CRYPTOCURRENCY WALLETS

Our definitive guide to cryptocurrency wallets

COIN RIVET

Independent British blockchain and crypto news

CONTENTS

CRYPTOCURRENCY WALLETS, EXPLAINED

A cryptocurrency wallet is a digital wallet used to securely send and receive currencies like Bitcoin and Ethereum. Unlike your everyday purse or wallet, cryptocurrency wallets don't actually store your coins and tokens.

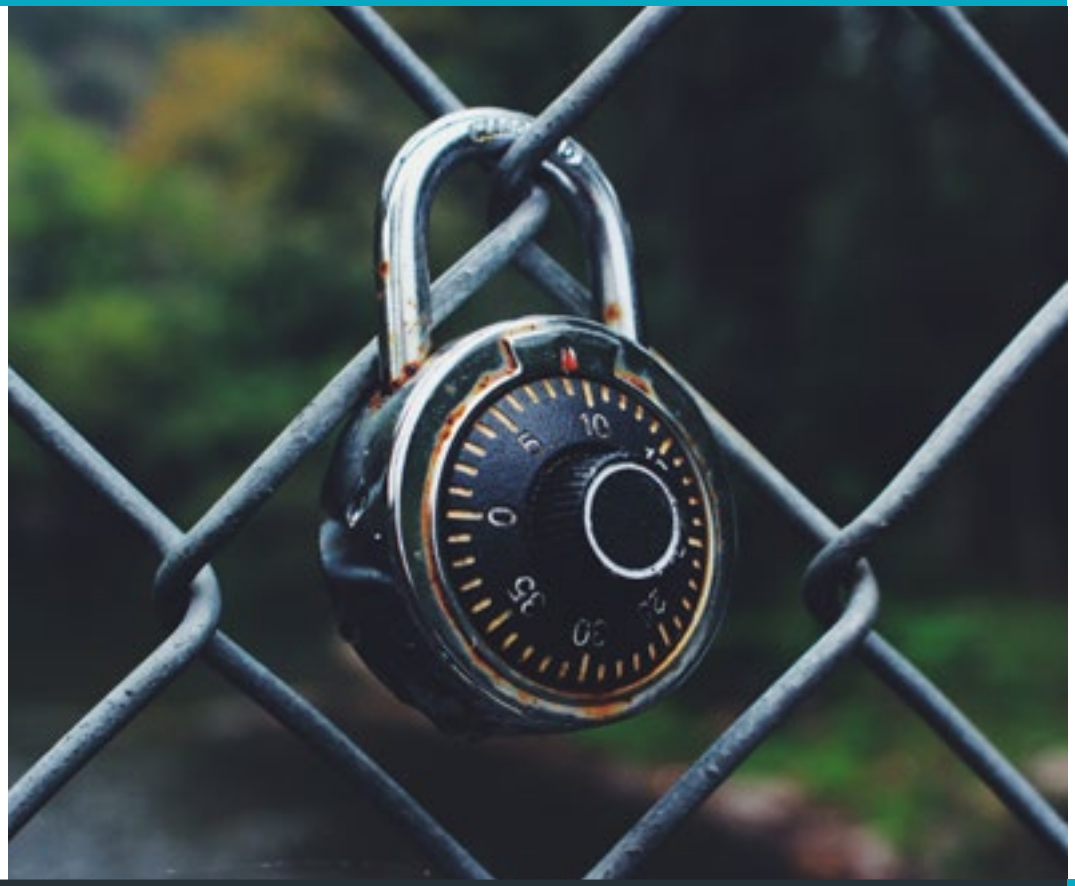
Your currency, whether it's Bitcoin or Ethereum, doesn't exist anywhere in a physical form. What exists instead is a record of any transactions you have made and these are added to a blockchain. To send or receive cryptocurrencies, you need a digital wallet that provides you with private and public keys.

Cryptocurrency wallets, as long as you look after your private key, keep your funds secure. They prevent unauthorised access to your currency and offer security against potential hackers and thieves.

An overview of public and private keys

Public key cryptography (also referred to as asymmetrical cryptography), is any cryptographic system that uses pairs of keys. A key is a piece of information that unlocks or decodes a cryptographic algorithm. There are two types of keys.

- **Public keys:** these may be shared widely and known to many people
- **Private keys:** these should only be known to the key owner



The use of public and private keys accomplishes two functions – authentication and encryption.

- Authentication is where the public key verifies that the message was sent by the holder of the paired private key.
- Encryption is where the paired private key holder) can decrypt a message encrypted with the public key.

