The Sovereignty Paradox: Managing a Bitcoin Legacy

Matt McClintock
matt@bespokegroup.io
www.bespokegroup.io

Abstract. Bitcoin is a peer-to-peer electronic cash system.[1] It is a reliable, efficient, private, disintermediated medium of exchange for users on the Bitcoin network. Bitcoin's programmatic supply decay rate–the function within the Bitcoin software that halves the rate of issuance of new bitcoins[2] on the network every 210,000 blocks–roughly every four years–makes bitcoin an unparalleled store of value against traditional forms of unbacked "fiat" currencies. Those who have accumulated bitcoins at scale must adapt the method by which they control the ownership and movement of their bitcoins to account for the fact that the value of bitcoin likely goes up forever in fiat currency terms. A blend of key mechanisms is necessary to strategically manage bitcoin across its various uses. Low friction, unilateral, and otherwise tax-neutral controls are acceptable for "transactional" bitcoins intended to be spent. Higher friction, tax-optimized, legally-protected controls are necessary to preserve and transmit generational wealth.

Many Bitcoiners bristle at the prospect of surrendering unilateral, "sovereign" control over their bitcoin. They confuse the principle of disintermediated confirmation of transactions with the idea that sovereignty begins and ends with the ability to directly control peer-to-peer transactions. This mindset is trapped in 2009. It is held hostage by the idea that bitcoin is no more than a medium of exchange.

Bitcoin has established its superiority as a generational store of value. The concept of sovereignty must mature beyond unilateral control of cryptographic private keys to an upgraded, more complete form of sovereignty. Upgraded sovereignty contemplates using resilient, legally-recognized ownership regimes, and exploiting opportunities in favorable jurisdictions to achieve tax efficiency, asset protection, robust privacy, and inheritance preservation.

As bitcoin's value increases it's increasingly important for bitcoin owners to graduate to higher levels of structured key security for larger balances–especially to the extent the Bitcoiner seeks meaningful benefits under the law. We will address various forms of managing bitcoin's economic value and propose a rubric to apply based on the value of an owner's bitcoins, the owner's intended transaction velocity, and more sophisticated objectives including tax mitigation, asset protection, privacy, and structured wealth transfer.

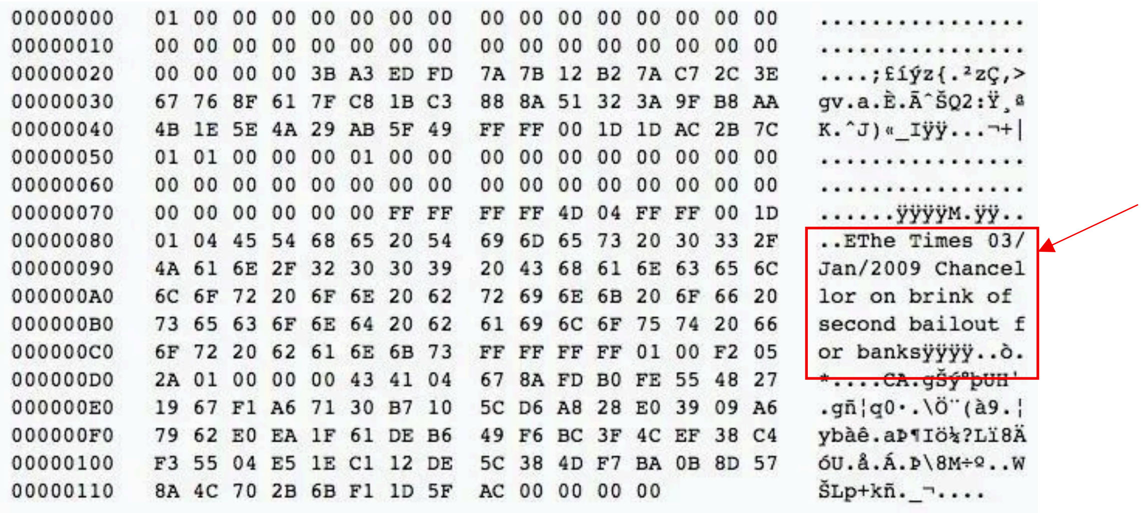
An evolved approach to key management is not contrary to bitcoin's value as a peer-to-peer medium of exchange. Rather, it's a recognition that bitcoin's superior design as a form of money gives it a tendency to rise indefinitely in terms of fiat currencies and as such, warrants thoughtful treatment and structure in societies governed by laws. Bitcoin remains a reliable medium of exchange for value in transactions over the internet and otherwise among users. But it also serves as an unmatched store of value as demand increases and as fiat debasement persists; "sats"[3] go farther than they ever did before. So long as bitcoin is subject to the tax laws of various nations and until those who inherit large sums of value in wealth can reliably manage that wealth without risk of mismanagement or other permanent loss, holders of significant wealth in bitcoin must evolve their thinking when it comes to managing their holdings. This paper seeks to examine a refined ownership framework for individuals with large bitcoin holdings.

Introduction

In October 2008, an author named Satoshi Nakamoto[4] published the Bitcoin whitepaper announcing a new methodology for a peer-to-peer electronic transaction network. Satoshi specifically sought to establish a system to facilitate commerce on the internet that did not require financial institutions to process or validate payments.[5] His solution relies on cryptographically-signed transactions which are compiled into sequential blocks of data. Each block of data is "hashed," giving each block of data a unique digital fingerprint. The block is timestamped by publishing the digital fingerprint (the hash) to a network of independent nodes–computers running the Bitcoin network software. Each block includes the previous block's timestamp in its own digital fingerprint, creating an ever-lengthening chain of connected blocks of data. Hence, the "block chain." Satoshi's solution has proven wildly successful, running without interruption and without a significant fault since January 3, 2009.

Although the Bitcoin network was established as a P2P electronic "cash" system–an intended *medium of exchange* in a trustless, distributed environment–there were clues from the beginning that Satoshi intended it to be something more. Because a blockchain is a database, it is possible to encode messages or data other than monetary transactions within the data blocks. In the first block mined and hard-coded into the Bitcoin network, Satoshi included the following message:

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks[6]"



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

Why *this* message? Was it coincidental that this was the title of the cover story in *The Times*[7] on the date Satoshi mined the genesis block? Was it a way to externally validate the date of the block by reference to an independent publication, like a hostage holding a newspaper in a proof-of-life photo? Unlikely, as the transaction's time and date were already embedded into the blockchain with the first block. More likely, Satoshi was signaling his intent to establish an entirely new monetary network: one that did not rely on–and could not be manipulated by–financial institutions or central governments.

Bitcoin's Monetary Policy

Satoshi programmed bitcoin such that the rate at which coins are generated on the network decreases over time. In its earliest days, computers that successfully combined and processed transactions and published hashed blocks to the network (Bitcoin's "mining" process) were awarded 50 bitcoins as compensation for contributing compute power to the network. By its design, a block is generated on the Bitcoin blockchain approximately every 10 minutes which on average, translates to roughly 144 blocks per day. At 50 bitcoins per block, the daily bitcoin issuance rate during Bitcoin's earliest years was 7,200 bitcoins each day.

In Bitcoin version 0.01ALPHA, Satoshi programmatically capped the total number of bitcoins that will ever be issued by the network at 21,000,000 coins. Further, he established a decaying rate of issuance by which the daily supply rate would be cut in half every 210,000 blocks–roughly every four years.[8] In doing so, Satoshi encoded increasing scarcity into Bitcoin's monetary supply rate, making bitcoin a form of money that gets harder–increasingly resistant to debasement, manipulation, or inflation–over time.

On November 28, 2012, when the blockchain reached block 210,001, Bitcoin's block reward was halved for the first time. The block reward was reduced from 50 bitcoins to 25 bitcoins, cutting the average daily issuance rate to 3,600 BTC. 210,000 blocks later on July 9, 2016, the block reward halved again to 12.5 bitcoins per block. This reduced average daily issuance rate to 1,800 BTC. On May 11, 2020, it halved again to 6.25 bitcoins per block. The average daily supply rate was cut to 900 BTC.

