

BITCOIN & DIGITAL ASSET ESTATE PLANNING

INTRODUCTION TO BITCOIN & SELF- CUSTODY

*What Bitcoin is, how self-custody works, and why
it creates an estate planning problem you need to solve*

Prepared by

Asaf David Fulks, Esq.

California State Bar #343622

asaffulkslaw.com

Document 0 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 guide is designed to provide a foundational understanding of Bitcoin, self-custody, and the estate planning challenges they create. It is not a substitute for professional legal counsel, and the author assumes no liability for actions taken based on information contained herein.

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

WHAT BITCOIN ACTUALLY IS

If someone told you Bitcoin is “digital money,” they gave you a shortcut that skips everything important. Bitcoin is better understood as a set of rules, enforced by software, running on a global network of computers that no single person or organization controls. Those rules govern the creation, transfer, and verification of units called bitcoin (lowercase when referring to the currency, uppercase when referring to the network and protocol).

Here is the essential version, stripped of jargon.

The Ledger

At its core, Bitcoin is a ledger — a record of who sent what to whom, and when. You have seen ledgers before: your bank statement is a ledger, a checkbook register is a ledger, a spreadsheet tracking who owes whom at the end of a poker night is a ledger. Bitcoin’s ledger is called the **blockchain**, and it is simply a list of transactions grouped into blocks, with each block linked to the one before it in an unbroken chain going back to January 3, 2009.

What makes this ledger different from every other ledger in history is that no one owns it, no one can edit it after the fact, and anyone on Earth can verify every entry in it. Your bank controls your bank statement and can modify, freeze, or close your account. No one can do that with Bitcoin. The ledger is maintained by thousands of independent computers (called nodes) running the same software, each holding a complete copy. If any single copy is tampered with, the rest of the network rejects it.

The Supply

There will only ever be 21 million bitcoin. This is not a policy decision that a board of directors might revisit — it is a rule written into the software itself, enforced by every node on the network. New bitcoin are created through a process called mining (covered in detail in Document 7 of this kit), and the rate of creation is cut in half approximately every four years in an event called the “halving.” As of 2026, over 20 million bitcoin have already been mined — more than 95% of the 21 million that will ever exist. The last fraction of a bitcoin will be mined around the year 2140.

This fixed supply is one of the properties that distinguishes Bitcoin from government-issued currencies. The U.S. dollar, the euro, the yen — every fiat currency in history has been subject to expansion by the institution that controls it. Bitcoin cannot be expanded. The rules do not allow it, and changing the rules would require

convincing the overwhelming majority of the network's participants to adopt new software — software that would devalue their own holdings. It has never happened. It is designed not to.

Units and Denominations

One bitcoin can be divided into 100 million smaller units called **satoshis** (or “sats”). A satoshi is to bitcoin what a cent is to a dollar, except the divisibility is far greater. You do not need to buy a whole bitcoin. You can own 50,000 satoshis, or 10 million, or any amount in between. When you see someone say they “stacked sats,” they mean they acquired some quantity of satoshis.

How Transactions Work

When you send bitcoin to someone, you are broadcasting a message to the network that says, in effect: “I am authorizing the transfer of X bitcoin from this address to that address.” That message is signed with your private key — a secret cryptographic code that proves you control the funds. The network verifies the signature, confirms that you have sufficient balance, and records the transaction in the next block. Once confirmed, the transaction is effectively permanent. There is no chargeback, no reversal, and no customer service department.

This is the double-edged nature of Bitcoin that runs through every document in this kit: the same properties that make it resistant to seizure, censorship, and inflation also make it unforgiving of mistakes. If you send bitcoin to the wrong address, it is gone. If you lose your private keys, your bitcoin is inaccessible — permanently. No one can help you recover it, because no one else has the authority to move it.

WHY BITCOIN MATTERS AS A STORE OF VALUE

You do not need to be a “believer” to understand why Bitcoin has value. You need to understand what properties a good store of value requires, and then evaluate Bitcoin against those properties honestly.

The Properties of Sound Money

Economists and historians have identified several characteristics that make something useful as money: it must be durable (it does not rot or break), portable (you can carry it), divisible (you can split it into smaller pieces), fungible (one unit is interchangeable with another), scarce (it cannot be created at will), and verifiable (you can confirm it is genuine). Gold meets most of these criteria, which is why it served as money for thousands of years. Paper currency meets some, but fails on scarcity — governments can and do print more of it.

