BITCOIN BUTLERS

Codex32: Seed Security on Paper

Checksum and split your Bitcoin seed by hand, with paper, pencil, and rotating wheels. No computer ever sees it.

What Codex32 Is

Codex32 (BIP-93) is a scheme for doing three things to your seed entirely by hand:

- **Checksumming:** catch a writing error before it costs you the funds
- **Splitting:** divide the seed into shares using Shamir's Secret Sharing, so no single piece of paper is a single point of failure
- **Verifying on paper:** all the math is done with printed lookup wheels (volvelles), not electronics

It is the most air-gapped backup that exists: your seed never touches a computer, not even to verify it.

Why Bother

Every time a seed touches electronics there is exposure: memory, swap files, keyloggers, screenshots, compromised firmware. Codex32 removes the entire category. Generate entropy with dice, write the seed in a checksummed format, split it into shares, verify everything with paper wheels. The only moment a computer is involved is the final wallet import, years later, if ever.

How It Works

The alphabet. Codex32 uses the same 32-character set as modern Bitcoin addresses, chosen to avoid confusion (no O/0, no I/1/l):

`QPZRY9X8GF2TVDW0S3JN54KHCE6MUA7L`

Shamir's Secret Sharing. Pick a threshold k and a share count n. With 2-of-3, any two shares recover the seed. The key property is mathematical, not probabilistic: fewer than k shares reveal exactly zero information about the secret.

The checksum. Each share carries a checksum that detects errors and can even correct one or two wrong characters, verifiable by hand.

Volvelles. Rotating paper wheels with windows act as mechanical lookup tables. Line up the windows, read the value. Slower than a computer, immune to malware, and genuinely beautiful objects.

The Process at a Glance

Creating	Recovering
1. Generate entropy (dice rolls)	1. Gather any k of your n shares
2. Create k initial shares with valid checksums	2. Work through the recovery worksheet
3. Derive the remaining shares on paper	3. Verify the checksum by hand
4. Distribute shares to separate locations/people	4. Import to a wallet (the only computer step)

Who It's For

- **Yes:** long-term cold storage, generational wealth, distributed inheritance shares, anyone who wants to fully understand their backup
- **No:** funds you need quick access to, or if you'd rather trust your signing device's RNG and steel plates (a fine choice for most people)

Try it without the math homework. Our free in-browser tools at **bitcoinbutlers.com** include codex32 utilities, and the printable volvelle booklet is at secretcodex32.com. Want a guided session for a Shamir-split inheritance backup? **bitcoinbutlers.com/butlers**

Spec: BIP-93 · Reference: github.com/BlockstreamResearch/codex32