The current halving epoch began on April 19, 2024, issuing 3.125 BTC per block. This established the current daily issuance rate of 450 BTC per day. Bitcoin's decaying supply rate is illustrated in the following table:

Epoch	**Date Range**	**Block Reward**	**Daily Supply (144 blocks/day)**
Genesis	Jan 3, 2009 – Nov 28, 2012	50 BTC	7,200
1st Halving	Nov 28, 2012 – July 9, 2016	25 BTC	3,600
2d Halving	July 9, 2016 – May 11, 2020	12.5 BTC	1,800
3d Halving	May 11, 2020 – Apr 20, 2024	6.25 BTC	900
4th Halving	**Apr 20, 2024 – ~ 2028**	**3.125 BTC**	**450**
5th Halving (est.)	~ 2028	1.5625 BTC	225

This halving mechanism makes bitcoin inherently disinflationary: as the cumulative number of bitcoins in circulation grows, the rate of new issuance decreases programmatically. By design, bitcoin becomes increasingly scarce as the blockchain grows. To the extent demand for bitcoin increases, that demand meets increasing scarcity, driving the price higher in fiat-oriented terms–especially as fiat currencies increase in supply. Without exception, each halving has driven a bull market that has caused bitcoin's price to rise significantly.

In January 2024, late in the third halving epoch, the U.S. Securities and Exchange Commission approved 11 bitcoin spot Exchange Traded Products, significantly lowering barriers to entry for retail investors eager to gain exposure to bitcoin's financial performance without requiring them to understand how to acquire and secure bitcoin itself. The ETPs met massive consumer demand, with more than $50 billion in net inflows from January 2024 through mid-July 2025.[9] Just as early ETP demand spiked, Bitcoin's daily issuance rate was halved from 900 BTC per day to 450 BTC per day. The resulting supply shock has driven bitcoin's average daily spot price consistently above $110,000 since July 2025.[10]

As a point of emphasis, the following table illustrates the average closing price[11] of bitcoin on each of the prior halving dates:

First Trading Day Post-Halving	**Daily Supply (144 blocks/day)**	**Cumulative BTC Supply**	**USD Price at Close (23:59:59 UTC)**	**Δ from prior halving**
Nov 28, 2012	7,200	10,500,000	$12.20	–
July 9, 2016	3,600	15,750,000	$650.96	+5,237%
May 11, 2020	1,800	18,375,000	$8,601.80	+1,221%
Apr 20, 2024	900	19,687,500	$65,012.58	+656%

This table illustrates that as the cumulative supply of bitcoins increases and as the daily supply is reduced by the halving mechanism, bitcoin has increased precipitously in value against USD. Notably, the rate of change from one halving cycle to the next has lowered as the Bitcoin network's supply rate slows. Bitcoin's USD price rose 523.7x from the first halving to the second, 122x from the second halving to the third, and 65.5x from the third halving to the fourth. The slowing rate of change and bitcoin's increasing USD value indicate a maturing market that increasingly recognizes bitcoin's unique quality as a store of value.

Even as bitcoin's market matures, established economic orders are showing signs of fracture. Within the United States, the Federal Reserve has been increasingly politicized, with its chairman routinely under pressure from elected leaders to adjust interest rates to meet political objectives. The U.S. shows further signs of caprice, with on-again, off-again, on-again tariffs and other actions that weaken confidence in the US Dollar as a reliable global reserve currency. As U.S. hegemony fades and a multipolar global order emerges, new trading blocs and alliances are turning to economic and trade solutions that discount America's reliability and consistency.

Uncertainty and mistrust of fiat systems have also grown within the United States. Investors seek investments based on sound economic policy, particularly in an era of accelerating currency debasement. As established global economic orders show signs of fracture, the certainty of the 21,000,000 bitcoin hard cap–enhanced by Bitcoin's decreasing supply rate–allows bitcoin to exemplify reliable fiscal restraint. This makes bitcoin an increasingly reliable safe-haven asset that is immune from structural manipulation.

Evolution of Bitcoin's Monetary Role

Since 2009, bitcoin has functioned successfully as P2P electronic cash to facilitate unencumbered trade across the internet. The disinflationary halving mechanism that slows the rate of token issuance on the network has caused the value of each bitcoin to dramatically increase in value against fiat currencies. As a result, each sat goes farther as a medium of exchange over time. For those who acquired many bitcoins early in Bitcoin's history, their P2P cash likely represented a small percentage of the user's total wealth in traditional terms. As decaying supply has met increasing demand–exacerbated by loose monetary policies in most fiat economies–bitcoin has exploded in fiat price to become an unparalleled store of value. The evolution from experimental P2P cash to generationally-consequential wealth requires an expanded view of key management standards to secure and transfer that value into the future. The evolution of bitcoin in a fiat economy requires evolved thinking.

It has been said that the test of a first-rate intelligence is the ability to hold two opposed ideas at the same time.[12] For Bitcoiners, here is one part of that test:

Bitcoin is an elegant ***medium of exchange*** as peer-to-peer electronic cash.

Bitcoin is an unmatched ***store of value*** and a foundation for generational wealth.

These two seemingly opposed ideas speak to bitcoin's evolution as money.

Idealogues, take heart: evolution does not mean that something is no longer what it once was–only that it is *that*, and has become *something more*. The essence of an evolved thing remains in its DNA, but it has matured beyond–or more accurately, now more fully manifests–its original design.

This is true with bitcoin. Satoshi offered it as a "peer-to-peer electronic cash system": a currency for the internet free from centralized parties or financial intermediaries. Its programmatic decaying supply *necessarily* makes it climb in value as the network expands in fiat-dominated economies. For many early Bitcoiners, what started as an experiment with an inconsequential level of personal wealth–no greater than their desired level of digital "cash" on hand–now vastly outweighs anything else as "digital gold." The process of strategically managing and transitioning that wealth in a world constrained by fiat laws and human frailties requires a level of sophisticated thinking that often feels both new and foreign–and for some, *antithetical*–to the "Bitcoiner's ethos." But just as bitcoin's monetary role has evolved, Bitcoiners' key management frameworks must evolve to meet bitcoin's expanded function as money and for many, as the foundation of personal and family wealth.

Your Keys, Your Coins; Not Your Keys…

The control of a Bitcoin wallet address is maintained by cryptographic key pairs, including public and private keys. The public key is an identifier derived from the private key. It allows others to verify transaction signatures and is used to generate the wallet's Bitcoin address, which can safely be shared to receive funds. The private key is the secret input a bitcoin owner uses to generate a transaction signature that allows bitcoins to transfer from the owner's address to another Bitcoin wallet address. Because the private key controls the ability to spend bitcoins in a wallet, establishing and maintaining rigorous security to manage private keys is imperative.

There are many ways to generate and secure private keys for bitcoin. We will broadly discuss various key generation and retrieval constructs, and then turn our attention to the issue of private key signature controls.

Key generation & storage

Asymmetric (public key + private key) cryptographic key pairs are created with application software operating within a key generation system. For our purposes, these can be broadly categorized as follows:

A **hot wallet** generates a key pair using the device's software or hardware random number generator (RNG) while connected to the internet. It stores the private key locally on the internet-connected device (e.g., phone, browser, or desktop), making it immediately usable for signing but also more vulnerable to theft.

Like a hot wallet, a **warm wallet** also operates online and connected to the internet, but it adds safeguards like 2-Factor Authentication, IP address whitelisting, or time-delayed withdrawals. A warm wallet is nominally less convenient than a hot wallet, but the additional safeguards reduce the risk of key compromise.

A **cold wallet** keeps the private key completely offline. The private key is stored on a hardware device, air-gapped computer, paper, or other offline medium. Because the private key never touches the internet, cold wallets offer far higher security but require additional steps to sign and broadcast transactions. Transactions are signed within the device and only the encrypted signature is transmitted to the blockchain.

Because hot and warm wallets are connected to the internet–potentially exposing private key material–they are only appropriate for minimal values of bitcoin. They are acceptable for the "loose change" or "small bills" one might carry in a wallet or purse ready for tips, coffee shops, or other small, high-velocity transactions.[13] Cold wallets are superior for more valuable bitcoin positions and where lower transaction velocity is acceptable. Examples include those amounts of bitcoin intended for larger purchases, gifts, or trades within the next several months.

The above describes various methods by which cryptographic key pairs are created and stored. We must now turn our attention to various methods by which key pairs are *controlled and managed* for strategic planning purposes. For bitcoins that will be used as P2P cash for near-term transactions–especially very modest amounts–low friction methods that do not establish formal title ownership are often suitable. For bitcoins that constitute a significant portion of the owner's wealth, higher friction methods that establish formal ownership in proven, tax-optimized, protective structures are required.