Bitcoin meets all of them. It is durable (it exists as data, not a physical object that degrades). It is portable (you can send any amount anywhere in the world in minutes). It is divisible to eight decimal places. It is fungible at the protocol level. It is scarce by design — the 21 million cap is absolute. And it is verifiable by anyone running a node, which can independently confirm every transaction in Bitcoin’s history.

What Bitcoin Is Not

Bitcoin is not a company. It has no CEO, no board of directors, no earnings reports, and no office. It is not a stock, a bond, or a derivative. It is not “backed” by anything in the way a dollar was once backed by gold — but neither is any modern fiat currency. The dollar is backed by the U.S. government’s ability to tax and its willingness to enforce legal tender laws. Bitcoin is backed by mathematics, energy expenditure, and the collective agreement of its network participants to follow the rules.

Bitcoin is also not “crypto” in the way that term has been used to market thousands of other digital tokens. The vast majority of those tokens are securities, collectibles, or outright scams with no meaningful decentralization, no fixed supply, and no track record. This kit addresses Bitcoin specifically. If you hold other digital assets, some of the custody principles may overlap, but the investment thesis and technical architecture are fundamentally different.

The Volatility Question

If you are new to Bitcoin, the first thing you probably noticed is that its price moves — a lot. This volatility is real, and it is worth understanding in context. Bitcoin is a young asset, in its second decade as of 2026, undergoing a process of global price discovery. Its volatility has decreased over each successive market cycle. Early-stage assets in the process of being monetized are inherently volatile; gold was volatile for decades after the collapse of Bretton Woods.

The relevant question for estate planning is not whether Bitcoin’s price will fluctuate tomorrow. It is whether the asset will exist and retain meaningful value over a multi-decade horizon. Bitcoin has survived multiple 80%+ drawdowns, regulatory crackdowns in major economies, the collapse of major exchanges, and relentless media obituaries. It continues to operate exactly as designed, producing a new block approximately every ten minutes, every single day since January 2009.

SELF-CUSTODY: THE ENTIRE POINT

This is the section that explains why this entire kit exists.

When you buy bitcoin through an exchange like Coinbase, Kraken, or River, the exchange holds your bitcoin for you — much like a bank holds your dollars. You have an account. You can log in, see a balance, and request a withdrawal. But while the bitcoin sits on the exchange, the exchange controls the private keys. You are trusting them not to get hacked, not to freeze your account, not to go bankrupt, and not to lose your funds through mismanagement. You are trusting a third party with a bearer asset.

The entire history of Bitcoin is littered with cautionary examples. Mt. Gox, once the world's largest exchange, lost 850,000 bitcoin in 2014. FTX collapsed in 2022, and billions in customer funds evaporated. QuadrigaCX's founder died with the only keys to the exchange's cold storage, leaving roughly \$190 million (CAD) inaccessible. These are not edge cases — they are the predictable consequences of trusting third parties with bearer assets.

What Self-Custody Means

Self-custody means you hold your own private keys. No exchange, no custodian, no third party stands between you and your bitcoin. You — and only you — can authorize transactions. This is the model Bitcoin was designed for. The white paper's opening line describes "a purely peer-to-peer version of electronic cash" that "would allow online payments to be sent directly from one party to another without going through a financial institution."

In practice, self-custody means your bitcoin is controlled by a **seed phrase** — a set of 12 or 24 words, generated by your wallet software or hardware device, that encodes your private keys. That seed phrase is your bitcoin. Not the hardware wallet, not the software, not the device — the words. If you have the words, you can recover your bitcoin on any compatible device, anywhere in the world. If you lose the words and have no other backup, your bitcoin is gone.

⚠ WHY THIS MATTERS FOR ESTATE PLANNING

Self-custody is the reason this kit exists. If your bitcoin is on an exchange, your executor can contact customer support, provide a death certificate, and work through the exchange's inheritance process. It is slow and frustrating, but it is possible. If your bitcoin is in self-custody, there is no customer support to call. Your executor needs the seed phrase, the passphrase (if one was set), and the knowledge of how to use them. Without those three things, your bitcoin dies with you.

Every other document in this kit — the Custody Audit Checklist, the Heir Letter, the Digital Asset Memorandum, the Executor Technical Guide, the Tax Summary, the Shamir's Secret Sharing Guide, and the Node & Mining Guide — exists to solve this problem. This introductory document explains why the problem exists. The rest of the kit shows you how to solve it.

