



A free and open-source Bitcoin course by Area Bitcoin

Creative Commons BY-SA 4.0 License

Table of Contents - Bitcoin 4 All - What is the best way to store Bitcoin and what are wallets

1. Introduction: Why Storing Bitcoin Matters

- 1.1 Beyond Buying: You Must Store It Safely
 - 1.2 Bitcoin Means Financial Responsibility
 - 1.3 Storing Bitcoin Is Empowerment
-

2. Why Not Trust Banks?

- 2.1 Your Bank Balance Is Not Really Yours
 - 2.2 Fractional Reserves and Bank Runs
 - 2.3 Banking Crises: US 2023, Credit Suisse, Lebanon 2023
 - 2.4 Brazil 1990s: The Collor Confiscation
 - 2.5 Cyprus 2013: Bail-in and Frozen Accounts
-

3. Bitcoin vs Fiat Custody

- 3.1 Fiat Is Melting Ice; Bitcoin Is Sound Money
 - 3.2 Bitcoin as a Bearer Asset: With Great Power...
 - 3.3 Self-Custody: No Middlemen, No Permission Needed
 - 3.4 "Not Your Keys, Not Your Coins"
-

4. Exchange Risks and Historical Lessons

- 4.1 Mt. Gox Collapse: 740,000 BTC Gone
 - 4.2 FTX, Celsius, BlockFi: Trust Is Not a Strategy
 - 4.3 War and Crisis: When Self-Custody Saves Lives
-

5. What Is a Bitcoin Wallet?

- 5.1 Wallets Store Keys, Not Coins
- 5.2 Wallets as Digital Keychains
- 5.3 Seed Phrases: The Master Backup
- 5.4 Why to Store Your Seed Offline
- 5.5 From Seed to Tree: How Wallets Generate Multiple Addresses

6. Are Seed Phrases Safe?

6.1 Can Someone Guess My Seed?

6.2 More Than Atoms in the Universe

6.3 Most Losses Are Due to Poor Storage, Not Hacks

7. Types of Wallets: Hot vs Cold

7.1 Hot Wallets: Practical, But Less Secure

7.2 Cold Wallets: Safe, But Less Convenient

7.3 Examples of Cold Wallets

7.4 Advanced Tools: Air Gapped, Passphrases, Multisigs

8. Custodial vs Non-Custodial Wallets

8.1 Custodial Wallets

8.2 Non-Custodial: True Bitcoin Sovereignty

8.3 Bitcoin-Only Wallets

9. Choosing the Right Wallet for You

9.1 Daily Use vs Long-Term Storage

9.2 Mobile Convenience vs Hardware Security

9.3 Matching Wallets to Your Profile and Goals

10. Final Thoughts

10.1 Why Self-Custody Is the Bitcoin Way

10.2 Wallets Are Tools for Freedom

10.3 Up Next: How to Set Up a Wallet and Withdraw Bitcoin

Bitcoin 4 All - Full Text

Bitcoin 4 All is a free and open source course created by Area Bitcoin. The goal is to help more people to understand Bitcoin and inspire anyone to be a multiplier of Bitcoin education.

About this eBook

Bitcoin 4 All is an educational initiative by Area Bitcoin. This material is licensed under Creative Commons BY-SA 4.0, which means you're free to share, adapt and distribute it for educational purposes as long as you give proper credit and do not use it commercially. Thanks to OpenSats for making this project possible and supporting Bitcoin education worldwide.

Published by Area Bitcoin – 2025

What is the best way to store Bitcoin and what are wallets?

Why is storing bitcoin so important? If you're just starting out in Bitcoin, this question makes a lot of sense! It's normal to think: "Well, don't you just buy and wait for the price to go up?" And here comes the surprise: you also have to learn how to safekeep it.

But relax, storing your bitcoin is no big deal! It is, though, a fundamental part of ensuring that, in a few years' time, all of today's effort will pay off and your bitcoin will still be with you, safe and untouched.



