

BITCOIN & DIGITAL ASSET ESTATE PLANNING

EXECUTOR TECHNICAL GUIDE

*A step-by-step guide for non-technical executors
responsible for securing and distributing Bitcoin*

Prepared by

Asaf David Fulks, Esq.

California State Bar #343622

asaffulkslaw.com

Document 4 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

This guide is written for executors, trustees, and personal representatives who may have **no prior experience with Bitcoin or cryptocurrency**. It assumes no technical knowledge. Every term is defined when first used, and every step is explained in plain language.

If you are reading this guide, someone has entrusted you with one of the most important responsibilities in digital asset estate administration: securing and distributing Bitcoin. The information below will help you do that without making an irreversible mistake.

THE CARDINAL RULE

When in doubt, do nothing. Bitcoin on the blockchain does not expire, decay, or disappear. The only way to lose it is to send it to the wrong address, expose the seed phrase, or trust the wrong person. Time is on your side. Use it.

CHAPTER 1

What You're Looking For

Before you can secure Bitcoin, you need to know what Bitcoin “looks like” in the physical world. Unlike a bank account or a stock portfolio, Bitcoin is not held by any institution. It exists as entries on a public ledger (the blockchain), and the only way to control it is to possess the private keys — secret codes that prove ownership. These keys are stored in devices and backups that you need to locate.

Hardware Wallets

A hardware wallet is a small electronic device — typically the size of a USB drive, a credit card, or a small calculator — that stores private keys offline. It is the most common and most secure way for individuals to hold Bitcoin. Here are the devices you are most likely to encounter:

Device	What It Looks Like	Key Details
Ledger Nano S / Nano X / Nano S Plus	Small USB-like device with a tiny screen and two buttons	Screen displays transaction details for verification. Connects to computer or phone via USB or Bluetooth. Uses a companion app called Ledger Live.
Ledger Stax / Flex	Larger device with a touchscreen, resembles a small smartphone	E-ink touchscreen display. May have a customized lock screen image. Uses Ledger Live app.
Trezor Model One / Model T / Safe 3 / Safe 5	Small device with a screen, connects via USB-C	Trezor Model T and Safe 5 have color touchscreens. Others use buttons. Uses Trezor Suite companion software.
Coldcard Mk4 / Q (and older Mk3)	Calculator-like device with a numeric keypad and small screen	Designed for advanced users. Can operate fully air-gapped (no USB connection required). Uses a microSD card for transaction signing. No companion app required.
BitBox02	Small, minimalist USB-C device	Gestures on device for navigation. Uses BitBoxApp companion software.
Foundation Passport	Looks like a small handheld device with a camera and screen	Air-gapped (uses QR codes and microSD instead of USB). Open-source. Uses Envoy companion app.

Look for these devices in safes, lockboxes, desk drawers, filing cabinets, or any secure location the decedent used for valuables. They may be in their original packaging or stored in a tamper-evident bag.

Seed Phrase Backups

A seed phrase (also called a recovery phrase or mnemonic phrase) is a list of 12 or 24 ordinary English words in a specific order. This is the master backup for a hardware wallet. If the hardware wallet is lost, destroyed, or erased, the seed phrase is the only way to recover the funds.

Seed phrases may be stored on:

- **Paper** — handwritten or printed on a card, often in a sealed envelope or hidden location
- **Stamped or engraved metal plates** — products like Seedplate, Cryptosteel, Billfodl, or BlockPlate that store words on fire/water-resistant steel or titanium
- **Metal washers on a bolt** — a DIY method where words are stamped onto individual washers

A seed phrase might look like this (this is an example only, not a real phrase):

EXAMPLE SEED PHRASE (24 words)

abandon ability able about above absent absorb abstract absurd abuse access accident account accuse
achieve acid acoustic acquire across act action actor actress actual

The words will always be common English words drawn from a standardized list of 2,048 words (the BIP-39 word list). The ORDER of the words matters — scrambled words are useless.

