What To Write Down to Recover Your Bitcoin Wallet In The Future

Jeff Hong ⋮ 7-8 minutes

Sometimes your wallet recovery seed phrase is not enough.

Wallet recovery can be a complicated endeavor. All wallets do not follow the same rules. The reason for this is that wallet developers don't implement the same standards, have their own specific standards, or implement standards differently when designing their wallets.

Thus, certain functions and methods may be unsupported. For wallet recovery, this results in varying ways your wallet is created and recovered that may not translate to another wallet software.

One day, the hope is that wallet developers will either all abide by the same universal standards or check all of the other standards to recover your wallet. But until then, it's best to make a note of some specific characteristics of your wallet for the best chance to recover your wallet in the future.

To find out information on each of the characteristics below, refer to your wallet's website or use a search engine of your choice (search "wallet name" "subject", e.g. trezor derivation path)

A good wallet should have documentation on each of the items below. If not, we would recommend choosing another wallet. The lack of documentation is not only a sign of irresponsibility but it introduces risk of recovery in the future.

Wallet Recovery Checklist

12/24 Recovery Seed Phrase*	Recommend Storing Separately
Seed Format	
Passphrase (if applicable)*	Recommend Storing Separately
Wallet Used	
Cryptocurrencies Held	
Address Format/Prefix	
Derivation Path	

*We **recommend** writing or storing your **recovery phrase** and **passphrase** separately from the rest of the items.

The other items are public information and bears little risk in being discovered (other than the fact you own cryptocurrency). It's best to store the rest of these items together in an easily accessible digital format (email, cloud storage, etc.) for your own convenience.

12-24 Word Recovery Seed Phrase

Your ***recovery phrase*** (also known as mnemonic seed, wallet backup, etc.) is an ordered set of 12-24 words that is randomly generated by your wallet. It stores the information that can be used to recover your wallet and coins when your wallet fails unexpectedly (such as damage, unable to access, misplaced, theft, etc).

Writing down your recovery phrase is first and foremost. Without this, there is almost no chance that you'll be able to recover your wallet if something unexpected happens.

Seed Format

Seed format refers the method or technique your wallet used to generate your recovery phrase. In other words, how your wallet took all the information it needed to recover your wallet and made it into a phrase.

Your wallet most likely follows the BIP39 standard (luckily most wallets do). Thus, you would write down *BIP39*.

There are other seed format standards such as Electrum, AEZEED, and SLIP39, but these are very wallet specific. If you aren't using Electrum, Lightning Network Daemon (LND), or splitting your recovery phrase using Trezor's Shamir Secret Shares, then don't worry about.

Passphrase (Optional Feature, If Applicable)

A passphrase is an optional feature of BIP39 that adds an additional layer of security on your seed. Think of it as an additional word to your seed phrase that can be (almost) anything. (A-Z, a-z, 0-9, special characters i.e. ASCII characters.)

Wallet's do not have this feature activated by default. You have to **manually** enact this feature. So, if you do not know what this is or did not activate the passphrase feature, don't worry about it.

If you did, remember to write it down as well. Your seed phrase by itself is technically a wallet with an empty ("") passphrase. Adding a passphrase creates a **different** brand new wallet on top of your seed. If you do not have your passphrase, you will not be able to recover your wallet.

Remember, there is no such thing as a “wrong” passphrase. Every different passphrase you enter is a entirely new wallet. Be careful when recovering your seed with a passphrase.

Wallet Used To Generate Recovery Phrase

Write down the name of the wallet you used when you generated your wallet (e.g. trezor, ledger, etc.)

This is probably the **simplest thing** you can note down to be able to recover your wallet in the future.

You can use the same wallet software (with your recovery phrase) if you need to recover your wallet. You can also look up the wallet's documentation if you need more information to recover your wallet on a different wallet software.

If the wallet you used no longer exists, writing down the name can help the research (for what standards it used) needed to recover your wallet. Thus, it's best to choose a well-known wallet with a long track record.

Cryptocurrency Name

If you are holding more than one type of cryptocurrency, it's also a good idea to note down which type of coins or tokens you have. **Do not write** how much you have; only the name.

Not all wallets support all cryptocurrencies and for most wallets, you have to "enable" which cryptocurrencies you have.

Writing down which cryptocurrencies you have will let you know in the future which wallets can recover your coins.

Address Format/Prefix

When you send bitcoin to your new wallet for the first time, it will give you a long combination of numbers and letters to send it to (e.g. 1CxAxBy5Ho7s8yrw2ARiq7YFL9YjrW5DJX). It will either start with a 1, 3, or bc1. This is your address.

An address is a string of alphanumeric characters used as an identifier to send cryptocurrency to (Like an email address or mailing address).

There are different types of addresses. The type or format of an address refers to how a wallet "makes" a transaction.

Some wallets may not support some address formats and thus, it would wise to write down which address format your wallet uses.

The easiest way to do this is to note down the **prefix** of your addresses.

For Bitcoin, there are three addresses in use:

Addresses starts with 1... (P2PKH or Legacy)

Example: **1**CxAxBy5Ho7s8yrw2ARiq7YFL9YjrW5DJX

Addresses starts with 3... (P2SH)

Example: **3**Jx91hgNCWSZqFSbjdvdNUCkiFd2zD2pBA

Addresses starts with bc1...(Bech32 or Native Segwit)

Example. **bc1**qyrl3q6a7dayq962c3m05s085xer49kkfkfazqp

Derivation Path

A wallet can have multiple "accounts" that stores your cryptocurrency (think of an actual wallet with multiple pockets).

A derivation path tells your wallet "where to store" those coins and thus how to "find" those coins using your recovery seed phrase (like a map).

The method in which your wallet stores your coins are described in Bitcoin Improvement Proposals.

Your wallet may support **one or more** of these derivation paths so it's important to write which ones your wallet supports.

Bitcoin Improvement Proposal	Derivation Path Notation
BIP32 (*Virtually All Wallets Use This*)	m/0'
BIP44	m/44'/0'/0'
BIP49	m/49'/0'/0'
BIP84	m/84'/0'/0'