[\(Slide 239\) - Bitcoin 4 All](#)

Bitcoin works differently from banks and the traditional financial system because it allows you to truly own your own money, without depending on anyone else, least of all banks. That's a powerful concept and it's the opposite of how most people keep their own money these days.

In the traditional financial system, the money you have in your bank account is not exactly under your control. Actually, it's the bank that takes care of it, and they do so under the promise that YOUR money will be safe with them.

- 1. IT'S NOT IN THE BANK**
- 2. IT'S NOT YOURS**
- 3. IT'S NOT MONEY**



[\(Slide 240\) - Bitcoin 4 All](#)

But history has proven that the money in the bank isn't even in the bank, it isn't yours and it isn't real money. This is because banks don't truly keep their customers' money: if everyone who has a bank account decides to withdraw their own money, the banks will go bust. They wouldn't stand for mass withdrawal movements.

IT'S NOT IN THE BANK



[\(Slide 241\) - Bitcoin 4 All](#)

This is what happened in the 2023 banking crisis in the US, when banks went bankrupt as customers rushed to withdraw money in fear of the bankruptcy of these intermediaries. Even Credit Suisse had to be rescued by UBS, otherwise it would go bankrupt. History is full of evidence of how banks don't have people's money in case everyone needs to withdraw their balances at once.

BANKING CRISIS MARCH 2023



[\(Slide 242\) - Bitcoin 4 All](#)

The money in the bank isn't even really yours. When you deposit money in the bank, it is no longer yours. That's right! The bank becomes the owner and you become a "creditor". You trust that they will store it properly and return it when you ask, but this trust does have its risks.



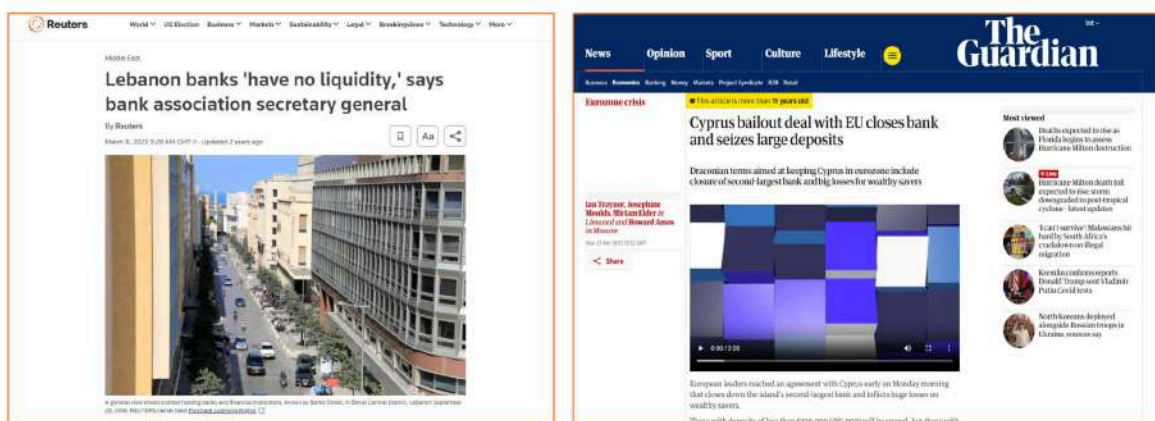
[\(Slide 243\) - Bitcoin 4 All](#)

Sounds safe, right? But it's not quite like that. Banks can go broke, as happened with Lehman Brothers in the 2008 crisis. Those who had money there were left in the lurch. Even with insurance and protection, these funds usually only cover part of the amount saved.

And if that wasn't enough, when you need to withdraw a larger amount, the bank can make life rather difficult for you. Endless questions, blocked transactions, daily limits... All because, while your money is there, the bank uses it to lend and invest as it sees fit.

Now picture this: in a real crisis, when you most need access to your money, the bank may simply not release it. That's why so many people are waking up to the importance of Bitcoin, where you have total control of your money, without depending on anyone.

