The Unofficial Guide to Your Bitcoin Inheritance Plan

A companion to the Little Shard template

> **This guide is your instruction manual for the "Little Shard"**—the single most important document in your Bitcoin self-custody setup. If you've ever worried about what would happen to your Bitcoin if you were gone tomorrow, you're in the right place. This isn't just about securing your assets; it's about ensuring they can be recovered and passed on to the people you care about.

Without a plan, your life's work could be lost forever, locked away in a digital vault with no key. The biggest risk in self-custody isn't a hacker; it's a poorly managed inheritance. The Little Shard template is your first step toward solving this problem. This companion guide will walk you through not just filling it out, but understanding *why* each field matters.

How to Use This Guide

First Time: 45 minutes to 1 hour

This includes gathering your documents, thinking through your answers, and setting up your calendar reminders.

Quarterly Updates: 10-15 minutes

Once you're set up, each quarterly review is quick and straightforward.

What You'll Need Before You Start

- **Devices:** All your hardware wallets, your phone, and your computer
- **Documents:** Your will or trust documents (if you have them), and contact information for your lawyer or CPA
- **Calendar:** You will be setting up recurring events. Don't skip this step

A Quick Security Reminder

This entire process is designed so that you **NEVER** write down your seed phrase, private keys, or any other spendable secret. The Little Shard is a map; it is not the treasure itself. It provides just enough information for your trusted successor to recover your assets, without creating a new security risk.

Technical Setup

The Little Shard is just a text file, but to be effective, it must be stored securely. This means it needs to be encrypted. Encryption scrambles the contents of your file so that it can only be read by someone who has the password.

How to Create the File

You can create the Little Shard file in any plain text editor. The simpler, the better. Avoid using complex word processors like Microsoft Word or Google Docs. Good options include:

- **Windows:** Notepad
- **Mac:** TextEdit (switch to plain text mode: Format > Make Plain Text)
- **Linux:** Gedit, Kate, or any other basic text editor

Simply copy the contents of the Little Shard PDF and paste them into your new text file. Save the file with a name that is descriptive but not too obvious, such as `personal_inventory.txt` or `family_continuity.txt`.

Encryption Instructions by Platform

Once you have your text file, you need to encrypt it. The best way is to store it as a secure note in a reputable password manager.

1Password

1. • Open and unlock your 1Password vault
2. • Click the "+" button to add a new item
3. • Select "Secure Note"
4. • Give the note a title (e.g., "Family Continuity Plan")
5. • Paste the contents of your Little Shard text file into the note
6. • Click "Save"

Your note is now encrypted and stored securely in your 1Password vault.

Bitwarden

1. • Log in to your Bitwarden vault
2. • Click "Add Item"
3. • Select "Secure Note"
4. • Give the note a name (e.g., "Personal Inventory")
5. • Paste the contents into the "Notes" field
6. • Click "Save"

Your note is now encrypted and stored in your Bitwarden vault.

Apple Notes (Encrypted Note)

1. • Open the Notes app on your Mac, iPhone, or iPad
2. • Create a new note
3. • Paste the contents of your Little Shard text file
4. • Click the lock icon in the toolbar
5. • Create a strong password for your locked notes
6. • Your note is now encrypted

Note: This is less secure than a dedicated password manager, but better than nothing.

Standard Notes

1. • Download and install Standard Notes
2. • Create a new note
3. • Paste the contents of your Little Shard text file
4. • The note is automatically encrypted and saved

KeePassXC

1. • Download and install KeePassXC
2. • Create a new database with a strong master password
3. • Add a new entry
4. • Give the entry a title (e.g., "Family Continuity Plan")
5. • Paste the contents into the "Notes" field
6. • Save the entry

Verify Encryption Worked

Once you have stored your Little Shard, verify the encryption is working: log out of your password manager or close the app, then try to access the note again. You should be prompted for your master password. If you can access the note without entering your password, something is wrong.

Section-by-Section Walkthrough

This is where we walk through every single field in your Little Shard template. Don't skip anything—every field exists for a reason. Filling it out completely is the difference between a useful continuity plan and a worthless text file.

Header Fields (30 seconds)

Owner (legal name): Your full legal name as it appears on government ID. Example: "Robert James Thompson" not "Bob Thompson". *Why: If someone finds this file, they need to know whose setup this documents.*

Preferred name: What you go by day-to-day. Example: "Bob" or "RJ". *Why: Makes the doc feel like yours, not a legal filing.*

Jurisdiction: Your primary residence state/country. Example: "California, USA" or "Ontario, Canada".

