What is a Seed Phrase?

Jeff Hong ⋮ 9-12 minutes

What is a Seed Phrase?

Your ***seed phrase*** (also known as recovery phrase, seed phrase, recovery seed, 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 bitcoin and cryptocurrency when your wallet device fails unexpectedly (such as damage, unable to access, misplaced, theft, etc).

You (or anyone else who knows your seed phrase) can input it into another wallet device (or multiple wallet devices) to access your coins. Thus, it is crucial that it is hidden in a secure location and stored/written on something that will last a lifetime.

Introduction To Your Seed Phrase

You've chosen a wallet to store your bitcoin or cryptocurrency. It is either a hardware wallet (like a Trezor or Ledger) or software wallet on your mobile phone or desktop computer.

When starting your wallet, it gave you a 12 or 24 word phrase of seemingly random words in a specific order.

This phrase is known as your ***seed phrase***. It can also goes by recovery phrase, mnemonic phrase, seed, etc.

Your wallet also might have informed you to **write your *seed phrase* down** somewhere secure. In the event the device your wallet is on gets lost, broken, destroyed, corrupted, stolen, etc. your seed phrase is the **one** thing that can restore and recover your wallet and coins on another device (like a secret username and password).

And remember, not only the words themselves are important but the **order of the words** are equally as important.

Your Wallet

Remember, your coins **are not stored** on your wallet device. They're stored on the blockchain (i.e. a universal network) and can be accessed by utilzing your seed phrase.

The device (your phone, computer, hardware wallet) is used to interact with this network (sending/receiving coins) but your seed phrase is the information can show ownership of those coins on that network (giving you the authority to send coins).

In other words, your device is storing the "access" to those coins, not the coins themselves.

This is crucial because electronics will break down at some point, but information (e.g. your seed phrase) can last forever. You're able to input your seed phrase another device to access your coins.

A Seed Phrase is Not Enough

A seed phrase (by itself) is not enough to recover your wallet and coins.

I know. What the heck. But think about it; a seed phrase is just a bunch of random words. Your wallet needs to be able interpret those words to make it something *meaningful*.

In order to fully interact and access your coins, your wallet needs to:

1. Understand the method your original wallet used to create your seed phrase
2. Know where to find your coins
3. Support the specific coin itself (e.g. bitcoin, ethereum, etc.)

1. Method Used to Create Your Seed Phrase: Mnemonic Phrase

Luckily, there is a widely used standard that many wallets use to create seed phrases. The method and format for a seed phrase is described in a Bitcoin Improvement Proposal (BIP). BIP's are various "features" and "rules" of Bitcoin. They are designated by a specific number. Topics of these BIP's can vary widely.

The topic of seed phrases fall under Bitcoin Improvement Proposal: 39 (BIP 39). It describes the method your wallet creates a mnemonic phrase -- a group of easy to remember words -- that is the "link" to your coins.

This format also includes a specific list of 2048 words (known as the BIP 39 wordlist) that the words in your seed phrase is pulled from.

If you're wondering if your wallet uses BIP 39, search your wallet name and the term "BIP39" in the search engine of your choice to find its documentation.)

2. Where To Find Your Coins: Derivation Paths

The method to create seed phrases are just one part of the equation. Your wallet needs to also know "where to find" your coins.

First, we need to understand what a wallet actually is. Your wallet is really just a bunch of linked numbers (even though it may not look like it), some of which are associated to coins (e.g. those long addresses you send coins to).

It's easier if you think of your wallet as a literal tree (with leaves, branches, etc). Your seed phrase is the recipe to create (and re-create) a specific seed that can grow a specific tree. That specific tree has a trunk, branches, twigs, and at the very end, leaves. Your coins are stored on those leaves.

But, if I asked you to find leaves, from a specific type of twig, from a specific type of branch, it could get pretty difficult. You'd need some sort of "map".

That "map" is a derivation path. It tells your wallet the path in which to take to find these coins. These "maps" or derivations paths are described in Bitcoin Improvement Proposals (BIP). The most common being described in BIP 44, BIP 49, and BIP 84. Whether a wallet supports a certain derivation path should be well documented or referenced on their website.

3. Coin Support

You might have noticed that not all wallets support all coins.

