SPLITSTEEL

Split your seed in two.
Give one half away.

Each half is mathematically nothing on its own. Only both together open the wallet - a backup no single burglary or fire can undo, and an inheritance plan with nobody to trust.

THE PI IS A BLENDER · STEEL IS THE VAULT · NEVER TYPE A SEED INTO A WEBSITE

This document never needs your words. It is safe to print, share, and leave on the bench.

CONTENTS

What is in this manual

Changes from v1 (published as “Blender Vault”): renamed; each half of the secret now exists more than once; every hex string carries a check group; the round-trip test is repeated from the finished objects before old paper is destroyed; the blender OS instruction is corrected; a dice-to-hex card, a parts list, an heirs’ letter and the July 2026 Coldcard postscript were added. v2.1: the boxed kit’s card ships pre-flashed with the open wizard image; media guidance relaxed beyond steel; a by-hand spot-check added to the mix step. **v3.0: the blender wizard is written and published; the medium is stated plainly as a durability choice and never a secrecy one, with USB, M-DISC, steel and paper compared; three copies of each half becomes the default; the two-machine rule for making copies is spelled out; the passphrase gets its own section; and an honest comparison with Seed XOR, Shamir, multisig and metal seed plates is added — along with the plain statement that this system has not yet had independent security review. v4.0: the wizard will now MINT a new seed before splitting one - dice, dice mixed with the machine, or the machine alone, each labelled with what it asks you to trust; the confusing pencil check**

became a guided spot check against the printed table; both halves are typed group by group into a grid you can move around in; the USB sticks are written one at a time so the halves cannot meet; each stick carries a START-HERE page that finishes the job on a laptop; the two-machine rule is stated for the burning and engraving hour, not just the sitting; recovery on an untrusted machine now ends with treat-the-seed-as-spent; plate sizes are given against what a punch set can actually reach; and Seed XOR is credited as prior art.prior art.

00 · HARD RULES

Read this before you touch a seed

This document never needs your words. Do not type a seed, pad, or ciphertext into any website, chat, cloud, or photo — including any website carrying this manual's name. The only machine that should ever see the real mnemonic is an air-gapped Pi you then wipe.

SPLITSTEEL is a **backup protocol**. It does not make a phone wallet a cold wallet, and it does not replace a hardware signer for life-changing amounts. Compose them; do not confuse them.

The Raspberry Pi is a **blender**: mix, pour, wash. If it burns, buy another. Nothing of value is ever stored on it.

XOR is not a new cipher. The one-time pad is Vernam (1917). Coldcard ships Seed XOR; Trezor ships Shamir. The product here is hex that does not look like words, a check group on every object, media matched to how long you need them, and geography.

Dice, not chip luck. The 2026 Coldcard drains happened because a vendor's random number generator was quietly weaker than advertised for five years. Bring your own entropy (section 04).

Do not destroy the old paper until the round-trip test has passed twice — once on paper, once reading only from the finished objects (section 08, step 8).

This system has not had independent security review. The mathematics is a century old and the software is public and tested, but the assembled protocol has not been audited or used at scale. Treat it as a strong design under review, not a proven product, and size your trust accordingly (section 17).

01 · THE IDEA

You will need the seed again. It should not exist until then.

Day to day you unlock the off-phone, spend, and power it down. The words are not involved. They exist for exactly one day — the bad one: phone lost, stolen, reset, or dead.

A one-time pad turns the entropy inside those words into **two blobs of hex**. Each blob is junk. Together they are the seed. Apart they are nothing — mathematically nothing, not "hard to guess" nothing. That is stronger than slicing English words into envelopes, because leftover BIP39 words can be brute-forced.

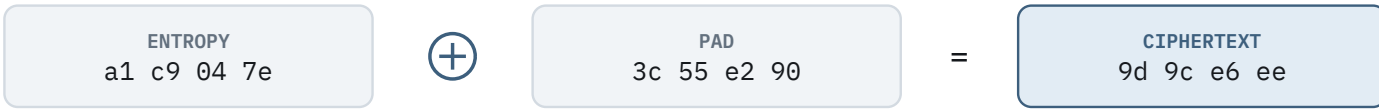
That one property is what everything else in this manual is built on. Because a half carries zero information, you can hand one to a solicitor and let them look; you can burn a copy on an ordinary computer; you can post one to a relative. None of it helps an attacker who does not have the other half.

The Raspberry Pi Zero 1.3 — the board with no Wi-Fi chip — is the blender. It converts words to entropy, mixes entropy with your pad, shows the result for as long as you need to write it, and is then wiped. If the blender melts in a fire, you buy another blender.

02 · XOR AND THE CHECK GROUP

Two junk numbers, one secret, one safety row

XOR (exclusive or) compares bits: same gives 0, different gives 1. It is its own inverse — run it twice with the same pad and the original comes back. If the pad is truly random, exactly as long as the entropy, and never reused, the split is information-theoretically perfect: either piece alone is indistinguishable from noise. This is the oldest respectable trick in cryptography.



Shannon-perfect if the pad is truly random, the same length as the entropy, and never reused.
The same operation run again with the same pad undoes it: ciphertext XOR pad = entropy.

Worked toy (not a wallet): entropy `a1` XOR pad `3c` = ciphertext `9d`. Then `9d` XOR `3c` = `a1` again. Your real run uses 32 hex characters (12 words) or 64 (24 words).

The check group — catch a mis-punched character

BIP39 words carry a checksum; raw hex does not — and one wrong character on an object is a silent, total loss. So give the hex its own. Write every string in groups of four. XOR **all the groups together**; the answer is one more group of four. Record it as the final row: the **check group**.