IT'S NOT YOURS



[\(Slide 243\) - Bitcoin 4 All](#)

But if you think "the bank would never do that to me", it's important to know that it has happened before and could happen again. Want an example? In Lebanon, in 2023, the economic crisis was so great that the banks simply stopped withdrawals. People woke up to find that they could no longer withdraw their own money.

HISTORICAL PRECEDENT



[\(Slide 244\) Bitcoin 4 All](#)

And it's not just there that this has happened. In Brazil, in 1994, people took a hit with the famous confiscation of the Collor Plan. The government froze everyone's savings accounts.

The result? People who had saved their money for a lifetime saw it confiscated without warning and with no chance of withdrawing it beforehand.

Another case was the Cyprus banking crisis in 2013. Banks closed their doors, accounts were frozen and the government decided to confiscate some of people's money to "save" the financial system. The government imposed direct confiscation on bank accounts as part of the bailout organized by the European Union. Accounts with balances over 100,000 euros were the most affected. For those who had more than this amount, the government simply confiscated a significant portion -- in some cases, up to 40% or more of the excess amount.

This means that if you had 200,000 euros in the bank, you could wake up with only 140,000 or even less, with no notice and no chance of recovering what was taken. This measure was called bail-in, where the burden of the crisis fell on the people who had money in the banks.

Situations like this make it clear that, in the traditional financial system, the money in the bank is never 100% under your control. With Bitcoin, on the other hand, you don't have to rely on banks or governments to protect your wealth.

These examples show that when the financial system crashes or collapses, the people who end up paying the price are the ordinary people who believed that their money was safe in these companies or institutions.



[\(Slide 245\) - Bitcoin 4 All](#)

Also, the money you leave in the bank isn't real money. It's fiat, it's an ice cube with no monetary properties that melts in value. Bitcoin is real money. It has sound monetary properties and tends to appreciate in value over time. Since you don't need anyone to store it, it gives people back control over their own money. But along with this freedom comes responsibility.

Bitcoin is a bearer asset, which means that only those who have the private keys that give access to the balance can move it. Unlike the traditional system, where banks hold your money (and decide what you can and can't do with it), in Bitcoin, you alone are responsible. If you lose your keys, you lose access to your Bitcoin forever.

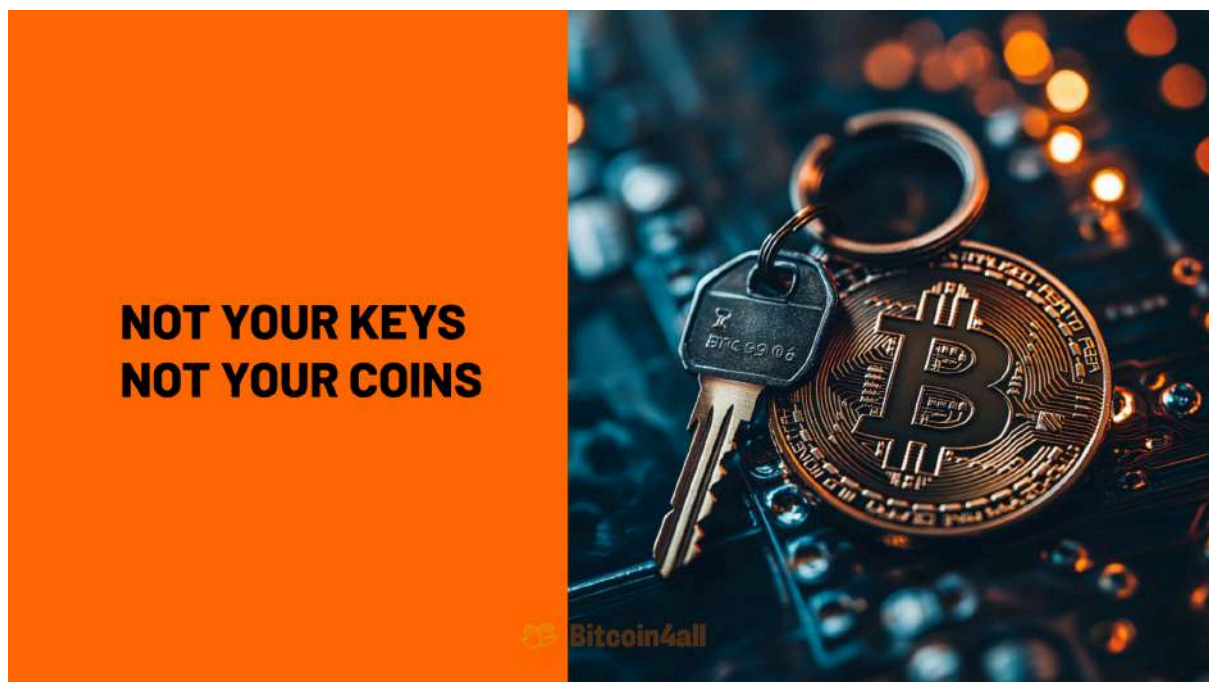
Protecting your bitcoin means ensuring that no one but you has access to your keys and, consequently, your money. It's a huge power!



