Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 9 OF 13

# Seed Phrases and Backups

The 12 or 24 words able to rebuild your whole wallet, how to keep them safe, and the people who will try to get them

6 min read  6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 9 OF 13

# Seed Phrases and Backups

IN ONE SENTENCE

A seed phrase is a list of 12 or 24 ordinary words that can recreate every private key in your wallet. Keep it and you can recover from a lost or broken device. Leak it and anyone can take everything, with no way to undo it.

## One backup for every key

In Lesson 8 we saw that a wallet creates a fresh address for every payment, and each address comes from its own private key. Backing up dozens of separate keys would be a nightmare. Modern wallets solve this by generating all of their keys from a single starting number, called the **seed**.

The seed is shown to you once, when you first set up the wallet, as a list of 12 or 24 words. This is your **seed phrase**, also called a recovery phrase. Feed the same words into almost any modern wallet app and it will recreate exactly the same keys, in the same order, and find all the same coins. The phone or hardware device can be lost, stolen or broken. As long as you have the words, your bitcoin is not gone.

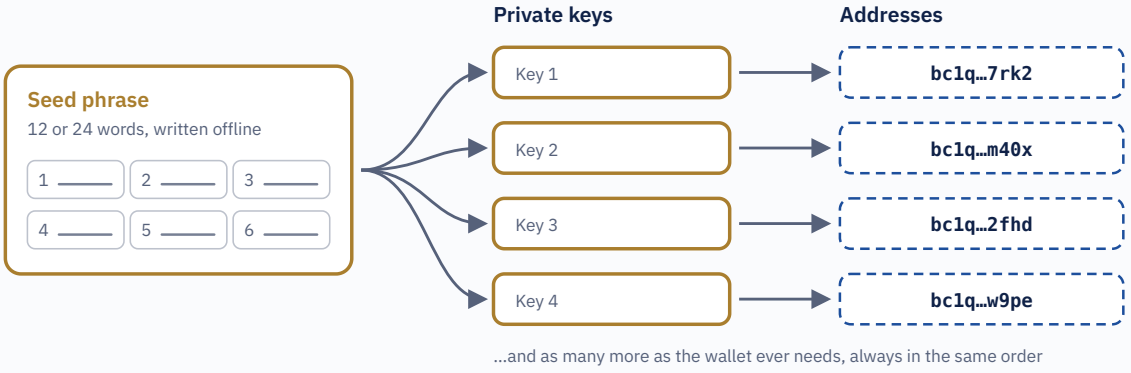



Figure 1. One seed phrase generates every private key in the wallet, and every key gives an address. Restore the phrase in any compatible wallet and the same keys and coins come back.

**ANALOGY: THE PHOTO NEGATIVE**

In the days of film cameras, the negative mattered more than any print. Lose a print and you could make another from the negative, as many times as you liked, in any photo lab. A seed phrase is the negative for your wallet. The app on your phone is just one print. But anyone else holding the negative can make their own prints too.

## Why words, and why these words

Behind the scenes, a seed is just a very large random number. Writing it down as 64 characters of digits and letters would invite mistakes, so a widely used standard turns it into words taken from a fixed list of 2,048 simple English words. Each word stands for a chunk of the number.

The list was built with care. In the English version, no two words share the same first four letters, so a smudged ending is still readable. The last word also works as a built-in check: if you copy one word wrong, the wallet will usually warn you that the phrase is invalid instead of quietly opening an empty wallet.

The words are chosen by the wallet at random, not by you. That is the whole point. A 12-word phrase can be one of about 340 billion billion billion billion combinations, a number with 39 digits. A sentence you invented yourself, or song lyrics, would be guessed quickly by programs built to try millions of common phrases.

Some wallets also let you add an optional extra password, often called a passphrase. With it, the 12 or 24 words alone are not enough to open the wallet. It adds protection, but if you forget the passphrase, the words will not help you either.

## Storing it: offline, durable, findable

A good backup has to survive three threats: thieves, accidents like fire or water, and your own memory years from now. Here is how common options compare:

| Where | Strong against | Weak against |
|---|---|---|
| **Written on paper, kept at home** | Hackers, since it never touches the internet | Fire, water, and anyone who finds it |
| **Stamped on a metal plate** | Hackers, fire and water | Anyone who finds it, unless it is well hidden |
| **Second copy in another place, such as a safe deposit box** | Losing the only copy in one disaster | More copies mean more places it could leak |
| **Photo, screenshot, notes app, email or cloud** | Nothing that paper does not handle better | Hacked accounts, synced backups and malware that scans images |

Whatever you choose, write the words in order, number them, and check every one against the screen. Then do a restore drill: with only a small amount in the wallet, wipe it or use a second device, type the words back in, and confirm the same addresses appear. Finding a mistake now is cheap. Finding it in an emergency is not.

## Nobody legitimate will ever ask for it

Because a seed phrase opens everything, it is the main target of crypto scams. The tricks vary, but the request is always the same: type your words somewhere. It may come as a support agent in your messages, a pop-up saying your wallet needs to be "synced" or "validated", a fake wallet app in an app store, or a website promising a free airdrop.

The rule is simple and has no exceptions. Your seed phrase is only ever typed into your own wallet, when you are restoring it yourself. No wallet company, exchange, developer or channel admin needs it, ever.

**A REAL EXAMPLE: THE FAKE REPLACEMENT WALLETS**

In 2020, a database at the hardware wallet maker Ledger was breached, and in December the names, home addresses and phone numbers of about 272,000 customers were posted online. Months later, some customers received a parcel in what looked like real Ledger packaging, with a letter saying their device was unsafe and a "replacement" was enclosed. The instructions asked them to enter their recovery phrase. The device had been tampered with, and the words went straight to the thieves.

