BITCOIN CUSTODY IN 2025:

Methods, Trade-Offs, and the Three Pillars of Secure Storage

bitcoin park

Prepared by:
Robert Warren, Head of Research and Education at Bitcoin Park

Designed by:
Jack Lesser, Operations Lead at Bitcoin Park Austin

CONTENTS

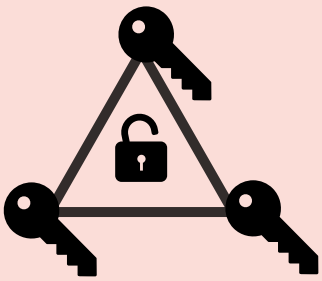
bitcoin park

EXECUTIVE SUMMARY

Self-custody is fundamental to the promise of Bitcoin. Cryptographically secured keys, holding a bearer asset on a distributed network allow for properties unlike any on earth. Yet, for newcomers to the space, the options and basics of custody are often confused by strange new technology and language, bizarre hardware, and businesses with impressive technologies but unclear differentiators. While Bitcoin's architecture **invites every holder to become their own bank**, most participants will choose a solution (or solutions) that best suits their use case, threat vectors, risk style, and total holdings.

The following whitepaper was designed, not to direct individuals towards a single provider or model, but rather, **to offer the lay-of-the-land** and assist in the difficult task of choosing solutions that work best for you. This is a community-driven effort, and could not have been produced without the critical eyes of our expert industry reviewers and Bitcoin Park members. We thank them for their incredible input, which has brought this whitepaper to life.

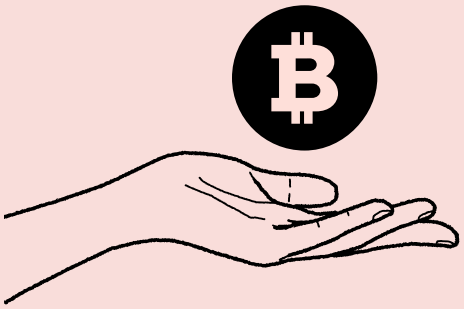
The custody landscape broadly spans three pillars— **Single-Signature (Single-Sig) models, Multi-Signature (Multi-Sig) models, and Fully Custodial models**. Each pillar can be assessed through various lenses, such as **insurance, multi-institutional custody (MIC), and miniscript**, that add functionality across three key variables: **security, privacy, and convenience**. Lightning-specific variations, which span custodial and non-custodial solutions are extremely useful for payments, but add complexity beyond the scope of this introductory whitepaper.


Single-Sig self-custody maximizes sovereignty and personal privacy but punishes mistakes mercilessly. Hardware wallets and signing devices are robust tools for self-custody, yet a lost seed phrase or forgotten 25th word incurs 100% loss. **Multi-Sig models** vary widely in execution, but all divide power amongst keys or institutional quorums. An array of companies offer service levels that scale from individual multi-signature schemes with external recovery resources, up to multi-institutional holdings within a custodial network. Specific "multi-institution" triads work to eliminate single custodian risk for large personal or institutional holders. Insurance providers now offer up to US $700 million in coverage, with an estimated $1 to $2 billion currently secured via insured channels-addressing threats that cryptography alone cannot mitigate. **Fully Custodial** platforms such as ETFs and exchanges excel at end user convenience, and may include insurance coverage, but users must perpetually guard against single points of failure, rehypothecation, underinsurance (e.g. major custodians of ETFs may lack full coverage of all assets under management), and the privacy consequences of strict know-your-customer (KYC) regimes.

No pillar is universally "best" for all users of Bitcoin, but fully self-custodial solutions such as single-sig (with or without passphrases) and multi-sig, which demand user participation in holding keys and signing transactions, are the gold standard for maximizing self-sovereignty over your Bitcoin.

In practice, sophisticated investors **blend solutions across myriad providers**: lightning-fast spending in a custodial or non-custodial Lightning wallet for day to day purchases, a hardware device for personal savings, an insured 2-of-3 multi-sig vault for retirement holdings or generational wealth. **Custody choice is a strategic allocation of trust**, a way to stand on the right side of technological change while safeguarding your personal capital.

