A Beginner's Guide to Crypto Wallet

Original:
https://www.btcc.com/en-US/academy/crypto-basics/a-beginners-guide-to-crypto-wallet

Buying cryptocurrency has never been easier, but learning how to store it properly and securely with a crypto wallet takes a lot more work.

Crypto wallets are like online bank accounts for your cryptocurrencies but with a few key differences: crypto wallets are not backed by government deposit schemes, they only hold cryptocurrencies (no regular funds here) and, crucially, you have full control over your money at all times.
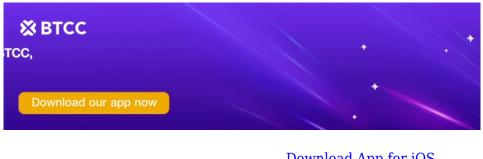
Non-custodial is the term given to cryptocurrency wallets, like MetaMask, Rainbow Wallet or Trust Wallet, that are separate from the accounts you may have on cryptocurrency exchanges. When you hold money on a crypto exchange, like Binance, Kraken or Coinbase, those companies are in control of your cryptocurrencies. But when you move your crypto to a non-custodial wallet, you hold the keys to your wallet.

These wallets are the key to the decentralized web and serve as the primary way to interface with decentralized finance protocols, like lending protocols, decentralized exchanges or non-fungible token (NFT) marketplaces. Crypto wallets are so foundational to decentralized finance that some people on Twitter or Discord refer to themselves solely by their cryptocurrency wallet addresses – anyone who introduces themselves with a username that starts with "0x" is referring to their Ethereum address.

Why Is a Crypto Wallet Needed?

Unless you're running a huge company holding so much cryptocurrency that you need the watchful eye of a specialized custodian – a third party that looks after your crypto for you – you're looking for a non-custodial wallet. These are, as mentioned, wallets to which only you hold the keys. You may have read the adage, "not your keys, not your crypto." This phrase is commonly used and stresses the importance of looking after your own crypto.

With non-custodial [crypto wallets](), your assets are backed by something called a private key. This functions as a password to your crypto wallet. You must shroud this in secrecy and never tell anyone about it. Should you lose your private key, you'll be able to use something called a secret phrase, or seed phrase. These are strings of 12 or 24 words that function as a backup password. It's important to hide these in a trusted place, ideally by holding parts of the phrase in different places. No company or individual should ever ask for your seed phrase – those that do are almost always scams looking to steal your funds.

Considerations for Choosing a Crypto Wallet

Different blockchains require different wallets. MetaMask, one of the most popular wallets, supports just a handful of networks, including Ethereum, Binance Smart Chain, Polygon (MATIC) and Avalanche (the common denominator is that these chains all support the Ethereum Virtual Machine (EVM)). MetaMask does not support Solana or Bitcoin, however, there are a number of other options including Trust Wallet that do support Bitcoin.

NFT support requires special attention. Most wallets natively support fungible tokens, like ethereum, bitcoin and so on. But non-fungible tokens – crypto art, like Tyler Hobb's Fidenza or the Bored Ape Yacht Club – are handled a little differently. Marketplaces like OpenSea, although not wallets, will automatically display your Ethereum NFTs if you connect your wallets. Rainbow Wallet displays NFTs within its app.

When choosing a wallet, a good rule of thumb is to check which wallets are recommended by a coin's community. Solana's community champions SolFlare and Phantom, while Monero's sings the praises of Cake Wallet. Bitcoincash.org recommends the Bitcoin.com wallet, among others.

Most of these wallets function as either desktop wallets, browser extensions or mobile wallets. Those that function as browser extensions are particularly useful when interfacing with decentralized finance (DeFi) protocols. The websites of Uniswap, [Aave](), Compound and more each have a "connect wallet" button. This functionality replaces the "log in to Google"/ "enter your email and password" of Web 2.

How to Create a Crypto Wallet

[Setting up a crypto wallet](#) only takes a couple of minutes. To get started with MetaMask, either download the app on your phone or install the browser extension. Then, MetaMask will ask you to set a password to the app, name your wallet, then write down your secret phrase (and then get you to check that you have done so). And that's it! You can then use your wallet to send or receive funds.

To find out your address, click the name of your wallet and MetaMask will copy it to your clipboard. Other wallets have near-identical setup processes.

[Download App for Android](#)   [Download App for iOS](#)

Hardware Wallets/Cold Wallets

The above is a survey of the popular web wallets, also known as "hot wallets" because you need an internet connection to use them. Hardware wallets, known as "cold wallets", are physical devices like USB sticks that you plug into your computer and only connect to the internet when they're docked. This makes them more secure, albeit a little cumbersome to use. Popular brands include Trezor and Ledger. Unlike hot wallets, you'll need to buy these hardware wallets from the official suppliers. Purchasing them secondhand or from a non-trusted supplier is incredibly risky as devices could be faulty, tampered with or contain malware.

While cold wallets are considered the absolute safest place to store your crypto as they are entirely offline and cannot be hacked, they also pose a similar risk: If you lose the physical drive and/or the private key, you will be unable to access your crypto. That's it. No password reset feature, no back button, zilch.

It's not just new crypto users who forget their passwords. Former chief technology officer of Ripple Labs, Stefan Thomas, admitted last year that he forgot the password to a crypto wallet containing 7,002 bitcoins (worth about $300 million as of March 22, 2022). He was left with only two guesses before his device automatically encrypted his coins and made them permanently unrecoverable.