When it comes to cryptocurrency, each piece of currency has its own private key. When you receive any type of digital token or coin, ownership of those coins is assigned to your wallet's address – as long as your private key matches the public address of said currency.

Your wallet address can be thought of in the same way as the sort code and account number on your fiat bank card. No one can access the wallet with only the public wallet address, they can only send funds to it if they wish.

Wallet addresses can also be searched in block explorers. Inputting a wallet address will show every transaction that wallet has sent out and received. Users can complete these searches to assess the history of the coins and how many wallets they have passed through.

The importance of private keys

Think of a private key like a key for a safety deposit box filled with valuable commodities. If you lose the key, or accidentally give it to someone else, you won't be able to access your holdings. It works in the same way with crypto. Lose your private key and your crypto is as good as gone.

Storing private keys is a critical part of securely storing cryptocurrency. There are a variety of wallet types that offer different levels of security in the event of theft or loss but most wallets have a feature that allows you to reset your private key. This is done by generating a 24-word mnemonic code which must be written down upon initiating the wallet.

HOW SECURE ARE CRYPTOCURRENCY WALLETS, REALLY?

It's important to note that the decentralised nature of cryptocurrency means that you're responsible for the safety of your own assets. According to leading members in the industry, cryptocurrency is the easiest asset in the world to steal.

So your choice of cryptocurrency wallet should be thoroughly researched. In short, your wallet is only as good as your approach to security.

Many wallets come with different security features built-in and there are a number of additional steps you can take to protect yourself. We take a look at some of those steps below.

Two-factor authentication

Two-factor authentication, commonly abbreviated to '2FA,' is a must when it comes to protecting your cryptocurrency wallet. Most, if not all, the top exchanges utilise 2FA. This practice requires users to enter two layers of identification to access their accounts. This gives users extra assurances about the level of security available, while deterring cybercriminals from malicious activity.

In instances where a hacker obtains your password, they would still need a second method of identification to access the account. This second method involves a human element, such as fingerprint scanning, that hackers aren't able to replicate.

Explore different types of wallets

Online wallets and mobile wallets are inherently vulnerable to criminality in the cyber space. Luckily, these aren't the only wallets available to cryptocurrency users. To improve overall cryptocurrency security, you could consider using hardware wallets. Hardware wallets can be more secure as they give you direct, offline access to your coins, they're protected by a private key, and they eliminate the risks of being hacked.

Two-factor authentication and strong passwords should still be used to enhance the security of your hardware wallet. This protects you in instances of wallet loss. If you misplace the physical wallet, you still have access to the currency address which allows you to programme a new hardware wallet. Access to your coins doesn't need to be lost. Paper wallets are also an option for users who want to minimise their online footprint. Keep your addresses and keys written down on paper and keep them in different locations. Using a paper wallet eliminates the need for any third party sites or applications, arguably providing you with the upmost security. However, lose any part of your keys or addresses and you'll also lose access to your cryptocurrency.

Avoid carrying large amounts of crypto in a mobile wallet

Mobile wallets and exchanges make trading on the go quick and easy, making them increasingly attractive to crypto users. Keeping a small amount of funds in your mobile wallet is a great idea for making instant purchases, however the simplicity of these wallets is often their downfall. Generally, you just need to download an application and go through a minor registration process but this simplicity also attracts hackers and other malicious attacks. With this in mind, it's not advisable or secure to carry large amount of cryptocurrency in your mobile wallet. Your funds could be easily compromised. If you're a serious investor or trader then consider hardware wallets.

So, in short, some wallets may offer specific features, but your wallet is only as good as your own approach to crypto security.

DIFFERENT WALLET TYPES: THEIR PROS AND CONS

There are a wide variety of wallets available on the market, with each coin typically offering its own wallet. For serious traders who dabble in more than one currency, though, there are multi-currency cryptocurrency wallets available.

These allow you to store different types of crypto at the same time.

But, if you're just beginning, there's a fundamental bit of knowledge you need to acquire. And that's the difference between hot and cold storage. Hot storage is connected to the internet, whereas cold storage isn't.

Electronic/software wallets

Any online wallet brings with it the inherent risks associated with cybercriminals. Security breaches, hacks, and theft can all take place if there is a vulnerability in the software. If access to your private key is gained, then your crypto can easily be lost.

Electronic wallets can be hosted on a cloud-based service. Hosted wallets more often than not focus on user-friendly interfaces, but while they look aesthetically pleasing, you are placing trust in a third party to hold your private keys. This can put you in a vulnerable position as online wallets may easily be hacked.