Created / Last updated / Version: Today's date when you first fill this out. Update "Last updated" every time you touch it. Version: Start with "1.0", bump to 1.1 for small changes, 2.0 for major restructuring.

Next scheduled review / Next annual drill: Review: 3 months from today. Drill: 12 months from today. *Put these in your calendar NOW before you continue.*

Part 0 — The Rhythm

This section is already written for you. Just read it and commit to it.

The single biggest mistake holders make: filling this out once and never opening it again.

Set 2 calendar reminders right now:

- Quarterly check-in (15 min) - *just verify everything still works*
- Annual drill (90 min) - *actually test recovery like your phone got destroyed*

If you can't commit to this rhythm, single-sig Bitcoin above $100k is risky. Consider the audit.

Part 1 — Key Management

Setup type: Choose one:

- **Single-sig:** One device controls everything. Most holders start here.
- **Multisig:** Requires 2+ devices to spend (like 2-of-3)
- **Hybrid:** Mix of single-sig and multisig across different wallets
- **Not sure:** You have Bitcoin but don't know your setup = RED FLAG. Stop. Email your tech contact. Don't guess.

Approx holdings range: Check the box. Nobody sees this but you. It helps you assess risk.

> ⚠️ **CRITICAL THRESHOLD**
>
> If you checked 500k-2M or 2M+ and you're still single-sig → you need the audit. Period.

Signing devices (NO secrets—just inventory + status):

Device #1: Brand/Model — Write exactly what you have:

- ✅ "Coldcard Mk4"
- ✅ "Ledger Nano S Plus"
- ✅ "iPhone 12 Pro with BlueWallet"
- ❌ "My hardware wallet" (too vague)

Purpose: "Primary signing device" or "Hot wallet for spending" or "Multisig key 1 of 3"

Stored where: Be specific enough to find it, vague enough to not dox yourself:

- ✅ "Home office desk drawer, locked"
- ✅ "Safe deposit box, Wells Fargo branch #3382"
- ❌ "The bank" (which bank? which branch?)

Last checked: Literal date you last verified it exists and works. If you haven't checked it in 6+ months, go check it *now* before finishing this doc.

Repeat for Device #2, #3, etc. If you only have one device, just fill out Device #1. No shame.

Backup method: How did you back up your seed phrase?

- **Seed:** Wrote down 12 or 24 words on paper/metal
- **Shards:** Split the seed into pieces (Shamir, multisig extended keys, etc.)
- **Other:** Encrypted digital backup, memory, passphrase scheme

> ⚠️ **CUSTOM BACKUP SCHEMES**
>
> If you checked "Other" and it's something creative → you need professional review. Clever backup schemes usually have fatal flaws.

Backup location #1 / #2: Where are your seed words / shards physically located?

- "Fireproof safe, master bedroom closet"
- "Safe deposit box, Chase Bank #2847, Midtown branch"
- "With attorney [name] at [firm], in sealed envelope"
- "Parent's home, locked filing cabinet"

> **RULE: Your backups should be in different locations than your devices.**
>
> If your house burns down, you should still be able to recover.

Last backup verification date: When did you last confirm you can actually **READ** your backup? Not "when did I write it down" — when did you last **look at it** and verify:

- It's still there
- It's legible
- You can access the location

If it's been 12+ months, go verify *today*.

Part 2 — Legal Protection

Ownership structure: How do you legally own this Bitcoin?

- **Individual:** It's just in your name, personal asset. Fine for <$500k.
- **Trust:** Bitcoin is owned by a revocable or irrevocable trust. Your trust docs should specifically mention digital assets.
- **LLC/Entity:** Owned by a business entity. Common for >$1M holders.

> ⚠️ **PROBATE WARNING**
>
> If you're above $500k and still checking "Individual" → talk to an estate attorney. Probate will be messy.

Trust / Will status: Do you have legal documents that cover what happens to your Bitcoin when you die?

- **Have trust:** You have a trust and Bitcoin is either in it or referenced. Check: Does your trust actually mention "digital assets" or "cryptocurrency"?
- **Have will:** You have a will, Bitcoin may or may not be mentioned. Problem: Wills go through probate. Your heirs might wait 9-18 months to access funds.
- **In progress:** You're working with an attorney on this
- **None yet:** Nothing formal exists. If you die tomorrow, your Bitcoin might be lost forever.

