SELF-CUSTODY, NEXT STEP

Bitcoin Multisig

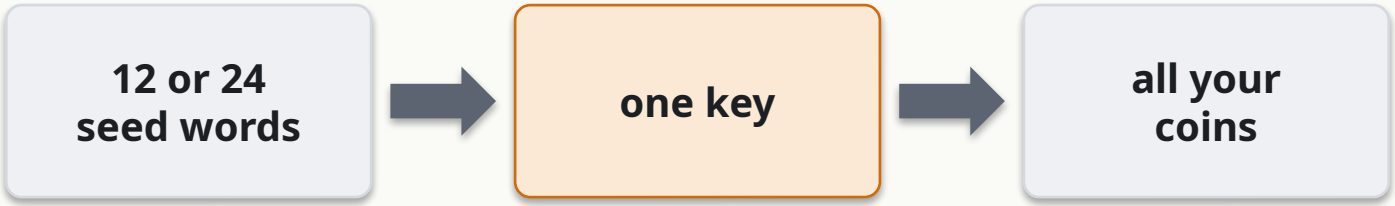
Why to use it, why not to, and what it changes about your backups. Then a live 2-of-3 setup and spend.

Kev · kevhq.com

Talk and live demo · 30 August 2026

THE PROBLEM

Single-sig: one secret carries everything



Whoever has the words has the coins.

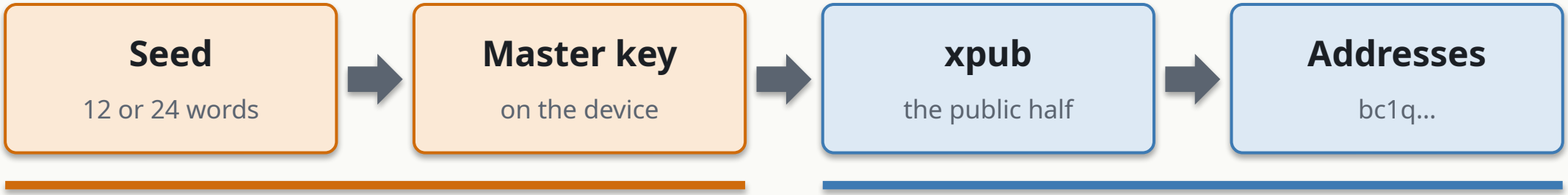
A passphrase, a steel plate, a safe: each **reduces the odds**.
None removes the **single point of failure**.

How one secret fails

- **Lost**: fire, flood, forgotten
- **Found**: the backup *is* the coins
- **Coerced**: one person, one place
- **Compromised device**
- **Your own typo**

REFRESHER

How your wallet works today



Your device has the key.
It signs. That's all it does.

Your software has the xpub.
It makes addresses and watches the balance. It can't spend.

Multisig changes one thing: **three xpubs, one wallet.**

THE IDEA

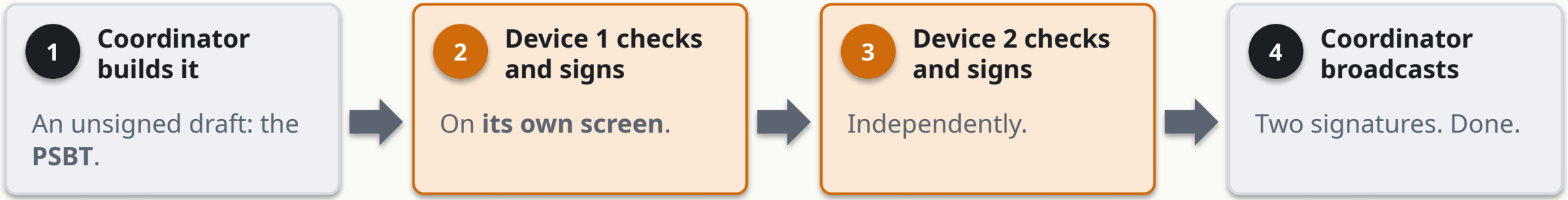
Multisig: N keys, any M of them can spend

2-of-3: any two sign. The third is never needed, so any one can be lost.
Other shapes exist: 2-of-2 has no redundancy, 3-of-5 is more of everything. Start at 2-of-3.