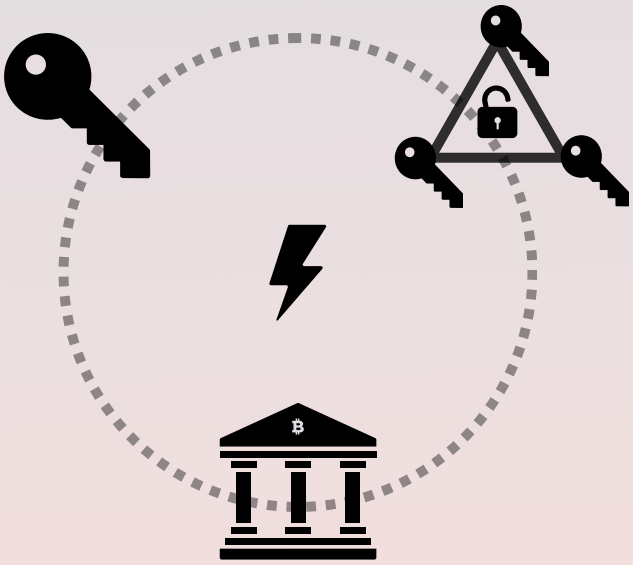


THE THREE PILLARS

Bitcoin converts private keys into unconfiscatable wealth; whoever controls the key or keys controls the coins. That promise is **transformative**, yet it thrusts everyday users into the unfamiliar territory of key management. The collapse of Mt. Gox in 2014 and FTX in 2022 revealed how disastrous misplaced trust can be. Conversely, stories of early HODLers losing laptops or paper wallets remind us that absolute self-custody can hurt the careless.

As the industry matures to serve a variety of users and use cases, there are three broad pillars that have emerged, each with its own robust set of offerings, trade-offs, and cost structures:

1. **Single-Sig Self-Custody**—the user alone holds one key, which allows for full control over funds, and a high degree of privacy, while demanding immense responsibility over security.
2. **Multi-Sig Collaborative Custody**—two or more keys spread across people, devices, or institutions, which allow for collaborative or multi-institutional responsibility over signing rights. Self custody multi-sig is absolutely possible and highly protective, but is technically beyond the scope of most Bitcoin users.
3. **Fully Custodial**—a third party holds 100% of the keys. Often the first way participants engage with bitcoin. Fully custodial solutions are the least private solution, and offer little protection against rehypothecation and dedicated insurance coverage with a focus on user convenience.

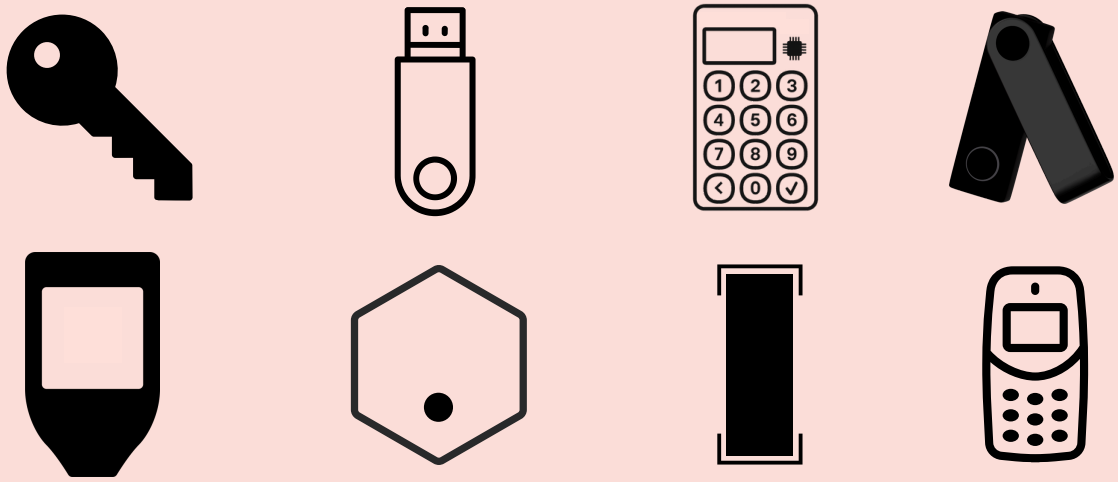


NOTE: Lightning solutions and various lightning wallets can weave through all three pillars. A custodial Lightning app like Wallet of Satoshi resembles pillar 3, while a self-managed node is akin to pillar 1. Our primary objective is to equip readers, whether retail savers, corporate treasurers, or public funds, with a research-grounded framework to match custody choices to risk tolerance and regulatory realities.