At recovery, XOR every group including the check. The answer must be `0000`. Any single misread or mis-stamped character breaks it. Same operation, no new mathematics, one more row on the object.

Worked example: pad `9f3a 1c07 5b2e a4d1`. `9f3a` XOR `1c07` = `833d`; XOR `5b2e` = `d813`; XOR `a4d1` = `7cc2`. The object's last row reads · `7cc2` · and the five rows XOR to zero.

03 · 12 VS 24

Same secret, different length

There is not a special "12-word key" and a different "24-word key." Both are BIP39 encodings of random bits plus a checksum. You XOR the **entropy hex**, never the English — and the pad must be exactly as long as that entropy.

Words	Entropy	Checksum	Pad / ciphertext
12 (the common phone-wallet default)	128 bits	4 bits	32 hex characters
15 / 18 / 21	160 / 192 / 224 bits	5 / 6 / 7 bits	40 / 48 / 56 hex
24	256 bits	8 bits	64 hex characters

The layers people mix up

1 · Entropy — the actual random bits. The words are a human encoding of this, plus checksum. This is what you XOR.

2 · BIP39 seed (512-bit) — PBKDF2 of the words plus the optional passphrase. Always 512 bits, whether you started from 12 or 24. You never punch this on steel.

3 · Wallet keys — BIP32 children of that seed. Attacking a Bitcoin key from its public key is about 2^{128} work anyway, which is why a proper 12-word phrase is already in that ballpark. 24 is margin: weak RNGs, other chains, defence in depth.

4 · Passphrase (**"25th word"**) — a separate secret that works with 12 or 24. It is not "the 24-word version," and it never enters this protocol's maths. Section 15.

04 · WHY DICE

In July 2026, "random" wasn't

Attackers swept roughly **$70–88 million** of Bitcoin from hardware-wallet users in coordinated waves over a few days. The cause was not phishing and not seized devices. A March 2021 firmware change in Coldcard's seed generation had silently fallen back to a predictable software generator instead of the chip's hardware RNG. Effective randomness collapsed to about **40 bits** on the Mk3 — a keyspace a rented GPU farm can walk through — and about 72 bits on later models before the July 2026 fixes.

Five years of seeds were affected. Updating firmware does not heal an old seed; owners had to sweep coins to fresh wallets. The users who were never at risk were the ones who had generated with **their own dice**.

That is the rule this protocol was already built on: **never let a chip invent your secret alone.** Your pad comes from casino dice on your own table (section 09). The wizard has no "generate a pad for me" button, deliberately. A vendor's five-year-old firmware mistake cannot touch a number that was never inside a vendor's chip.

Sources: thehackernews.com (Aug 2026, "Coldcard flaw linked to $70M theft") · engineering.block.xyz ("Predictable RNG fallback in COLDCARD firmware") · blog.coinkite.com/coldcard-mk3-seed-generation-warning

Making a new seed, here, on the bench

If the seed you hold might be weak or might have been seen, the wizard will mint you a fresh one before it splits anything. Splitting does not add entropy: a weak seed cut in half is still a weak seed, so this step comes first or not at all. Twelve words is the default - 128 bits, and half the rolling. Twenty-four is the same method, twice.

Three sources, and the screen says plainly what each one asks you to trust:

SOURCE	EFFORT	WHAT YOU ARE TRUSTING
Dice mixed with the machine	~36 rolls	Nothing, once you check it. The machine prints its number FIRST, before a die is touched, so it cannot steer the result; the two are combined, and the answer is good if EITHER source is good. Then it walks you through every group by hand on the printed table.
Your dice alone	~36 rolls	Your dice being fair, and your reading of them.
The machine alone	instant	That whoever flashed the card did not swap the program. The generator itself is sound - the kernel will not hand out random numbers before it has gathered enough entropy - but the image is not yet reproducible byte for byte, so there is no published number you could check a card against.

Mixed is not a compromise between the other two. Exclusive-or of two sources is good if either one is good, so it is stronger than dice alone and stronger than the machine alone, for the same effort as dice alone. It is the recommendation.

The machine-only path is kept deliberately. For somebody who will not roll dice, the alternative is not dice - it is keeping a seed they already distrust, which is worse than any of these.

Whichever source you choose, the wizard makes you write the words down and read them back from your own paper, and refuses to continue if what you type is not what it generated - even when what you typed is a

perfectly valid phrase. Then it insists on a small test receive into an address derived from the paper words, and spending it back out, before any real money moves. Nothing before that has proved a wallet will accept these words.

Afterwards the old seed is **retired**, not merely replaced: move every coin on every chain that seed ever touched, then destroy its old backups, so that nobody in twenty years recovers an empty wallet and concludes they have done something wrong.

05 · THE OBJECTS

Two halves. Three copies each. Nothing is twelve English words.

The blender — Pi Zero 1.3, no wireless on the board. It is kitchen equipment: mix, pour, wash. It generates nothing by itself, stores nothing, and is wiped after every sitting. Not the W, not the 2W, not a Pico W — those have radios. It is also the only machine that ever sees your whole seed.

The pad — 128 or 256 bits of dice-rolled hex, in groups of four, with its check group as the last row. It looks like factory serial numbers. A thief does not even recognise it as a wallet. This is half the secret.

The ciphertext — entropy XOR pad, written the same way, with its own check group. Useless without the pad. It never lives in the same hiding place as any pad.

