

BITCOIN & DIGITAL ASSET ESTATE PLANNING

SHAMIR'S SECRET SHARING GUIDE

*How to split your seed phrase into multiple shares
so no single person or location can compromise your Bitcoin*

Prepared by

Asaf David Fulks, Esq.

California State Bar #343622

asaffulkslaw.com

Document 6 of 8 — Bitcoin Inheritance Kit · Version 1.7 (June 2026)

© 2026 Asaf Fulks Law. All Rights Reserved.

IMPORTANT DISCLAIMERS

This document is provided for informational and educational purposes only and does not constitute legal advice.

No attorney-client relationship is created by your use of this document.

Consult a licensed attorney in your jurisdiction for advice specific to your situation.

Prepared by Asaf David Fulks, Esq. — California State Bar #343622

What Is Shamir's Secret Sharing?

Shamir's Secret Sharing (SSS) is a cryptographic technique invented by Israeli cryptographer Adi Shamir in 1979. It solves a fundamental problem in security: how do you protect a secret so that no single person can compromise it, but a trusted group can reconstruct it when needed?

The core idea is simple: instead of storing your seed phrase as a single backup that anyone who finds it can use, SSS mathematically splits the secret into multiple shares. You define how many shares are created (n) and how many are needed to reconstruct the original (m). This is called an m -of- n scheme.

Why It Matters for Estate Planning

The standard approach to Bitcoin backup — writing your 24-word seed phrase on a piece of paper or stamping it on a metal plate — creates an all-or-nothing security model. Anyone who finds that single backup controls your funds. If you store it in one place, a fire or flood destroys it. If you copy it to multiple locations, you multiply the number of places it can be stolen from.

SSS eliminates this tradeoff by introducing threshold security:

- **No single share is useful.** If someone finds one share, they learn absolutely nothing about your seed phrase. Not a single word. The share is mathematically meaningless on its own.
- **Redundancy without risk.** You can distribute shares across multiple geographic locations. Even if one or more locations are compromised (theft, fire, natural disaster), the remaining shares can still reconstruct the secret — and the compromised shares reveal nothing.
- **No single point of trust.** You can distribute shares among multiple trusted people. No individual person can access your funds alone, but the group (or a subset of the group) can act together when needed.

I SSS vs. MULTISIG — THEY ARE NOT THE SAME THING

Shamir's Secret Sharing splits a single seed phrase into shares that reconstruct the original secret. Multisig (multi-signature) uses multiple independent private keys that each sign a transaction separately. Both provide threshold security, but they work differently:

- SSS: One wallet, one seed phrase, split into shares. Shares must be combined to reconstruct the seed, which is then used to sign. The seed exists as a whole during reconstruction — this is a brief window of vulnerability.
- Multisig: Multiple wallets, multiple independent keys. Keys never need to be combined. Each key signs independently. No single point of reconstruction.

Multisig is generally considered more secure for ongoing use because the full secret never exists in one place. SSS is simpler to implement and is well-suited for backup and estate planning scenarios where the reconstruction event is rare (i.e., your death or incapacity).

The 2-of-3 Scheme

The 2-of-3 scheme is the most common and practical SSS configuration for individual Bitcoin holders. You create 3 shares, and any 2 of them can reconstruct your seed phrase. This means:

- You can lose one share (theft, fire, loss) and still recover your funds with the remaining two.
- No single share holder can access your funds alone.

- Your heirs need to obtain only 2 of the 3 shares to inherit.

How It Works

Imagine your seed phrase as a single point on a graph. SSS generates a mathematical curve (a polynomial) that passes through that point. Each share is a different point on that curve. With one point, you cannot determine the curve (there are infinitely many curves through a single point). With two points, you can determine the exact curve and therefore reconstruct the original point — your seed phrase.

You do not need to understand the mathematics to use SSS. The hardware and software tools described below handle everything automatically. But it helps to understand this: the shares are not “pieces” of your seed phrase. They are not the first 8 words, the middle 8 words, and the last 8 words. Each share is a complete, independent mathematical object that reveals nothing about the original.

