A Beginner's Guide to Cryptocurrency Wallets updated on 8th July 2021

A cryptocurrency wallet is basically a software that enables you to track, send and receive coins through the blockchain like a bank account. Every wallet has a public key and a private key. A public key is something that everyone on the blockchain can see (Ex: 0xFAIJFD7WIUFDN…). Your **public key** is what identifies your account on the network. Think of it as your email address, because when someone wants to send you cryptocurrency, they will send it to this address. The **private key** is a string of 64 characters that can be generated from a 12-word seed phrase. It basically serves as the password of your account. It is used to sign transactions and to prove that you own the related public key. The seed phase is your personal access to the wallet and is either a random 12 word or 24 word set. The seed phrase should be written down and secured so that you only have access to it.

Why do you need a wallet if you can buy coins on sites like Coinbase or Binance?

There's an old saying in Tennessee that says: **"Not your keys, not your coins."** What it actually means is that if you keep your cryptocurrencies on an exchange (such as Coinbase, Binance, Kraken, Robinhood, etc.), you don't actually own those coins, because you don't have the keys to the related wallet. You technically own the exposure to those coins. You gain access to those wallets by logging into these exchanges, but your account can - theoretically - be deleted in the blink of an eye, or the exchange can get hacked, attacked, etc. And with it, your funds can disappear forever. If you want to learn more about this, make sure to look up Mt. Gox's hacking in 2014, almost $500 million dollars gone. It is an unfortunate event, but one that puts you on guard.

Wallet Types

There are 4 types of wallets that you should be using. Ideally, you can pick the one that fits your crypto habits the most. You should avoid using Web wallets. As always, if you can, please pick the safest wallet type in order to minimize the risk of losing your cryptos.

Hardware / Offline / Cold Wallet- This is an offline storage device (e.g. hard disk, USB stick). You might have heard the names Ledger or Trezor, these are the 2 biggest brands at the moment. The ledger supports over 1200 cryptocurrencies, while Trezor supports over a thousand. It is also the most secure way to store your cryptocurrencies.

Types:

Ledger Nano S and X (https://www.ledger.com/)- The most popular hardware wallet brand in the world, currently sells 2 different sticks. The S is the cheaper alternative, but if you handle transactions between multiple cryptocurrencies frequently, the larger storage of the Nano X should be more convenient. The Nano X also has Bluetooth 5.0 support. You can read more about Ledgers on their website.

Trezor (One and Model T)- Trezor is the other popular hardware wallet brand. The Trezor One is the cheaper alternative ($59), while the Model T is more expensive but comes with extended functionality and additionally supports cryptocurrencies such as ADA, XMR, XTZ, etc.

Despite the security of hardware devices themselves, **the weakest link is always the people using them.** If possible, avoid buying used hardware wallets, even though both Trezor and Ledger have security measures to avoid the attempt of installing malwares.

Beware that **Ledger was targeted by a cyberattack that led to a data breach** in July 2020. A larger subset of detailed information has been leaked, approximately 272,000 detailed information such as postal address, last name, first name, and telephone number of our customers. However, not a single coin was stolen as hackers did not gain access to private keys. Please keep this in mind when making your decision.

In July 2021 there have been reports of malicious tempered Ledgers being sent around to several users with a target to scam those users. If you get one do not use it. Learn about how these work and the measures in place to show they are untampered with.

**DO NOT BUY USED HARDWARE WALLETS or from sites such as EBAY, ALIEXPRESS etc. Even Amazon can be considered as dangerous! Always check the hardware wallet for any signs of tampering before using!!! Always buy from official sites, I personally would avoid sites such as Amazon or others.

Desktop Wallet / Hot Wallet- These are wallets that are installable on different desktops and are compatible with Windows, Mac, and Linux. Your keys are stored on your computer, and you can use this wallet even when you're offline. Note: Desktop wallets tend to be more advanced than mobile wallets, and usually come with more technically complicated features that can increase privacy or allow for more flexibility when it comes to signing transactions. Remember to be smart when sending funds and to consider gas/fees when transferring crypto.

Types:

Metamask- This is arguably the best browser based wallet with the best support. Metamask is mainly for ERC-20 tokens or Ethereum tokens but supports other chains. It works as a browser extension on FireFox, Chrome, etc. It is super easy to use and a good hot wallet.

Binance Wallet- This is another browser extension that is for the Binance Chain and Binance Smart Chain. Remember that there are two chains to it is important to send the correct tokens to the correct wallet addresses.

Exodus- This is a very user-friendly and easy to understand, reliable wallet. As of now, it is probably the most popular desktop wallet. Available on Windows, Mac and Linux as well.

Atomic- It is also a user-friendly and reliable wallet. Atomic supports 500+ assets and allows staking various cryptocurrencies. Available on Windows, Mac and Linux.

The top two are what I would recommend but there are others out there so DYOR and find one that works for you! MetaMask and Binance Wallet are used to link to Uniswap, PancakeSwap, or other DEXs (Decentralized Exchanges) available.

Mobile Wallet / Super-Hot Wallet- These applications are installable on your mobile phone and are not accessible via PC. Beware that even though an app can hold crypto, it doesn't mean it is NOT custodial. (e.g. Coinbase has a mobile app, but it is custodial, meaning that they control your coins.) Exodus or Atomic mobile apps are recommended if you decide to create a mobile wallet.

Types:

Trust Wallet- Trust has been getting very popular. They have options for staking certain coins and allow to see specific nodes. I do not have experience with the staking at the moment.

Coinbase Wallet- Another good mobile wallet that makes it easy to connect to Coinbase if you use Coinbase Pro. You can also store NFTs on there.

Exodus and Atomic Wallet- Both are also available on mobile.

Note: Many coins have their specific wallets such as Algo, ADA, VET and others. Those wallets sometimes have perks such as staking, delegating and such. Staking means that you lock or soft lock your coins and you get rewards in either more of the same coin or coins such as VeThor.

Paper Wallet- A paper wallet is essentially a piece of paper including your public and private key, or a QR code (so that you can quickly scan them and add the keys to a software wallet to make a transaction). It's a really safe way to store your cryptos because your keys are not connected to any servers. The only way someone can steal your cryptos is if they steal this paper.

If you choose to go the physical way of storing keys, I highly recommend that you buy a piece of soft metal and a cheap Dremel tool to etch the keys into the plate. it takes about 20 minutes to get it done but its 1000x times safer. Paper burns, gets wet, gets eaten by pets and such, metal or steel does not.

When Sending Funds

Always be cautious and double-check everything. It helps to send extremely small portions to an address first to make sure it goes through. Once you get the transfer of 0.01% of your funds, you know it is correct. Keep your devices malware-free, and do not click on anything suspicious (such as emails from "Binnance", crazy bonus links from "Coimbase", etc.). If exchange supports anti phishing code (Binance, Kucoin and others do) be sure to check it out!

Lastly, when moving funds to a wallet you NEED to consider fees. Do not send transactions willy-nilly, gas prices can be expensive and add up so be smart with transactions. If you want to send funds from one exchange to another, send using cheap alt coins like Algorand, Bitcoin Cash, BNB, etc. There is always someone who tried to transfer 20$ of BTC just to find that half of that amount was needed to cover the gas fees.

Do I really need to use a wallet?

Yes and no. Leaving your Bitcoin at the exchange or brokerage you bought it from is generally (Remember Mt. Gox) a very secure option. Leaving it in non-crypto exchanges like Robinhood is less secure as Robinhood will delay transactions and decline sells when prices or liquidity crashes. Also, wallet security depends on you and how much you did to keep it secure.

Information by me, u/Weaver96, and u/anakanin.