Custodial Lenses

Within the three pillars of Bitcoin custody exist various modifying 'lenses' that can offer additional security, privacy, and convenience. Currently, the most available are, insurance, Multi-institutional custody (MIC), and miniscript. **Insurance** solutions vary by bitcoin amount and custody type, and can be written either to a custodian or to an individual policyholder. These policies vary widely in cost, underwriting, and payout methodology, and consumers must be aware of policy idiosyncrasies and provider limitations. **MIC** is emerging as a best-in-class option for institutional holders, and offers accommodations for various regulatory regimes as well as corporate internal controls. **Miniscript**, a technical innovation proposed via BIP-379, structures the Bitcoin native scripting language, which allows users to safely construct complex spending conditions or 'scripts' for creativity within single and multi-sig solutions without counterparty risks.

PILLAR 1 — SINGLE-SIGNATURE SELF-CUSTODY



Illustrative hardware self-custodial signing devices

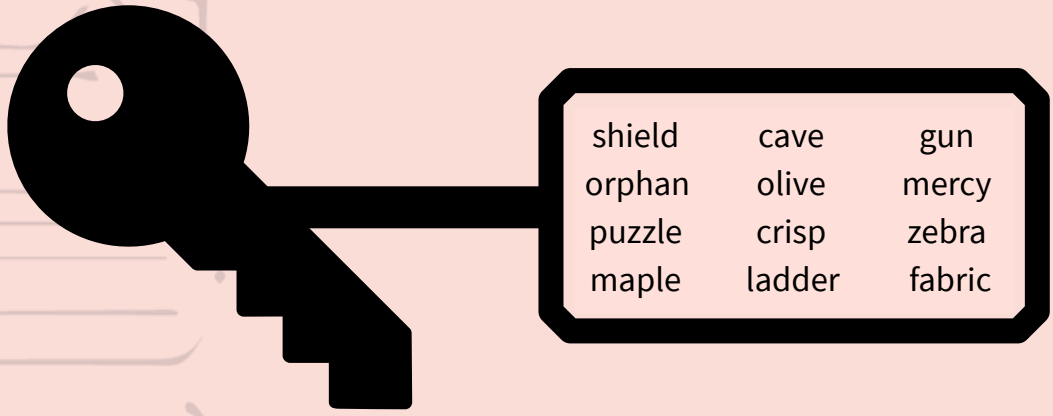
1.1 Definition & Appeal. Single-sig represents **the most self-sovereign form of Bitcoin** ownership: one secret equals full control. From cold-storage hardware and signing devices (Coldcard, Ledger, Trezor, Passport, and many more) to mobile Lightning wallets (Phoenix, Breez, and many more), users can eliminate third-party risk and achieve maximum pseudonymity without third party dependencies.

1.2 Security Profile. Executed flawlessly with air-gapped hardware, metal backups, and strong passphrases, single-sig attains **top security** against remote hacks and institutional seizure. Conversely, user mistakes drop security to zero: a lost seed or a seed entered on a phishing site results in immediate loss of access to coins. Hot wallets introduce additional online attack vectors, reducing practical security while being advisable only for smaller, daily-spend balances.

1.3 Privacy & Regulation. With no mandatory KYC, single-sig affords **industry-leading privacy**. When paired with address hygiene practices on-chain anonymity approaches a maxima. Use of exchange withdrawals or public IPs can still leak personal data; hence operational security matters. Regulation is non-existent until coins re-enter the fiat perimeter via exchanges or other KYCed platforms, typically when selling for another currency.

