This work starts after Tails has booted with networking set to Disabled, and before any plate is stamped. Five casino dice are required, and every face has to be readable. Faces 1 through 4 are kept. Faces 5 and 6 are rolled again. The work is done three times, for three keys, and the computer is shut down fully between them. An established private setting is required, and there cannot be a camera in the room.

The faces

- 1 is 00. 2 is 01. 3 is 10. 4 is 11.
- 5 and 6 are not bits. Roll those dice again.
- Read the dice left to right, the same way every shake.
- Example: 4, 6, 1, 3, 2 becomes 11, skip the 6, then 00, 10, 01.
- Write only 0 and 1. At least 256 bits are required. More is fine. The extra bits are folded down.

Turn the bits into 24 words

01. Boot Tails. Networking Disabled. Copy the checked converter and the Ian Coleman page from the data USB to the Desktop.

02. Run the converter. Paste the bits. It prints 24 words. Word 24 is the check. Do not invent it. Do not fix it.

03. Open the Ian Coleman page in the offline browser. Entropy type: Binary. 24 words. Paste the same bits. The 24 words must match. If they differ, stop. Do not pick the prettier list.

04. Write the 24 words on the grid. Read them back out loud once.

05. Shut Tails down. Wait until the screen is dark. Then start the next key. Seed 2 is a new set of rolls. Seed 3 is a new set of rolls. Never continue a list from the previous boot.

```
$ cd ~/Desktop
$ python3 bip39_dice_converter.py
```

The last word is a check

The 24 words are not 24 free choices. The last word carries a short check so a copying mistake is caught before metal is stamped. At least two of these checks are used. If they disagree, the work stops.

- Two tools, same bits, same 24 words. Converter, then the offline Ian Coleman page. Do not pick the prettier list.
- Let the wallet refuse a bad list. Sparrow or Electrum, networking off, will open a valid list and reject a broken one. If it will not open, do not change a word to force it.
- The math, if it needs to be seen. Twenty-four words are 264 bits. The first 256 are the dice. The last 8 are the check. Only word 24 can change to make that true. It is not chosen. The converter appends it after the file has been checked.

Next. The 2-of-3 is built next. One seed is loaded per boot. Two lists are never loaded in one session. The recording grid is the next page. Print extra copies.

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.