Who Holds the Shares

The power of 2-of-3 is in the distribution. Here are three common configurations:

| Config | Share 1 | Share 2 | Share 3 |
|---------------------|-----------------|--|--|
| A: Self + Locations | Your home safe | Safe deposit box (different bank branch) | Trusted family member's safe (different city) |
| B: Self + People | You (home safe) | Spouse / partner | Attorney or trusted advisor |
| C: Distributed | Attorney | Trusted family member | Second trusted family member or advisor (different city/state) |

Configuration A is best for individuals who want to maintain sole control during their lifetime. You can access your Bitcoin at any time using the shares at your home and safe deposit box. Your heirs can recover by obtaining any two of the three locations.

Configuration B is common for married couples. Either spouse plus the attorney can recover. Both spouses together can recover without involving the attorney.

Configuration C maximizes trust distribution but means you must contact one of the three holders whenever you need to access your own funds. This is appropriate when the SSS wallet is a long-term cold storage vault that you do not expect to access frequently.

Geographic Distribution

The shares should be physically separated to protect against localized disasters. A good rule of thumb:

- No two shares should be in the same building.
- At least one share should be in a different city or state.
- Consider the geographic correlation of natural disaster risk (e.g., two shares in the same earthquake zone or flood plain reduce your redundancy).

The 3-of-5 Scheme

For larger holdings, complex family structures, or institutional-grade security, a 3-of-5 scheme provides greater redundancy and flexibility. You create 5 shares, and any 3 can reconstruct the seed phrase.

When to Use 3-of-5

- Holdings exceeding \$500,000 in value
- Blended families with beneficiaries in different households
- Business partnerships where multiple stakeholders must be involved
- Situations where you want to tolerate the loss of up to 2 shares
- High-security cold storage vaults intended for multi-generational wealth

Example Distribution

| Share | Holder | Location / Notes |
|---------|-------------------------------------|--|
| Share 1 | You (the principal) | Home fireproof safe |
| Share 2 | Spouse / partner | Spouse's separate secure location |
| Share 3 | Estate planning attorney | Attorney's vault / secure file storage |
| Share 4 | Trusted family member | Safe deposit box in a different city |
| Share 5 | Second advisor or corporate trustee | Different state or region |

With this configuration, you and your spouse can access the funds during your lifetime by obtaining any one additional share from the attorney or family member. After death, three of the four remaining holders can reconstruct the secret without any single holder being able to act alone.

⚠ MORE SHARES = MORE COMPLEXITY

Every additional share is another object you must track, secure, and plan for. Each holder must understand what they have, how to store it, and whom to contact in the event of your death. If you cannot reliably maintain communication with all share holders and verify that shares remain secure, a simpler scheme (2-of-3 or even standard single-backup with a passphrase) may be more appropriate. The best security scheme is the one you can actually maintain.

Tools for Implementing SSS

There are two primary approaches to implementing Shamir's Secret Sharing for Bitcoin: hardware wallet support via the SLIP-39 standard, and software-based splitting of an existing BIP-39 seed phrase.

SLIP-39 (Shamir Backup) — Hardware Wallet Native

SLIP-39 is an open standard (developed by SatoshiLabs, the creators of Trezor) that integrates SSS directly into the wallet generation process. Instead of generating a standard 24-word BIP-39 seed phrase, the wallet generates shares from the start.

| Device / Tool | SLIP-39 Support |
|--|---|
| Trezor Model T / Safe 3 / Safe 5 | Native SLIP-39 support. Can generate Shamir backups during initial device setup. Most user-friendly implementation. |
| Keystone 3 Pro | Supports SLIP-39 import and generation. Air-gapped operation via QR codes. |
| Coldcard Mk4 / Q | Does NOT support SLIP-39 — it can neither generate nor import SLIP-39 shares. It is primarily a BIP-39 device whose only native split scheme is Seed XOR (which requires all parts to reconstruct). A SLIP-39 share created on a Trezor or Keystone cannot be imported into a Coldcard. |
| Ledger (Nano S Plus / X / Stax / Flex) | No native SLIP-39 support as of 2026. Ledger uses BIP-39 exclusively. SSS would need to be implemented at the seed level using external tools. |

✓ RECOMMENDED APPROACH

If you are setting up a new wallet specifically for SSS, a straightforward and secure path is to use a Trezor Safe 3 or Safe 5 (or a Model T you already own) with native SLIP-39. The device handles share generation, and you never handle the raw seed phrase. Each share is a set of 20 or 33 words (depending on the strength chosen) that looks similar to a standard seed phrase but is mathematically a share, not the complete secret.