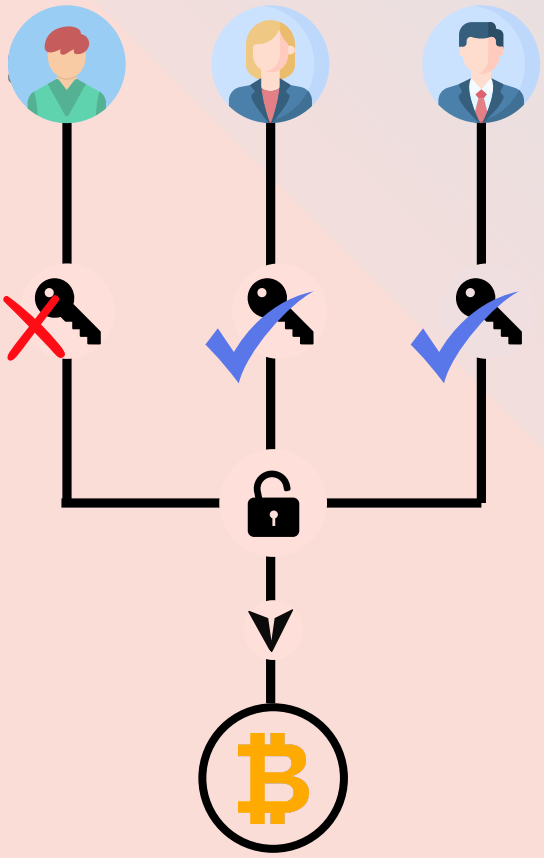
1.4 Externalities. Self-custody disperses coins across thousands of addresses, boosting network decentralization and reducing systemic honeypots. The primary negative externality is **permanent coin loss** from individuals forgetting seeds, a lack of inheritance planning, or simple user error, which are estimated to have removed millions of BTC from circulation. Additionally, policymakers sometimes frame self-custody as an AML (anti-money laundering) risk, foreshadowing potential regulatory friction.

1.5 Takeaway. Single-sig is ideal for **tech-confident individuals or activists** whose primary threats are censorship or confiscation and primary desire is individual sovereignty. It demands discipline: secure backups, inheritance planning, and phishing vigilance. For most, it serves as the sovereign anchor in a multi-layer custody stack.



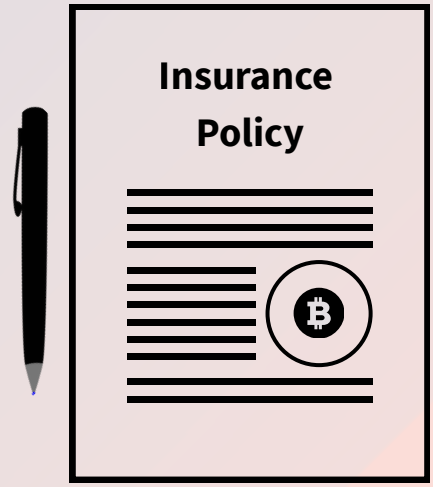
Illustrative 12-word seed phrase

PILLAR 2 — MULTI-SIGNATURE COLLABORATIVE CUSTODY



Illustrative 2-of-3 multisig transaction

2.1 Definition & Appeal. Multi-sig requires **a quorum of keys (e.g., 2-of-3, 3-of-5) to authorize spending**, distributing control across devices, locations, or institutions. The approach neutralizes single-point failures while preserving user ownership. Models range from DIY multi-sig (not covered in this paper), to managed services like Unchained, Casa, Nunchuk or (user + service), and pure **multi-institution triads** (Onramp, BitGo, and Coincover), with numerous hybrids such as Unchained's multi-institutional offerings, and **community federations** such as Fedimint or Blocksteam's Liquid Network. Insurance offerings marry cryptographic controls to centuries-old risk pools, calming fears that "one slip equals total loss." Insured custody solutions vary widely, from catch-all third party policies under large, single custodians, to multi-institutional multi-sig with named policies and detailed coverage beyond typical "commercial crime" insurance.