Why three copies of each half

XOR is all-or-nothing: lose either half and the coins are gone. That is this protocol's real weakness, and the cure is embarrassingly simple — copies. Three copies of each half, in separate places, means you would have to lose all three pads, or all three ciphertexts, before anything is unrecoverable. Copies cost pennies and add no steps to the ceremony; a threshold scheme like Shamir solves this more elegantly but at real cost in complexity (section 17).

And the copies do not have to match. The medium is a durability choice, never a secrecy one — a half is junk wherever it lives. Put the copy you will actually touch on a USB stick, and the copy that must outlive you on steel or M-DISC. Section 06.

PAD · THREE COPIES

Home one copy	Family, another town one copy	Solicitor one copy

CIPHERTEXT · THREE COPIES

Work / lock-up one copy	A friend one copy	Safe-deposit box one copy

no place appears in both rows - any one place can burn or be burgled

06 · CHOOSING YOUR MEDIA

The maths does not care what you write it on

Every medium below is equally **secret**. A one-time-pad half carries zero information about your seed whether it is stamped in titanium or biroed on a receipt. The only thing the medium decides is **how long it survives unattended** — and how likely a human is to recognise and keep it.

Medium	Unattended life	Readable by eye	Needs a reader
Stamped / punched stainless	decades to centuries	yes	no
M-DISC archival optical	centuries (projected)	no	any DVD drive
Archival paper + pigment, laminated	decades	yes	no
USB stick / SD card	years, uncertain	no	any computer
NFC tag	about 10 years	no	reader — and it is a radio
Ordinary paper, inkjet, in a drawer	years, fragile	yes	no

How to read that table

Flash forgets. Unpowered USB sticks and SD cards lose charge over years, and heat makes it worse. They are excellent for the copy you check and refresh; they are not a bury-and-forget medium, and neither is an NFC tag, which is the same technology in a nicer shape (and adds a radio to a protocol that deliberately has none).

M-DISC is the archive answer. Ordinary writable discs use a dye that fades; M-DISC etches the data into a rock-like inorganic layer, and the projections run to centuries. Writing needs an M-DISC-capable burner, but reading works in any ordinary DVD or Blu-ray drive, which matters enormously for heirs. It is also write-once, so nobody can quietly alter it.

Steel is the only medium that needs no technology at all. A stamped plate is readable by a human eye in a century, with no drive, no format, and no software. That is worth more than it sounds — every digital medium is a bet that something will still read it.

A good default

Pair a convenient medium with an archival one, and never let both halves sit on fading storage. For most people: **USB for the copy you touch, M-DISC or steel for the copy that must outlive you**, and the third copy on whatever is cheap and elsewhere. If you only ever make one kind, make it steel.

Whatever you choose, every object carries its check group, and every object gets tested by the round-trip in step 8 — not the paper you copied it from.

07 · PARTS LIST

Everything on the bench, with prices

Street prices, August 2026, rounded. Most drawers already hold half of this. Nothing on the list touches a secret except the dice and the objects you write your halves on.

Part	What exactly, and why	Typical
Raspberry Pi Zero v1.3	The board with **no wireless chip**. Not Zero W, not Zero 2 W. If unavailable, any old laptop with the Wi-Fi card physically removed does the same job.	£12–20
Official micro-USB power supply	Stable 5 V; brownouts corrupt cards mid-sitting.	£8
Micro-SD card, 8–32 GB, branded	Carries the wizard; wiped or destroyed after the sitting. **In the boxed kit this arrives pre-flashed with the open wizard image** — hashes printed on the box, reflash from source if you prefer your own download.	£6

Mini-HDMI to HDMI adapter + cable	The Zero's video output is mini-HDMI.	£6
Small HDMI screen	Any monitor or the living-room TV — in a room with no cameras.	£0–25
Micro-USB OTG adapter + wired USB keyboard	Wired, not wireless — no radios at the table.	£10
2 × USB sticks, small, branded	One half each — the first copies the blender writes, and the shuttle for making the rest. Never both halves on one stick.	£8
2 × stainless plates, 304/316, 1.5–2.0 mm, about 60 × 90 mm	The keeper pair: one pad, one ciphertext. Blank "engraving plates" or offcuts both work. Aluminium is the classic mistake — it melts at ~660 °C.	£10–16
Letter/number punch set, 3–4 mm, hardened	A dent survives a fire after every coating is gone. You need 0–9 and a–f.	£15–25
Ball-pein hammer + steel bench block	Clean strikes; the kitchen worktop is not an anvil.	£12–18
2 × casino-grade dice (or one hexadecimal D16)	Sharp-edged, unweighted. This is the entropy source — the one part quality matters for.	£6–10
Optional: M-DISC burner + 4 M-DISCs	The archive tier (section 10). A USB burner runs better off a laptop than off the Zero. Reading later needs only an ordinary DVD drive.	£30–55
The three printed cards	Dice card and ARITHMETIC CARD on one sheet (laminate it), and a pad of SEED GRID CARDs, one per new seed. Pages 11 and 12 of this manual, or splitsteel-cards.pdf on the website. The boxed kit ships them printed.	£0–3
Pencil, paper pad, metal tin	Working scraps live in the tin; the tin's contents are burned at the end of the sitting.	£3
Optional: fireproof document pouches, tamper-evident numbered bags	Pouches slow a house fire around an object; numbered bags reveal curious relatives.	£20

Total for a complete fresh kit: about **£95–160**, plus £30–55 if you add the archive tier. The manual and the software are free and always will be.

Substitutions that are fine: any permanently offline computer as the blender; punched washers instead of plates; a D16 hex die instead of two d6; laminated card instead of a third plate. Substitutions that are not: anything with a radio, anything that photographs the table, any "seed tool" website on a live machine.

