Theory of Blockchain

Session 8:

Bitcoin – Part 3

Module 3 – Wallets

What are crypto wallets?

- Crypto wallets are a type of digital wallet specifically used for storing digital currencies.

- They are basically applications that can help you access blockchain platforms and help you retrieve and use your crypto assets.

- Crypto wallets technically do not store digital currencies. They help to connect to the blockchain platform that stores your assets.
  - They need your public key to go over the chain and see how much has been sent to your public key.
  - They need your private key if you want to spend some of that money.
    - You can keep the private key for yourself, but must provide the signature whenever necessary.

Types of Crypto Wallets

Here are the main types of crypto wallets:

1. Software Wallets
2. Hardware Wallets
3. Paper Wallets
4. Brain Wallets

Each type of wallet has its own advantages and considerations regarding security, convenience,etc.

Software - Desktop Wallets

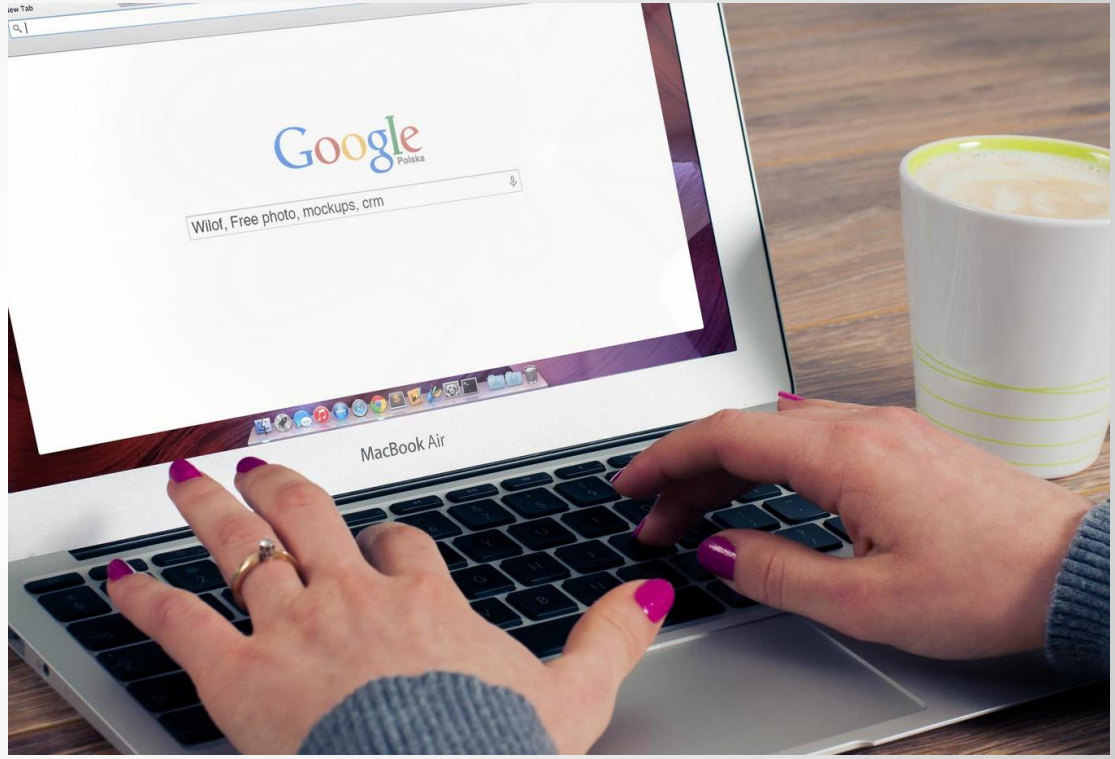
These wallets are software applications installed on a computer or laptop. They provide full control over the user's private keys and are typically more secure than online wallets.

Software - Mobile Wallets

These wallets are mobile applications that can be installed on smartphones or tablets. They offer convenient access to cryptocurrencies on the go and often have additional features like QR code scanning (for public key/address exchange).

Software - Web Wallets

Also known as online wallets, these wallets run on web browsers and are accessible from any device with an internet connection. Web wallets are convenient but may have higher security risks compared to other types.



Hardware Wallets

Hardware wallets are physical devices designed specifically for storing cryptocurrency private keys offline. They offer a high level of security by keeping the private keys isolated from internet-connected devices. But if you lose the device, you lose the money.

Paper Wallets

Paper wallets involve printing out the public and private keys on a physical piece of paper. This method provides offline storage and is considered highly secure if generated and stored correctly.

Brain Wallets

Brain wallets allow users to generate and store private keys using a passphrase or a combination of words. The private keys are derived from the passphrase, and users must remember it to access their funds. Brain wallets can be convenient, but they are also vulnerable to brute-force attacks if weak passphrases are used.

Custodial vs Non-Custodial Wallets

Custodial wallets are provided by third-party companies or exchanges. With these wallets, users trust the service provider to (generate or) secure their private keys. While they offer convenience, they also take some control over the funds.

Custodial vs Non-Custodial Wallets

In **non-custodial wallets** the user is the only one with access to their private keys, and therefore, has complete control over their assets. The tradeoff between the custodial and non-custodial wallets usually lies in having less responsibility of safeguarding the crypto vs having more direct control.

What Comes Next …

- We introduced different types of wallets. They are not only for Bitcoin. There are wallets for different cryptocurrencies.
- We learned that some wallets take and keep your private key while others do not.
- We finalize the Bitcoin topic here and move to a different blockchain in the next session.

See you in the next module …