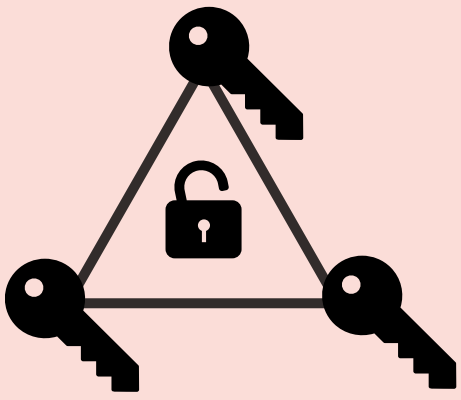


2.2 Security Profile. Splitting keys across independent hardware devices and geography mitigates key loss, disasters, and physical assaults or kidnappings, known in the industry as "wrench attacks". Collaborative services add guided recovery, pushing effective security high. Complex scripts or lost configuration files can introduce new failure modes, but institutional grade solutions such as Onramp offer thoroughly vetted testing and documentation to manage internal controls. AnchorWatch's "Trident Vault" uses another advanced strategy, where client and company each hold a key with Lloyd's of London coverage against coercion or disaster. This allows for resumption of full customer control after policy expiration, as well as fallback to multi-institutional custody in case of lost keys. These options lift baseline security against loss substantially, though detailed consideration of custodian and insurance policy structure are still necessary to protect against edge case losses of funds.

2.3 Privacy & Regulation. DIY multi-sig rivals single-sig for privacy. Collaborative services know some user metadata (Vault xpubs, which show addresses as well as address balances) but companies design workflows to minimize data retention. Upgrades such as Taproot now let multi-sig outputs appear as ordinary single-sig, obscuring wallet type on-chain. Regulatory outlook is friendlier than single-sig because multi-sig's recovery features increase regulation and allow for external audit and provable transaction histories-relevant for funds held in IRAs or other regulated accounts. Still, KYC with outside services lowers user anonymity severely. Insurance underwriting demands identity verification and risk questionnaires, so privacy improves only marginally versus fully custodial solutions (Pillar 3).

2.4 Externalities. Positively, multi-sig reduces the frequency and severity of coin-loss incidents and protects large treasuries from most insider theft. It fuels an ecosystem of key-management startups and inheritance planning tools, creating jobs and standards. Potential negatives include reliance on a popular cosigner: e.g., if Casa or Unchained were coerced to stop signing customer transactions, clients could face friction, though most models let clients transact with their own quorum or utilize timelocking or other advanced scripting to reduce this risk. **MIC models**, while ensuring far greater institutional standards are met, will add costs, complexity, and some regulatory burden. **Insurance** costs include premiums (ranging from 5-100 bps annually) and the addition of an insurer as a counterparty, as well as consideration of the gap between custodian insurance limits and total assets under management: e.g. A custodian with $1 billion under management is only insured up to $500 million.

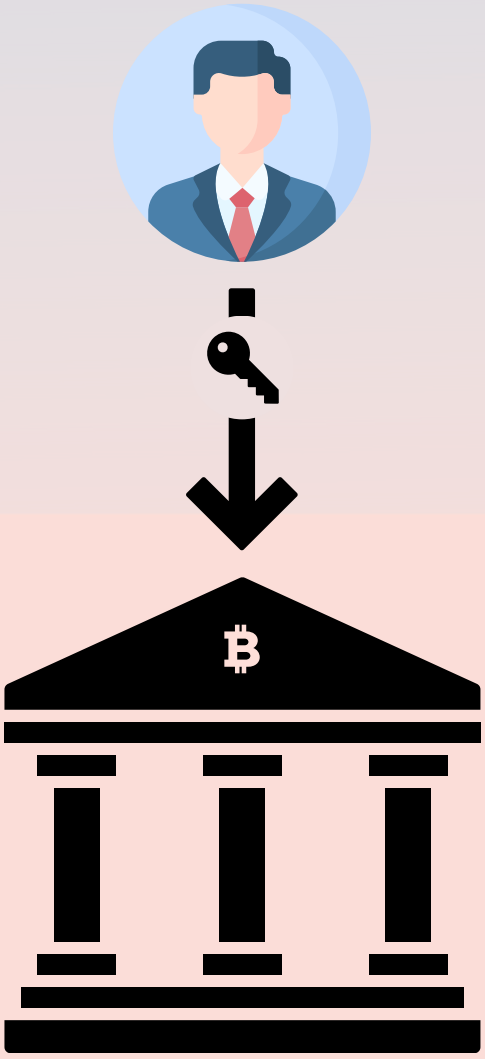
2.5 Takeaway. Multi-sig is often the **"Goldilocks zone" for large retail and institutional balances:** high resilience, shared responsibility, and optional professional assistance without ceding total control. Expect it to become a mainstream standard as UX improves, taproot-enabled fee savings propagate, and privacy improvements through tools like musig and taptrees gain greater adoption. MIC adds institutional legitimacy and internal controls, and insured custody shines for high-value treasuries and families seeking peace of mind without surrendering total control. They are a bridge that can reassure conservative capital that Bitcoin can meet fiduciary standards.