Key signature control methods

There is a broad spectrum of methods by which a bitcoin owner might establish control over cryptographic private keys. These range from unilateral key control–methods by which the owner is the single point of control (and thus, the single point of failure)–to various forms of delegated, collaborative, or facilitated and managed control. We seek to establish a mental model with which the bitcoin owner might assess appropriate key control methods based on the owner's short-, mid-, and long-term objectives, as well as broader objectives for tax optimization, wealth preservation, or managing large inheritances. We will explore various general key management constructs and when each may be optimal, and close with an expanded view of the concept of sovereignty for large bitcoin holdings.

Leaving bitcoin on an exchange

Bitcoin's history consistently demonstrates that leaving bitcoins on an exchange is among the least secure methods of holding bitcoin long-term. Exchange hacks, rug-pulls, bankruptcies, and proof of unreserved or deeply fractionalized holdings on exchanges throughout bitcoin's history provide ample evidence that exchanges must only be used *for exchange.* Although it was not the first major exploit of an exchange to result in lost bitcoins (and far from the last), the 2014 hack of the Mt. Gox exchange remains the most vivid example of the risk of leaving coins on an exchange.[14]

An exchange is one form of a delegated hot wallet in which private keys are generated on-demand and stored by the exchange. Only bitcoins that are very recently acquired or soon to be traded or disposed of should be held on an exchange. Coins intended to be held indefinitely–and certainly bitcoin positions with economic significance to the owner–must promptly be removed from any exchange and elevated to a higher level of key management. A bitcoin owner is highly unlikely to ever recover bitcoins lost from the exploit or failure of an exchange.

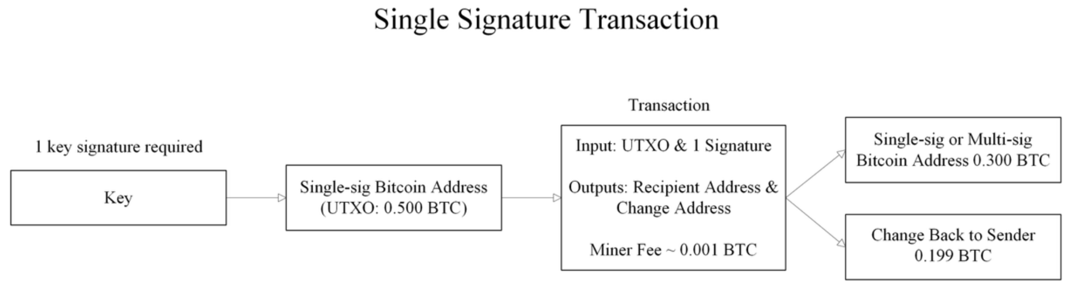
Failures like Mt. Gox gave rise to the popular maxim, *"Not your keys, not your coins."* In short form, this means a Bitcoiner must secure possession of their coins in a framework within which he or she controls the private key signing authority. Otherwise, there can be no assurance that the coins are actually available and spendable by the owner. For most exchanges, assets are usually commingled with those of other customers–and often with the exchange's own assets. As such, assets are neither title held nor bankruptcy remote.

For several years, *"Not your keys…"* meant that a bitcoin owner must secure their private keys in a wallet over which the owner exercises unilateral control. This, in turn, led to a broader conviction that unilateral control is essential to affirm ownership of private keys.

Single-signature (unilateral) self-custody

We will use the descriptor *unilateral self-custody* to describe any construct under which a bitcoin owner singlehandedly controls the ability to sign bitcoin transactions without relying on the action of any third party. In simple terms, self-custody key management uses a single-signature ("single-sig") wallet, where one private key is sufficient to authorize a Bitcoin transaction. This private key is typically managed either by software on the owner's smartphone or computer (a "hot" or "warm" wallet) or by a dedicated hardware device that generates private keys and signs transactions offline (a "cold" wallet) before the transactions are published to the blockchain. There are scores of applications and peripheral hardware devices designed to manage unilateral self-custody in a single-sig construct.

An illustration of a single-signature transaction is illustrated below:


Single Signature Transaction
1 key signature required
Key
Single-sig Bitcoin Address (UTXO: 0.500 BTC)
Transaction
Input: UTXO & 1 Signature
Outputs: Recipient Address & Change Address
Miner Fee ~ 0.001 BTC
Single-sig or Multi-sig Bitcoin Address 0.300 BTC
Change Back to Sender 0.199 BTC

Single signature key control establishes the key holder as the single critical point of failure. If the key holder loses access to the wallet or becomes incapacitated or dies without successfully establishing a succession mechanism to transfer control to their preferred successor, the bitcoin held in the wallet is likely forever inaccessible. Advanced technologies including programmatic dead-man's switches and more rudimentary backup phrase redundancies (fragmented or duplicated paper or metal private key seed phrase backups) are among the options available to enable a successor to recover the private key to a single-sig wallet.

As we will see in advanced key management structures below, single-sig key constructs–regardless of the transfer or key succession mechanism–provide no legally-recognized tax efficient method to transfer large sums of bitcoin. Nor do they establish values-aligned frameworks under which less mature or less sophisticated recipients can rise to the responsibility of managing significant bitcoin wealth.

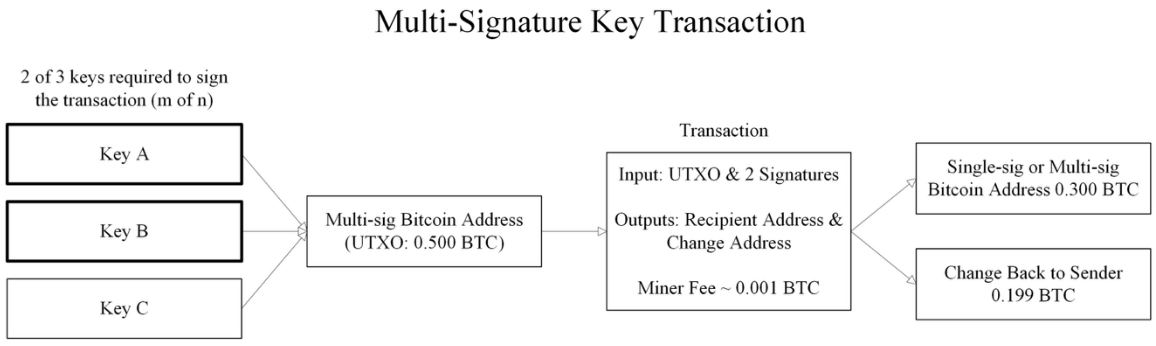
For these reasons, single-sig private key constructs should be limited to those fractions of bitcoins (i.e., sats) that the owner intends to spend in transactions as peer-to-peer cash. Larger "store of value" sums intended for mid- to long-term savings or for building generational wealth require more advanced levels of key management.

Multi-signature (collaborative) cold storage

As the name suggests, multi-signature or multi-sig describes a private key management construct that requires multiple private keys–usually held by multiple parties–to sign a bitcoin transaction before the bitcoins in a wallet can be spent. The Bitcoin network allows scripting to define how coins in a wallet address may be spent. Wallets that are established with a multi-signature key signing construct require that "*m of n*" private key signatories join in signing a bitcoin transaction before the bitcoins can move from that wallet address.

For example, if a bitcoin wallet address has a “2 of 3” multi-sig key construct, that wallet will have three private key signature profiles. In order for bitcoins to be spent from that wallet address, at least two of the key signature holders must sign the Bitcoin transaction in order for the bitcoins to move from the wallet. Multi-sig wallets can be established with any number of “*m of n*” key signature requirements (e.g., “3 of 5”, “5 of 7” …)

An illustration of a multi-signature transaction is illustrated below:


Multi-Signature Key Transaction
2 of 3 keys required to sign the transaction (m of n)
Key A
Key B
Key C
Multi-sig Bitcoin Address (UTXO: 0.500 BTC)
Transaction
Input: UTXO & 2 Signatures
Outputs: Recipient Address & Change Address
Miner Fee ~ 0.001 BTC
Single-sig or Multi-sig Bitcoin Address 0.300 BTC
Change Back to Sender 0.199 BTC

Multi-sig key control is appropriate for bitcoin that the owner intends to hold for many months or years. It is intentionally a *mid-friction* solution designed largely to prevent a single key holder from being the sole point of failure for consequential sums of bitcoin. Importantly, it allows the bitcoin owner to assign key signature authority to individuals he or she trusts, allowing those individuals to recover the bitcoin in the wallet if the bitcoin owner becomes incapacitated, is subject to duress, or when the owner dies.

As we will discuss in greater detail below, using multi-sig in tax-optimized or asset-protected wealth strategies is possible, but may not align with the large bitcoin owner’s broader wealth objectives. Multi-sig should be seen as a superior option for sums of bitcoin that the owner does not intend to spend in the near term, and/or for bitcoin the owner intends to pass outright to future beneficiaries when tax optimization, structured wealth transfer, and asset protection are not priorities.