- **Enforced by Bitcoin itself**, not an app, not a company.
- **The keys never meet.**
- **Losing one key is an inconvenience**, not a catastrophe.

THE IDEA

How a multisig spend happens



PSBT: Partially Signed Bitcoin Transaction. A file with no private keys in it, so it is safe to carry by SD card, QR code or cable.

- **Verify on the device screens**, not the laptop.
- **The keys never meet.** Each device signs and hands the file on.
- **Slow by design.** Two devices in two places means nothing gets drained in a hurry.

RISKS IT COVERS

What 2-of-3 protects you from

A lost or destroyed key	COVERED	The other two spend.
A stolen key or found backup	COVERED	One key can't spend.
One compromised device	COVERED	If the other two are different makers.
A vendor fails or is coerced	COVERED	If you mix vendors.
Coercion: the $5 wrench	PARTLY	Only if the keys are out of reach.
Malware swaps the address on your laptop	PARTLY	Only if you verify on a device.

THE NEW SINGLE POINT OF FAILURE

The descriptor problem

To spend from a 2-of-3 you need **two private keys** and **all three public keys**.

The third public key comes from the third device, or from the **descriptor** backup.

Two seeds, no descriptor = locked. Forever.
The most common way people lose multisig funds. Keep the descriptor with every seed.

New words on your backup

Seed	12 or 24 words. The private key. **Secret.**
Fingerprint	`7a3f21c9`: a name tag for one key. Not secret.
Derivation path	`m/48'/0'/0'/2'`: which drawer. Use the standard.
xpub	The public half of one key. Watches, never spends. Private, not secret.
Descriptor	The recipe: rule + all the xpubs. Rebuilds the wallet anywhere.

A descriptor, roughly

```
wsh(sortedmulti(2,
  [7a3f21c9/48'/0'/0'/2']
  xpub6D…nQ4
  [c04d9e12/48'/0'/0'/2']
  xpub6F…wxK
  [58b1a7f0/48'/0'/0'/2']
  xpub6E…Lm9
))
```

fingerprint / path / xpub, three times, plus the rule

BACKUP ANATOMY

What to store with each seed

Location 1

e.g. home

Seed words: key A

the only secret, stamped in metal

Wallet descriptor

rule + all three public keys. Paper, plus a digital copy

A note

“[Name, phone, email]. Key A of 3 of a bitcoin multisig wallet. Recovery plan: in my will.”

Location 2

e.g. family

Seed words: key B

the only secret, stamped in metal

Wallet descriptor

rule + all three public keys. Paper, plus a digital copy

A note

“[Name, phone, email]. Key B of 3 of a bitcoin multisig wallet. Recovery plan: in my will.”

Location 3

e.g. bank box / friend

Seed words: key C

the only secret, stamped in metal

Wallet descriptor

rule + all three public keys. Paper, plus a digital copy

A note

“[Name, phone, email]. Key C of 3 of a bitcoin multisig wallet. Recovery plan: in my will.”

- Descriptor: **not a seed**. Shows balances, can't spend.
- **No map.** Never write where the other keys are.
- The *where* goes in **one** letter, with your will.
- **Print it at home**, from the laptop. No cloud print, no office printer.

Descriptor with every seed, in every location. Any two envelopes must recover everything.

What's in the bag

A sample setup. One way of doing it, not the only way.

FIREPROOF BAG · fibreglass, zipped. Handles water and a short fire, not a long one.

TAMPER-EVIDENT BAG · serial number logged elsewhere

Hardware device

with this key on it. PIN can be in here too.

Seed on steel

verified on the device before sealing.

Descriptor

QR (error correction) + plain text + device config file.

The note

name, contact, what this is, “recovery plan in my will”.

Silica gel

indicating type. Swapped at the yearly check.

Nothing else

no installers, no map, nothing that lives only on a memory card.

Outside the bag

- **Label**: wallet name, key B of 3, sealed date.
- **In the password manager**: bag serial, contents list, last-check date.
- **One bag a year**: open, check, refresh silica, reseal, log the new serial.
- **No passphrase** on these keys. The multisig already does that job; a passphrase is one more thing to lose.