PILLAR 3 — FULL CUSTODIAL SOLUTIONS

3.1 Definition & Appeal. Full custody mirrors legacy finance and banking with multiple publicly traded ETFs and custodians such as Coinbase, Xapo, River, Strike or Komainu, who acquire Bitcoin and store private keys in fortified data centers and present users with familiar dashboards. This model excels at liquidity, seamless mobile UX, and integrated tax reporting. For thousands of newcomers, it is the earliest on-ramp.

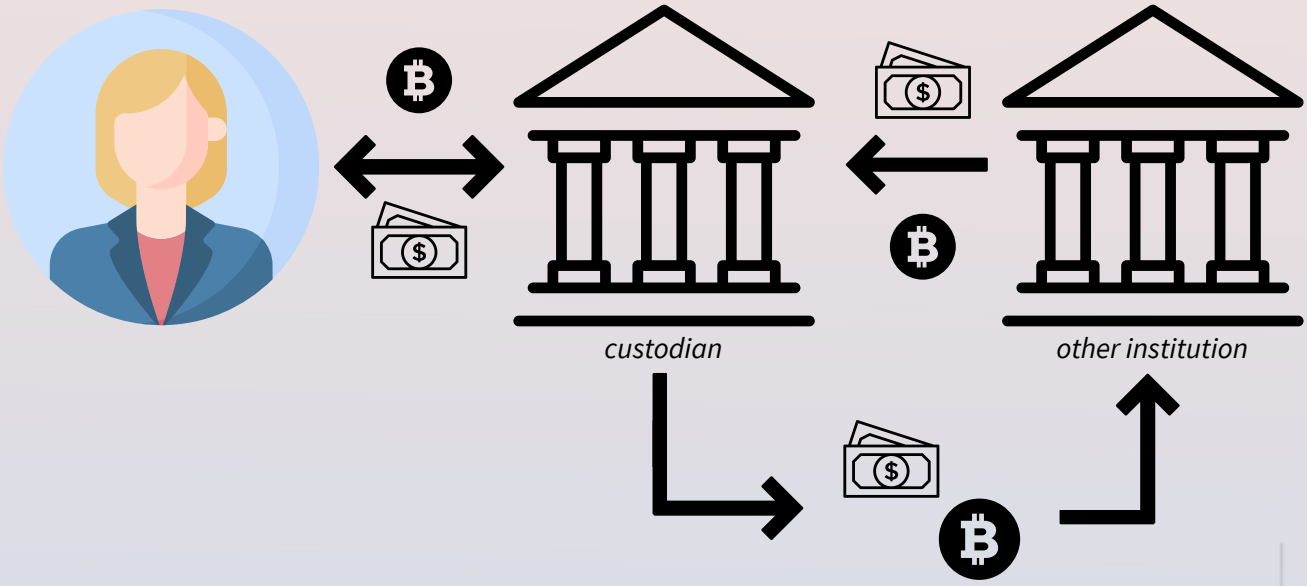
3.2 Security Profile. Leading custodians employ cold storage for 95%–99% of assets, hardware-security modules (HSMs), and multi-approval workflows. Coinbase insures its hot wallets up to US $320 million, and BitGo powers dozens of exchanges with bank-level controls. Yet, catastrophes such as hacks, technical failures or internal misuse prove risks of concentration.



3.3 Privacy & Regulation. Because AML/KYC rules treat exchanges like money-service businesses, privacy scores are necessarily low. Every withdrawal address is tied to an identity; regulators can freeze exchange accounts or demand reports. Additionally, full custodial solutions can share data with both government agencies and private chainalysis services. Users must weigh the risk of data breaches and the loss of personally identifiable information to bad actors against comfort and speed.