08 · BUILD THE VAULT

One sitting, then never again

Do this once, slowly, at a table with no phone cameras. The existing paper seed stays alive until the round-trip test has passed **from the finished objects**. Rushing step 11 is how people file their coins under a wrong character. In the boxed kit, the wizard on the pre-flashed card walks every step below; the steps are also the audit trail for exactly what it does. The wizard, its test suite and the image-baking script are published in full in the /blender/ folder alongside this manual — one auditable Python file, standard library only, dice only, nothing ever written to disk.

1 Kit

Everything from section 07 on the table, plus this manual printed and the dice card from section 09. Decide the optional passphrase in advance (section 15) - do not improvise secrets at the bench.

2 Make the blender

Kit path: the card in the box is ready - insert it, boot, and the wizard takes over. **Building your own:** flash Raspberry Pi OS on another computer with no Wi-Fi credentials, copy the /blender/ folder to the card, and run its install script. Confirm there is no wireless interface. Either way: a room with no cameras pointed at the screen.

3 The sticks, counted first

Two USB sticks go in before a single die is rolled. The wizard counts them and will not begin with only one. Finding out you brought one stick should cost you nothing - not forty minutes.

4 Where the words come from

The first question is whether you already have a seed, or want a new one. If the seed you hold might be weak or might have been seen - a device with a bad generator, a phrase once typed into a website - make a new one here first (section 04). Otherwise type in the words you have; a mistyped or out-of-order word is caught by the checksum before anything else happens.

5 Cast the pad

Dice and the card: roll a fresh random hex string the same length as the entropy - about 36 rolls for 12 words, 72 for 24. The wizard maps each pair as you call them, or takes a pad you rolled earlier at the table. **It will never roll the pad for you.** Write it in groups of four with its check group.

6 Mix

The blender XORs entropy with pad - the output is the ciphertext. Write it in groups of four with its own check group. The wizard immediately XORs back and confirms the original entropy returns.

7 The spot check

The one step that does not trust the machine. It picks three positions and shows you a pad character and a ciphertext character; you look each pair up on the **printed** XOR table on your card and type what you find, and it grades you. A dishonest program could show a doctored table on a screen. It cannot reach into your pocket. If you have not got the card, it is page 11 of this manual - print it before you start.

8 Round-trip, from paper only

The screen clears and you re-key both halves from your own handwriting, group by group. The wizard rebuilds the words and compares them to the seed you began with. Reading back off the screen would only prove the screen agrees with itself; this is the step that catches paper that is wrong.

9 Write the sticks, one at a time

One stick in the machine, never two - so the two halves have no way of meeting on the same one. Each is written, read back, and the half re-derived from what actually landed on it, before you mark it **R** or **B** and unplug it. Then the other goes in.

10 Finish on two computers

Each stick carries a page called START-HERE.html that opens with a double-click on any computer and walks that half through to finished: burn the M-DISC, engrave or punch the plate, put it away. **R goes to one computer and B to another, and stays that way.** This is the hour in which the two halves can quietly meet, and nothing on a screen will tell you it happened.

11 Round-trip from the objects, then burn the paper

Now do the recovery again, **reading only off the finished plates and discs**, check groups first. The object is the backup, so the object is what you test. Only when the words come back from the objects do you burn the scraps in the tin.

12 Scatter, wipe the blender

The copies go to separate places so that no hiding place holds both halves - and a half can be handed to a solicitor or a friend openly, because it is junk to them. Wipe or destroy the card. The phone never photographs any of it. This manual stays public - it contains no secrets and never will.

The maths, if you would rather do it yourself

```
def xor_hex(a, b):
    a = "".join(a.split()).lower()
    b = "".join(b.split()).lower()
    if len(a) != len(b) or len(a) % 2:
        raise ValueError("same even hex length required")
    return bytes(x ^ y for x, y in zip(bytes.fromhex(a), bytes.fromhex(b))).hex()

def check_group(s, size=4):                 # record this as the last row
    s = "".join(s.split()).lower()
    c = 0
    for i in range(0, len(s), size):
        c ^= int(s[i:i+size], 16)
    return format(c, "0%dx" % size)         # XOR of ALL rows incl. check == 0

# entropy    XOR pad  ->  ciphertext
# ciphertext XOR pad  ->  entropy
```

09 · THE DICE CARD

Two rolls, one hex character

Roll two casino dice — a **first** and a **second**, kept distinct (different colours help). Read the character where the row meets the column. The four corner outcomes are rerolls; that is what keeps every character exactly as likely as every other. 32 characters for a 12-word seed, 64 for 24, then the check group.

	1	2	3	4	5	6
1	0	1	2	3	4	5
2	6	7	8	9	a	b
3	c	d	e	f	0	1
4	2	3	4	5	6	7
5	8	9	a	b	c	d

6	e	f	roll again	roll again	roll again	roll again

Example: first die 4, second die 2 — row 4, column 2 — write **3**. First 6, second 5 — roll both again.

Why the rerolls: two dice give 36 outcomes; 36 does not divide by 16, but 32 does. Using 32 outcomes and rerolling the other four makes every hex character land exactly twice — perfectly uniform, no bias for a thief to lean on.

Print this page and take it to the table. **Do not roll your real pad into any screen that has ever seen the internet.** The card and a pencil are the tools.

The ARITHMETIC CARD — the XOR table, print this too

The wizard calls this page the **ARITHMETIC CARD**. This is the table the wizard's **spot check** sends you to, and the reason it can be trusted: a dishonest machine could show you a doctored table on screen, but it cannot reach into your pocket and change a printed card. Find the pad character in the left column, the ciphertext character along the top, and read off where they meet - that is the entropy character. No arithmetic, no binary, just a lookup.