Facilitated/Qualified Custody

Bitcoin custody facilitated by a third party–including by “Qualified Custodians” as defined by the Investment Advisers Act of 1940[15]–appears on its face to be antithetical to the bitcoin ethos of disintermediated financial transactions in a peer-to-peer electronic cash system. Indeed, for bitcoin *intended to be used as cash*, facilitated custody presents unnecessary friction and costs for bitcoin owners. Further, facilitated custody *that is not qualified custody* is likely no better than the practice of keeping large sums of bitcoin on an exchange and should be avoided for reasons we addressed above.

As we have discussed, Satoshi’s core thesis in developing the Bitcoin network was to establish a decentralized payment system based on cryptographic proof instead of trust to facilitate commerce on the internet without reliance on institutional intermediaries to manage or settle transactions. As P2P electronic *cash,* this remains a true function of bitcoin. But as we have also discussed, the network’s programmatic decaying supply mechanism has caused bitcoin to be *both* a decentralized medium of exchange *and* an unparalleled store of value.

For many early adopters of bitcoin who hold hundreds, thousands, or more bitcoins in single-sig or multi-sig key frameworks, their holdings have become a form of wealth that will likely outlive them. For these bitcoin owners who are citizens of the United States–regardless of where they live–and for bitcoin owners who either intentionally or accidentally[16] become U.S. taxpayers, this level of bitcoin wealth presents massive potential tax liability that can be significantly reduced or eliminated.[17] We will briefly discuss the scope of this tax exposure below, and will suggest options to mitigate it.

More important, these bitcoin owners are in a position of wealth to enrich their loved ones or to be agents of change through intelligent philanthropy beyond the ability of most individuals. For these Bitcoiners, carefully structured key management–often including facilitated and *Qualified* custody–plays an important role.

One essential consideration for third party facilitated custody is whether the third party satisfies the core of the SEC's "custody rule." The custody rule requires that custodians hold customers' assets in separate accounts, and that customer assets be segregated from the institution's own assets. *This asset segregation feature is paramount.* If the custodian does not establish separate title-held accounts for customers, the customers' assets will be exposed to claims against the custodian in the event of litigation. At worst, if the custodian becomes insolvent or files for bankruptcy, the depositors are unsecured creditors against the general assets of the custodian. In addition to losing significant economic value, the customer loses privacy as a plaintiff in a public court proceeding.

The purpose of the custody rule is to differentiate between asset custodians who are willing to employ requisite safeguards to ensure the security of depositors' holdings, and those who are not. Private key custodians who satisfy the custody rule should be seen as "best in class" third parties capable of responsibly managing bitcoin in custodial accounts. They are custodians willing to go above and beyond what is technically required in order to establish credibility in managing custody of large values of assets, including bitcoin. The spectrum of qualified custodians is broad, ranging from state-chartered institutions and foreign banks, to federally-chartered institutions in the United States.

Notably, bitcoin is not a security and thus it is not subject to regulation by the SEC. As a result, third party custodians who facilitate the management of bitcoin key material are not required to comply with the custody rule or any other aspect of securities law in the United States, which arguably makes reference to the custody rule irrelevant.

We propose that the rule is quite relevant indeed, even if it is not required. Moreover, if a future change in policy at the SEC were to cause bitcoin to be regulated as a security, the custody rule will be germane indeed. This further argues in favor of using fully regulated custodians to support consequential bitcoin holdings. As we will discuss below, qualified custody for bitcoin works elegantly within legally-recognized, tax efficient, private wealth strategies.

Facilitated and qualified third party custody should be reserved for large values of bitcoin that the owner does not intend to spend for the foreseeable future. Often combined with sophisticated wealth management strategies designed for tax efficiency or significant asset protection, it is necessarily a higher-friction environment for private key management.

Facilitated custody–whether "qualified custody" or not–generally relies on one of a few different private key generation and management frameworks. In broad terms, these include:

Multi-Institutional Multi-Signature (MIMS)

Multi-Party Computation (MPC)

Hardware Security Module (HSM)–based systems

Each of these has particular benefits and limitations that should inform the bitcoin owner's mental model for private key management.

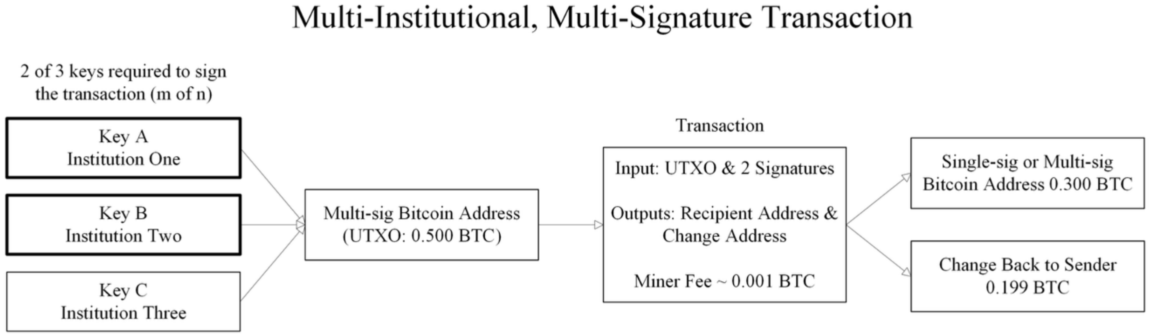
Multi-Institutional Multi-Signature (MIMS)

A MIMS framework applies the traditional multi-signature construct described above on page 7 but instead of individuals holding private key signature devices, the devices are held by corporate institutions. The objective is to provide continuity in the event one or more individual key holders becomes incapacitated, dies, or is unresponsive to the bitcoin owner's objectives. MIMS may be appropriate for large sums of bitcoin that the owner does not intend to move or liquidate for long periods of time.

Coupled with a completed gift irrevocable trust–sometimes structured as a multi-generational "dynasty" trust–MIMS has been promoted as a solution to allow a bitcoin owner to shift the value of bitcoin out of his or her estate for gift or estate tax (collectively, "transfer tax") purposes. Once the bitcoin owner severs "dominion and control" for transfer tax purposes and establishes legal title in a properly designed trust, the value of the bitcoin owned by the trust should escape future transfer tax liability for many generations, perhaps indefinitely.

MIMS is a low-velocity, high-security, high-friction key management framework. It requires that a bitcoin owner surrender all access to private key material for the bitcoin within the MIMS framework. By dividing private keys across multiple unrelated financial institutions, the bitcoin owner should have high confidence that assets will not be mismanaged or misappropriated.

A Multi-Institutional Multi-Signature (MIMS) transaction functions identically to a conventional multi-sig but with designated institutions–rather than individuals–holding private keys. An illustration of a MIMS-signed transaction is illustrated below.


Multi-Institutional, Multi-Signature Transaction
2 of 3 keys required to sign the transaction (m of n)
Key A Institution One
Key B Institution Two
Key C Institution Three
Multi-sig Bitcoin Address (UTXO: 0.500 BTC)
Transaction
Input: UTXO & 2 Signatures
Outputs: Recipient Address & Change Address
Miner Fee ~ 0.001 BTC
Single-sig or Multi-sig Bitcoin Address 0.300 BTC
Change Back to Sender 0.199 BTC

Multi-Party Computation

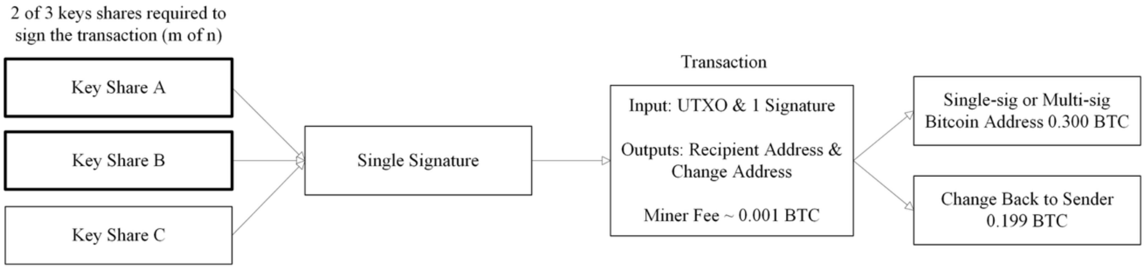
Transactions signed with multiple private key signatures–*multi-sig*, described briefly above provide an on-chain record as to which key signatures joined in the transaction. When the key holder is known or specifically assigned in an organized multi-sig framework, this provides on-chain auditability as to which signatures initiated and confirmed any transaction.

