Does My Wallet Store My Coins?

Jeff Hong ⋮ 3-4 minutes

October 24, 2021

No, not really.

Your wallet doesn't store your coins (thaat's actually the beauty of it!). Rather, it stores the ability to access and transact with your coins (i.e. your keys).

What does that mean and if my wallet doesn't store my coins, where are they stored?

Your coins are **"stored" on the blockchain**. Think of it as a *huge, universal list* that records every single transaction associated with said coin.

Each transaction shows **who sent whom coins** and **how many they sent them**.

For example:

- Bill sent Sally 2 coins
- Sally sent Tom 3 coins
- Tom sent Bill 1 coin
- etc.

It wouldn't be very private if names were associated with the transactions.

So instead of names, each transaction shows the addresses generated from the respective persons wallet (think of it like an anonymous email address).

In fact, a wallet can generate a *virtually infinite* number of different addresses (thus, more anonymity) but they'll all be associated with said wallet.

The amount of coins you have are determined by adding all of the transactions associated by the addresses generated by your wallet.

Back to our example:

- Bill started out with 5 coins.
    - Bill sent Sally 2 coins (Bill has 3 coins leftover)
    - Tom sent Bill 1 coin (Bill got 1 coin)
- Bill has 4 coins total.

So if my coins are stored on the blockchain, what does my wallet actually do?

When you generate a new seed or import a seed to a wallet, it uses those 12-24 words to **generate a set keys** (think of it like an actual set of keys but digital) which are stored on your

wallet device.

Your wallet uses those keys to generate addresses.

When you receive coins, your keys generate an address you can provide others to send to.

When you send coins, your keys **authorize** sending coins from an address it generated to someone else's address (creating a transaction recorded on the blockchain).

Thus, those keys show ownership for all the transactions of the addresses that they generated to recieve and authorized to send.

Your wallet interface simply adds all of those transactions of the address associated with your keys to show you the amounts.

So to be frank, your wallet stores your keys.

Concluding thoughts

It's honestly misleading to call a device a "wallet". It's more like a keychain since it doesn't store your coins, but allows access to your coins.

This is why securing your seed is so important.

From just your 12-24 word seed phrase, a wallet can use that **re-create and recover** all the data needed to access your coins.

It can inputted into **as many** devices as you want (at the same time) and they will all share the same authority over those coins. This means someone else can to without you knowing if they have access to your seed.

So it is **imperative** to keep your seed safe and ensure it's longevity in the event your wallet device fails.

If you're interested in learning more about seed security, check out the articles below:

- Where to Store Your Seed Phrase
- The Best Way to Store Your Seed Phrase
- 10-Step Beginner's Guide To Bitcoin Wallet Set Up & Security
- Guide To Securing Your Bitcoin Seed Recovery Phrase