particular SEED, but will always appear in the same order.

You have your SEED --> You have your keys!

Never lose your **SEED**!

If you use a SEED+Passphrase then never loose your **SEED + Passphrase.**

If you also use all of the above + Device PIN then Never lose your **SEED + Passphrase**. PIN is device specific, and it's not used for address derivation, but it's good not to forget it.

The wallet will derive different keys and addresses using only your **SEED** then using **SEED + Passphrase**. (Different input→ Different output)

Any **multicurrency** HD wallet will use one SEED (or SEED + Passphrase) to derive addresses for all the types of coins you use.

Learn to use it

How and why

Before you use the blockchain, the wallets, before even you create your first address, it's wise to learn how it works, how to use it and do it securely and safely.

All blockchain networks have their test networks (testnet). You can read on Bitcoin Wiki, *The **testnet** is an alternative Bitcoin block chain, to be used for testing. Testnet coins are separate and distinct from actual bitcoins, and are never supposed to have any value. This allows application developers or bitcoin testers to experiment, without having to use real bitcoins or worrying about breaking the main bitcoin chain.* Testnets are usually runing on a newer version of the block chain, in order to test the new implementations. For a beginner, a testnet, can serve as a laboratory, where all the experiments take place. You can try to create, abandon, recover addresses, test the differences between HD and classic wallets, create, sign, broadcast transactions, watch the testnet ledger and Txs while you change your balances, and do whatever you wish.

Be sure that **you're actually using a testnet** (and not mainnet), when you're experimenting! The same keys and addresses that work on testnets, are also working on mainnet. Be **extremely careful**, sending funds from mainnet to testnet will lead to loss of your funds!

It's that simple:

When you use testnet → make sure you're connected to testnet

When you use mainnet → make sure you're connected to mainnet

Remember, your actions on blockchain are irreversible! However, on a testnet you can experiment for as long as you wish and try everything you can imagine.

You can create an address **specifically** for usage on testnets. Don't use this address on mainnet. This way you'll never mix things up and get confused, while you preserve the safety of your funds.

A simple yet powerful backup strategy: 3-2-1

When talking about critical data protection, prevention of losing the data or access to them is also included. If you 'duck' it you'll find the practice of a simple yet powerful method of 3-2-1 backup. It simply means having at least 3 copies of your data, at least 2 different mediums, while one is located off site. It's like diversifying an investment portfolio. See example below.

As we know a master private key looks like some random words in a specified order and form, and **No Keys** means **No Access** to your funds. That's why you need to backup your master private key of, let's say, your Bitcoin address generated by trezor HD wallet.

Following the simple rule of 3-2-1 strategy:

At least 3 different copies of your data:
One copy on a hard drive mounted on a PC (preferably not connected to any network) + one copy in a USB (preferably encrypted) or "burned" on a CD + one hardcopy on paper (preferably laminated) and /or metal.
At least 2 different mediums:
The hard disk (USB & CD are considered digital copies) + paper (considered physical copy).
At least 1 different location:
Choose at least one of the above, and relocate it somewhere safe. For example, keep your paper backup in a locker, at a different location than the rest.

Using 13 instead of 3 copies does not harm but it's making things harder when it comes to security and privacy management of these copies. **Remember to keep things simple and clean!** Be **cautious** when using cryptography or other tools in order to protect your data by password or PIN. You must know what and how to use the tools you choose. Keep in mind **nature hazards** (fire, water) that could damage any form of your backup.