

BITCOIN & DIGITAL ASSET ESTATE PLANNING

CUSTODY AUDIT CHECKLIST

Prepared by

Asaf David Fulks, Esq.

California State Bar #343622

asaffulkslaw.com

Document 1 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.

This checklist is designed to help you identify vulnerabilities in your Bitcoin and digital asset custody arrangements as they relate to estate planning and inheritance. It is not a substitute for professional legal counsel, and the author assumes no liability for actions taken based on information contained herein.

⚠ SECURITY WARNING — READ BEFORE COMPLETING

With self-custody comes extraordinary freedom — and extraordinary responsibility. By completing this checklist, you are creating a detailed map of your Bitcoin holdings, key locations, and security arrangements. This document serves two purposes: it is your personal recovery reference if your keys, steel plates, or hardware wallets are ever lost, damaged, or destroyed — and it is the roadmap your heirs will need to access your Bitcoin if something happens to you. You need to understand the tradeoff you are making:

If you do NOT complete this document, your Bitcoin will almost certainly be lost permanently when you die or become incapacitated. Your heirs will have no way to find it, access it, or recover it. It will join the estimated 3–4 million BTC already lost forever. Even during your lifetime, if a fire destroys your steel plate, your hardware wallet fails, or you forget which safe deposit box holds your backup, this document is your recovery lifeline.

If you DO complete this document and it falls into the wrong hands, someone could use the information to locate and steal your funds. There is no insurance, no fraud protection, and no reversal. The theft would be permanent and total.

That is the tradeoff. You are choosing to reduce the risk of permanent loss in exchange for increasing the risk of theft. This is the right choice — but only if you treat the completed document with the same gravity you treat the seed phrases themselves.

Once completed: Do not email this document. Do not store it in cloud storage. Do not photograph it. Store the completed version in a fireproof safe, a safe deposit box, or with your estate planning attorney — and nowhere else. If you would not leave your seed phrase sitting on your kitchen counter, do not leave this document there either.

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

HOW TO USE THIS CHECKLIST

Bitcoin's core value proposition — that no third party can seize, freeze, or confiscate your holdings — creates a corresponding estate planning challenge: no third party can recover them for your heirs, either. If your private keys are lost, there is no bank to call, no "forgot password" link, and no court order that can reverse the outcome. The Bitcoin is gone.

This checklist is designed to systematically identify every point where that could happen to your holdings. It walks through four areas:

- **Section A — Holdings Inventory:** A complete accounting of every wallet, exchange account, and digital asset you own.
- **Section B — Key Management:** Where your seed phrases, passphrases, and PINs are stored, and who can access them.
- **Section C — Single Points of Failure:** Scenario-based questions that expose the situations where your Bitcoin becomes permanently inaccessible.
- **Section D — Action Items:** A prioritized list of vulnerabilities to fix, generated from your answers above.

Be thorough. Be honest. The person who will need this information the most is the person who cannot ask you to clarify it.

SECTION A: HOLDINGS INVENTORY

Complete every row. If you hold assets across multiple wallets or exchanges, use one row per account. Accuracy here is critical — your executor cannot distribute what they cannot find.

A.1 Self-Custody Wallets

Hardware wallets, software wallets, mobile wallets, paper wallets, multisig setups. Include watch-only wallets.

Wallet Name / Label	Type	Make / Model	Location	Approx. Balance	Last Verified

Type: Hardware / Software / Mobile / Paper / Multisig / Watch-Only. Add rows as needed. For each self-custody wallet, also record its output descriptor (or, at minimum, the master public key / xpub plus the derivation path) and store it with this checklist — the output descriptor is the portable artifact your heirs need to rebuild a watch-only wallet and see the

full balance across all address types. (An output descriptor is a short text string your wallet software can export — if this is unfamiliar, ask your technical advisor to capture it for you.)

A.2 Exchange & Custodial Accounts

Every exchange, brokerage, or custodial platform where you hold digital assets (Coinbase, Kraken, River, Swan, etc.). Record collaborative-custody accounts (e.g., Unchained, Casa, Nunchuk) here as well, and document their multisig configuration in §B.4.

Exchange / Platform	Account Email	2FA Method	Assets Held	Approx. Value

2FA Method: Authenticator App / Hardware Key (YubiKey) / SMS (flag as vulnerability) / Email. For each account, also note whether a beneficiary or transfer-on-death (TOD) designation is on file — such a designation overrides your will, trust, and this kit.