A THIRD CATEGORY: SPOT ETFs, IRAs, AND BROKERAGE BITCOIN

This kit focuses on the two custody models that create the hardest inheritance problems: self-custody (you hold the keys) and exchange or custodial accounts (a company holds the keys for you). But there is a growing third category your estate plan should account for: Bitcoin held through a regulated financial account rather than as the coin itself. This includes spot Bitcoin exchange-traded funds (ETFs) such as IBIT or FBTC, Bitcoin held inside an IRA or other retirement account, and Bitcoin held through an ordinary taxable brokerage account (typically as ETF or fund shares).

These holdings behave like traditional securities, not like keys on a metal plate — there is no seed phrase to secure. Instead, they commonly pass by a beneficiary or transfer-on-death (TOD) designation recorded with the brokerage or IRA custodian (where one is in place), which means they can bypass probate and the instructions in your will, trust, or Digital Asset Memorandum. The same is true of any account held in joint tenancy with right of survivorship, which passes automatically to the surviving co-owner. They also follow different tax rules (see the Tax Summary for Heirs — for example, Bitcoin in a traditional IRA does not receive a stepped-up basis). If you hold Bitcoin this way, keep your beneficiary designations current and consistent with the rest of your estate plan, and list these accounts in your Custody Audit Checklist.

HARDWARE WALLETS

If the seed phrase is your bitcoin, the hardware wallet is the device that generates, stores, and uses it securely. A hardware wallet is a small, purpose-built electronic device — roughly the size of a USB drive or a small calculator — designed to keep your private keys offline and sign transactions without ever exposing those keys to a computer or the internet.

What a Hardware Wallet Does

Your computer or phone is connected to the internet, which means it is exposed to malware, phishing, keyloggers, and every other attack vector that exists in the digital world. A hardware wallet solves this by keeping your private keys on a secure chip inside the device. When you want to send bitcoin, your wallet software creates the transaction on your computer, sends it to the hardware wallet for signing, the hardware wallet signs it using the private key stored on its chip, and then returns the signed transaction to your computer for broadcast. At no point does the private key leave the device.

Think of it like signing a check inside a locked vault. The check comes in through a slot, you sign it, and the signed check comes back out. But no one ever enters the vault, and the pen never leaves it.

Major Hardware Wallet Brands

As of 2026, the most widely used hardware wallets include:

Trezor was one of the first hardware wallets on the market. The Trezor Model One and Model T have been widely used for years. The company recently released the Trezor Safe series. Trezor devices run open-source firmware, which means the code is publicly auditable. They connect via USB and are managed through the Trezor Suite desktop application.

Ledger makes the Nano S Plus, Nano X, and the touchscreen Ledger Stax and Flex. Ledger devices use a secure element chip (the same type of chip used in credit cards and passports). Their firmware is not fully open-source, which is a point of contention in the Bitcoin community, but the devices have a strong track record. They connect via USB or Bluetooth and are managed through Ledger Live.

Coldcard is built specifically for Bitcoin (it does not support other cryptocurrencies). It is popular among users who prioritize security and Bitcoin-only simplicity. Coldcard supports air-gapped operation — meaning it can sign transactions without ever being physically connected to a computer, using a microSD card to transfer data. The Coldcard Mk4 and the newer Q model with a QWERTY keyboard are the current options.

BitBox02 by Shift Crypto offers a Bitcoin-only edition with a minimalist design and open-source firmware. It connects via USB-C and is managed through the BitBoxApp.

Foundation Passport is another Bitcoin-only, open-source hardware wallet with an air-gapped design. It uses a camera and QR codes for transaction signing instead of USB or Bluetooth.

Any of these devices will serve the purpose of securing your bitcoin. The choice between them is a matter of personal preference regarding open-source philosophy, connectivity method, and user interface. What matters for estate planning is that your heirs know which device you use, where it is stored, and — most importantly — where the seed phrase backup is located. The hardware wallet can fail, break, or be lost. The seed phrase is what matters.

SEED PHRASES: 24 WORDS THAT CONTROL EVERYTHING

When you initialize a hardware wallet for the first time, it generates a seed phrase — typically 24 words selected from a standardized list of 2,048 English words (defined by a standard called BIP-39). These 24 words, in the exact order they are given to you, encode the master private key from which all of your Bitcoin addresses are derived.