[\(Slide 246\) - Bitcoin 4 All](#)

With Bitcoin, for the first time in history, your money is inaccessible to third parties. Only you can move it. That's why self-custody is the best way to store bitcoin. When you do this, you eliminate the vulnerabilities of relying on third parties who may fail. Either because they didn't take good care of it or because they wanted to get their hands on other people's money on purpose.

True financial freedom is back in your hands. So why not use this superpower that Bitcoin offers, right?



[\(Slide 247\) - Bitcoin 4 All](#)

Bitcoiners keep repeating the famous phrase: "Not your keys, not your coins". And you know what? They're absolutely right.

Exchanges, which were supposed to be just a place to buy bitcoin, ended up becoming a modern version of banks, only in the Bitcoin world. And just as banks can go bust and take their customers' money with them, exchanges can also go bust and disappear with the bitcoin that were in their custody.

If you leave your bitcoin on the exchange, you are running the same risk that people run when they leave everything in the bank. The difference? With Bitcoin, you have the option of being your own bank.



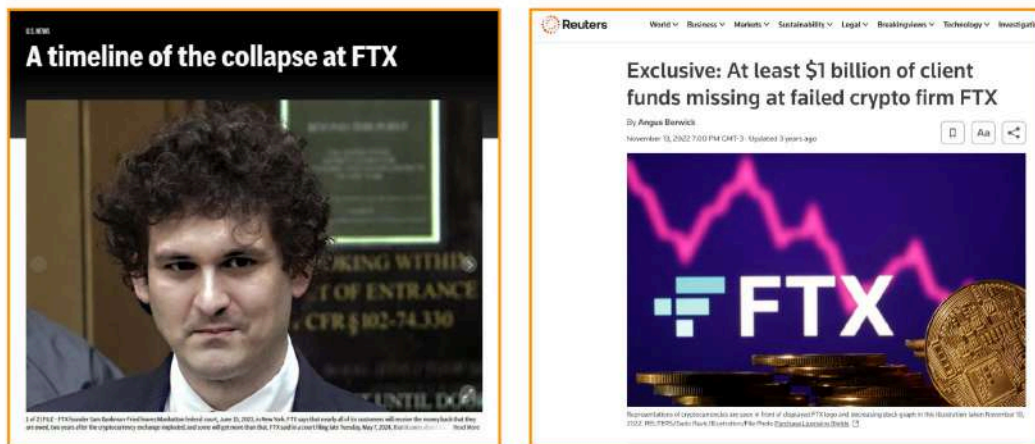
[\(Slide 248\) - Bitcoin 4 All](#)

This became more than clear with the case of Mt. Gox, which was the largest exchange in the world back in 2014. The platform was hacked and poof... 740,000 customers' bitcoin disappeared. At the time, that was already an absurd amount of money: millions of dollars. Today, it would be billions.

And it wasn't just Mt. Gox. More recent cases, such as the collapse of FTX, show that trusting exchanges or banks with your eyes closed is a huge risk. If something goes wrong, be it a hack, mismanagement or fraud, you could lose everything you had, and the chance of recovering it is very slim.