By contrast, multi-party computation, or "MPC", relies on a mathematical computation model to generate and store single private keys without requiring that the key material be assembled in a single place. MPC uses application coding to establish multiple shards of a single key. This shifts private key generation and signature application off-chain and into a software application.

Analyzed on-chain, MPC transactions are indistinguishable from ordinary single-signature transactions because at blockchain level, there is no ability to determine which shards of the private key were used to sign the transaction.

An illustration of MPC-signed transaction is illustrated below:

Multi-Party Computation (MPC)


2 of 3 keys shares required to sign the transaction (m of n)
Key Share A
Key Share B
Key Share C
Single Signature
Transaction
Input: UTXO & 1 Signature
Outputs: Recipient Address & Change Address
Miner Fee ~ 0.001 BTC
Single-sig or Multi-sig Bitcoin Address 0.300 BTC
Change Back to Sender 0.199 BTC

Hardware Security Module ("HSM")-based key management

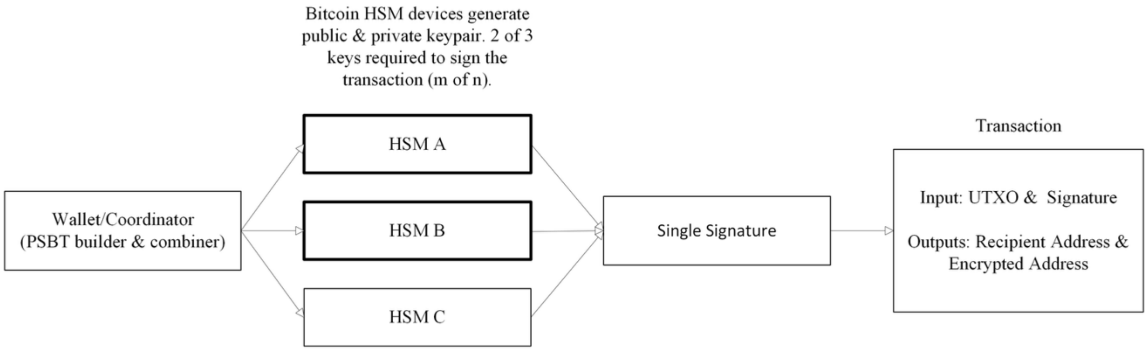
A Hardware Security Module (HSM) is a dedicated device used to generate, store, and use cryptographic keys without exposing private keys outside the device. They are used extensively in traditional finance and other industries that require high-security infrastructure. Key generation occurs inside the HSM using a hardware random number generator (RNG) that is typically FIPS 140-2 or 140-3 certified.[18] HSMs are tamper-resistant: they are designed to instantly erase cryptographic keys automatically in the event of tampering or on demand by the end user.

A Bitcoin HSM generates the asymmetric keypair (private + public keys) internally within the device. The public key can then be safely exported. To spend bitcoins from the address, the HSM signs the transaction with the private key inside the HSM device and only the encrypted signature is published to the blockchain.

Only authenticated users or authorized apps (via PINs, designated roles, or API credentials) can request operations from the HSM device. Because of widespread use in highly regulated industries that rely on secure encryption, HSMs are often used by large exchanges, institutional funds, and qualified custodians to securely sign Bitcoin transactions.

An illustration of an HSM-generated key pair and HSM-signed transaction is illustrated below:

Hardware Security Module (HSM)


Bitcoin HSM devices generate public & private keypair. 2 of 3 keys required to sign the transaction (m of n).
Wallet/Coordinator (PSBT builder & combiner)
HSM A
HSM B
HSM C
Single Signature
Transaction
Input: UTXO & Signature
Outputs: Recipient Address & Encrypted Address

We will explore various use cases for each of these key management constructs below. As we will see, the optimal key construct depends on the owner's strategic priorities and objectives, whether it's important for the owner to establish title ownership to bitcoin, the fiat-denominated value of the bitcoins held, the degree to which the owner is willing to surrender control, and the owner's expected spending velocity of the bitcoins. In most cases, a combination of key management regimes is appropriate.

Title Ownership of Bitcoin

Like physical gold, bitcoin is a "bearer asset." When bitcoin is held in self-custody, possession of the private key creates the presumption of ownership. Assets that are owned outright may be managed freely, but they do not enjoy the tax advantages or enhanced legal protection that formal structuring can provide. For assets of consequential value, transfer of outright ownership does not provide beneficial guardrails that can protect inheritors from mismanagement, poor decision making, or similar negative outcomes that can be avoided with thoughtful structuring. Without a title-bearing structure to formally establish legal ownership of bitcoins, it is impossible to take advantage of legal protections offered by estate or wealth management strategies in a fiat-driven system.

Why is it desirable to establish legal title within a peer-to-peer electronic cash system? A fair question, and to the extent bitcoin is only P2P cash, it is hardly necessary. Like physical fiat cash in a wallet or purse, small sums of bitcoins intended for spending need few protections, if any. But to the extent bitcoin is a consequential store of value for the owner, establishing title ownership to bitcoin within a legally-recognized framework is essential.

There is no other way to establish corporate ownership or to take advantage of legitimate tax mitigation, personal asset protection, structured philanthropy, and inheritance management strategies without establishing title ownership in properly-designed trusts or other legally-recognized planning devices. Legally-recognized tax and other benefits are determined by reference to property laws. Various legal and strategic benefits afforded by trusts, LLCs, foundations, and other recognized entities are only available to the extent the entity is properly established under the law, funded with assets titled in the entity, and carefully and actively managed to maintain operational compliance. The entity's private key management framework determines whether the entity has sufficiently established legal title to its bitcoin.

Establishing Fiduciary, not Personal Ownership

Various entities–including trusts, corporations, LLCs, foundations, etc.–are governed by one or more fiduciaries. A *fiduciary* is an individual or another entity that holds title to property on behalf of the entity the fiduciary manages. The fiduciary manages and controls the assets of the entity for the benefit of others who are identified as *beneficiaries* of the entity. The fiduciary is duty-bound to be objective, fair, competent, and attentive, and to comply at all times with the law and the entity's governing documents. A fiduciary's failure to carry out its duties constitutes *breach* of the law and of contract, exposing the fiduciary to liability and adverse legal consequences.

The fiduciary's role is established by the law of the jurisdiction under which the entity is established, and expanded or modified by the entity's governing documents. For example:

- In the case of a trust, the fiduciary is referred to as the "trustee," whose duties are determined by the trust instrument and the governing law in which the trust is established.
- In the case of an LLC, the fiduciary is either the "manager" or the "managing member," whose duties are determined by the LLC's operating agreement and the governing law in which the LLC is established.

- In the case of a corporation or a foundation, the fiduciary is often comprised by a board of directors whose duties are determined by bylaws or similar documents, as well as the governing law in which the corporation or foundation is established.

The fiduciary's role is well established in human history dating as far back as the Code of Hammurabi.[19] The ancient concept first recognized in Mesopotamia has matured over millennia, with expansive, robust, and diverse duties imposed on fiduciaries and with various legal and social consequences for failure to appropriately manage entrusted property.

A fiduciary's ability to *control and manage* assets entrusted to the fiduciary is elemental. If a fiduciary does not have the ability to manage and safeguard (control) the assets entrusted to the fiduciary, the fiduciary relationship is illusory. Whether the fiduciary manages and safeguards real property, investments, corporate equity, gold, or bitcoin, the fiduciary must maintain *legally-recognized control* over the assets in the fiduciary's care.

Benefits of Establishing Fiduciary Ownership

As we have discussed, legal and strategic benefits afforded by fiduciary-managed entities require that the entity is both properly established and bitcoin belonging to that entity is titled in the entity and under the fiduciary's legal control. We will briefly discuss some of the many benefits such structures are designed to provide.

Corporate Treasury Management

In August 2020, MicroStrategy Incorporated (now Strategy, Inc.) began aggressively adding bitcoin to its corporate balance sheet, announcing that it purchased 21,454 bitcoins at the total purchase price of $250,000,000.[20] As of August 11, 2025, Strategy had accumulated 628,946 bitcoins held in corporate treasury at the aggregate purchase price of $46,100,000,000.[21] The company actively reports its current BTC holdings on its website at https://www.strategy.com/.

