12, 18 or 24 Words: Picking the Right Count at Restore

November 20, 2026 · Document #434 · bip39-phrase.com



Photo by Zoshua Colah on Unsplash

Choose the original BIP39 word count at restore, check every backup page, and understand why adding or removing words changes the wallet.

Contents

Which word counts does BIP39 allow? 1

Why wallets offer different restore options 2

Count the complete backup before selecting a length 2

FAQ 3

Sources 3

Example sequences from the BIP39 wordlist 4

Reading a BIP39 phrase 5

See also 5

A wallet asking you to choose 12, 18 or 24 words is asking for the length of your existing backup. Choosing a longer option does not make that backup stronger. To recover the intended wallet, you must enter the complete original phrase in its original order, then supply any BIP39 passphrase and compatible wallet settings.

Which word counts does BIP39 allow?

BIP39 defines five valid mnemonic lengths: **12, 15, 18, 21 and 24 words**. A restore screen showing only three options supports a subset of the standard's lengths.

Each BIP39 word represents 11 bits through its position in a 2,048-word list. Those bits encode randomly generated entropy followed by a checksum derived from the SHA-256 hash of that entropy.

Words	Entropy bits	Checksum bits
12	128	4
15	160	5
18	192	6
21	224	7
24	256	8

The checksum explains why the words cannot be treated as an arbitrary list. Their number, spelling and order determine whether they form a valid BIP39 mnemonic. The checksum is encoded within the phrase; there is no separate checksum word to leave out.

Longer phrases encode more entropy when generated correctly. During restoration, however, the task is to reproduce a wallet that already exists. Word count is a property of its backup, not a security preference you can change on the restore screen.

Why wallets offer different restore options

Wallet software and device firmware implement their own recovery interfaces. A product may generate only one phrase length, accept several lengths for imports, or restrict recovery to the lengths its developers chose to support. Its generation and restoration options can therefore differ.

Support also depends on the backup scheme. A recovery screen may expect BIP39 words, a different mnemonic format, or shares from a scheme such as SLIP39. Similar-looking lists do not establish compatibility. Even a matching word count does not prove that a backup uses BIP39.

Before entering anything, check the wallet’s official documentation for the exact device, application and recovery method. Look for explicitly supported mnemonic lengths and backup formats. Firmware or application updates can change the available choices, so use the documented mechanism rather than assuming every product supports all five BIP39 lengths.

If your confirmed BIP39 backup has 15 or 21 words but the restore interface offers neither, use a compatible recovery method or wallet that explicitly accepts that length. Do not select the nearest available count.

Count the complete backup before selecting a length

Count from the physical backup itself, keeping its original order and layout intact. A partial sheet can look like a complete phrase when the remaining words are elsewhere.

1. Gather every part of the backup. Check a second card, the back of each sheet, folded sections and any continuation marked by an arrow or page number.

2 Identify the actual recovery-word entries. Exclude headings, dates, handwritten instructions, position numbers and labels such as “wallet backup.”

3 Follow numbered positions where present. A card containing positions `1–12` and another containing `13–24` together hold a 24-word phrase. Two cards each containing `1–12` may instead be duplicate copies; inspect their labels and contents before combining them.

4 Count each position, including repeated words. A repeated word still occupies its own place. Do not remove duplicates or rearrange entries.

5 Count again in the same order. Confirm whether columns run down first or across first using numbering or the original backup instructions.

6 Select the matching length and enter the words through the wallet’s documented recovery process. Keep the phrase out of websites, support chats and online word counters.

Keep any separately recorded **BIP39 passphrase** separate from this count. Sometimes called a “25th word,” it can contain arbitrary text and is not an additional mnemonic word. A 24-word mnemonic with a passphrase still requires the 24-word option.

A phrase can only be restored at its original length because removing or adding words changes the encoded data and the input used to derive the seed. BIP39 derives a 512-bit seed using PBKDF2-HMAC-SHA512 with `2048` iterations, incorporating both the mnemonic and the passphrase.

Truncating 24 words to 12, or padding 12 words to 24, will usually fail checksum validation. A modified phrase can occasionally pass validation, but it will derive a different seed. A valid checksum confirms neither that you copied the intended backup nor that it controls your funds.