The lesson is simple: leaving your bitcoin with a broker is asking for a gamble. It's best to get them out and put them away yourself. When you take care of your keys, you take care of your money.

FTX COLLAPSE



[\(Slide 249\) - Bitcoin 4 All](#)

FTX was one of the biggest examples of why not to leave your bitcoin on exchanges. In 2022, overnight, it turned out to be a gigantic fraud. Thousands of clients lost what they had and are still fighting in court to try to recover their funds. And you know what's worse? These processes can take years, and many people may never see their money returned.



[\(Slide 251\) - Bitcoin 4 All](#)

And it wasn't just FTX. Other large companies, such as Celsius and BlockFi, also went bankrupt, leaving their customers completely in the lurch. On the other hand, if you do self-custody, i.e. you store your bitcoin yourself, all this is no longer a problem. You don't depend on anyone, least of all companies that may be fraudulent or inefficient.

The final argument in favor of self-custody as the best way to store bitcoin is also because it protects you in extreme scenarios. In situations of economic crisis, war or authoritarian

regimes, having direct control over your bitcoin can be the difference between escaping with your resources or losing everything.

During the war between Ukraine and Russia, many bank accounts were frozen. But those who had bitcoin safely stored were able to cross borders and take their money with them.



[\(Slide 252\) - Bitcoin 4 All](#)

There was even the case of a refugee who managed to travel to Poland with 2,000 dollars in bitcoin, stored on a simple USB stick. If it hadn't been for the bitcoin in self-custody, this war refugee would never have been able to take any of the money, as all citizens' accounts have been blocked. Bulletproof vests, helmets and supplies could only be delivered to protect the population because donations were made in bitcoin to those on the front line. Meanwhile, the money in the banking system was closed and inaccessible to the local population.

In the end, self-custody is the only way to ensure that your bitcoin are out of reach of bankruptcies, hacks, crises or government seizures. And in such an uncertain world, this is the best way to protect your financial freedom.

OK, now that you've understood that getting Bitcoin off the exchange is important, along comes the question: "where exactly do I store my bitcoin"?

BITCOIN WALLETS



[\(Slide 253\) - Bitcoin 4 All](#)

The safest way to store your bitcoin is in your own wallet.

There are different types of wallets and they all fulfill exactly the same function, which is to store your keys that allow you to move your bitcoin balance. Dedicated devices are wallets that store the keys offline, away from the computer or cell phone, and aim to offer greater security for those who want to store bitcoin for the long term.

There are also mobile, computer and tablet wallets. These are computer programs or mobile applications that store your keys. As they are always online, they are wallets that can be used on a day-to-day basis, for smaller transactions that require practicality. As these devices are generally always connected to the internet and interacting with other digital environments, they end up being more susceptible to hacker attacks. That's why this type of wallet isn't suitable for storing large amounts of bitcoin or any value that you want to keep more securely for the future.

The amazing thing is that Bitcoin is information -- and you can store information anywhere. That's why you can have a Bitcoin wallet printed on a sheet of paper (a paper wallet) or engraved on a piece of metal. You can even memorize this information and turn your brain into a Bitcoin wallet.

Each type of wallet has a function, but not all are suitable for all situations. So it's up to you to choose which type of wallet to use at any given time.

But there's an irony here....

BITCOIN IS ALWAYS IN THE BLOCKCHAIN



[\(Slide 254\) - Bitcoin 4 All](#)

Bitcoin wallets don't have any bitcoin in them! It sounds like a joke, but it's not! Bitcoin are never stored in wallets. They're always on the blockchain (or timechain) and never leave it. What a wallet does is store and protect the keys that give access to the balance and allow bitcoin to be moved from one address to another. They are always at an address on the network and not inside the wallet app or device.