In order to substantiate that the company–and not its principals or board members individually–owns Strategy's bitcoin reserve, the company stores *"...substantially all of the bitcoin we own in custody accounts at U.S.-based, institutional-grade custodians."*[22] This establishes a framework of corporate ownership, treasury security, and management continuity independent of any individual or individuals at Strategy.

Tax Optimization

For highly affluent or high-income bitcoin owners, and for those who seek to reduce the impact of wealth erosion from taxes, establishing fiduciary-controlled ownership in tax optimized strategies becomes a high priority. The United States imposes several forms of tax that may be mitigated through careful advanced planning. These include:

Ordinary income tax–tax on value received in exchange for goods and services. A U.S. taxpayer who receives bitcoin or other property as compensation or as payment owes ordinary income tax on the value of bitcoin received.[23]

Capital gains tax–tax on realized appreciation of gain above the taxpayer's "basis," or acquisition value. The gain is the difference between the sale price and purchase price, multiplied by the number of units, and the tax owed is the gain multiplied by the taxpayer's applicable tax rate.[24] This is true whether the taxpayer trades BTC for USD, for another cryptoasset, for any other form of property, or as payment for goods or services. At the time of this writing there is no exemption under U.S. tax law from capital gains treatment for any transactions involving bitcoin, however small.

Gift tax–tax on the value of property transferred by gift to a third party (including transfers to certain trusts or other entities) during the taxpayer's life, provided an exemption or deduction does not apply.

Estate tax–tax on the value of property transferred to a third party (including trusts or other entities) by operation of the taxpayer's death, provided an exemption or deduction does not apply.

Generation-Skipping Transfer Tax–an additional transfer tax beyond the gift and estate tax that applies to transfers during life or at death, to a "skip person". A skip person may be a descendant of the taxpayer who is more than one generation below (e.g., a grandchild), or an unrelated individual who is at least 37½ years younger than the taxpayer. The tax applies unless a GSTT exemption, allocation, or statutory exclusion shelters the transfer.

Most of these forms of tax can either be significantly mitigated or avoided completely, but only to the extent carefully designed, legally recognized, and fiduciary controlled strategies are implemented and properly funded. As discussed above at page 9 and in endnotes 16 and 17, the U.S. tax laws apply to all U.S. citizens and green card holders regardless of where they live, as well as individuals who may unintentionally become U.S. taxpayers because of the amount of time they spend in the U.S. or other factors.

Structured Philanthropy

Many Bitcoiners have achieved a level of wealth that far exceeds both their expectations and their desires for personal consumption. Moreover, many believe that establishing a generational legacy goes beyond materially enriching children and future generations. For them, dedicating a meaningful portion of wealth to support charitable initiatives is part of the inheritance they wish to leave behind.

Further, the U.S. tax code materially incentivizes charitable giving. Many strategies that support charitable giving also generate meaningful tax savings both in terms of income tax (ordinary and capital gains) as well as transfer tax (gift, estate, and generation-skipping). While some charitable benefactors are content with episodic outright gifts to charity, many more understand that carefully structured charitable trusts and related strategies can both generate tax deductions and create significant charitable legacies, while often *amplifying* the value the donor gives to their inheritors or retains for themselves.

- Outright gifts are usually given ad hoc, with no strings attached. The donor receives a present-year tax deduction based on the nature of the gift–cash or property, which includes bitcoin–and the type of charity receiving the gift.
- Structured, "planned" giving–often in the form of various charitable trusts–can generate charitable deductions, allow appreciated bitcoin to be sold in a tax-free environment, and pay a portion of the trust back to the donor or to other beneficiaries for greater tax-optimized, economically advantageous outcomes.

Most Bitcoiners retain high conviction that even after a gift has been given to a charitable beneficiary, the gift should continue to be held in bitcoin until there is a clear need to liquidate the bitcoin to fiat. Most charitable recipients are not equipped to receive and retain bitcoin in managed cold storage. However, carefully structured donor advised funds and other charitable strategies allow a donor to gift bitcoin to charity and direct that the bitcoin be held indefinitely until the charity has a need for fiat assets.

Asset Protection

Individuals with consequential wealth–and particularly those in high profile or high liability professions–are often justifiably concerned that third parties may initiate litigation that exposes their wealth to risk of loss. As a general rule, a successful plaintiff "steps into the shoes" of the unsuccessful defendant and to the extent the defendant has unilateral control over their assets, those assets are at risk of forfeiture to the plaintiff. This is as true for bitcoin as for any other type of asset.

Powerful creditors can arise in many contexts–some expected, and others quite surprising. In seeking to insulate assets from the claims of potential creditors, a wide range of strategies provides varying levels of protection:

> **Basic "homestead" exemptions**–Within the United States, each jurisdiction provides a set of statutory protections against claims. These range from very miserly to somewhat generous, but no state currently provides statutory asset protection for bitcoin or other bearer assets beyond very modest values.
>
> **Corporate veils**–Limited liability companies, limited partnerships, and corporations protect company assets from personal claims against the company's owners. The protection of the corporate veil depends largely on the jurisdiction in which the company is formed, and *entirely* on whether the company is structured, documented, and managed properly and consistently.
>
> **U.S. domestic irrevocable trusts**–Roughly one-third of states in the U.S. allow an individual to establish various types of irrevocable trusts that shield personal assets from creditor claims. Levels of protection vary from state to state, and residents of some states may not be permitted under local law to benefit from the asset protections of a state in which they do not reside.
>
> **Non-U.S. entities and trusts**–Some trust jurisdictions outside the United States provide heightened protection from potential creditors. In a few cases, even claims brought by a government agency may be barred from properly-established irrevocable trusts or corporate entities governed by the laws of a foreign jurisdiction.

To the extent bitcoin is properly titled to a trust, foundation, LLC, or similar entity, the bitcoin can be shielded from the claims of creditors to the same degree as other assets. But in all cases, the bitcoin owner must 1) establish an appropriate legally-recognized strategy, 2) sever dominion and control over the bitcoin, 3) establish fiduciary title ownership within the legally-recognized strategy, and 4) rigorously maintain compliance of the strategy to benefit from its protective veil.

Wealth Management / Inheritance Preservation

Bitcoin wealth is a very new form of wealth. As the value of BTC has grown rapidly in fiat-denominated terms, many bitcoin owners are only beginning to think about how bitcoin will impact the lives of future generations of inheritors. Just as prior generations have used long-established legal strategies to secure traditional wealth for inheritors, newly-affluent Bitcoiners must apply traditional methods to transfer bitcoin wealth in efficient, protective, and productive ways.

Inheritances delivered outright to an inheriting heir have all of the following limitations. This is true whether the inheritance is composed of real estate, equities, precious metals, fiat accounts, or bitcoin. Assets received outright:

- Are not protected from the beneficiary's potential creditors–including a future divorcing spouse.

- Are often quickly commingled with the beneficiary's own assets and are often quickly dissipated as "found money."
- Are not insulated from the beneficiary's mismanagement due to immaturity, lack of sophistication, poor decision making, or other frailties such as loose spending, gambling, or addictive behaviors.
- Will be countable in the beneficiary's taxable estate, if he or she is a U.S. taxpayer or otherwise resides in a jurisdiction that applies gift, inheritance, or estate tax.

Legally-recognized wealth strategies have long addressed these and other existential issues that threaten the security of traditional generational wealth. Those same structures–appropriately modernized to contemplate bitcoin's unique qualities–must also be used to allow generational bitcoin wealth to succeed in future generations.

Layering Strategies

Meaningful strategic outcomes require careful structuring to establish fiduciary title-held ownership within legally-recognized entities. Options range from limited, opaque strategies that require the bitcoin owner to surrender all control over private keys and transactions, to more dynamic, owner-guided, layered strategies. Presently in the United States, very few trust companies or professional fiduciaries have requisite understanding and expertise to support bitcoin in segregated, title-held, qualified custody. The scarcity of suitable fiduciaries typically results in higher fiduciary fees and a limited range of options. By carefully layering strategies with multiple entities–and often, multiple trusts owning those entities–affluent Bitcoiners can enjoy the benefits of fiduciary-controlled management without sacrificing transparency, high velocity, flexibility, and optimal levels of personal control.

A Graduated Framework for Key Management

We have explored the dual role of bitcoin as peer-to-peer electronic cash and as a consequential store of value. We have considered various key management constructs including hot-, warm-, and cold storage of key material, as well as single-sig, multi-sig, and various forms of facilitated bitcoin custody. We have further discussed various reasons for which a bitcoin owner might consider establishing legally-recognized title ownership of bitcoin in one or more fiduciary-managed wealth structures. We will now briefly consider when a bitcoin owner might use each key framework to tailor an appropriate wealth strategy.