FAQ

What if I count 13 or 23 words?

Those are not BIP39 mnemonic lengths. Check for missing entries, continuation cards or a separately written passphrase. Do not delete or invent words to force a match.

Can I upgrade 12 words to 24 during recovery?

No. To change backup length, create a new wallet with a newly generated phrase, verify its backup and transfer your assets to it.

Why is the wallet empty after accepting my phrase?

Acceptance does not prove you restored the intended wallet. Check the exact phrase, BIP39 passphrase, network, account and derivation path. A different passphrase produces a different wallet without a wrong-passphrase error.

Sources

- BIP39: Mnemonic code for generating deterministic keys (github.com)
- Trezor python-mnemonic: Reference implementation of BIP39 (github.com)

> Continue reading on bip39-phrase.com: What Is a Seed Phrase? How a Recovery Phrase Works
> More on this topic: Recovery

Example sequences from the BIP39 wordlist

Randomly generated sequences of words from the BIP39 English wordlist. None of them passes the BIP39 checksum, so no wallet will accept them: they show the format only. Never store funds with a phrase you found in a document.

Example 1			
1 search	2 hill	3 pistol	4 future
5 embody	6 festival	7 idle	8 holiday
9 imitate	10 reunion	11 kit	12 spin

Example 2			
1 home	2 author	3 apple	4 enable
5 chair	6 timber	7 artefact	8 question
9 brother	10 win	11 dragon	12 curtain

Example 3			
1 cram	2 curious	3 security	4 modify
5 test	6 short	7 dignity	8 corn
9 excite	10 pen	11 ship	12 brush

Example 4			
1 adapt	2 pear	3 expand	4 mosquito
5 order	6 early	7 eyebrow	8 field
9 also	10 ring	11 base	12 orange

Example 5			
1 blossom	2 gold	3 hedgehog	4 affair
5 fix	6 anxiety	7 adjust	8 sister
9 shed	10 hundred	11 club	12 play

Example 6			
1 pistol	2 power	3 clerk	4 sunny
5 perfect	6 same	7 mosquito	8 find
9 arrow	10 dry	11 mask	12 dove

Example 7			
1 rude	2 error	3 camera	4 suggest
5 vital	6 lucky	7 entire	8 all
9 movie	10 roast	11 slice	12 owner

Example 8			
1 online	2 fatigue	3 session	4 motor
5 pretty	6 kick	7 bottom	8 atom
9 jaguar	10 buddy	11 verify	12 code

Reading a BIP39 phrase

Every word stands for an 11-bit number: its position in the 2048-word list, counted from 0. Here is Example 1 decoded word by word. Each word links to its page on bip39-phrase.com, where the list is numbered from 1.

#	Word	Index (0-2047)	Word no.	11 bits
1	search	1552	1553	11000010000
2	hill	861	862	01101011101
3	pistol	1323	1324	10100101011
4	future	756	757	01011110100
5	embody	579	580	01001000011
6	festival	681	682	01010101001
7	idle	901	902	01110000101
8	holiday	870	871	01101100110
9	imitate	907	908	01110001011
10	reunion	1474	1475	10111000010
11	kit	983	984	01111010111
12	spin	1679	1680	11010001111

The 12 words carry 132 bits: 128 bits of entropy followed by a 4-bit checksum. The checksum must equal the first 4 bits of the SHA-256 hash of the entropy.

`Entropy (hex): c20d7695af4486aa5c2b66717709ebe8`

This sequence ends in the checksum bits 1111, but SHA-256 of its entropy starts with 1101, so wallets reject it as an invalid phrase. That is the point of the checksum: about 15 of every 16 random or mistyped sequences fail it.

See also

- Picking a Seed Phrase Executor: Trust Before Skill · October 27, 2026

- Leaving Off the Last BIP39 Word: A False Trick · January 8, 2025
- Asking a Chatbot for a Seed Phrase: Why It Fails · November 12, 2026
- Diceware Lists and BIP39 Words: Different Jobs · October 30, 2026

Educational document. The example sequences are random and fail the BIP39 checksum: they are not wallets and must never hold funds. Security notes: bip39-phrase.com/security/