> 🚨 **RED FLAG CHECK**
>
> If you have >$100k in Bitcoin and selected "None yet" → this is your highest priority. Not technical setup. Legal structure.

Attorney/Firm & CPA/Firm: Write down WHO handles your estate/tax stuff. If these fields are blank and you have significant holdings → **you need this team.**

Examples:

- Attorney: "Jennifer Walsh, Walsh & Partners Estate Law, (555) 234-8899"
- CPA: "Marcus Chen, Chen Tax Advisory, (555) 876-3344"

If you don't have these professionals:

- <$100k: Probably okay for now
- $100k-500k: You should have a CPA minimum
- $500k+: You need both, and they should coordinate

Part 3 — Continuity

Last full recovery drill: When did you last pretend you lost your device and had to recover everything from backup?

Partial drill:

- Verified you can see your seed phrase backup
- Checked that your devices still turn on
- Confirmed passwords still work

Full drill:

- Actually wiped a device and restored from seed
- Or set up a second device from your backup
- Confirmed you can see your balance and could transact

If you've NEVER done a drill → schedule it in the next 30 days.

Drill result:

- **Pass:** Everything worked, recovered successfully
- **Issues found:** Something was wrong (illegible backup, forgot password, couldn't access location)

If you found issues, fix them before the next drill.

Part 4 — Professional Team

Your "continuity captain": Who's your go-to person if you're incapacitated?

- Your spouse
- Your attorney
- Your tech-savvy sibling
- Your CPA

NOT your kids (unless they're adults with crypto knowledge).

This person should know:

1. That this Little Shard file exists
2. Where to find it
3. How to decrypt it (password location)
4. Who to call for technical help

Technical support contact: Who helps you with Bitcoin tech questions?

Completion Checklist

Before you save and encrypt this file:

- ☐ All header fields filled (name, jurisdiction, dates)
- ☐ Calendar reminders set (quarterly + annual)
- ☐ Every device documented with location and last-check date
- ☐ Backup locations specified (and you can access them RIGHT NOW)
- ☐ Legal gaps identified (trust/will status honest)
- ☐ At least one human contact listed (continuity captain)
- ☐ Recovery drill scheduled in next 30-90 days

Now encrypt this file (refer back to Section 2 for encryption instructions).

When to Request an Audit

You should consider the Self-Custody Continuity Audit if:

- You checked $500k+ holdings and anything in Part 2 is blank
- You have no legal documents (trust/will) covering your Bitcoin
- You're still single-sig above $500k
- You haven't done a recovery drill in 12+ months
- Your "technical support" field is empty
- You found issues during your last drill
- You have devices or backups you can't currently access
- You're not sure if your CPA/attorney actually understand Bitcoin custody

WHAT THE AUDIT GIVES YOU

- A completed Little Shard (we do it together)
- Single-sig vs multisig recommendation for your situation
- Trust/will alignment checklist you can share with your attorney/CPA
- Prioritized fix plan (what to tackle first)

[REQUEST AUDIT BUTTON/LINK]

After You Complete It

Filling out your Little Shard is a huge step, but it's not the final one. A plan that lives in a vacuum is a plan that will fail. This section covers the critical follow-up actions that turn your document from a simple text file into a living, breathing continuity plan.

Where to Store It

As discussed in the Technical Setup, your Little Shard file MUST be encrypted. The primary copy should live in your password manager or encrypted vault of choice. However, you should also consider a backup of the encrypted file itself. This is NOT a backup of your seed phrase, but a backup of the encrypted Little Shard file.

Good options for storing a backup of the encrypted file include:

- A USB drive stored in a fireproof safe
- A secure cloud storage service (like Dropbox or Google Drive), as long as the file itself is encrypted with a strong password
- With your estate attorney, on a physical medium (like a USB drive)

Who Should Know It Exists (and Who Shouldn't)

This is a delicate balance. You need someone to know that the Little Shard exists and how to access it in an emergency, but you don't want to create a new security risk.

Your Continuity Captain: This person (or persons) MUST know that the Little Shard exists. They should know its name, where to find the primary copy, and where to find the password to decrypt it. The password itself should be stored separately from the file.

Your Executor/Trustee: Your legal representative should be aware that you have a digital asset inheritance plan and that a "continuity captain" has been designated to execute it.

Everyone Else: No one else needs to know. Do not talk about your Little Shard at family gatherings. Do not mention it to your friends. The more people who know about it, the greater the risk.