This is worth restating, because it is the single most important concept in this entire kit:

THE SEED PHRASE IS YOUR BITCOIN.

Whoever has these 24 words, in order, controls the bitcoin. Not the hardware wallet. Not the PIN. Not the software. The words. If your house burns down and your hardware wallet melts, but you have the seed phrase written on a steel plate in a safe deposit box, you can buy a new hardware wallet, enter the 24 words, and your bitcoin will appear. If someone finds your seed phrase and enters it into their own wallet, they can take every satoshi — and you will have no recourse.

Passphrases (The 25th Word)

Many hardware wallets support an optional **passphrase** — sometimes called the “25th word.” This is a user-chosen word or phrase that, when combined with the 24-word seed phrase, creates an entirely separate set of wallets. The same 24 words with a different passphrase produce completely different addresses and balances. This is a powerful security feature: even if someone steals your seed phrase, they cannot access your bitcoin without the passphrase.

It is also a powerful way to lose your bitcoin permanently. If you set a passphrase and forget it, or if you die and your heirs do not know it exists, the bitcoin is gone. There is no recovery mechanism. The passphrase is not stored on the hardware wallet and cannot be retrieved from it. If you use a passphrase, it must be documented separately and securely, and your heirs must know that it exists and where to find it. The Custody Audit Checklist (Document 1) asks about this explicitly.

Backup Methods

Your seed phrase must be backed up on a medium that will survive fire, flood, and time. The most common approaches include:

Paper: The simplest method. Write the words on the card that came with your hardware wallet and store it in a secure location. Paper is vulnerable to fire and water damage, so this is best used as a secondary backup or stored inside a fireproof container.

Steel or metal plates: Products like Cryptosteel, Billfodl, and Seedplate allow you to stamp, engrave, or assemble your seed phrase on a stainless steel plate that can survive a house fire. This is the most robust primary backup method for most holders.

Shamir’s Secret Sharing: An advanced method that splits your seed phrase into multiple shares, requiring a threshold number of shares to reconstruct the original. For example, you might create five shares and require any three to recover the seed phrase. This allows you to distribute shares geographically without any single share being sufficient to access your funds. Document 6 of this kit covers Shamir’s Secret Sharing in detail.

What you should **never** do with a seed phrase: photograph it, type it into a computer, email it, store it in cloud storage, save it in a password manager connected to the internet, or say it out loud near a device with a microphone. The seed phrase must remain offline and physical at all times.

BASIC TOOLS EVERYONE SHOULD KNOW

You do not need to be a software engineer to use Bitcoin effectively. But there are a few tools and concepts that every holder should understand.

Wallet Software

Your hardware wallet connects to wallet software on your computer or phone. This software communicates with the Bitcoin network, displays your balance, constructs transactions for signing, and broadcasts signed transactions. Common options include:

Sparrow Wallet is a desktop-only Bitcoin wallet widely regarded as the most capable option for self-custody users. It supports all major hardware wallets, multisig setups, coin control, and connects to your own node. It is open-source and Bitcoin-only. If you are serious about self-custody, Sparrow is the standard choice.

Electrum is one of the oldest Bitcoin wallets, available on desktop and Android. It is lightweight, feature-rich, and open-source. It supports hardware wallets and can connect to your own Electrum server for privacy.

BlueWallet is a mobile wallet for iOS and Android that supports both on-chain Bitcoin and Lightning Network transactions. It can be paired with a hardware wallet for watch-only functionality.

Manufacturer software includes Trezor Suite, Ledger Live, and similar applications made by hardware wallet companies. These work well for basic operations but may lack the advanced features available in independent wallets like Sparrow.

Block Explorers

A block explorer is a website or application that lets you look up any Bitcoin transaction, address, or block on the blockchain. It is the Bitcoin equivalent of looking up a transaction on your bank's website — except anyone can look up anything, because the blockchain is public.

Common block explorers include mempool.space (a popular open-source option — it provides fee estimates and shows the current state of the mempool), blockstream.info, and various others. You enter a Bitcoin address or transaction ID, and the explorer shows you the history: every transaction associated with that address, the amounts, the fees, and the confirmation status.

Block explorers are useful for verifying that a transaction has been confirmed, checking the balance of an address, and understanding transaction fees. They are also useful for your executor: if they have your Bitcoin addresses (from your Custody Audit Checklist), they can verify balances without needing access to your hardware wallet.

