

BIP39 Coin-Toss Worksheet

You will generate a 12-word seed phrase by tossing coins.
You need: your BIP39 wordlist, 11 coins, and a pen.
To verify the checksum, you will need an air-gapped device.
Work top to bottom, one word per row.

Why coins? A seed phrase must be drawn from *true, unbiased randomness*, and a human brain cannot produce that. Numbers you make up yourself are predictable and can be guessed by an attacker who then drains your wallet. A fair coin gives one honest bit per toss, so 128 tosses build a phrase no one can reproduce or foresee. Do not invent, pick "random-looking", or reuse any bits. Toss every coin and record exactly what falls.

- 1

Toss. Shake all 11 coins well and throw them, then drag all coins flat straight down into its square. Use a ruler or something straight.
- 2

Record bits. Mark 1 for heads, 0 for tails in each bit square.
- 3

To index. Sum the bit-values (coin legend below) of every heads. Write that number in the index boxes.
- 4

Look up. Find that index in your wordlist.
- 5

Write the word. Copy it onto the line. Next row.

1 COIN TOSS RESULTS

Place all coins flat in a circle each. If it landed **heads**, add the value below it. If it was **Tails**, ignore it. The sum of all **heads** values is your word's index.

Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0	Heads = 1 Tails = 0
1024	512	256	128	64	32	16	8	4	2	1

2	11 BITS: A NUMBER BETWEEN 0-2047	3	INDEX	4	5	WORD
1		→				
2		→				
3		→				
4		→				
5		→				
6		→				
7		→				
8		→				
9		→				
10		→				
11		→				
12		→				

Word 12 — checksum Toss only 7 coins into the first 7 squares (the wide group). Leave the 4 gold checksum squares as 0 0 0 0 for now. Look up the resulting index → this is your first candidate word. Enter the full phrase into your signing device and try this word plus the next 15 in the wordlist, one at a time, until the device accepts the phrase (valid checksum).

Security: While generating a seed phrase, make sure no one is watching, listening, or recording. Do this in a room with no cameras, microphones, or other recording devices, such as CCTVs, smartphones, smart TVs. You shouldn't rely on electronics to do the binary to decimal transformation math, but if you must, use a single purpose digital calculator. After you have securely backed up your seed phrase, **DESTROY THIS DOCUMENT FULLY**