The table is not a key and holds no secret. It is the same table for every vault ever made, it is printed on the website as well as here, and you could write it out from scratch on a napkin. It replaces the program, not the missing half: a lookup needs a row and a column, so one half plus this table is exactly as useless as one half on its own. Both halves, or nothing.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Worked example: the pad character is **A** and the ciphertext character is **3**. Row A, column 3 gives **9**. If the wizard says that character of the entropy is anything other than 9, stop the sitting - either the machine is wrong or a character was written down wrongly, and both are worth catching before you punch steel.

The table is symmetric, so it does not matter which of the two you call the row. That is the same property that means your plates never need labelling: XOR does not care about order.

The SEED GRID CARD — print one for every new seed

When the wizard mints a new seed from your dice and this machine together, it shows the three numbers as three grids and asks you to write them here, box for box: A is the machine's number, B your dice, C the new seed. The ninth box of each row is its check group, copied like the rest.

Then you prove C yourself. For each box, find the A character in the left column of the ARITHMETIC CARD and the B character along the top; where they meet is the C character. Eight boxes, about four minutes, and from then on the program is off the trust path: it did not choose your seed, you can see that it did not.

A the machine's number

1	2	3	4	
5	6	7	8	check

B your dice

1	2	3	4	
5	6	7	8	check

C the new seed = A combined with B

1	2	3	4	
5	6	7	8	check

Worked example, from a real sitting: box A1 reads **5A3B** and box B1 reads **6DB4**. 5 meets 6 on the table at 3; A meets D at 7; 3 meets B at 8; B meets 4 at F. So box C1 is **378F**, and the wizard's screen must show the same.

The card holds a seed once C is written. Treat it like the words: it goes wherever the words go, and nowhere else.

10 · MAKING THE COPIES

The two-machine rule

The blender is the only machine that ever holds your whole seed. Everything after it handles **one half at a time**, and a half is junk — which means the computers you use to make copies do not need to be air-gapped, do not need to be trusted, and do not need any skill to operate. One rule replaces all of that:

The two halves never meet on the same computer.

Burn or copy the pad's objects on one machine. Take the other stick to a different machine — another room, another building, a friend's desk — and make the ciphertext's objects there. Neither machine ever reconstructs anything, because neither ever holds both halves. An ordinary laptop is fine for this.

Why this matters more than air-gapping. A general-purpose PC may carry dormant malware. Air-gapping it during the ceremony buys you nothing if it reconnects afterwards — malware that read both halves out of memory simply waits and exfiltrates later. A machine that only ever saw one half has nothing worth waiting for. Separation beats isolation, and it is far easier to get right.

Recovery is the exception: that is the one moment both halves legitimately come together, and it belongs on the blender or another wiped, never-networked machine. Never on a random PC. Section 12.

Burning the archive discs

If you are making M-DISCs (section 06), the same rule applies: **two pad discs on one machine, two ciphertext discs on another.** Colour-code them — say red discs for the pad, blue for the ciphertext — and never let a red and a blue share a location.

Each disc holds 4.7 GB and your half is 32 or 64 characters, so fill the rest with a complete recovery kit: the wizard source, this manual, and a plain-text readme that says what the disc is and what to do with it. All of that is public, and the half is junk without its partner, so the disc gives nothing away. Label it "put me in a computer and open readme.txt." A disc that explains itself is worth far more to your heirs than a cryptic plate.

Two practical notes. Add parity files (par2 or dvdisaster) so a scratched disc still reconstructs — it costs nothing on a 4.7 GB disc. And verify by **ejecting, reinserting and reading each disc back** before the discs count as made; burns fail silently, and discs are cheap.

11 · ORDINARY DAYS

Leave the vault in the ground

Spending does not use the seed. Unlock the phone, send, power off. Do not open "view recovery phrase." Do not QR-sync to a second device. Do not switch on iCloud or Google wallet backup — that is a second copy of the keys in a company cloud, outside every plan you have made.

If you need to know an object still exists, visit the hiding place. Do not assemble a pad and a ciphertext in one room "just to look." Together, in one place, they are the wallet — treat the combination like the money itself.

If any of your copies are on USB sticks, put a yearly reminder somewhere: plug each one in, confirm the file reads, and rewrite it. Flash fades quietly; steel and M-DISC do not.

12 · THE BAD DAY

How you get the words back

1. Collect one pad copy and one ciphertext copy. Not in a café. Not on a webcam. A private room.

2. Boot the blender — or any computer that has never touched a network and never will again. A melted blender is not a blocker; any blender will do, and the software is public. **Not a random laptop:** this is the one moment both halves are together, so it is the one moment the machine must be trustworthy.

3. Check groups first: every string must XOR to `0000`, including its check row. If it does not, you misread a character — find it now, not after.

4. XOR ciphertext with pad. That is the entropy; the wizard turns it back into the 12 or 24 words. Write them on a scrap.

5. Restore the wallet — or better, a hardware signer — on a clean device, entering your passphrase there if you set one. Confirm addresses and balances before you relax.

6. Burn the scrap. Wipe the blender. The objects go back to their separate places, and the words stop existing again.

Afterwards - the step people get wrong

If the machine you used was an ordinary one - a laptop, a work computer, anything that has been on the internet and will be again - then both halves have now been together on a machine nobody can vouch for. **Treat the seed as spent.** That is not a certainty; it is the only safe assumption, and acting on it costs almost nothing.

In this order: do not reconnect that machine until the money has moved; write the words on **paper**, never a photograph; on a different device, ideally a hardware wallet, make a brand new wallet; restore the old words there and move **everything** - every coin, every token, every chain those words ever touched; and only once the old wallet is empty does it stop mattering that the computer saw it.