Software Wallets

Software wallets are applications installed on a computer or smartphone. Common software wallets include Sparrow Wallet, Electrum, BlueWallet, and Bitcoin Core. They may appear as:

- A desktop application on the decedent's computer (check the applications folder or desktop shortcuts)
- A mobile app on their smartphone (look for Bitcoin-related app icons)
- A browser extension (less common for Bitcoin; more common for Ethereum-based assets)

Software wallets are typically protected by a password. The Bitcoin they control can also be recovered using the seed phrase, so the seed phrase backup is what matters most.

Exchange Accounts

Exchanges are online platforms where people buy, sell, and sometimes store cryptocurrency. Common exchanges include Coinbase, Kraken, Gemini, River, Swan Bitcoin, and Cash App. Unlike self-custody wallets, exchange accounts are held by a company — similar to a brokerage account.

Evidence of exchange accounts may include:

- Emails from the exchange (search the decedent's email for "Coinbase," "Kraken," "Gemini," "River," "Swan," "Cash App," etc.)
- A mobile app on their phone
- Bank or credit card statements showing transfers to/from an exchange
- Tax documents (Form 1099-MISC, 1099-B, or 1099-DA from an exchange)
- IRS Form 8949 or Schedule D on prior tax returns showing cryptocurrency transactions

Other Items to Look For

Depending on the decedent's level of involvement with Bitcoin, you may also encounter:

- **A Bitcoin node** — a small computer (often a Raspberry Pi in a case, or a dedicated device like Umbrel, Start9, or myNode) that runs the Bitcoin network software. Nodes verify transactions but do not typically store funds — with one exception: a Lightning node holds bitcoin in open payment channels, so do not power down a Lightning node or wipe its drive before consulting a technical advisor (abrupt shutdown can complicate channel recovery; see Document 7).
- **Mining equipment** — specialized hardware (ASIC miners like Antminer, Whatsminer, or Avalon) used to mine Bitcoin. These are loud, generate heat, and consume significant electricity. Mined Bitcoin may be deposited into a wallet or mining pool account.
- **YubiKeys or hardware security keys** — small USB devices used for two-factor authentication on exchange accounts. These are not wallets, but they may be required to log into exchange accounts.
- **microSD cards** — may contain wallet backup files, multisig configuration files, or partially signed Bitcoin transactions (PSBTs). Do not discard them.

CHAPTER 2

Securing the Assets

THE FIRST 48 HOURS

— CRITICAL: DO NOT MOVE ANYTHING

Your only job in the first 48 hours is to SECURE, not to TRANSFER. Do not attempt to move Bitcoin from one wallet to another. Do not attempt to “consolidate” holdings. Do not attempt to sell. Do not attempt to “test” a seed phrase by entering it into a website or app. Every one of these actions creates an opportunity for irreversible loss.

Immediate Actions

1. **Locate and physically secure all hardware wallets.** Place them in a locked safe, a locked drawer, or another secure location. Do not connect them to any computer or attempt to turn them on.
2. **Locate and secure all seed phrase backups.** If they are on paper, place them in a sealed envelope. If on metal plates, secure them alongside the hardware wallets. Do not photograph them. Do not transcribe them into a phone, computer, or any digital device.
3. **Secure the decedent’s phone and computer.** These may contain software wallets, authenticator apps (needed for exchange 2FA), and email access (needed for exchange password resets). Do not factory-reset these devices. Keep them charged.
4. **Locate the decedent’s Heir Letter and Custody Audit Checklist.** These documents, if they exist, will tell you exactly what the decedent owned and where everything is stored.
5. **Secure any microSD cards, USB drives, or YubiKeys found near the hardware wallet or in the decedent’s personal effects.**
6. **Document what you find.** Photograph the devices (exterior only — do not photograph seed phrases). Note the location where each item was found. This will be important for the estate inventory.

What NOT to Do in the First 48 Hours

- **Do not enter the seed phrase into any website, app, or device.** If anyone or any website asks you to “verify” or “validate” a seed phrase online, it is a scam.
- **Do not share the seed phrase with anyone** — not by text, email, phone, photo, or in person — unless that person is the designated Digital Executor or technical advisor identified in the decedent’s estate documents.
- **Do not attempt to guess a hardware wallet PIN.** Behavior on incorrect PIN entry varies by device — some erase after a small number of attempts, others impose exponentially increasing delays, and some (e.g., Coldcard) offer an opt-in self-destruct PIN. Refer to the decedent’s documentation and the manufacturer’s manual before attempting entry. If a self-destruct is ever triggered, the funds are not lost — they remain on the blockchain and can be recovered from the seed phrase backup on a new device.