Software-Based SSS for Existing BIP-39 Seeds

If you already have a wallet with a standard BIP-39 seed phrase and want to apply SSS without migrating to a new wallet, you can split the existing seed using software tools. This approach requires more caution because the full seed phrase will exist on a device during the splitting process.

| Tool | Description |
|------------------------|---|
| Ian Coleman's SSS Tool | Companion to the well-known BIP-39 tool. Browser-based; must be run offline. Available on GitHub. |
| SeedXOR (Coldcard) | Not SSS but a related concept: XOR-based seed splitting native to Coldcard (it can split a seed into 2, 3, or 4 parts). Simpler than SSS but with different security properties (all parts must be present to reconstruct). |

⚠ CRITICAL: AIR-GAP REQUIREMENTS

If you use a software tool to split an existing seed phrase, the seed phrase will be present on the computer during the splitting process. This **MUST** be done on an air-gapped (permanently offline) computer. A live-boot Linux USB (such as Tails OS) is strongly recommended. Never enter your seed phrase on a computer that is connected to the internet, has ever been connected to the internet during the session, or has any wireless capability enabled. After splitting, securely wipe (factory-reset) the computer's storage — or, if you used an amnesic live system such as Tails OS, simply power it off, since Tails writes nothing to the host.

Step-by-Step: Setting Up SLIP-39 on a Trezor

1. **Purchase a Trezor Safe 3 or Safe 5 directly from trezor.io (the Model T is discontinued for new sale but remains supported if you already own one). Verify the package is sealed and tamper-free.**
2. **During initial setup, select “Shamir Backup” instead of “Standard Backup.”**
3. **Choose your threshold scheme.** The device will ask you to set the total number of shares (n) and the number required to recover (m). For a 2-of-3 scheme, set m=2, n=3.
4. **Record each share separately.** The device will display each share one at a time. Write each share on a separate piece of paper or stamp it on a separate metal plate. Label each share clearly (e.g., “Share 1 of 3”).
5. **Verify each share.** The device will ask you to re-enter each share to confirm it was recorded correctly. Do not skip this step.
6. **Distribute the shares to your pre-planned locations and holders.** Document the distribution in your Custody Audit Checklist and Digital Asset Memorandum (record where each share is, but not the share contents).
7. **Test recovery before funding the wallet. Only after step 5 confirms every share is correctly recorded, reset the device (the reset erases the on-device secret) and attempt a recovery using your threshold number of shares. Confirm that the same wallet is regenerated. Only then should you transfer funds to the wallet.**

Risks and Limitations

SSS is a powerful tool, but it is not without trade-offs. Understanding these limitations is essential to making an informed decision.

The Reconstruction Vulnerability

The most important limitation of SSS (as opposed to multisig) is that at the moment of reconstruction, the full seed phrase exists in one place — on whatever device is combining the shares. For ongoing wallet use, this means every time you need to sign a transaction, you must reconstruct the secret, creating a brief window of vulnerability. For estate planning purposes, this is less of a concern because reconstruction is expected to happen once: when your executor or heirs need to access the funds.

Share Management Complexity

Every share must be tracked, stored securely, and periodically verified. Share holders must be kept informed of their responsibilities. If you move, change attorneys, or experience a falling-out with a share holder, you need to re-split and redistribute. The more shares you create, the more operational overhead you introduce.

Compatibility Limitations

SLIP-39 shares cannot be used to recover a BIP-39 wallet, and vice versa. If you set up a wallet with SLIP-39, you are committing to the SLIP-39 ecosystem. If your chosen hardware wallet is discontinued, you will need a different SLIP-39-compatible device or software to recover. As of 2026, SLIP-39 support is less widespread than BIP-39.

No Protection Against Coercion

SSS protects against theft and loss, but it does not protect against coercion. If an attacker can compel multiple share holders to surrender their shares simultaneously (e.g., a kidnapping scenario involving family members), the scheme provides no defense. For coercion resistance, a time-locked custody arrangement (in which the funds cannot be moved until a specified block height or date even with the correct keys, generally using Bitcoin script timelocks such as OP_CHECKLOCKTIMEVERIFY) or institutional custody arrangement may be more appropriate.

Software Tool Risks

Software-based splitting tools are only as trustworthy as the software itself and the computer it runs on. Risks include: malicious code in the splitting tool, malware on the computer that captures the seed during entry, improper random number generation, and user error during the splitting process. Using a SLIP-39-native hardware wallet avoids all of these risks.

