Take absolute ownership

of your Bitcoin, zero-trust, built to outlive any third party.

Companion sheets for the presentation.

Do this on a closed-door table: Tails with networking off, dice, two-tool verification, 2-of-3, titanium plates. A single point of failure is the threat. One computer. Two boots. The Tails USB is the offline machine. Hardware signers are optional later, and only from more than one maker.

Do not write seed words, xpubs, or transaction IDs in this packet. Keep the recovery log separate. Print extra copies of the dice page.

Contents

Also keep at the table

The presentation, on the site or in 01_Slides.pptx.
10_Recovery.xlsx — locations only. Not in this PDF.
Official Tails, Sparrow, Electrum, and Ian Coleman files.
Extra copies of the dice page.

Home setup checklist

Online setup, before the data USB

- Run ./verify_kit.sh before the data USB.
- One failure means format the drive and stop.
- Only then copy files to the data USB.

Then the rest of the setup

- Tails flashed. Networking Disabled every boot.
- Do not create Persistent Storage.
- Three seeds, one at a time. Full shutdown between them.
- Dust in. Two Tails boots sign. Dust out.
- Plates stamped and read back. Then split them.

One computer. Two boots.

Boot 1 is this computer with the network on. It watches and builds a payment. It never holds a seed. Shut it down fully. Boot 2 is the Tails USB on that same hardware, with networking off. The stick is the offline computer. Shutdown forgets the session.

Boot 1 · network on

Watch-only Sparrow. The map and xpubs only.

Builds the payment and exports an unsigned file.

Later broadcasts the signed file.

Never type, paste, or photograph a seed.

Boot 2 · Tails USB

Networking Disabled before the desktop appears.

One seed in memory. Sign. Full shutdown. Then the next seed.

A second USB carries files only. Never the seed.

Do not create or unlock Persistent Storage.

The only secret that crosses a USB is a signature file, not a seed. A networked machine with a seed loaded is burned. Treat that session as finished.

Check the files

Open a terminal on the online computer. Put the downloads next to verify_kit.sh.

- Run chmod +x verify_kit.sh
- Run ./verify_kit.sh or double-click it.
- It checks pinned SHA-256 hashes. Not signatures.
- One failure means format the drive and stop.
- Only then copy files to the data USB.
- Two tools must still agree on the words.

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.

Sparrow Wallet on Tails at home

Offline signing on your Tails USB. Networking stays disabled the entire session.

Before you begin: a verified Sparrow Linux standalone archive (sparrowwallet-*.tar.gz) must already sit on the clean data USB. Verify SHA-256 and the GPG / minisign signature on the online computer first. Do not download Sparrow from inside Tails.

Launch Sparrow offline

01 **Boot Tails offline.** Networking to Disabled. Start Tails.

02 **Copy the archive** from the data USB to the Desktop.

03 **Extract.** Terminal: cd ~/Desktop then tar -xvf sparrowwallet-*.tar.gz then ls

04 **Launch.** cd Sparrow then ./bin/Sparrow — wait 15–30 seconds.

Sign in the airgap session

01 Import the 2-of-3 wallet from the output descriptor, or restore **one** software keystore from one seed.

02 File → Open Transaction → From File → select the .psbt.

03 Read destination, amount, change, and fee against your written notes. Then Sign.

04 Export with a new filename such as tx-partial-s1.psbt. Close Sparrow. Shut Tails down fully.

Safety at home

- Keep networking disabled. If it is on, shut down and treat the session as burned.
- Load only one seed at a time. Seed 3 stays boxed unless Seed 1 or 2 is gone.
- Full shutdown before you carry the data USB back to the online computer.
- Test the whole path with a small amount before savings touch this wallet.

Sign and broadcast at home

Default path: two offline Tails sessions. Optional path after the key exists: sign on hardware wallets you imported the airgapped seed into. Either way, one seed per session, and two independent makers if hardware is in the quorum.

Step 1 — Build the spend (online watch-only)

01 Open watch-only Sparrow. Recheck the receive history so you know this is the right wallet.

02 Send tab: destination, amount, fee. Read every field against a written note.

03 Finalize for signing. Export tx-unsigned.psbt to the data USB.

Step 2 — First signature (Tails session 1, or hardware A)

01 Boot Tails, networking disabled. Launch verified Sparrow. Or unlock hardware wallet A that already holds Seed 1.

02 Restore Seed 1 only (Tails) — or confirm Seed 1 is the only key on that device. Open tx-unsigned.psbt. Confirm fields. Sign.

03 Export tx-partial-s1.psbt. Full shutdown of Tails, or unplug the hardware signer.

Step 3 — Second signature (Tails session 2, or hardware B)

01 Fresh Tails boot, networking disabled. Restore Seed 2 only. Or unlock hardware wallet B from a different vendor.

02 Open tx-partial-s1.psbt. Confirm the first signature and unchanged spend. Sign.

03 Export tx-signed.psbt. Full shutdown.

Step 4 — Broadcast (online computer)

01 Watch-only Sparrow: File → Open Transaction → fully signed file.

02 Confirm fully signed and fields unchanged. Broadcast. Record the txid in 10_Recovery.xlsx.

If you export a key onto hardware

- Generate the seed on airgapped Tails first. Import the finished 24 words. Do not let the device roll its own entropy for this stack.
- Multi-vendor examples (not a ranking): Foundation Passport, Blockstream Jade, BitBox02, SeedSigner / Krux. Official shops only.
- Two keys on two brands. Never three of the same box. A bricked vendor is one lost key — plates and geography still hold the wallet.
- If Sparrow and Electrum disagree about the PSBT, stop. Do not sign. Test with a small amount first.

Titanium plates and geographic split

Paper fails in the ways houses fail. Stamp each seed once at home, verify the stamp, then separate the plates so no single address holds a quorum. Geography is how you retire the last single point of failure.

Why metal

Paper / notebook	Ink runs. Fire wins. Do not stop here.
Steel plates	Survive most house fires and flooding. Watch cheap stamps.
Titanium stamp plates	Higher melt point, no rust, compact. Recommended default.
Digital copies	Photos, clouds, printers, password managers — treat as a leak.

How to stamp at home

01 Private room. No phones. Plate on a steel block. Stamp each letter deep.

02 Number words 1–24. Quiet label such as S1 — not your name, not “Bitcoin.”

03 Read the plate back against the paper seed. A mis-stamped word is a bricked backup.

04 Restore from the plate on offline Tails and confirm first addresses.

05 Destroy paper only after the plate-restore check passes.

What goes on each plate

Plate A

Seed 1 only

Home safe / fire box

Never Seed 2 or 3 here

Plate B

Seed 2 only

Off-site #1

Same address as A or C

Plate C

Seed 3 only

Off-site #2

Same address as A or B

Print the output descriptor and keep 10_Recovery.xlsx. Store that packet with Plate A and a copy at one off-site — never beside all three seeds. Hardware wallets do not replace these plates. Once a year at home: restore from plates, receive dust, spend dust, update locations. Write a letter that points to this packet and which two locations are needed — not the words.