- **Do not connect the hardware wallet to the internet** or install any software until you have consulted with a qualified technical advisor.
- **Do not discard any electronic device, cable, microSD card, or piece of paper with words on it without first consulting a technical advisor. What looks like a random list of words may be a seed phrase worth hundreds of thousands of dollars.**
- **Do not announce the existence of the Bitcoin holdings publicly.** Do not post on social media, do not discuss in group settings, and do not disclose to anyone who does not need to know.

Notify the Right People

Within the first few days, contact the following individuals (if the decedent has identified them):

- **The designated Digital Executor** — the person named in the Digital Asset Memorandum with authority to manage digital assets
- **The estate planning attorney** — who can advise on legal authority and probate requirements
- **The designated technical advisor** — a trusted individual with Bitcoin expertise who can assist with verification and transfer

If the decedent did not designate specific individuals, consult with the estate attorney about engaging a qualified cryptocurrency estate specialist.

CHAPTER 3

Verifying Holdings

Before any Bitcoin is moved, you need to confirm what the decedent actually owned. This verification can be done without moving funds and without exposing private keys. It is a read-only process.

Understanding Addresses and Balances

Every Bitcoin wallet has one or more public addresses — long strings of letters and numbers that function like an account number. These addresses are public information; anyone can look up the balance of any Bitcoin address. Having an address does not allow anyone to spend the Bitcoin. Only the private key (or seed phrase) allows spending.

A typical Bitcoin address looks like one of these:

Type	Example Format	Notes
Legacy (P2PKH)	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa	Starts with “1” — oldest format (this is Bitcoin’s historic genesis address — an example only, not your own)
Nested SegWit	3J98t1WpEZ73CNmQviecnyiWrnqRhWNLy	Starts with “3”
Native SegWit (Bech32)	bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq	Starts with “bc1q” — most common modern format
Taproot (Bech32m)	bc1p5cyxnuxmeuwuvkwfem96lqzszd02n6xdcjrs20cac6yqjjwudpxqkedrcr	Starts with “bc1p” — newest format

Using a Block Explorer

A block explorer is a free website that lets you look up any Bitcoin address and see its balance and transaction history. Think of it as a public ledger search engine. This is the safest way to verify holdings because it does not require access to private keys or any special software.

Recommended Block Explorers

Explorer	URL	Notes
Mempool.space	mempool.space	Open-source, privacy-focused. Widely used.
Blockstream Explorer	blockstream.info	Operated by Blockstream. Clean interface.

Explorer	URL	Notes
Blockchain.com Explorer	blockchain.com/explorer	Well-known but ad-heavy. Functional.

Step-by-Step: Looking Up a Balance

1. Open a web browser and navigate to **mempool.space** (or another block explorer listed above).
2. In the search bar, paste or type the Bitcoin address you want to look up.
3. Press Enter. The explorer will display the current balance and a complete transaction history for that address.
4. Record the balance. Note both the BTC amount and the approximate USD value (most explorers show both).
5. Repeat for each address listed in the decedent's Custody Audit Checklist or Heir Letter.

i IMPORTANT: One Wallet, Many Addresses

Modern Bitcoin wallets generate a new address for every transaction for privacy reasons. A single wallet may have dozens or hundreds of addresses. Looking up a single address may show only a fraction of the wallet's total balance. To see the complete balance, you typically need to open the wallet in its companion software (e.g., Ledger Live, Trezor Suite, Sparrow Wallet) using the hardware wallet device. The block explorer method works best when the decedent recorded specific xpub keys or total balances in their audit checklist.

Verifying Exchange Accounts

For assets held on exchanges (Coinbase, Kraken, etc.), verification requires logging into the account or contacting the exchange's estate/inheritance department.