Then the old halves are retired. Make a fresh backup of the new words and destroy the old plates and discs, so that nobody in twenty years recovers an empty wallet and believes they have done something wrong. This is where money is actually lost: people move the main balance, forget the rest, and destroy the backup.

13 · FIRE AND THEFT

The placement

The rule: **no hiding place holds both halves.** Three copies of each half, spread so that every location holds pad copies or ciphertext copies, never both. Any one location can burn to the ground, and any one location can be burgled, without costing you anything.

If this is lost	You still need	Alive?
The blender (any time)	Nothing	Yes. Buy another blender.
Any one location	One surviving copy of each half	Yes — that is what the copies are for.
Every pad copy	—	No. The ciphertexts are noise without a pad.
Every ciphertext copy	—	No. Same problem, mirrored.
A pad and a ciphertext in one tin	—	That tin was the wallet. Never do this.

Two ordinary house fires in two towns on the same night is a disaster movie. Two relatives on the same flood plain, though, is not geography — pick places whose bad days cannot be the same day.

Theft reads differently

A burglar who takes one object gets a string of junk hex — nothing to google, no brand, no word list, and mathematically no information about your seed. This is the part that no whole-seed metal plate can offer, and it is why a half can be handed to a solicitor openly.

The scenario that does hurt is a thief who takes a pad and a ciphertext and recognises what they are. Placement is the first defence — no location holds both. The passphrase is the second, and it turns even that haul into a decoy (section 15).

14 · METAL

A stamper may see hex. A stamper must never see both halves.

This is why the objects carry hex instead of words. A commercial engraver holding one string of anonymous hex cannot open anything; a stamper holding twelve English words can. The hex is still half the secret, so: **one string per shop** — pad or ciphertext, never both, even months apart. Anonymous hex, no labels on the plate or the invoice, cash, collected in person. Never let a shop keep the CNC file "for reprints," and never ship a plate to the house that already holds the other half.

At home, punched or deep-stamped letters beat pretty engraving:

Material and method	What it survives — and what kills it
Punched / stamped letters in 1.5–2 mm stainless	Best. The dent remains after every colour is gone; shrugs off water, decades and house fires. The keeper pair.
Stainless, deep rotary or fibre engraving	Usually survives fire. Ugly, still hex.
Thin steel, shallow laser mark	Warps, blues, soot in the groove. Sometimes readable after fire.
Thin anodised aluminium, diode laser	Often dies in fire — aluminium melts at ~660 °C and the "engraving" was the coating.
Etched or stamped plastic tag	Fine for a spare: waterproof, cheap, legible for years. Any fire kills it; UV makes it brittle.
Laminated paper or card	Fine for a spare: survives damp and handling. Fire and decades of light do not respect it.

Minimum metal set: one pad and one ciphertext stamped in stainless, in different buildings — the keeper pair. The remaining copies can be any medium from section 06. Two pretty aluminium sheets that each contain everything is how people lose coins to one cooker fire.

Plate size decides the method

A blank has to be big enough for the stamps, not just for the characters. A common letter and number punch set has a body about 6mm across for a 3mm character, and it is the body that sets the spacing, not the glyph. That rules out small blanks:

BLANK	SIZE	HAND PUNCH, 12 WORDS	HAND PUNCH, 24 WORDS
CD-sized disc or case insert	120 x 120mm	yes, with normal 6mm stamps	yes
Keeper plate	90 x 60mm	only with 4mm stamps or slimmer	only at 2.5mm

Credit-card size	85.6 x 54mm	only with 3mm stamps or slimmer	no

So for stainless, build around **120 x 120mm**. That is not a preference - a CO2 laser cannot mark bare stainless at all, so on steel the method is punching, and punching needs the room. The case insert has a second advantage: it stores flat inside the CD case next to that half's M-DISC, one colour per case.

The smaller blanks stay useful for the **laser** route on anodised aluminium or coated plate, where a 90 x 60 gives a comfortable 8.8mm character for a 12-word half. Two materials, two sizes, same information.

Steel is not the expensive part. A 3000 x 1500 x 2mm sheet of 304 yields roughly 288 120mm blanks - about two pounds each, or twelve pounds for a full six-blank vault. Ask the supplier to cut them; cutting several hundred pieces yourself costs far more than the metal.

15 · THE PASSPHRASE

Keep it in your head, and out of the blender

A BIP39 passphrase — the "25th word" — is not part of your entropy and never enters this protocol's maths. It is an independent factor: the words alone open a different, decoy wallet, and only words plus passphrase open the real one.

Which makes it the exact backstop for this protocol's one residual risk. Every scenario where someone reunites both halves — a burglar who takes two objects, a location that held a pair, two machines compromised by the same attacker — ends with them opening a decoy and finding nothing. The split and the passphrase cover each other's failures.

So it never touches the blender. You type it into your wallet at restore time, not into the Pi. That way even a compromised blender that leaked your entire seed still cannot open your real wallet. Splitting the passphrase across its own pair of objects would hand the blender both secrets and throw that firewall away — so this protocol does not do it, and neither should you.

How to back one up

Memorise it — that is the primary store. Memorable to you, not guessable by others. Then **one or two sealed written copies** in trusted, separate hands — the will, a family member — for inheritance and for the day memory fails. The one placement rule: a passphrase copy never shares a location with a seed half, so no single place holds enough to matter.

It needs no dice, no hex, and no ceremony. It is not half of anything; a single copy is safe on its own, because it is useless without a seed that lives somewhere else entirely.

