

**RESEARCH REPORT**  
**CRYPTO WALLETS**

*Overview of Crypto Wallets: Hot vs. Cold, Custodial vs. Non-Custodial*

Ayisha Mohammed  
2024  
Crypto Research Project

Crypto wallets store crypto currencies. Was that your very first thought? well that's not the case technically!

## **WHAT IS A CRYPTO WALLET?**

- It can either be a Software program, Hardware device Even a piece of paper that stores your "Public and Private keys".
- These keys are which locates/points to your crypto assets on a blockchain.

## **PUBLIC KEY**

- A public key (also known as "public address") is a cryptographic key used to receive cryptocurrency.
- Can share with everyone. safe to share with others.
- Just like your bank account number, which people use to send you money.
- If you lose your public key, it can be retrieved from the blockchain's ledger.

## **PRIVATE KEY**

- A private key [" Secret key"] is a cryptographic key similar to a password (like a Pin number).
- Used to sign cryptocurrency transactions.
- Never share with anyone, as it's the only way to access your crypto assets.
- If you lose it, then you lose your asset forever!!

Wallets can either be Custodial or Non-custodial, depends on who has control/access over your private keys






## **CUSTODIAL WALLET**

- A third party (crypto exchange) responsible for managing your private keys.
- Service provider gets complete control of your money.
- People rely on custodial wallets because managing private keys is not an easy task.
- It's important to choose a trusted and reliable service provider that will keep your private keys and funds safe.
- Custodial wallets that offer insurance coverage for theft or misuse of funds.

## NON-CUSTODIAL WALLET

- A non-custodial wallet is a wallet in which you are responsible for storing and managing your private keys.
- Unlike custodial wallet, you have full control over your digital assets.
- It becomes your own bank with round-the-clock (24/7) access to your funds.
- It's extremely difficult to retrieve a lost private key for non-custodial wallets, users need to be extra careful.

## CUSTODIAL VS NON-CUSTODIAL WALLET

| Custodial vs Non-Custodial wallet  |  |  |
|--|--|--|
|  | Custodial                                  | Non-Custodial  |
|  Ownership of private key     | Wallet providers kept the keys of users    | Users themselves have their keys                         |
|  Real-time transaction        | Not possible as the user needs permission  | Possible as users have complete control over their funds |
|  Security level               | High risk of breaches and hacking attempts | No risk of online hacking                                |
|  Recovery of funds            | Possible                                   | Not possible   |
|  Having offline accessibility | Not available                              | Available  |

**Security:** Non-custodial wallets are generally more secure than custodial wallets as the user has complete control over their private keys.

**Ease of use:** Custodial wallets are generally easier to use than non-custodial wallets, as the user does not need to worry about the technical aspects of managing their wallet, since third party takes care.

**Control:** Non-custodial wallets give the user complete control over their cryptocurrency, whereas custodial wallets give control to a third party.

**Trust:** Custodial wallets require the user to trust a third party to manage their cryptocurrency, whereas Non-custodial wallets do not require any trust in a third party.

**Cost:** Custodial wallets may have additional fees associated with them, whereas Non-custodial wallets are often free to use.

**Speed:** With a custodial wallet, every transaction requires approval from the central exchange while Non-custodial wallet users directly authenticate transactions without involving centralized entities, so they're usually faster

**Creating a new account:** Account creation for custodial wallets need to Know Your Customer (KYC) and Anti Money Laundering (AML) forms This can be a lengthy and time-consuming process.

Non-custodial wallets, on the other hand, do not require KYC / AML. Thus, creating a non-custodial wallet may be faster to set up.

## **EXAMPLES:**

Custodial - Binance, Free Wallet, BitMex, and Bitgo.

Non-Custodial - Metamask, Trust Wallet, Ledger Nano X, Trezor One, Zengo, Edge, Electrum, Exodus, Wasabi, and Phantom

## **HOT [online] AND COLD [offline] WALLETS**

### **WHAT IS A HOT WALLET?**

- A hot wallet, sometimes known as a software wallet connected to internet.
- A piece of software you install on your smartphone or laptop.
- It is normally protected by a password set by you, ensuring that nobody can physically access the wallet via your device.
- So why exactly is a hot wallet known as "hot"?
- The defining feature of this type wallet is that it generates your seed phrase online, and subsequently stores your private keys online too.