## Why this matters for traders

- **Trading chats are hunting grounds.** Scammers join busy crypto groups, copy the names and photos of admins, and message people directly offering help or a "wallet check". MARKET TALKS will never ask for your seed phrase, private keys or passwords, and neither will any real team.
- **Your exchange account has its own seed-like secrets.** Exchange accounts do not use seed phrases, but your two-factor authentication backup codes play a similar role. If someone gets them along with your password, they can take over the account. Store them offline, just like a seed phrase.
- **Plan for the people after you.** Researchers estimate that millions of bitcoins are already lost for good, many because the only person who knew the keys died or forgot them. If you hold meaningful amounts, think about how a trusted person could recover them one day, without giving anyone access today.

## Key terms

| | |
|---|---|
| **Seed** | The single large random number from which a wallet generates all of its private keys. |
| **Seed phrase** | The seed written as 12 or 24 words. It can recreate every key in the wallet. Also called a recovery phrase. |
| **Word list** | The fixed list of 2,048 words that seed phrases are drawn from, so that any compatible wallet can read them. |
| **Checksum** | A built-in check, carried in the last word, that helps a wallet notice when a phrase has been copied wrong. |
| **Passphrase** | An optional extra password added to a seed phrase. Without it, the words alone cannot open the wallet. |
| **Restore drill** | Practicing a recovery from your written seed phrase before you store serious money in the wallet. |

## Key takeaways

1. Modern wallets generate every key from one seed, shown to you as a seed phrase of 12 or 24 words.

2. With the seed phrase, you can rebuild your wallet on a new device even if the old one is lost or broken.
3. The words come from a fixed list of 2,048, are chosen at random by the wallet, and the last one acts as a check for mistakes.
4. Keep the phrase offline and durable, never in photos, notes apps, email or cloud storage, and test a restore with a small balance.
5. Anyone who asks for your seed phrase is trying to steal from you. It is only ever typed into your own wallet.

## Test yourself

Circle one answer for each question. The answer key with explanations is on the next page. You can also take this quiz online at markettalks.info and see your score instantly.

**1. What can a seed phrase do?**

A. Reset your exchange password
B. Recreate every private key in your wallet
C. Speed up your transactions
D. Cancel a payment you already sent

**2. Your phone with your wallet app is stolen. You have your seed phrase written down. What should you do?**

A. Restore the wallet from the seed phrase on another device
B. Contact Bitcoin's customer support
C. Accept that the coins are lost
D. Ask the exchange to reverse the theft

**3. Why should you not make up your own seed phrase from a favorite quote?**

A. Wallets cannot read sentences
B. It would make transactions slower
C. Phrases people invent are easy for programs to guess
D. Quotes are protected by copyright

**4. Which is the safest way to store a seed phrase?**

A. A screenshot in your photo gallery
B. A note in your email drafts
C. A file in your cloud drive
D. Written or stamped offline, kept somewhere safe from fire and theft

**5. What does the last word of a seed phrase help with?**

A. It sets the wallet's password
B. It works as a check that catches most copying mistakes
C. It decides which coin the wallet holds
D. It shows the wallet's balance

**6. Someone in a trading group messages you offering to fix your wallet if you share your seed phrase. What is happening?**

A. It is normal support practice
B. They need it to check your balance
C. It is a scam, because no legitimate helper needs your seed phrase
D. They are verifying your identity

# Answer key

1 B

**Recreate every private key in your wallet**

The seed phrase is a written form of the seed that all your keys are generated from. Any compatible wallet can use it to rebuild the same keys and find the same coins.

2 A

**Restore the wallet from the seed phrase on another device**

The coins live on the blockchain, not in the phone. Restoring from the seed phrase gives you control again, and moving the funds to a new wallet right away protects them.

3 C

**Phrases people invent are easy for programs to guess**

The security comes from the words being chosen at random from a huge number of combinations. Human-chosen phrases are far more predictable.

4 D

**Written or stamped offline, kept somewhere safe from fire and theft**

Anything stored on an internet-connected account or device can be reached by hackers or malware. An offline, durable copy avoids that risk.

5 B

**It works as a check that catches most copying mistakes**

Part of the last word is calculated from the others, so if one word is copied wrong, the wallet will usually say the phrase is invalid.

6 C

**It is a scam, because no legitimate helper needs your seed phrase**

Anyone with your seed phrase can take everything in the wallet. Real support teams never ask for it, so the request itself proves it is a scam.

SOURCES


- Bitcoin Improvement Proposal 39, mnemonic code for generating keys (GitHub): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer, criminals mailing altered Ledger devices to steal cryptocurrency: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- Cointelegraph, up to four million bitcoins may be gone forever (Chainalysis estimate): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

CONTINUE LEARNING

# Up next: Lesson 10 Custody: Exchange Account or Your Own Wallet

This lesson is part of the free Blockchain track at the MARKET TALKS Education Center: Beginner, Intermediate and Advanced lessons, each with a quiz and a downloadable PDF.

**Education Center**
Lessons from first principles to advanced topics

**Markets Analysis**
Technical and fundamental analysis on major markets

**Reports**
Bitcoin, Gold, Silver, SPX and more

markettalks.info

Telegram @MARKET_TALKS

For education only. Nothing in this document is financial advice. © 2026 MARKET TALKS. You are welcome to share this PDF unchanged.