



Dice Log – Roll your own seed

BitBox02 Diceware · 24 words (23 rolled, word 24 = checksum from the device) · Self-Experiment 1a

⚠ **Once filled in, this sheet is the key to everything held on this seed.** Never photograph it, never scan it, never type it into anything digital. After the check on the device, copy the words onto the backup card and destroy this sheet – or store it like the backup itself.

⚠ **For self-experiments:** A documented seed counts as compromised and is never used for real coins.

METHOD (SHORT VERSION – DETAILS IN THE BITBOX HOWTO)

You need: 5 casino dice · 1 coin · the printed BitBox word table (LookupTable) · pen · BitBox02 (also applies to the BitBox02 Nova – same firmware, same restore path)

1. Throw all 5 dice plus the coin together. Every die showing **5 or 6** is thrown again – only 1–4 count. (No coin? One extra throw: 1–3 = heads, 4–6 = tails.)
2. Read the dice from left to right (top to bottom if in doubt) and write them in below.
3. Look the word up in the word table: **die 1 = page**, **dice 2–4 = row**, **die 5 + coin = column**. Write the word in.
4. Repeat 23 times, then enter all words on the BitBox02: **"Restore from recovery words"** → 24 words.

1 Page · **2** **3** **4** Row · **5** + **H/T** Column

	D1 Page	D2	D3	D4	D5	Coin H/T	Word
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

	D1 Page	D2	D3	D4	D5	Coin H/T	Word
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							

Word 24 (checksum): After word 23 the BitBox02 shows **eight valid options**. Pick one of them at random – for example with the same scheme as the column: one die (1–4) plus the coin gives option 1–8.

TIME

Start: _____
End: _____
Rerolls (5/6)
approx.: _____

NOTES / FAILED ATTEMPTS (FOR THE LOGBOOK)

VERIFICATION – WITHOUT THESE STEPS THE SEED IS WORTH NOTHING

- ☐ All 24 words checked on the device: **"Manage device"** → **"Show recovery words"** – word by word against this sheet.
- ☐ Words copied by hand onto the backup card (no photo, no text file).
- ☐ This sheet destroyed – or from now on stored like the backup itself.