### **SEED PHRASE?**

- A seed phrase is a sequence of 12 or 24 random words that provide the information required to recover a lost or damaged cryptocurrency wallet

### **WHAT IS A HOT WALLET FOR?**

- Private keys online make transacting very straightforward.
- Just log in and start interacting with online applications. If you're new to the crypto world, the hot wallet can be an attractive starting point.
- It's easy to download, gives you custody of your private key and makes it easy to interact with crypto platforms.
- But all of these great benefits come with some significant security implications.

## PROS OF HOT WALLETS

- **Convenience:** Hot wallets offer quick and easy access to your crypto assets, making them suitable for everyday use and trading.
- **User-Friendly:** They are often user-friendly and come with intuitive interfaces, making them accessible to beginners.
- **Integration:** Many hot wallets are integrated with crypto exchanges, enabling seamless trading.
- **Accessibility:** With an internet connection, you can access your hot wallet from anywhere.

## CONS OF HOT WALLETS

- **Security Risks:** Hot wallets are more susceptible to hacking and cyberattacks due to their online nature.
- **Lack of Control:** Users don't have full control over their private keys, as the wallet service provider often holds them.
- **Not Ideal for Large Holdings:** Keeping significant amounts of crypto in a hot wallet is risky, especially for long-term storage.

## WHAT IS A COLD WALLET?

- A cold wallet is commonly misunderstood to be simply the opposite of a hot wallet – but this is inaccurate.
- While a cold wallet device generates and store your private keys in an offline environment.
- It also has another essential trait: it never interacts with smart contracts.

## WHAT IS A COLD WALLET FOR?

- A cold wallet is perfect for protecting high-value crypto assets long-term primarily due to its security features.
- It keeps your keys offline and protects you from on-chain threats, malicious smart contract functions and apps.

## PROS OF COLD CRYPTO WALLETS

- **Increased Security:** As they are not connected to the internet, they are insulated from potential hacking attempts and other cyber threats. Having possession of your private keys grants you full ownership and control over your assets.
- **Offline Storage:** When it comes to the long-term storage of your digital assets, cold wallets are the ultimate choice, cold wallets offer a secure and reliable solution for those looking to hold onto their assets for the long term.
- **Control Over Private Keys:** With a cold wallet, you are the only one who holds the private keys to access your cryptos. This eliminates the need to rely on a third party for the safety of your assets.

## CONS OF COLD CRYPTO WALLETS

Here are some of their shortcomings to consider before deciding if a cold wallet is the right storage solution for you.

- **Physical Loss or Damage:** A cold wallet, whether it's a hardware wallet or a paper wallet, is typically small and easy to carry around means it can be easily misplaced, stolen, or damaged.
- **Limited Accessibility:** They can be less accessible than hot wallets. This means that you may not be able to access your funds quickly in case of an emergency.
- **Dependence on Third-Party Devices for Some Types:** For some types of cold wallets like hardware wallets, you depend on a third-party device for storage and security. This means you have to trust the device manufacturer and the security features they provide. Additionally, if the device breaks or gets stolen, you may lose access to your assets.

Before considering whether a cold wallet is the best storage option for you, these are all crucial aspects to think about.

## EXAMPLES

- **HOTWALLETS:** Coinbase, Metamask, Trust wallet, Exodus wallet, Robinhood, Edge.
- **COLD WALLETS:** Types: Hardware wallet [similar to USB drives] [\$50 to \$250]
- Paper wallet [just printed copies of private keys]
- ELLIPAL Titan 2.0, Ledger Nano S Plus, Trezor Model One etc.

## CONCLUSION

- In the world of crypto, understanding the nuances of hot wallets and cold wallets is essential for safeguarding your assets.
- Hot wallets offer convenience and accessibility.
- Cold wallets prioritize security and control.
- Your choice between the two should depend on your specific needs, risk tolerance, and the nature of your crypto activities