



Würfelprotokoll – Seed selbst würfeln

BitBox02-Diceware · 24 Wörter (23 gewürfelt, Wort 24 = Prüfsumme vom Gerät) · Selbstversuch 1a

⚠ **Nach dem Ausfüllen ist dieses Blatt der Schlüssel zu allem, was auf diesem Seed liegt.** Nie fotografieren, nie scannen, nie digital abtippen. Nach der Geräte-Verifikation die Wörter auf die Backup-Karte übertragen und dieses Blatt vernichten – oder es wie das Backup selbst lagern.

⚠ **Für Selbstversuche:** Ein dokumentierter Seed gilt als kompromittiert und wird nie für echte Coins verwendet.

METHODE (KURZFASSUNG – DETAILS IM BITBOX-HOWTO)

Du brauchst: 5 Casino-Würfel · 1 Münze · die ausgedruckte BitBox-Wörtertabelle (LookupTable) · Stift · BitBox02 (gilt auch für die BitBox02 Nova – gleiche Firmware, gleicher Wiederherstellungs-Weg)

- Alle 5 Würfel + Münze zusammen werfen. Jeder Würfel, der **5 oder 6** zeigt, wird neu geworfen – es zählen nur 1–4. (Keine Münze? Ein extra Wurf: 1–3 = Kopf, 4–6 = Zahl.)
- Würfel von links nach rechts ablesen (im Zweifel oben nach unten) und unten eintragen.
- Wort in der Wörtertabelle nachschlagen: **Würfel 1 = Seite**, **Würfel 2–4 = Zeile**, **Würfel 5 + Münze = Spalte**. Wort eintragen.
- 23-mal wiederholen, dann alle Wörter an der BitBox02 eingeben: „**Von Recovery-Wörtern wiederherstellen**“ → 24 Wörter.

1 Seite · **2** **3** **4** Zeile · **5** + **K/Z** Spalte

	W1 Seite	W2	W3	W4	W5	Münze K/Z	Wort
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

	W1 Seite	W2	W3	W4	W5	Münze K/Z	Wort
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							

Wort 24 (Prüfsumme): Die BitBox02 zeigt nach Wort 23 **acht gültige Optionen**. Eine davon zufällig wählen – z.B. mit demselben Schema wie bei der Spaltenwahl: ein Würfel (1–4) + Münze ergibt Option 1–8.

ZEIT

Start: _____
Ende: _____
Neuwürfe (5/6)
ca.: _____

NOTIZEN / FEHLVERSUCHE (FÜRS LOGBUCH)

VERIFIKATION – OHNE DIESE SCHRITTE IST DER SEED NICHTS WERT

- ☐ Alle 24 Wörter am Gerät geprüft: „**Gerät verwalten**“ → „**Recovery-Wörter anzeigen**“ – Wort für Wort gegen dieses Blatt.
- ☐ Wörter handschriftlich auf die Backup-Karte übertragen (kein Foto, kein Textdokument).
- ☐ Dieses Blatt vernichtet – oder es wird ab jetzt wie das Backup selbst gelagert.