There are other types of software wallets, such desktop installations that grant you, the user, security over your keys. This is naturally safer than trusting a third party with your private keys, but you then have to make periodic backups. If you don't and your computer/device is compromised or simply stops working, you could lose all of your cryptocurrency. Don't forget that you can still be hacked with this type of wallet.

Hardware wallets

Cold wallets are typically safer than hot wallets as they minimise the risks of cybercrime. You also don't have to trust a third-party to look after your private keys. Hardware wallets are usually small devices, such as USBs, that can connect to the internet to engage in transactions. Hardware wallets are incredibly secure because they function offline and they can't be hacked unless you connect one to the internet.

Paper wallets

A cryptocurrency paper wallet is a way of storing crypto offline in cold storage. To have a paper wallet users must print out their public address and private keys on a piece of paper then store it securely where nobody has access.

The reason many cryptocurrency holders use a paper wallet is because they don't need to worry about a piece of hardware or software failing.

Although the three wallets listed above are the main types, there is a wider range available for your needs.

Watch-only cryptocurrency wallet

With a watch-only wallet you can keep track of transactions, but transactions can't be initiated since there is no private key stored in the wallet. The private key can be kept safe in another location.

Multi-signature (multi-sig) cryptocurrency wallet

A wallet where multiple users have to sign a transaction using their private key.

Brain cryptocurrency wallet

A brain wallet requires you to remember the information required to regenerate the private and public key pair. This is often facilitated by memorising a mnemonic sentence - the seed (or basis) of which is generated by software.

Deterministic cryptocurrency wallet

A single key (or seed) can be used to generate an entire "tree" of key pairs. The single key serves as the root of the tree. The advantage of this system is if a hard drive becomes corrupted and the wallet unrecoverable, a new wallet can be created using the same seed. All of the addresses and private keys from the old wallet will return.

Non-deterministic cryptocurrency wallet

Each key is randomly generated on its own accord. Any backups of the wallet must store each and every single private key used as an address, as well as future keys that may have already been given out as addresses but not received payments yet.

Your choice in a crypto wallet should come down to your own research, requirements, and what you think will work best for your needs. Here, we have warned you to proceed with caution. Below, we'll take a look at some of the leading wallets you can use.

FIVE WALLETS YOU COULD USE

Cryptocurrencies, whether Bitcoin or any altcoin, face a lot of market volatility. With no control over how the markets act, it's important that you take precaution over the type of wallet you use.

Here are five that could prove useful for your requirements, but there are many more available on the market.

1. Ledger Blue

Ledger Blue is a handheld hardware wallet that features a 3.5-inch touchscreen and supports bluetooth and USB connectivity. It is designed to run multiple companion apps to allow keys to be stored for a number of currencies. Compatible with desktop or mobile, it features two-step authentication for additional security.

2. Jaxx

This multi-currency cryptowallet was created in 2014 by Ethereum co-founder Anthony Diiorio. It supports many currencies including Bitcoin, Ethereum, Litecoin, Dash, Zcash, Augur, Salt, Civic, Qtum, Blockchain Capital, Bancor. The wallet can be accessed via desktop and mobile device that can be paired so transactions are up-to-date the next time a user switches between devices.

3. Trezor

Trezor can be described as the original and most secure hardware wallet. It's a small device that can be connected to a computer. Created by SatoshiLabs it's the world's first secure Bitcoin hardware wallet. These days it also supports other popular cryptocurrencies such as Bitcoin Cash, Dash, Ethereum, Ethereum Classic, Litecoin, Zcash plus Ethereum powered tokens.

4. My Etherwallet

My Etherwallet, especially designed for Ethereum, is a "paper based" wallet so even though the wallet is created using the web, all of your information and currency are stored on your computer and not on wallets' servers.

5. Bitcoin Core

Bitcoin Core is the software that runs the entire Bitcoin network. A secure digital wallet is included in the software and it can be used to send and receive Bitcoin. Storing your Bitcoin in the wallet will allow users to contribute to the Bitcoin network by validating transactions and storing a copy of the blockchain.

At Coin Rivet, we make it easy to keep up with the latest wallets on the market and all the latest security information. Access our insights at anytime to stay one step ahead in the world of cryptocurrency.

Bringing you news, analysis, opinion and insight from the fast-moving blockchain world. Our team of journalists and contributors cover the likes of cryptocurrencies, wallets, exchanges and ICOs across a wide range of sectors including retail, fintech, banking and gaming. We go beyond the press releases and marketing hype to tackle all the industry topics that matter.

Featured in

FOX NEWS EXPRESS COINGEEK

coinrivet.com