1. **Identify which exchanges the decedent used.** Check their email for account confirmations, their Custody Audit Checklist, and their bank statements for transfers to exchanges.
2. **Contact the exchange's support team.** Most major exchanges have a dedicated estate or inheritance process. You will typically need: a certified death certificate, Letters Testamentary or Letters of Administration from the probate court, government-issued ID of the executor, and a completed estate claim form (provided by the exchange).
3. **Request an account statement.** This will list all assets held in the account as of a specific date.
4. **Do not attempt to log in using the decedent's credentials.** This may trigger security locks, 2FA challenges you cannot complete, or account freezes. Go through the official estate process.

Creating an Inventory

As you verify each holding, compile a comprehensive inventory:

Asset / Wallet	Location / Platform	Balance (BTC)	Value (USD)	Date Verified

This inventory will be needed for probate filings, tax reporting, and distribution to beneficiaries. The fair market value on the date of death is particularly important for stepped-up basis calculations (see Chapter 4).

CHAPTER 4

Transferring to Beneficiaries

This is the step where Bitcoin actually changes hands. It is the highest-risk phase of the process because Bitcoin transactions are irreversible. Once Bitcoin is sent, it cannot be recalled, reversed, or disputed. There is no “undo.”

⚠ BEFORE TRANSFERRING ANYTHING

Confirm that you have legal authority to act (Letters Testamentary, Letters of Administration, or trustee certification). Confirm that you have verified all holdings (Chapter 3). Confirm that you have consulted with a tax professional about the tax implications of the transfer. Confirm that you have the correct receiving address from the beneficiary.

When to Transfer

Do not transfer Bitcoin until all of the following conditions are met:

- You have legal authority to distribute estate assets
- All debts, taxes, and administrative expenses of the estate have been paid or reserved for
- You have verified the beneficiary’s identity and their designated receiving address
- The probate court has approved distribution (if required in your jurisdiction)
- You have consulted with both the estate attorney and a tax professional

How to Transfer Bitcoin from a Hardware Wallet

⚠ SEND A TEST TRANSACTION FIRST

For any large transfer, before sending the full amount: send a small test transaction first (e.g., \$25–\$100 worth of Bitcoin) using the same steps below. Wait for the test transaction to confirm. Have the beneficiary verify receipt in their own wallet. Only after the test transaction is confirmed and acknowledged should you initiate the full transfer. This is standard practice for any significant Bitcoin transfer and eliminates the risk of catastrophic address error.

This process should be performed with the assistance of the decedent’s designated technical advisor or a qualified cryptocurrency specialist. The general steps are:

1. **Connect the hardware wallet to a computer** with the appropriate companion software installed (Ledger Live, Trezor Suite, Sparrow Wallet, etc.).
2. **Enter the PIN to unlock the device.** Refer to the decedent’s documentation for the PIN. Do not guess.
3. **Open the companion software and verify the wallet’s balance.** The balance shown in the software should match your verified inventory from Chapter 3.
4. **Obtain the beneficiary’s receiving address. The beneficiary should generate this address from their own wallet and provide it to you directly (not through a third party). Verify the address through a second communication channel (e.g., if they text it, confirm by phone call). If a**

beneficiary is a minor, do not transfer Bitcoin directly to the minor; consult the estate attorney about transferring to a custodian under the Uniform Transfers to Minors Act, to a guardian of the minor's estate, or to a trust.

5. **Create the transaction in the companion software.** Enter the beneficiary's address and the amount to send. The software will calculate the network fee.
6. **Verify every detail on the hardware wallet's screen. The hardware wallet will display the receiving address and the amount. Confirm that the address on the device screen matches the address the beneficiary provided — every single character, from the first to the last, not just the first and last few. Address-poisoning malware can generate a look-alike address that matches the beginning and the end while differing in the middle, so checking only a few characters is not enough.**
7. **Approve the transaction on the hardware wallet. Once approved, the transaction will be broadcast to the Bitcoin network.**
8. **Record the transaction ID (TXID).** The companion software will display a transaction ID after broadcasting. Save this. You can use it to track the transaction on a block explorer.
9. **Wait for confirmations.** A Bitcoin transaction is considered final after 6 confirmations, which typically takes about 60 minutes. For large amounts, some practitioners wait for more confirmations.

How to Transfer from a Multisig Wallet

If any of the decedent's wallets used multisignature (multisig) — meaning two or more independent keys must sign each transaction — the transfer process differs from a single-key hardware wallet. Multisig wallets are commonly used for larger holdings and for collaborative custody services such as Casa, Unchained, and Nunchuk.

