# How to Create your Bitcoin Seed Phrase with a Coin

Printable step-by-step guide — 24 words from 256 coin flips, 100% offline.

Every hardware wallet generates your seed phrase with a random number generator you cannot audit. This guide replaces it with a coin: no firmware, no supply chain, no update server. Follow it on paper, with every screen out of the room.

## What you need

- ☐ A coin. Any coin.
- ☐ A pen (not a pencil).
- ☐ **Coin Flip Seed Sheet**, printed.
- ☐ **BIP39 Word List**, printed.
- ☐ **Coin Flip Passphrase Sheet**, if you also want a passphrase.
- ☐ A quiet room, alone. Around 20 minutes.

## Rules before you start

- Do it **alone**, with the door closed.
- **No phones in the room.** Cover any webcam and unplug smart speakers.
- **Never type anything into a device that is online.** Not into a notes app, not into a browser, not “just to check”.
- Do not say the results out loud.
- Flip properly: from your thumb, letting the coin land on the table. Vary the height and the force.

## The 9 steps

### 1 Decide what heads means

**Heads = 1. Tails = 0.** That is the whole convention. Write it at the top of your sheet so you never doubt it halfway through.

### 2 Understand the sheet

The Coin Flip Seed Sheet has **24 rows**, one per word. Each row has **11 boxes**, labelled `1024 512 256 128 64 32 16 8 4 2 1`. Each box is one coin flip:

- **Heads** — write a `1` in the box.
- **Tails** — write a `0` in the box.

**Always write something, never leave a box blank.** A blank box has to mean one thing only: “I have not flipped for this one yet”. If you only marked the heads, you could not tell an empty box apart from a tails you already flipped, and re-flipping it would silently change your seed phrase.

### 3 Flip the coin 253 times (rows 1 to 23)

Start at row 1, box `1024`, and work left to right, row by row, all the way to row 23. That is 11 flips per row, 23 rows, **253 flips**.

You can take a break whenever you want: **the first blank box is always where you left off**. Never go back and “correct” a box that already has a digit in it.

### 4 Row 24 gets only 3 flips

On row 24 **the last 8 boxes are greyed out**. Do not flip those.

- Flip **3 times** only: the boxes `1024`, `512` and `256`, writing your 1s and 0s as usual.
- Leave the 8 grey boxes empty. They are the **checksum** and will be calculated in step 7.

You have now flipped 253 + 3 = **256 times**: the full 256 bits of entropy of a 24-word seed phrase.

### 5 Add up each row

Go row by row and add the numbers printed under the boxes **that hold a 1**. Boxes with a `0` add nothing. Write the result in the **Sum** column.

```
Example: 1s under 512, 256, 32, 16 and 2  →  512 + 256 + 32 + 16 + 2 = 818
```

Every sum is a number between `0` and `2047`. Anything above 2047 means you added a number twice: redo that row. Do this for rows 1 to 23 and **leave row 24's sum empty**.

### 6 Look up your words

The BIP39 Word List is numbered from `0` to `2047`, exactly like your sums, so there is nothing to adjust and nothing to add. Find each sum and write the word in the **Word** column. In the example above, `818` is the word `green`.

Copy every word letter by letter. You now have **words 1 to 23**.

### 7 Get the 24th word

The last word carries your 3 remaining flips plus 8 checksum bits calculated from all the previous words. It is the only step you cannot do with a pen, because it requires a SHA-256 hash. Most devices show you **8 possible words** for position 24, one per combination of your 3 flips.

> **How to pick your word out of a list of 8.** Add up row 24 like any other row: only your 3 flips count, so the sum can only be `0`, `256`, `512`, `768`, `1024`, `1280`, `1536` or `1792`. Your word is the one whose **number in the BIP39 list falls between that sum and that sum + 255**. Exactly one of the 8 does. Example: heads-tails-heads (1024 + 256 = 1280) → the word numbered between 1280 and 1535.

