Generate Bitcoin entropy with dice

Unbiased 5 × d6 · 256-bit BIP39 seed · Done offline at home · No hardware wallet required

A d6 has six faces. Treating all six as bits biases the result. Keep only faces 1–4 (exactly two fair bits). Discard 5 and 6 and shake those dice again.

Face	1	2	3	4	5	6
Bits	00	01	10	11	—	—
Action	KEEP	KEEP	KEEP	KEEP	REROLL	REROLL

How to roll, convert, and verify offline

01 Shake five dice. Read left to right every time. Keep 1–4 as two bits. Skip 5 and 6.

02 Append only 0s and 1s. Example: 4, 6, 1, 3, 2 → 11 00 10 01 → **11001001**.

03 Aim for 320–400 bits (~50–60 shakes), minimum 256. Extra bits are hashed down to 256.

04 Boot Tails with networking disabled. Convert with a verified script or local Ian Coleman HTML.

05 Write all 24 words. Word 24 is the checksum — do not invent it.

06 Restore in Electrum and Sparrow while still offline. First addresses must match.

07 Repeat independently for Seed 2 and Seed 3. Shut Tails down. Destroy the raw bit notes.

Safety. Generate and convert only offline. Never type a real seed on a computer that is online. Casino dice and a consistent reading order reduce bias and recording mistakes.

Dice recording sheet

Read left to right. Write only 00 / 01 / 10 / 11. Leave a cell blank if that die was 5 or 6. Print extra copies — each seed needs ~50–60 shakes.

Seed # 1 2 3 **Date** _____ **Reader** _____ **Checker** _____

#	Die 1	Die 2	Die 3	Die 4	Die 5	Bits this shake
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

Running bit count (filled pairs × 2): _____ Target ≥ 256, better 320–400. Do not photograph this sheet. Destroy it after the 24 words are stamped and verified.