You will need: (1) the wallet's coordinator software configuration file (typically .bsms or .json — recorded in the decedent's Custody Audit Checklist §B.4), (2) the required number of key signers (e.g., 2 of 3), and (3) a copy of Sparrow Wallet or the original coordinator software (e.g., Caravan, Nunchuk).

The general workflow uses partially signed Bitcoin transactions (PSBTs): open the wallet in coordinator software using the configuration file, construct the transaction, then route the PSBT to each required signer in turn. Each signer adds their signature and returns the partially signed PSBT. Once the threshold is met, the fully signed transaction is broadcast.

This process is significantly more complex than a single-key transfer and should be performed only with the assistance of the decedent's designated technical advisor or a qualified collaborative-custody specialist. Do not attempt a multisig recovery without the configuration file; without it, the wallet cannot be reconstructed even if all key seeds are available.

How to Transfer from an Exchange

If the decedent held Bitcoin on an exchange, the exchange's estate process will typically handle the transfer. Once the exchange has verified your authority and identity, they will either:

- Transfer the assets to a wallet address you designate, or

- Liquidate the assets and send the proceeds via wire transfer or check to the estate account
- Follow the exchange's specific instructions. Each exchange has its own timeline and requirements.

Tax Reporting

Every transfer or sale of Bitcoin triggers potential tax obligations. Key reporting requirements:

Form / Concept	What It Covers
Stepped-Up Basis (IRC § 1014)	The beneficiary's cost basis is the fair market value on the date of death, not the decedent's original purchase price. This can eliminate years of unrealized capital gains.
IRS Form 8949	Reports individual sales or dispositions of capital assets, including cryptocurrency. Required whenever Bitcoin is sold, exchanged, or otherwise disposed of.
Schedule D (Form 1040)	Summarizes capital gains and losses from Form 8949. Attached to the individual's annual tax return.
Estate Tax Return (Form 706)	Required if the total estate exceeds the federal estate tax exemption (approximately \$15 million per individual in 2026, indexed for inflation, following the One Big Beautiful Bill Act of 2025 which made the elevated exemption permanent — verify current threshold with a tax professional). Bitcoin holdings are included in the gross estate at fair market value on date of death.
California Considerations	California does not impose a separate inheritance or estate tax. However, capital gains from a subsequent sale of inherited Bitcoin are subject to California state income tax.

Consult a CPA or tax attorney with cryptocurrency experience before selling any inherited Bitcoin. The Tax Summary for Heirs document in this kit provides additional detail.

CHAPTER 5

If Something Goes Wrong

Despite best efforts, executors sometimes encounter problems. This chapter covers the most common issues and the appropriate response to each.

Lost or Missing Seed Phrase

If the hardware wallet is available but the seed phrase backup cannot be found:

- The funds are still accessible through the hardware wallet device itself, as long as you have the PIN.
- Once you have legal authority to act, and with the assistance of a technical advisor, generate a new wallet and write down and verify its seed phrase before sending anything to it; only then transfer the funds, following the Chapter 4 transfer safeguards (test transaction first; verify the full receiving address). Before transferring, confirm you have checked every address type on the original wallet (see “Restored Wallet Shows a Zero Balance,” below) so that funds at other derivation paths are not left behind.
- If the hardware wallet is also missing or damaged and the seed phrase cannot be found, the funds may be permanently inaccessible. Consult a cryptocurrency recovery specialist (see below), but be realistic about the odds and extremely cautious about scams.

Forgotten or Unknown PIN

If you do not know the hardware wallet PIN:

- Check the decedent’s Heir Letter, Digital Asset Memorandum, or Custody Audit Checklist for the PIN or its location.
- Check for a sealed envelope, a note in a safe, or other secure location where the decedent may have recorded it.
- **Do not guess. Hardware wallets respond differently to incorrect PIN entry — some erase, some delay exponentially, some have opt-in self-destruct configurations. Without documentation of the exact device and configuration, even a single guess can be destructive. Stop and consult a technical advisor.**
- If the seed phrase backup exists, you can restore the wallet onto a new device without needing the PIN. The seed phrase supersedes the PIN.