Default: skip it. More coins are lost to forgotten passphrases than are ever saved by them, and the split is already strong. Add one when the sum justifies the risk — and understand plainly that forgetting it means the money is gone, with nobody to appeal to.

16 · HEIRS

The objects must fool a thief — not your executor

Hex that a burglar walks past is hex a grieving family bins. The fix is a sealed letter lodged with your will. It names **what exists and who holds which half**, and contains no secrets at all: no hex, no map, no passphrase. It can be read aloud in a solicitor's office without risking a coin.

This is where the protocol is at its strongest. Because a half is mathematically junk, you can hand one to a solicitor, a sibling or a safe-deposit box openly — they may look, copy it, or lose interest, and none of it matters. No trust, no subscription, and no company holding a share of your keys. If your copies are M-DISCs, each one carries its own software and instructions (section 10), so an heir with any computer and this letter has everything.

If you set a passphrase, decide now which living person or arrangement carries it — or accept, in writing, that the coins die with you.

TO MY EXECUTOR — OPEN WITH MY WILL

There is money in a cryptocurrency wallet. Its backup is a set of **small objects marked with letters and numbers** — metal plates, discs, or memory sticks — that look like serial numbers. They are worthless alone and unlabelled on purpose. Do not discard any such object you find, however dull it looks.

_____ holds one kind. _____ holds the other kind. There are spares elsewhere. Bring one of each kind together only at the point of recovery, with a technically competent helper you chose — not one who volunteers.

The full public recipe for turning them back into the wallet is called **SPLITSTEEL**; a printed copy is kept _____ , and any disc among the objects also contains the software and instructions. Follow it exactly. Type nothing from the objects into any website or phone.

Regarding the extra passphrase: _____ .

Signed _____ Date _____

17 · WHAT THIS IS NOT

And what it composes with

SPLITSTEEL never touches your coins, keys or addresses. It backs up the seed behind whatever you already use, so it sits underneath your setup rather than replacing it. Here is the honest position against everything it might be confused with.

Compared with	The honest position
Coldcard **Seed XOR**	Same mathematics, different presentation. Their shares are word-shaped — each looks like a real seed — and the feature is tied to their device. Ours are hex that does not look like a wallet at all, on any hardware, with check groups and media guidance. Prior art, credited.
Shamir / SLIP39	Genuinely better on loss: any 2 of 3 shares rebuild the secret. We are 2-of-2 — lose a half and the coins are gone. Our answer is redundancy (three copies of each half), which is simpler to perform but less elegant. If threshold recovery matters more to you than simplicity, use Shamir.
Multisig (2-of-3 and friends)	Stronger for large sums: no single moment ever assembles a whole seed, and keys can be rotated or replaced. It is the right structure for life-changing amounts. It is also not a competitor — multisig still has keys, and every key still needs a backup. **Split each key with this.**
Metal seed plates (Cryptosteel, Billfodl, CryptoTag)	Beautiful metal, single point of failure: the whole seed in one object a knowledgeable thief recognises. Word-index numbers are not obfuscation — the BIP39 list is a public file. Our objects are anonymous and individually worthless.

Custody and inheritance services	No subscription, no company, no shares held by a third party, nothing to breach. The trade is real: nobody is coming to help you either.
A hardware signer	Different job entirely. A signer spends without exposing keys; this backs the seed up. Compose them: a signer with a dice-generated seed, backed up this way.

And the plain warning

This system has **not had independent security review**, and has not been used at scale by people who are not its authors. The cryptography is a century old and the software is public and tested against the official BIP39 vectors, but assembled protocols fail on human factors, not on mathematics. Before anyone puts life-changing money behind it, it needs adversarial review and real users trying it and failing in the ways real people fail. Until then: use it for sums you can afford to be wrong about, and tell us what breaks.

Seed XOR, and what is actually different here

The mathematics in this manual is not new, and it is not ours. Coldcard has shipped **Seed XOR** since firmware 4.1.0 in 2021: the same exclusive-or split, documented for metal plates, with each share itself a valid BIP-39 phrase. Anyone who knows the field knows this, and a protocol that pretended otherwise would deserve the reception it got.

Their design has real advantages over this one. Because each share is a normal seed phrase, it fits any metal backup product already on the market, and each share can be funded with a small amount as a decoy. It has been in the field since 2021.

What is different here is narrower, and it matters most on the day nobody planned for. Their shares are words, so combining them without the device means converting each word to an eleven-bit number, XOR-ing 264 bits across boundaries that do not line up with the words, stripping checksum bits and converting back - not something a person does at a kitchen table. These halves are hex, so combining them is 32 lookups on the printed table in section 09. No device, no vendor, no software. For an heir in 2050 with no working hardware, that is the whole difference.

The other difference is that nothing here needs a particular company's product to split or to recombine. That is a claim about dependency, not about cryptography.

18 · SELL THE BOX, NEVER THE SECRET

If this ever becomes a product

You can sell a kit and a name. You cannot own the mathematics, and you must never touch anyone's hex. XOR of entropy is Vernam (1917); BIP39 is a standard; Coldcard already ships Seed XOR. A patent will not save you. Brand, an idiot-proof kit, and never being a honeypot is the only commercial shape that is not a scam or a copy.

Product	Do it?	Why
Kit: Pi Zero 1.3, USB pair, stainless blanks, dice, punches, pre-flashed card, this manual	Yes	Open the box, boot, roll dice. Margin on hardware; the protocol is the manual in the box. £80–150.
Archive add-on: M-DISC burner and four discs	Yes	The inheritance tier, and the part no competitor packages.
Plain hex objects — no word lists, no wallet branding	Yes	The thing the market under-serves. Word plates train thieves.