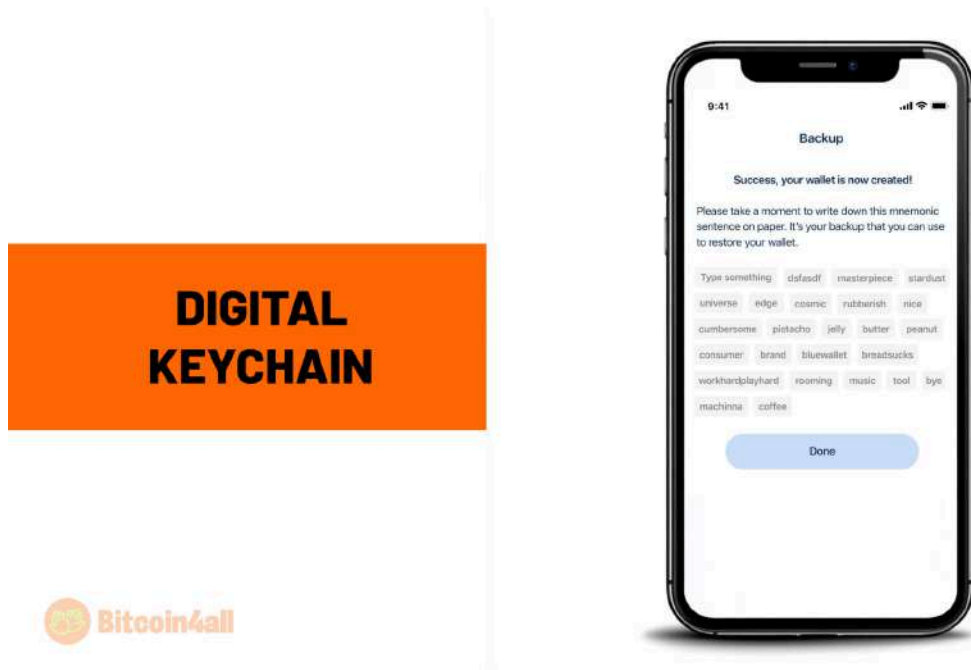
DIGITAL KEYCHAIN



[\(Slide 255\) - Bitcoin 4 All](#)

Wallets are like a digital keychain that stores the codes that authorize transactions with your balance, cryptographically proving that you are the true owner of that balance and can move it around. Just as on a physical keychain, where you can have different keys that open different doors in different places, in your digital wallet your keys give you access to different

types of balances and transactions. That's why your digital wallet works like a digital keychain.



[\(Slide 256\) - Bitcoin 4 All](#)

When you set up a wallet for the first time, it will generate a sequence of words for you, like this one on the screen. These words are known as seed phrases. These are words for recovering your wallet. With them you can recover your balance on any other device or application, even if your original device breaks, is lost or destroyed by some unexpected misfortune.

That's why you need to be careful with these words. They are the ones that recover your balance and allow you to move your BTC. That's why it's important to write them down carefully, legibly, in the exact order in which they appear and keep them in a safe place where only you know where they are. If you store your words well, you'll always have access to your bitcoin, but if you don't take good care of it and someone else finds it, they'll be able to move your balance and take your bitcoin for themselves.

SEED PHRASE



[\(Slide 257\) - Bitcoin 4 All](#)

Many people who start accumulating their bitcoin find it a bit archaic to keep their words on a piece of paper, but the advantage of keeping your seed words written on paper or on a more resistant material such as metal is that this type of backup drastically reduces the chances of hacks or of someone gaining digital access to your bitcoin.

Paper or metal are old "technologies" that no one can hack because they are always offline. In addition, anyone can write a list of words on a piece of paper.

Bitcoin is information. You can even memorize your words and take your Bitcoin wherever you want in your mind. If this information is stored in a computer file, a screenshot of your cell phone or a WhatsApp message, it's easier for an attacker to steal your funds. Not because your wallet was hacked, but because you left that information much more exposed than on a piece of paper that only you have access to. It's much more difficult for someone to access a piece of paper. This is only possible if the person finds out where you left this information by stealing the paper on which your seed words are written down.

The expression "seed phrase" is intentional. It's from there that you can generate thousands of different private keys and Bitcoin addresses for different balances. In the same way that from a seed in the ground you can grow a tree that branches out into thousands of fruit-bearing branches.