When SSS Is Overkill

Not everyone needs Shamir's Secret Sharing. For many Bitcoin holders, simpler methods provide adequate security without the added complexity. SSS is likely overkill if:

| Your Situation | Simpler Alternative |
|---|--|
| Holdings under \$50,000 | Standard BIP-39 seed phrase with (optionally) a passphrase (25th word) — if you use one, document it for your heirs (see the Custody Audit Checklist §B.2). Store the seed on a metal plate in a fireproof safe, with a second copy in a safe deposit box. |
| Single trusted heir (e.g., spouse who is technically capable) | Give the heir direct access to the seed backup location. Use a passphrase stored in a separate location as a second factor. |
| You already use multisig | Multisig provides threshold security at the transaction level, which is strictly stronger than SSS. Adding SSS to a multisig setup introduces unnecessary complexity. |
| You use a collaborative-custody service with inheritance features (e.g., Unchained, Casa) | These services have built-in inheritance protocols. SSS is redundant if the service already provides collaborative custody with key distribution. |
| You cannot reliably maintain contact with all share holders | A scheme you cannot maintain is worse than no scheme. If you move frequently, change advisors, or have strained family relationships, the operational burden of SSS may outweigh its benefits. |

A Decision Framework

Use this simple test to decide whether SSS is right for you:

| Question | If Yes... |
|---|---------------------------|
| Are your holdings large enough that losing them would be financially devastating? | SSS is worth considering. |
| Do you have 3 or more trusted people or locations you can use for share distribution? | SSS is feasible. |
| Are you willing to periodically verify that all shares remain secure and accessible? | SSS is maintainable. |
| Is your estate plan complex enough to justify the added overhead? | SSS is appropriate. |

If you answered “No” to any of these questions, a standard seed phrase backup with geographic redundancy and a passphrase may be the better choice. Security is not about using the most advanced tool — it is about using the right tool for your situation and maintaining it consistently.

Collaborative Custody and Managed-Inheritance Services

Everything in this guide so far assumes you manage your own backup — a single seed, Shamir shares, or a multisig you run yourself. There is a middle path between full do-it-yourself and handing your coins to an exchange: collaborative custody. You still hold a key (or keys), so no company can move your Bitcoin on its own — but a service holds an additional key and provides the software, support, and, most importantly, a built-in, tested process for your heirs to inherit. It is a form of self-custody, not a surrender of it.

Two models are common. Managed multisig — for example, Unchained, Casa, or Nunchuk — uses a 2-of-3 or 3-of-5 arrangement in which you hold one or more keys, the service holds one, and a documented procedure transfers control to your heirs. Time-locked inheritance — for example, Nunchuk's Autonomous Inheritance or Liana — lets a backup key become spendable only after a set delay if you stop checking in, so your heirs can claim after the timelock without anyone's permission, while you keep full control during your lifetime.

The tradeoffs are real. In exchange for less do-it-yourself risk and a tested inheritance path, you pay an ongoing fee and you rely on the company continuing to operate. Reputable services give you the keys and data to recover independently if they ever shut down — confirm that before you sign up. You also accept some setup, identity-verification, and privacy overhead. Features, fees, and recovery terms change, so verify each service directly before relying on it.

Consider collaborative custody if your holdings are large enough that a do-it-yourself mistake would be devastating, if you doubt your heirs could carry out a self-managed recovery, or if maintaining a precise paper trail yourself feels riskier than paying a service to manage key distribution. Stay with self-managed backup — a single seed, Shamir shares, or your own multisig — if your holdings are modest, if the cost is not justified, or if you value maximum independence from any third party.

Whichever you choose, you still use this kit. A service manages your keys; it does not tell your family that the service exists, which accounts are involved, or whom to contact — that is what your Custody Audit Checklist, Heir Letter, and Digital Asset Memorandum do. Document the service, your account, the inheritance process, and your points of contact there exactly as you would document any wallet, so your managed plan and your written plan point to the same place.

Need Help Designing Your Custody Architecture?

Choosing between SSS, multisig, and standard backup depends on your holdings, your family structure, and your risk tolerance. Asaf Fulks Law can help you design a custody scheme that balances security, accessibility, and inheritability.

asaffulkslaw.com • asaf@asaffulkslaw.com