Single Signature Control: High velocity, zero friction spending

For purposes of transacting in bitcoin as P2P cash and for low-value, high-velocity transactions, a single-signature key framework is most appropriate. These constructs allow the bitcoin owner to hold unilateral signature authority for transaction spends without reliance on any third party to join in the signature transaction. Because the single-key authority creates a single point of failure, more robust key management frameworks should be used as the value of sats is increasingly material to the bitcoin owner's wealth. The owner must assess whether hot, warm, or cold storage of private keys is most appropriate for the level of value of the bitcoin within the wallet, considering that hot (internet-connected) storage is the least secure method for managing private keys.

Single-signature control of private keys is suboptimal for fiduciary ownership of bitcoin. While it is possible to substantiate fiduciary ownership–provided the designated fiduciary unilaterally controls the key material–it merely shifts the single point of failure from the bitcoin owner to the fiduciary. Title held fiduciary control for bitcoin should be managed by multi-sig, MPC, or HSM-managed key signature frameworks.

As the value of the owner's holdings increases, it becomes increasingly important to establish a legally-recognized, fiduciary-managed structure that holds title to the bitcoin. Each of the following key constructs may be appropriate, with varying levels of transparency, velocity, and owner control.

Collaborative Multi-Sig: Moderate velocity, low-friction control

A multi-sig key management construct within which the owner selects trusted individuals as key holders allows for collaborative management of modest values of bitcoin. It provides continuity if the owner or any individual signature holder is unavailable, incapacitated, or deceased. Many multi-signature key management applications provide succession systems to replace a key holder as necessary and as determined by the vault owner.

Multi-sig held by individuals is possible in the fiduciary context only where all the individuals controlling private signature keys are designated fiduciaries. For example in the case of a trust, all key-holding individuals must also be designated as co-trustees to properly establish title. In the case of a revocable trust under which the bitcoin owner may serve as trustee–and where no present tax or asset protection benefit is available–individual-held multi-sig provides key management continuity and facilitates low-friction, moderate velocity bitcoin spending.

More protective wealth structures–including various forms of irrevocable trusts and other strategies optimized for present tax or asset protection benefits–require key management constructs that more fully remove the bitcoin owner from direct control over private key material. Each of these will require a form of facilitated custody described above on page 8.

Institutional Multi-Sig: Low velocity, high friction control

Multi-Institutional Multi-Signature (MIMS) key control allows a bitcoin owner to establish fiduciary-owned key management in a blockchain-native multi-signature construct. The bitcoin owner cannot hold any signature power within this framework; all key material is held by third party institutions. Those institutions must have legally-recognized and enforceable contractual obligations to the designated fiduciary of the applicable wealth strategy (e.g., the named trustee of an irrevocable trust).

Because multiple institutions hold key material, and because the key signatories must only act as directed by the entity's designated fiduciary (i.e., trustee) MIMS presents a low velocity, high friction key control regime. It is suitable for bitcoin positions that will be held indefinitely and for which the bitcoin owner no longer wants direct involvement in the management of the bitcoin within the fiduciary-controlled strategy.

Strategic, Facilitated Custody: Moderate velocity, moderate friction control

Other forms of facilitated custody may use various forms of key management, including multi-signature, MPC, or HSM-based constructs. Depending on the wealth strategy employed, the bitcoin owner may have more direct visibility to the bitcoin wallet and in some cases, partial key control.

As we have discussed, establishing title to bitcoin within a legally-recognized wealth strategy is imperative if and to the extent the bitcoin owner values the tax, asset protection, or inheritance preservation qualities offered by the strategy. Designing and implementing the optimal structure requires an understanding of the owner's objectives, various types or combinations of strategies that may achieve those objectives, an establishing fiduciary-controlled key management in a key construct the bitcoin owner will accept.

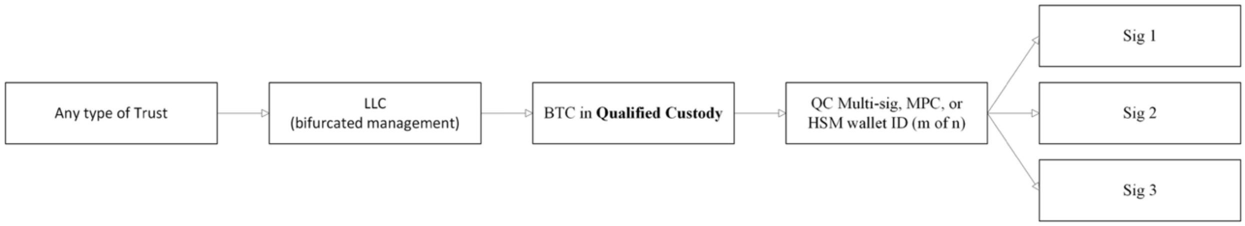
For example, if the bitcoin owner wishes to use jurisdiction-specific strategies such as non-U.S. irrevocable trusts, a key management construct that retains the key material within the United States accomplishes very little in terms of the asset protection non-U.S. strategies might provide.

> Moreover, layered strategies–such as innovative forms of limited liability companies held *within* irrevocable trusts–allow multiple layers of privacy, various forms of key management including managed multi-sig, MPC, or HSM-managed keys. Depending on the key construct in use and the bitcoin owner's objectives, the owner may not only have direct in-app visibility to all key-related transactions, but may also be able to directly hold a portion of key authority within the protective strategy.

More innovative, layered strategies offer superior resilience, greater flexibility, and higher levels of asset protection and inheritance preservation all within a moderate velocity, moderate friction environment for even the largest bitcoin balances.

A simplified illustration of facilitated qualified custody in a layered strategy is illustrated below:

Layered Strategy Transaction



An Expanded View of Sovereignty

The concept of sovereignty is deeply revered as the apex value among many Bitcoiners. After all, Satoshi Nakamoto explicitly designed Bitcoin as *"...a system for electronic transactions without relying on trust."*[25] He proffered Bitcoin as a system to allow parties to *"...*transact *directly with each other without the need for a trusted third party"* (emphasis added) to validate or authenticate the transaction.[26]

This function remains entirely true to the extent the bitcoin is used in internet commerce only as a transactional medium of exchange. Indeed, transactions are transmitted and validated by independent nodes operating on the Bitcoin network without any action by a centralized or trusted authority to affirm any transaction. But until such time as the owner wishes to transact, bitcoin's increasing function as a store of value commands a greater understanding of sovereignty in the context of protecting consequential wealth.

Within most bitcoin communities, the concept of sovereignty has centered on the *"Not your keys, not your coins…"* maxim. This framing is limited to the understanding of bitcoin as a transactional medium; it breaks down under bitcoin's economic superiority as a generational store of value. Sovereignty must go beyond unilateral signature control of cryptographic private keys. Within societies governed by laws, a more expansive understanding of sovereignty contemplates using resilient, legally-recognized strategies and fiduciary-managed ownership regimes, and exploiting opportunities in specific jurisdictions to achieve tax efficiency, asset protection, and inheritance preservation.

Sovereignty is *the ability to control the totality of decision making* for one's wealth according to his or her wishes. Unilateral private key control fails the test of this expanded definition of sovereignty.

Conclusion

Bitcoin is a network driven by open source code. It's a protocol upon which developers continue to iterate. It has persisted since January 2009 (16.5 years at this writing) and as it has grown, it has evolved into a monetary system that is more than a brilliant, decentralized form of peer-to-peer electronic cash. It has become an unmatched store of value and the foundation of tremendous personal wealth capable of spanning generations–if managed intelligently.

A cypherpunk experiment in peer-to-peer money has established itself as the bedrock of generational wealth for many early adopters. The economic reality of bitcoin in a society bound by tax laws–coupled with the reality that many who will inherit significant bitcoin wealth are not adequately prepared to inherit great wealth at scale–requires an advanced framework for managing this form of wealth.

While bitcoin's future remains unwritten, it is foreseeable that bitcoin continues its trajectory of value growth, especially when compared against loose monetary policy within fiat-based money systems. Bitcoin's evolution to a higher form of money requires a clear-eyed, pragmatic approach to structuring key management systems and title-held ownership structures to mitigate against permanent loss due to avoidable tax erosion, mismanaged inheritance, failed programmatic code-based solutions, confiscation from tax evasion or litigation, and other existential risks to personal wealth.