- **SeedSigner — the only one that takes your flips directly.** `Seeds` → `+ Create a seed` → `Calc 12th/24th word` → `24 words`. Enter your 23 words, choose **coin flips** when it asks for the remaining entropy, and enter the 3 flips of row 24 in order. It gives you word 24 straight away, with no list to choose from.
- **Coldcard Mk4 and Q.** `Import Existing` → `12/18/24 Words` → `24 Words`, then type your 23 words. After the 23rd, the Coldcard computes and shows the **8 valid options** for word 24: pick yours with the rule above.
- **Krux.** `New Mnemonic` → `Words`, then type your 23 words. For the 24th, the keypad only lets you type words with a valid checksum, so type the one matching your flips. If you leave it empty, Krux picks a valid word by itself and your 3 flips are not used.
- **Foundation Passport (firmware 2.3.0+).** It accepts a 23-word import and calculates the checksum word for you. It does not ask for the 3 extra flips of row 24, so those are not part of the result: the seed ends up with 253 bits of entropy instead of 256, still far beyond anything brute-forceable.
- **An offline computer, if you have none of the above.** Download the Ian Coleman BIP39 tool **before** you start (github.com/iancoleman/bip39/releases), move the single HTML file to a computer with **no internet connection**, select `Binary [0-1]` as the entropy type and type the 256 digits exactly as they are on your sheet, row by row, left to right. It shows the complete 24-word phrase. Shut the computer down afterwards.

> Whatever you choose, it must be offline: a tool that calculates your last word also sees the other 23. If your device is not on this list, do not worry — most hardware wallets only accept a complete, valid phrase, so get word 24 with one of the options above and then restore the 24 words on your device as usual.

### 8 Load the phrase into your wallet

Type the 24 words into your hardware wallet as a wallet restore. If the device rejects the phrase, the checksum is wrong: a word was misread or a sum was miscalculated, so go back and check each row.

Once it is accepted, **send a small amount of bitcoin, wipe the device and restore it from your written backup**. Do this before moving any serious amount. A backup you have not tested is not a backup.

### 9 Destroy the sheet

Your seed sheet is a plaintext copy of your private keys. Once the words are stamped on metal and the restore is tested, burn the sheet or shred it and dispose of the pieces separately. Never photograph it, never scan it, never keep it “just for now” in a drawer.

## The same method, for an 8-word passphrase

A passphrase (the “25th word”) is a second secret that unlocks a completely different wallet. Picking it out of your head is the classic mistake: attack dictionaries are built from songs, books, names and dates. Flip for it instead, on the Coin Flip Passphrase Sheet:

1. Flip **11 times per word**, writing a `1` for heads and a `0` for tails, exactly as before.
2. Do it for the 8 words: **88 flips per passphrase**.
3. Add up each row and write the sum, from `0` to `2047`.
4. Look up each sum in the BIP39 Word List and write the word.

There is **no checksum here**, so all 8 words come straight off the sheet: nothing to calculate, no device needed. Write the passphrase in **lowercase, with a single space between words**, and no capitals, numbers or accents.

> A passphrase has no checksum: any typo silently opens a different, empty wallet, with no error message. Back it up on metal, in a different place from your seed phrase, and test the recovery before funding it.

## Common mistakes

- **Flipping 264 times.** Row 24 only takes 3 flips. The 8 grey boxes are the checksum.
- **Leaving the tails boxes blank.** Write the `0`. A blank box must always mean “not flipped yet”.
- **Starting the word list at 1.** The list runs from 0 to 2047, and so do your sums. No adding 1 anywhere.
- **Reusing the same coin flip for two boxes.** One flip, one box.
- **Typing the words into a phone “just to check”.** That is how seeds leak.
- **Skipping the restore test.** Test with a small amount before you trust the backup.
- **Keeping the paper sheet.** It is a full copy of your keys.