Understanding Fees

Every Bitcoin transaction requires a fee paid to miners (the computers that process and confirm transactions). Fees are not based on the amount being sent — a \$10 transaction and a \$10 million transaction can cost the same fee. Instead, fees are based on the size of the transaction in bytes and the current demand for block space. When the network is busy, fees rise because users compete to have their transactions included in the next block. When the network is quiet, fees drop.

Tools like mempool.space show the current fee environment and recommend appropriate fee rates. Your wallet software will typically suggest a fee based on how quickly you want the transaction confirmed. For

estate planning purposes, what matters is that your heirs understand that fees exist and vary, and that they should not panic if a transaction is not confirmed immediately — it will be, once the fee is sufficient or the network congestion clears.

WHY STANDARD ESTATE PLANS MISS BITCOIN

Most estate planning attorneys are competent professionals who understand wills, trusts, and probate. They can structure an estate to minimize tax liability, avoid probate, and ensure your wishes are carried out. But the overwhelming majority of them have never held a hardware wallet, never seen a seed phrase, and do not understand why Bitcoin requires an entirely different approach.

Why Traditional Plans Fail

A traditional estate plan assumes that your assets are held by institutions. Your bank knows your account balance. Your brokerage holds your stocks. Your insurance company has your policy on file. When you die, your executor contacts those institutions, provides a death certificate, and begins the transfer process. The institutions cooperate because they are legally required to, and because the assets are under their control.

Bitcoin in self-custody does not work this way. There is no institution to contact. There is no death certificate process. There is no court order that can compel a blockchain to release funds. If your executor does not have the seed phrase, the passphrase, and the knowledge of how to use them, the bitcoin is permanently lost. Your will can say “I leave my Bitcoin to my daughter” — and that statement will be legally valid and utterly useless if she cannot access it.

What Must Be Planned For

A complete Bitcoin estate plan must address every link in the chain between your death and your heirs' access to the funds. Your heirs need to know that Bitcoin exists in your estate in the first place — it is not automatically discovered like a bank account or a house with a title. They need to know how much you hold and where it is held: which wallets, which devices, which exchanges, which locations. They need the seed phrase for every self-custody wallet, stored securely. They need the passphrase, if one is set. They need to know what a hardware wallet is, how to use it, and what software to install. They need clear instructions written in plain language, not in technical jargon. And they need someone — you, through your documents, or an attorney who understands this technology — to guide them through the process.

This is exactly what the Bitcoin Inheritance Kit is designed to provide.

The Kit at a Glance

This kit contains eight documents, each serving a specific function:

Document 0 (this document): Introduction to Bitcoin and self-custody for anyone who needs foundational understanding.

Document 1 — Custody Audit Checklist: A systematic inventory of every wallet, exchange account, seed phrase location, and single point of failure in your custody setup.

Document 2 — Heir Letter Template: A plain-English letter to your loved ones explaining what you own and how to access it.

Document 3 — Digital Asset Memorandum: A confidential legal instrument that supplements your will or trust with digital asset specifics, kept separate to avoid public disclosure.

Document 4 — Executor Technical Guide: Step-by-step instructions for a non-technical executor tasked with securing and distributing Bitcoin.

Document 5 — Tax Summary for Heirs: What your heirs need to know about cost basis, stepped-up basis, and reporting obligations.

Document 6 — Shamir's Secret Sharing Guide: How to split your seed phrase into multiple shares for geographic distribution and redundancy.

Document 7 — Running Your Own Node & Mining Bitcoin: For holders who want full sovereignty, plus how mining and node infrastructure fit into estate planning.

A Note from the Author

I wrote this kit because I live in this space. I am a California-licensed attorney, a solo Bitcoin miner running an Avalon Q ASIC on solar power, a full node operator, and a computer science graduate with more than twenty years in the technology industry. I hold my own keys. I run my own node. I verify my own transactions. And I have seen firsthand how many otherwise well-prepared people have no plan for what happens to their bitcoin when they die.

This is not a theoretical problem. It is an urgent, practical one — and the tools to solve it are in your hands. Start with the Custody Audit Checklist. Fill it out completely and honestly. Then work through the rest of the kit. The time you invest now is the difference between your heirs inheriting your bitcoin and your bitcoin joining the millions of coins already lost forever.

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

Need Help Planning Your Bitcoin Inheritance?

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

asaffulkslaw.com • asaf@asaffulkslaw.com