Seed words also facilitate storage and prevent errors in self-custody. This is because they represent a large code, with random letters and numbers that are very easy to miss when writing down. Words, on the other hand, are more intuitive, have meanings you can even memorize and are easier to write and less likely to miss.

CHANCES OF GUESSING



[\(Slide 258\) - Bitcoin 4 All](#)

But the question always arises: "What if someone guesses my words? Could they steal my bitcoin?" The answer is: no. It's absurdly difficult to simply guess your seed phrase.

The number of combinations of possible seeds is so great that it's almost incomprehensible. There are more possible combinations of 24-word seed words than there are atoms in the universe! It's unlikely to guess anyone's words, practically impossible.

It's infinitely easier for someone to steal your bitcoin by stealing your seed, if you don't store it well, than to try and guess by trial and error. That's why most people who lose their bitcoin do so because they didn't watch their words -- and not because someone else guessed. Bitcoin has no bank account, no manager and no support. Bitcoin is a language, it's a tool. It's up to you to use your keys responsibly and take good care of them.

WHICH WALLET TO CHOOSE?



HOT WALLET

- Online
- Practical
- Apps or software on your phone or computer
- Easy-to-use everyday storage



COLD WALLET

- Offline
- Safe
- Dedicated devices or offline key generation
- Saves safely for the long term



[\(Slide 259\) - Bitcoin 4 All](#)

Okay, now that you've understood that wallets give you the sovereignty to store, receive and send bitcoin how, when and where you want, that they generate words that allow you to recover your balance even if the original wallet breaks down... Lastly, let's look at the types of wallet and in which situation to use each one.

There are two main categories of wallets: cold wallets and hot wallets.

Hot wallets are named as such because they are always online and connected to the internet at all times. This type of wallet is very practical to use and move balances around. When you need to make a transaction you can just open it and make the payment or transfer. They are usually applications or programs that you install on your computer, generate keys, store and sign transactions. You just open the app and use it. But this practicality comes with some risks: this type of wallet is more vulnerable to hacker attacks on the device, it has a larger attack surface. Hot wallets are recommended for storing small amounts of bitcoin, those that you might use on a daily basis.

Cold wallets, on the other hand, are so called because they remain offline most of the time, which reduces the attack surface. This type of wallet is more secure and works like a digital safe, which is why it is recommended for storing your bitcoin balance for the future. This category includes hardware devices that are manufactured specifically to generate and store your keys offline. Some models allow you to make air gapped transactions and never connect to the internet, meaning you can sign transactions without plugging your wallet into the internet. Cold wallets are paper wallets, hardware wallets, metal wallets and even brain wallets, which are completely analog -- all you need is your brain and a good memory to store the words.

Cold wallets are ideal for storing valuables that you want to protect for the future. Setting up a cold wallet and using it is the first security step, but if you want to move forward on this topic, there is, for example the creation of multisigs, air gapped signatures, passphrase and other features that you can learn as a continuation of Bitcoin4All.

A final important point when choosing a wallet is to opt for self-custodial wallets, which provide the words of recovery. This way you can retrieve your balance from any other wallet

using these words. There are also wallets that don't offer the words and just keep the keys for you. These wallets are known as custodial wallets. They work almost like exchanges. They're responsible for storing your bitcoin and require you to trust them. Therefore, custodial wallets are not recommended for storing your bitcoin for the long term.

That's why choosing a wallet depends on how you want to use it, what your goal is with the balance you want to store and what your profile is. If you want to send bitcoin for quick payments, all you need is an app on your cell phone. If you want to store bitcoin with maximum security because it's been your hodl for years, then it's best to use a dedicated device. If you're Bitcoin-only like us and don't want to know about any shitcoins living in the same wallet as your bitcoin, no problem: there are wallets that are Bitcoin-only.

So in this lesson you learned why self-custody is important, what Bitcoin wallets are and how they work. In the next lesson we'll take the first step towards your sovereignty and show you how to set up a wallet from scratch and withdraw your bitcoin from the exchange. See you next time!