How to Share Access with Your Continuity Captain

Sharing access with your continuity captain is the most critical and sensitive part of this process. Here are a few options, from most to least secure:

1. Password Manager Emergency Access: Many password managers (like 1Password and Bitwarden) have a feature that allows you to grant emergency access to a trusted individual after a waiting period. This is the gold standard. Set up your continuity captain as your emergency contact.

2. Sealed Envelope with Attorney: Give your attorney a sealed envelope containing the master password to your password manager or the password to your encrypted note. The envelope should only be opened upon your death or incapacitation.

3. In-Person Briefing: Sit down with your continuity captain and walk them through the process of accessing the Little Shard. Do not give them the password directly. Instead, show them where to find it.

Setting Up Your Maintenance Calendar

Your inheritance plan is a living process. You MUST set up calendar reminders to maintain it. Open your calendar now and create two recurring events:

Quarterly Check-in (15 minutes)

- Review your Little Shard
- Confirm you can access your devices and backups
- Make sure your contact list is up to date

Annual Drill (60–90 minutes)

- Perform a full recovery simulation
- Pretend a device is lost or destroyed
- Use your backups to restore access to your funds

First 30-Day Action Items

To make this less overwhelming, here are your action items for the next 30 days:

☐ Complete your Little Shard. Fill out every field to the best of your ability.

☐ Encrypt your Little Shard. Store it in your chosen password manager or encrypted vault.

☐ Designate your continuity captain. Have the conversation. Make sure they understand their role.

☐ Set up your calendar reminders. Do it now. Don't wait.

☐ Schedule your first full recovery drill. Put it on the calendar for sometime in the next 1-3 months.

Common Mistakes

Even with the best intentions, it's easy to make mistakes when setting up a self-custody inheritance plan. Here are some of the most common (and costly) errors we see, and how to avoid them.

"I stored my device and backup in the same location."

This is the classic mistake. If your house burns down, is flooded, or is burglarized, you could lose both your primary signing device and your seed phrase backup at the same time. This is a total loss of funds.

> **RULE: Your backups must be stored in a separate physical location from your devices. No exceptions.**

"I encrypted it but forgot where I put the password."

An encrypted file is useless if you or your successor can't decrypt it. The password to your Little Shard is just as important as the file itself. You must have a plan for your continuity captain to access the password. This could be through your password manager's emergency access feature, a sealed envelope with your attorney, or another secure method.

"I filled it out but never tested recovery."

A plan that hasn't been tested is not a plan; it's a prayer. You MUST perform regular recovery drills to ensure that your backups are legible, your devices are working, and you remember the process. The time to find out your backup is corrupted is not when you're in a real emergency.

"I didn't tell anyone it exists."

This is the silent killer of Bitcoin inheritances. If you are the only person who knows about your Little Shard, it will die with you. Your continuity captain MUST know that the file exists, where to find it, and how to decrypt it. Without this crucial link, your Bitcoin is likely lost forever.

Frequently Asked Questions

"Can I store this in Dropbox/Google Drive?"

You can store the *encrypted* Little Shard file in a cloud storage service like Dropbox or Google Drive, but you should not store the unencrypted text file there. The file itself must be encrypted before you upload it. Also, be aware that if your cloud storage account is compromised, an attacker could get a copy of your encrypted file. They would still need the password to decrypt it, which is why a strong, unique password is so important.

"Should I print this?"

We do not recommend printing the Little Shard. A printed copy is much harder to secure than an encrypted digital file. It can be lost, stolen, or read by anyone who finds it. If you absolutely must have a physical copy, store it in a fireproof safe or a safe deposit box, and treat it with the same level of security as your seed phrase backup.

"What if I have multiple wallets?"

The Little Shard template is designed to be flexible. If you have multiple wallets, you can either create a separate Little Shard for each one, or you can add sections to your existing Little Shard to document each wallet. For example, you could have a "Part 1A - Key Management (Wallet 1)" and a "Part 1B - Key Management (Wallet 2)."

"Is this file legally discoverable?"

Yes. In a legal proceeding, such as a divorce or a lawsuit, you could be compelled to produce your Little Shard. This is another reason why it is so important that the Little Shard does **not** contain any spendable secrets. The file is a map; it is not the treasure. It documents your setup, but it does not give anyone direct access to your funds.

READY TO GET STARTED?

You now have everything you need to create a professional, secure, and inheritable Bitcoin custody plan. Start with your Little Shard template, follow this guide, and set up your calendar reminders today.

Questions? Need professional guidance? [REQUEST AUDIT BUTTON/LINK]