Going back to our tree example, certain "branches" can grow only specific "leaves". These "leaves" can only store a certain coin.

This should be somewhat straightforward but your wallet must support the coin in order to interact with it. The software must have the capability to recognize said coin.

Whether a wallet supports a certain coin (again) should be well documented or referenced on their website.

Recovery

Different wallets have different instructions for recovering a wallet but in general, you're going to be typing/choosing words in the specific order of your seed phrase to re-generate your wallet on that new device/software.

That wallet re-create that "tree" using your seed phrase and begin "looking" for your coins utilizing the derivation paths it supports and the coin you told it you have.

Inputting your seed phrase on a wallet that doesn't support a specific seed format, derivation path, or coin does not mean those coins are gone. It just means, you are unable to send/receive/recognize since the software doesn't support it. You simply have to find a wallet that does.

Can Someone Guess My Seed Phrase?

Remember when we said that your seed phrase comes from a specific list of 2048 words. Someone would have to guess all the words AND put them in the correct order. There are 777,788,267,247,859,345,059,141,959,844,041,626,185 possible combinations for a 12 word seed phrase.

In other words, it ain't going to happen anytime soon.

But the number of combinations decreases the more words someone one else knows. Thus, it is important that you keep your seed phrase hidden and secret.

If you're wondering, no you cannot pick and choose your own seed phrase. The last word of a seed phrase must be a *very specific word*. This word is called a "checksum". Without going into technical jargon, it is something your wallet software uses to check if the rest of the words are following the "rules". So let your wallet generate a seed for you.

Seed Phrase Security

You can use your seed phrase to generate and re-generate your wallet **as many times** as you want and in **as many devices** as you want (Yes, your wallet can be on more than one device at one time)

Pretty nifty huh? Those 12-24 words are the link to your coins that you can take literally anywhere and can last forever. You should think of your seed phrase as your wallet.

Thus, it is imperative that how ever you store or write your seed phrase, it is not only hidden but will last.

There have been many instances of people making headlines by losing bitcoin:

- Bitcoin Investor Loses $50,000 as His Wallet, Backups Get Damaged by Fire
- I Forgot My PIN: An Epic Tale of Losing $30,000 in Bitcoin
- 51 BTC locked up, can’t remember seed/passphrase
- Drug dealer loses $58M in bitcoin after landlord accidentally throws codes out
- 533 Bitcoin Hard Drive Lost

Don't be one of them. Seriously.

Over 4 million bitcoin (20% of total circulation) have been lost forever. Don't add yours to that.

Not only are you protecting your seed phrase against other people, you're protecting your seed phrase from your own stupidity (yes, we're all just a little stupid sometimes), natural occurrences (like pests, flooding, fires, and storms), and the test of time.

Time includes physical deterioration such as corrosion and fading; and mental deterioration such as forgetfulness.

So again, make sure your seed phrase is written down or stored on something that you'll be able to access **for a long time**.

That means it has to be durable and at the same time accessible. (That doesn't mean to bury your seed phrase 6 ft into the ground. You are storing your seed phrase for your future self. Don't make them mad.

Securing your seed phrase is a job that requires common sense and thoughtfulness. It is important that you do as much as you need to in order to not only feel safe but confident in accessing your bitcoin seed in the future when you need it.

We've written a few topics on seed phrase preservation and security:

- Guide to Securing Your Bitcoin Wallet Recovery Phrase
- Hiding Your Bitcoin Wallet Recovery Seed Phrase
- Long-Term Preservation of Your Cryptocurrency Wallet Recovery Seed Phrase

Metal Seed Phrase Storage

We recommend storing your seed phrase on something physical like paper or metal. Why? Because it is not connected to something than can be hacked and can last a **really long time**.

When we say "stored on metal" we really mean "written on metal". Metal such as stainless steel or titanium are great materials for longevity and durability of your seed phrase (more so than paper). Metal protects your seed phrase from wear and tear, heat/fire, and water/corrosion damage.

Blockplate uses an innovative method to securely store offline your seed phrase on durable, long-lasting steel. It has been tested against the competition and proven not only to be indestructible but the absolute simplest way to store your seed phrase on metal.