A.3 Other Digital Assets

Lightning channels, staking positions, DeFi protocols, NFTs, mining operations, node rewards, domain names, Nostr identities, or any other digital asset with monetary or sentimental value.

Asset Description	Platform / Protocol	Access Method	Approx. Value

Asset Description	Platform / Protocol	Access Method	Approx. Value

A.4 Total Holdings Summary

Total Estimated Value (Self-Custody)	\$
Total Estimated Value (Exchange/Custodial)	\$
Total Estimated Value (All Digital Assets)	\$

Date of this inventory: ____ / ____ / ____ Update this inventory at least annually or after any significant acquisition, sale, or wallet migration.

⚠ PHYSICAL SECURITY & THE “\$5 WRENCH” RISK

This checklist and your Heir Letter deliberately concentrate, in one place, the total value of your holdings and a map of where everything is — exactly the information a physical-coercion attacker (a so-called “\$5 wrench attack”) wants. Reduce that risk: (1) do not store the total-value figure together with the location map — keep them separate; (2) keep a small “decoy” balance reachable with the seed phrase alone, and hold the real funds behind a BIP-39 passphrase, so a coerced unlock reveals only the decoy; (3) do not co-locate the passphrase with the seed phrase, and consider escrowing the passphrase with your attorney rather than documenting it alongside everything else — but it must always remain recoverable by your heirs (escrowing it with your attorney still counts as documenting it; never simply leave it out of your estate plan); (4) limit who knows the existence and size of your holdings. Coercion attacks on Bitcoin holders have risen sharply — treat the location of large balances as strictly need-to-know.

SECTION B: KEY MANAGEMENT

This is the most security-sensitive section. Seed phrases are the master keys to your Bitcoin. If someone obtains your seed phrase, they control your funds. If nobody can find your seed phrase, your funds are permanently lost.

B.1 Seed Phrase Backup Inventory

#	Wallet Associated	Word Count	Storage Medium	Physical Location	Who Knows Location?

Storage Medium: Paper / Stamped Metal (e.g., Seedplate, Cryptosteel) / Engraved / Digital (flag as HIGH RISK). Word Count: 12 or 24. Verify each backup is still readable at least annually, and test recovery to a spare device at least once after creating each backup — both are essential and easy to neglect. After any such test recovery, securely wipe (factory-reset) the spare device, because it now holds a live copy of your seed phrase.

CRITICAL: Digital Storage Red Flags

If you have stored seed phrases in ANY of the following, mark as URGENT in Section D: cloud storage (iCloud, Google Drive, Dropbox), password managers, email (sent or drafts), photos/screenshots on phone, notes apps synced to cloud, text messages, or any internet-connected device. A seed phrase stored digitally is a seed phrase waiting to be stolen.

B.2 Passphrase / 25th Word

A BIP-39 passphrase (sometimes called the “25th word”) creates an entirely separate set of addresses from the same seed phrase. If you use one, your heirs must have BOTH the seed phrase AND the passphrase to access funds.

Do you use a passphrase / 25th word?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Where is the passphrase stored?	
Is it stored separately from the seed phrase?	<input type="checkbox"/> Yes <input type="checkbox"/> No

B.3 Hardware Wallet PINs & Device Access

Your hardware wallet PIN protects against physical theft but does NOT replace your seed phrase. If the device is reset or destroyed, only the seed phrase can recover your funds.

Device	PIN Location	Firmware Current?	Duress PIN Set?	Backup Device?

Duress PIN: Some hardware wallets (e.g., Coldcard) support a decoy PIN that opens a secondary wallet with minimal funds. Note if configured.

B.4 Multisig Configurations

If any of your wallets use multisig (multiple keys required to sign a transaction), document the configuration. Your executor needs to know the threshold, who holds each key, and where the wallet configuration file (e.g., .bsms, .json) is stored.

Wallet Label	Scheme (m-of-n)	Key Holders	Coordinator SW	Config File Location

Coordinator Software: Sparrow, Electrum, Caravan, Nunchuk, Casa, Unchained, etc. The config file is essential for recovery.

SECTION C: SINGLE POINTS OF FAILURE ANALYSIS

Answer each scenario honestly. The goal is to identify every situation where your Bitcoin becomes inaccessible. There are no wrong answers — only dangerous ones you haven't planned for.