WHEN IT GOES WRONG

When a key is lost or stolen

You can't swap a key. A new key means a new wallet.

1. **Build a new 2-of-3**
   A fresh key plus the two good ones.
2. **Move everything**
   One spend. One fee.
3. **Redo every envelope**
   Plate, descriptor, letter.
4. **Keep the old wallet watch-only**
   For stragglers.

One fee and an afternoon of backups. It will happen once.

Lost or destroyed

No rush. Two keys still work. Move within weeks.

Stolen or leaked

No panic: one key can't spend. But move soon: the next loss is fatal.

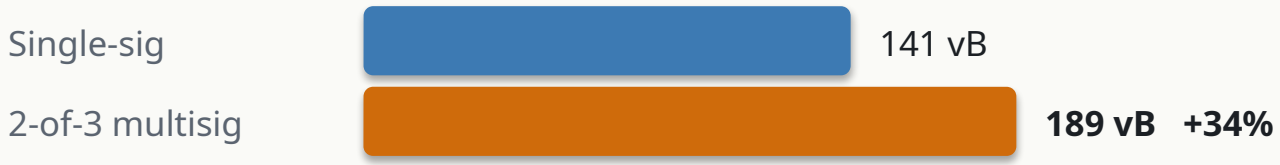
TRADE-OFFS

The cost

Two signatures and the whole script, paid per byte.

One input

Typical send (1 in, 2 out)



A third to a half more per spend. Consolidate when fees are low. Multisig spends are also recognisable on-chain.

And more moving parts

- **Coordinator software**: Sparrow, Nunchuk, Specter, Electrum. Know how to reinstall it.
- **Every spend is a round trip**: build, sign, sign, broadcast.
- **Three devices** to buy, store, charge and update. Each must know the wallet.
- **Spending is slow.** That's the point, and the price.

TRADE-OFFS

When not to use it, and what instead

- **Too little** to justify the gear, fees and hours.
- **Money you spend often.**
- **You're not fully confident in your own setup.**
- **You won't maintain it.**
- **Your heirs can't operate it.**
- **All the keys in one place anyway.**

RULE OF THUMB

Multisig for the **coins you won't touch for years**. Single-sig, done carefully, for everything else.

What to use instead, or alongside

Passphrase

Single-sig + a 25th word. A second secret, not redundancy.

Shamir backup

One key split into shares. Protects the backup, not the signing.

Collaborative custody

A company holds one of three keys. Can't spend alone; you pay.

BEST PRACTICE

Best practice

Setting up

1. **Standard derivation paths**

   Boring is recoverable.

2. **Mix vendors**

   One bug shouldn't touch two keys.

3. **Register the wallet on every device**

   So each can verify addresses, including change.

4. **Verify the first address on a device**

   The laptop screen is not proof.

Living with it

5. **Recovery test before real money**

   Two seeds + descriptor, on a clean machine.

6. **Descriptor with every seed**

   Paper plus a digital copy. Redo it when the wallet changes.

7. **Yearly health check**

   Sign with each pair: A+B, B+C, A+C. Don't broadcast.

8. **Write the recovery letter**

   With your will, not in the envelopes.

LIVE

Demo: 2-of-3, three makers, twenty euro

1. **Three keys, three devices, three makers**: cable, USB drive, QR code.
2. **Build the 2-of-3** from the three xpubs.
3. **The coins are already there**: built, funded and deleted earlier. This *is* the recovery test.
4. **Register the wallet** on the devices.
5. **Spend with two keys.** The third stays in the drawer.

TAKEAWAYS

- Multisig **removes the single point of failure** and creates a new one: the **descriptor**.
- Standard paths. Mixed vendors. Descriptor in every location. **Test the restore.**
- Use it for the **coins you won't touch for years**. A careful single-sig is still the right answer for everything else.
- Losing one key should be a **bad afternoon**, not a life event. That is what you are buying.

Kev · kevhq.com

Slides, notes and the backup checklist at kevhq.com