A website that mixes seeds	Never	A honeypot. One XSS and you are the headline.
“We’ll stamp your backup for you”	No	You become a stamper with a customer list.
A phone app blender	No	Phones have radios.

How the company does not die on day one: open-source the wizard and the image (done — see the /blender/ folder); never receive a pad, ciphertext or word by any channel; sell hardware, not custody; print the liability plainly on the box. Do not compete with Coldcard on signing — they own spend-without-a-hot-phone. Own the backup that does not look like a seed, and the inheritance plan a solicitor can actually hold.

19 · GLOSSARY

What the words mean in this protocol

Air-gap — A machine with no network on purpose — no Wi-Fi, no Bluetooth, no cable to a live computer. The blender is air-gapped always; machines that only ever see one half do not need to be.

BIP39 — The standard that turns random bits into 12 or 24 dictionary words plus a checksum, and derives a 512-bit seed from them. Most phone wallets use it.

Blender — The Pi (or any air-gapped computer) used only to mix. Kitchen equipment: mix, pour, wash. The only machine that ever sees your whole seed, and it stores nothing.

Check group — The XOR of all a string’s four-character groups, recorded as its last row. At recovery everything including the check must XOR to 0000. Catches any single misread character.

Ciphertext — Entropy XOR pad. Looks like random hex; useless alone; stored apart from every pad. Three copies.

Dice — The entropy source for the pad. Casino-grade, private rolls, mapped through the dice card. The wizard will not roll for you, deliberately. See section 04.

Entropy — The actual random bits — 128 for 12 words, 256 for 24; written as 32 or 64 hex characters. The thing you XOR.

Half — Either the pad or the ciphertext. Mathematically junk on its own — which is why it can be handed to a solicitor, copied on an ordinary PC, or posted to a relative.

Keeper pair — The two copies you make in stainless — one pad, one ciphertext — for maximum durability. The remaining copies can be any medium.

M-DISC — Archival optical media: data etched into an inorganic layer, projected to last centuries. Written with an M-DISC burner, read by any ordinary DVD drive. Write-once.

One-time pad — A key as long as the message, truly random, never reused, mixed by XOR. Perfect secrecy in theory; here the “message” is the entropy.

Pad — The dice-rolled random hex. Half the vault. Looks like a serial number. Three copies, separate places, never beside a ciphertext.

Passphrase (**“25th word”**) — An extra secret BIP39 mixes into the 512-bit seed. Optional, memorised, and deliberately never entered into the blender. The words without it open a decoy. Section 15.

Pi Zero 1.3 — The Raspberry Pi with no wireless module. W, 2W and Pico W have radios — not blenders.

Round-trip test — Ciphertext XOR pad must equal the entropy, and the entropy must turn back into the exact original words — proven once on paper and once from the finished objects, before old paper dies.

Two-machine rule — The halves never meet on one computer. It is what lets ordinary, un-trusted PCs make copies safely. Section 10.

Wizard — The open-source program that walks the sitting on the blender: one Python file, standard library only, nothing written to disk. Published with its tests.

Tick it on paper. The ticks are not a backup.

Print this page. Do the sitting with it beside the dice, and keep the print with the public how-to — never with a secret.

- [ ] Pi Zero 1.3 bought — not W, not 2W, no radio on the board
- [ ] Media chosen for each half — three copies each, mixing durable and convenient
- [ ] Keeper pair in stainless, 1.5–2 mm — one pad plate, one ciphertext plate
- [ ] Two USB sticks for what the blender writes; M-DISCs or cards for the rest
- [ ] Casino dice (or a hex D16) and the dice card, printed
- [ ] Letter punches or a deep engraver ready
- [ ] Blender ready: kit card booted, or the wizard installed yourself — no Wi-Fi credentials, ever
- [ ] Room checked: no cameras, phone left outside
- [ ] Seed converted to entropy hex — 32 chars for 12 words, 64 for 24
- [ ] Pad rolled with dice to the same length, written in groups of four
- [ ] Check group computed and written for the pad
- [ ] Ciphertext = entropy XOR pad, with its own check group
- [ ] Round-trip on paper passed: ciphertext XOR pad -> entropy -> the exact words
- [ ] Two groups re-XORed by hand with a pencil — the blender agrees with the paper
- [ ] Three copies of each half made — no labels, names, or coin words anywhere
- [ ] Any disc burning done one half per computer — the halves never met on one machine
- [ ] Round-trip repeated reading only from the finished objects
- [ ] Old paper seed destroyed only after the object round-trip
- [ ] Copies split so no hiding place holds both halves
- [ ] Passphrase decided — memorised and sealed separately, or skipped; never typed into the blender
- [ ] Heirs' letter filled in, sealed, lodged with the will
- [ ] The blender's card wiped or destroyed

SPLITSTEEL field manual, version 4.0 — 29 August 2026. A public recipe: copy it, print it, hand it on. It is not financial advice, not a warranty, and not a substitute for independent review before you trust it with life-changing money. XOR will not save a pad rolled with a weak generator, an object labelled “Bitcoin,” or a round-trip test you skipped.

Prior art and reading: Vernam (1917) and Shannon (1949) on the one-time pad · seedxor.com (Coldcard’s word-shaped XOR shares) · SLIP-0039 (Shamir) · github.com/iancoleman/bip39 · thehackernews.com and engineering.block.xyz on the 2026 Coldcard entropy failure. The wizard, its tests and the image-baking script are in the /blender/ folder.

the Pi is a blender · steel is the vault · never type a seed into a website