Damaged Hardware Wallet

If the hardware wallet is physically damaged (water, fire, impact):

- Do not attempt to power it on. Damaged electronics can behave unpredictably.
- If the seed phrase backup exists, purchase a new hardware wallet of the same make/model (or any BIP-39 compatible device) and restore from the seed phrase. The funds are on the blockchain, not on the device.
- If no seed phrase backup exists, consult a data recovery specialist who works with cryptocurrency hardware. This is a niche field — verify credentials carefully.

Restored Wallet Shows a Zero Balance

If you restore a seed phrase into a new wallet and it shows a zero balance, do not panic and do not assume the funds are lost or the backup is wrong. The most common cause is a mismatch in the derivation path or address type between the original wallet and the software you are restoring into. Bitcoin wallets can use several address types — legacy (addresses beginning with 1, derivation path m/44'), nested SegWit (beginning with 3, m/49'), native SegWit (beginning with bc1q, m/84'), and Taproot (beginning with bc1p, m/86'). If the restoring wallet defaults to a different type than the original used, it derives different addresses and shows no balance, even though the funds are safe on the blockchain.

What to do: restore into wallet software that lets you choose or scan multiple derivation paths (Sparrow Wallet is recommended) and check each script type (m/44', m/49', m/84', m/86'); also try incrementing the account index (account 0, then 1, then 2). Better still, if the decedent recorded the wallet's output descriptor (see the Custody Audit Checklist), recover using that descriptor — it encodes the exact script type and derivation path and removes the guesswork. Only conclude that funds are missing after a knowledgeable advisor has checked every standard derivation path. Never discard the seed phrase backup because a single restore attempt showed zero.

Transaction Sent to Wrong Address

If Bitcoin is sent to an incorrect address:

- **There is no way to reverse a Bitcoin transaction.** Once confirmed on the blockchain, it is final.
- If the address belongs to someone you can identify (e.g., an exchange or known individual), you can contact them and request a return. They are under no obligation to comply, but some may cooperate.
- If the address is unknown, the funds are effectively lost. This is why address verification (Step 6 in Chapter 4) is critical.

Scam Awareness

The period following a death is when beneficiaries and executors are most vulnerable to scams. Be aware of the following:

COMMON SCAM PATTERNS

- “Recovery experts” who contact you first and promise to recover lost Bitcoin for an upfront fee — they will take your fee and disappear
- Fake wallet software or phishing websites that look like legitimate wallet apps but steal your seed phrase when you enter it
- Social media impersonators posing as Coinbase/Ledger/Trezor support offering to “help” with estate access
- People claiming the decedent owed them Bitcoin and demanding immediate payment
- Emails claiming to be from an exchange, asking you to “verify your identity” by clicking a link
- “Crypto inheritance consultants” with no verifiable credentials or bar membership

How to Protect Yourself

- Never share seed phrases with anyone who contacts you first.

- Verify the identity of anyone who claims to be a professional. Check bar memberships, business registrations, and online reviews.
- Use only official websites. Type URLs directly into your browser — do not click links in emails.
- Be skeptical of urgency. No legitimate process requires immediate action.
- Consult the estate attorney before paying anyone for cryptocurrency-related services.

Legitimate Resources

If you need professional help beyond what this guide provides:

Resource	Description
Estate planning attorney	Your first call. They coordinate the legal process and can refer you to qualified technical professionals.
Bitcoin-literate CPA or tax attorney	Essential before selling any inherited Bitcoin. Look for practitioners who specifically list cryptocurrency on their website.
Hardware wallet manufacturer support	Ledger, Trezor, Coldcard, and Foundation all have official support channels. Use only the manufacturer's official website (not links from emails or search ads).
Asaf Fulks Law	asaffulkslaw.com — Bitcoin estate planning consultations from an attorney who mines Bitcoin, runs a full node, and understands self-custody at the protocol level.

Need Help as an Executor Handling Digital Assets?

Asaf Fulks Law provides executor guidance for Bitcoin and digital asset estates.

One-on-one consultations with an attorney who understands self-custody.

asaffulkslaw.com • asaf@asaffulkslaw.com