Bitcoin owners' sophistication around key management has not kept up with the reality that the value of bitcoin has risen in fiat-denominated terms more rapidly than any other asset in known human history. In its brief history, Bitcoin has gone from experimental concept to a multi-trillion dollar asset class in which each bitcoin now consistently exceeds $110,000.

Holders with economically consequential sums of bitcoin must evolve their thinking to keep pace with bitcoin's evolution. This requires a sober-minded consideration of every form of private key management to size bitcoin management intelligently: from unilateral control to multi-sig, to tax-optimized and legally-recognized structures relying on qualified custody.

Mature bitcoin sovereignty relies on wealth management strategies that provide tailored, thoughtful, experienced planning and active support. It leverages advanced legal, financial, and global market understanding. A broad spectrum of key management and title ownership regimes must be applied to address a bitcoin owner's competing objectives for high velocity-low friction spending and cross-generational, tax optimized, protected inheritance planning.

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (*https://bitcoin.org/bitcoin.pdf*). I will refer to this document generally as the *Bitcoin Whitepaper*.

[2] Consistent with traditional usage within many Bitcoin communities, initial capitalized "Bitcoin," denotes the network itself, as well as its role as an asset class and monetary system. Uncapitalized "bitcoin" refers to the units of value–the tokens or coins–produced by and transacting on the Bitcoin network.

[3] Named for Bitcoin's founder, Satoshi Nakamoto, A "sat" is the common reference for the smallest divisible fraction of a bitcoin: 1/100,000,000 of one bitcoin. https://en.bitcoin.it/wiki/Satoshi_(unit)

[4] The true identity of Satoshi Nakamoto remains unknown as of this writing. For purposes of simplicity, I will use the singular masculine pronoun "he" when referring to Nakamoto, as "Satoshi" is traditionally a masculine name in Japanese meaning "wise," "intelligent," or "clever." (*see https://en.wikipedia.org/wiki/Satoshi*) Much debate has focused on whether Satoshi was a single individual who combined and evolved the work of prior cryptographers and network engineers–and if so, whether Satoshi is the individual's true name or more likely, a pseudonym–or whether Satoshi was or is a collaborative of individuals. Certain individuals have claimed to be Nakamoto, and others have speculated that certain early known developers are or were Bitcoin's founder. In every case the identity of Satoshi Nakamoto remains a mystery. Throughout the whitepaper, Satoshi uses the first person plural "we" and "our" to describe the collaborative development process of the Bitcoin network. Whoever or whatever Satoshi Nakamoto is or was, he, she, it, or they are likely amused at the obsession over their identity. Regardless, the network Satoshi introduced in January 2009 has continued uninterrupted to this day and the value of bitcoin continues to climb.

[5] S. Nakamoto, *Bitcoin Whitepaper, at 1.*

[6] https://www.blockchain.com/explorer/blocks/btc/0

[7] The full article from *The Times* referenced by Nakamoto is available online at https://archive.ph/ia9C7

[8] https://github.com/0xMagnuz/Bitcoin-v0.1/blob/master/posts/release.md
[9] https://cointelegraph.com/news/us-bitcoin-etfs-reach-50b-milestone-just-18-months-after-launch
[10] See generally, https://www.statmuse.com/money/ask/bitcoin-price-day-by-day-july-2025
[11] In truth, bitcoin and other crypto markets trade 24/7/365, so the markets never "close." For purposes of determining the close of bitcoin and other cryptoasset markets, daily Open, High, Low, and Close in crypto markets generally reset at 00:00:00 Coordinated Universal Time (UTC). Thus, the close is typically determined by reference to bitcoin's price at 23:59:59 UTC each day of the year.
[12] F. Scott Fitzgerald, *The Crack-Up.*
[13] Please note that as of this writing, the United States Internal Revenue Service has defined bitcoin as a form of "convertible virtual currency" and treated as property for tax purposes. Moreover, there is no *de minimis* transaction exception to bitcoin under the Internal Revenue Code. This means that any transaction *no matter how small* will trigger a capital gain or loss recognition event for a U.S. taxpayer. This creates a great challenge for those who seek to use bitcoin for small P2P transactions, as failure to prove basis for capital gains tax purposes will result in a determination of *zero* basis, meaning that even small purchases with bitcoin could technically trigger capital gains tax recognition on the full value of each transaction.
[14] The Mt. Gox exchange was the venue of the first known exchange hack, with 25,000 bitcoins stolen in June 2011. Several other exchanges were hacked in following years, but all pale in comparison to Mt. Gox's major–and resulting fatal–hack in February 2014 when an estimated 744,000 to 850,000 bitcoins were stolen from the exchange. https://forwardsecurity.com/wp-content/uploads/2025/04/EvolutionOfCryptoExchangeBreaches.pdf
[15] The Investment Advisers Act is codified at 15 U.S.C. § 80b-1 through 15 U.S.C. § 80b-21. Full text is available at https://www.govinfo.gov/content/pkg/COMPS-1879/pdf/COMPS-1879.pdf
[16] As an example, non-U.S. citizen, non-green card holder may be deemed to be a U.S. tax resident under the "substantial presence" test and subject to U.S. tax on worldwide income. Similarly, a green card holder who no longer resides in the U.S. would still be treated as a U.S. taxpayer until the green card is formally surrendered. See I.R.C. §7701(b)(1)(A) (defining "resident alien" for tax purposes to include (i) any individual who is a lawful permanent resident at any time during the calendar year (the so-called "green card test"), or (ii) any individual who satisfies the substantial presence test); I.R.C. §7701(b)(3)(A) (substantial presence test, requiring at least 31 days of U.S. presence in the current year and a total of 183 days calculated under a weighted three-year formula); Treas. Reg. §301.7701(b)-1(b)–(c) (providing rules for determining residency under the green card and substantial presence tests, including day-counting conventions and exceptions); IRS Publication 519, U.S. Tax Guide for Aliens, ch. 1 (2024) (explaining that non-U.S. citizens may become U.S. tax residents either by holding a green card or by meeting the substantial presence test, in which case they are generally subject to U.S. taxation on worldwide income).
[17] As described in endnote 16, U.S. citizens and long-term (green card) residents are subject to U.S. income tax on worldwide income, regardless of where they live. Similarly, citizens and residents are subject to gift and estate tax liability on their worldwide assets. This remains true even if the U.S. citizen or resident has not entered the U.S. for many years. Only careful expatriation pre-planning can mitigate this liability.
[18] FIPS 140-2/3 is the U.S. government's standard for how cryptographic modules like HSMs are designed, tested, and certified. The standard is managed by the National Institute of Standards and Technology (NIST). Devices that are "FIPS certified" have passed rigorous, independent lab testing and are approved for handling sensitive government or financial data. https://csrc.nist.gov/projects/cryptographic-module-validation-program
[19] See generally §§120–125, *Hammurabi's Code of Laws,* ca. 1780 BCE. English translated text available at https://sourcebooks.fordham.edu/ancient/hamcode.asp.
[20] https://www.sec.gov/Archives/edgar/data/1050446/000119312520215604/d921849dex991.htm
[21] https://www.sec.gov/Archives/edgar/data/1050446/000095017025106241/mstr-20250804.htm
[22] https://www.sec.gov/Archives/edgar/data/1050446/000095017024015847/mstr-20231231.htm#item_1a_risk_factors (at 19.)
[23] See I.R.C. §61(a)(1) (defining gross income to include *"compensation for services, including fees, commissions, fringe benefits, and similar items")*; Treas. Reg. §1.61-2(d)(1) (which provides that if services are paid for in property, the fair market value of the property must be included in income as compensation); Treas. Reg. §1.61-14(a) (clarifies that gross income includes all accessions to wealth not otherwise excluded); IRS Notice 2014-21, 2014-16 I.R.B. 938, Q&A-8 (states that a taxpayer who receives virtual currency as payment for goods or services must include the fair market value of the currency in gross income as of the date received).
[24] Under Internal Revenue Code §1001(a), *"the gain from the sale or other disposition of property shall be the excess of the amount realized therefrom over the adjusted basis provided in §1011 for determining gain."* The amount realized (AR) is defined under §1001(b) as *"the sum of any money received plus the fair market value of*

property (other than money) received." The adjusted basis (AB) is determined under §§1011–1016. See also Treas. Reg. §1.1001-1(a): *"Except as otherwise provided, the gain or loss realized from the conversion of property into cash, or from the exchange of property for other property differing materially either in kind or in extent, is treated as income or loss sustained."*

[25] S. Nakamoto, *Bitcoin Whitepaper*, at 8.

[26] Id., at 1.