C.1 “If You Died Tonight”

Question	Your Answer
Does anyone know you own Bitcoin?	
Does anyone know where your hardware wallet(s) are?	
Does anyone know where your seed phrase backup(s) are?	
Could your executor find your seed phrases without your help?	
Does your will or trust reference digital assets?	
Have you designated a digital executor with technical competence?	
Would your heirs know NOT to share seed phrases with “helpers”?	
Have you set any account-level beneficiary, legacy-contact, or inactive-account designation (e.g., Google Inactive Account Manager, Apple/Facebook Legacy Contact, an exchange beneficiary form) that could conflict with your will, trust, or Digital Asset Memorandum?	
Does your durable power of attorney expressly authorize your agent to access your digital assets and the content of your electronic communications? (Required for §879.1 / SB-1458 coverage if you become incapacitated.)	

C.2 “If Your House Burned Down”

Question	Your Answer
Are all seed phrase backups stored in a single location?	
Are any backups on paper that could be destroyed by fire/water?	
Do you have at least one backup in a separate geographic location?	
Would you lose access to your exchange 2FA if your phone was destroyed?	
Do you have TOTP recovery codes stored off-site?	
Are your hardware wallets and seed backups in the same location?	

C.3 “If Your Phone Was Destroyed or Stolen”

Question	Your Answer
Do you use a mobile wallet with funds on it?	
Is your mobile wallet backed up (seed phrase written down)?	
Is your authenticator app (TOTP) backed up or synced?	
Could someone with your phone unlock it and access wallets?	
Do any exchange accounts rely on SMS-based 2FA?	
Would losing your phone lock you out of any exchange account?	

C.4 Additional Threat Scenarios

Question	Your Answer
Could a disgruntled family member access your seed phrases?	
Have you ever entered a seed phrase on a computer or phone?	
Have you ever photographed or screenshot a seed phrase?	
Do you use the same password for multiple exchanges?	
Is your email account (linked to exchanges) secured with a hardware key?	
Have you verified your backup actually works (test restore)?	

SECTION D: ACTION ITEMS

Review your answers from Sections A through C. Every “No” answer, every gap in your inventory, and every scenario where your heirs would be unable to access your holdings represents a vulnerability. List them here in order of severity.

D.1 Prioritized Vulnerability List

Rate each vulnerability: CRITICAL (total loss of funds possible), HIGH (significant risk of loss or delay), MEDIUM (suboptimal but not immediately dangerous), LOW (best practice improvement).

#	Vulnerability Identified	Priority	Action Required	Completed

D.2 Common Critical Vulnerabilities

If any of the following apply to you, they should be your first action items:

Vulnerability	Applies?	Resolved?
Seed phrase stored only in one location	<input type="checkbox"/>	<input type="checkbox"/>
Seed phrase stored digitally (cloud, email, photo, password manager)	<input type="checkbox"/>	<input type="checkbox"/>
No one knows you own Bitcoin or where to find your keys	<input type="checkbox"/>	<input type="checkbox"/>
Passphrase (25th word) exists but is not documented for heirs	<input type="checkbox"/>	<input type="checkbox"/>
Exchange accounts use SMS-based 2FA	<input type="checkbox"/>	<input type="checkbox"/>
No will or trust references digital assets	<input type="checkbox"/>	<input type="checkbox"/>
All backups are in the same building as your hardware wallet	<input type="checkbox"/>	<input type="checkbox"/>
Multisig wallet configuration file is not backed up	<input type="checkbox"/>	<input type="checkbox"/>
You have never performed a successful test recovery from your seed backup to a spare device	<input type="checkbox"/>	<input type="checkbox"/>
Your heirs would not recognize a hardware wallet or seed phrase	<input type="checkbox"/>	<input type="checkbox"/>

D.3 Next Steps

Once you have completed this audit:

1. **Address all CRITICAL vulnerabilities immediately.**
2. Complete the Heir Letter Template — the plain-English letter that tells your loved ones what you own and how to access it.
3. Execute the Digital Asset Memorandum — the legal document referenced by your will or trust that authorizes your executor to access your digital assets.
4. Ensure your executor has a copy of the Executor Technical Guide.
5. For substantial holdings, consider Shamir's Secret Sharing, multisig, or a collaborative-custody service — use the decision framework in the Shamir's Secret Sharing Guide included in this kit.
6. Schedule a consultation with a Bitcoin-literate estate planning attorney to review your complete plan.

Need Help Securing Your Bitcoin Inheritance Plan?

Asaf Fulks Law offers one-on-one consultations with an attorney who actually mines Bitcoin, runs a full node, and understands self-custody at the protocol level.

asaffulkslaw.com • asaf@asaffulkslaw.com