3.4 Externalities. When exchanges dominate, Bitcoin's supply concentrates in corporate vaults—potentially undermining network decentralization and presenting a risk of rehypothecation. Positively, big custodians drive institutional legitimacy by passing SOC2 audits and lobbying for clear industry regulations.

3.5 Takeaway. Full custody is "training-wheels Bitcoin." It can be appropriate for small balances, active traders, and regulated entities legally barred from self-custody. But prudent users withdraw surplus holdings into more sovereign setups.



Illustrative rehypothecation of funds

CHOOSING A CUSTODY STRATEGY

Map Your Threat Model

PRIMARY RISK	RECOMMENDED BIAS	RATIONALE
Exchange insolvency	Single-Sig or Multi-Sig	Removes most counterparty risks
Key loss / death	Multi-Sig w/ service or Insured	High-touch recovery path
Physical coercion	Multi-Sig and/or Insured	Single key useless to attacker
Regulatory reporting	Single-Sig (private), Federated, Multi-Sig without service provider	Minimizes KYC footprint
Board compliance	All options, contingent on governance structure	External audits + insurance satisfy fiduciaries

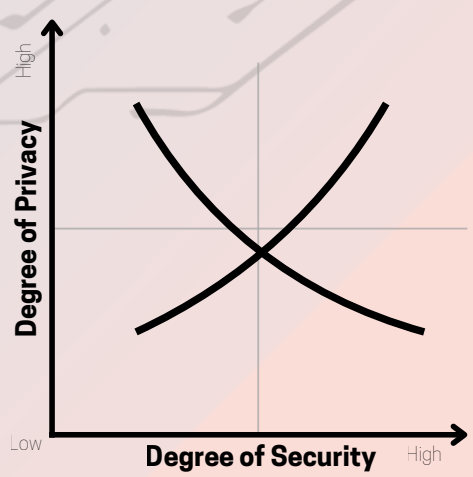
Hybrid Holdings

While your optimal custody solution should match personal goals, total holdings, risk profile, and life stage, many individual holders with meaningful savings in bitcoin **might allocate holdings using multiple tools** as detailed below.

Your solution should fit your personal use case. Technically minded individuals with substantial holdings will find themselves biased towards self-custodial single-signature and multi-signature schemes, while non-technical family offices might choose to allocate only through insured providers or multi-institutional models. Additionally, as Bitcoin continues to monetize, holdings should change to reflect changing values.

- **Petty Cash** for coffee-money and quick transacting in a Lightning or hot mobile wallet.
- **Checking Account Amounts** in a single-sig hardware device for medium-term needs.
- **Savings Account Amounts** in a single-sig hardware device with or without a passphrase, or an entry level multi-signature provider for medium to long term large purchases and a financial 'safety net'.
- **Retirement Sized Savings** in a 2-of-3 insured multi-sig vault or insured custody for long-term savings.
- **Corporate Holdings** in multi-institutional or multi-sig custody with insurance coverage.

This layering hedges against primary failure modes without excessive added complexity and biases towards a conservative holding scheme. Business use cases will vary from the above, as total volume and size of transactions become more important in managing fees, cashflow, and corporate holdings.



The Cost Curve Heuristic

When considering which tools to employ in custodying your holdings, it is helpful to employ the heuristic of the cost curve. That is, how expensive is a particular solution relative to the degree of protection against total loss. Hardware wallets often cost $80-200 each, while Casa and Unchained provide entry-level multi-signature offerings for $250 per year. AnchorWatch insurance adds ~0.4% yr. By contrast, unrecoverable loss is 100%. Viewed through that lens, you can compare the cost of a hardware wallet against the total potential loss of funds secured (and your own confidence in maintaining and ensuring custody of your keys) against various professional-grade custody solutions with various cost structures and protections.

Conclusion

Bitcoin custody has advanced in leaps and bounds from improvised paper wallets to insurance-backed, policy-driven, cryptographically verifiable vaults. This maturation is indicative of an ongoing macro trend of innovation-platform convergence, where various advancing technologies such as AI, energy, Bitcoin and freedom technologies are converging, and co-creating industry resilience. In this sense, we should expect bitcoin custody tools to leverage the state-of-the-art across all emerging domains, which is fundamentally an optimistic and empowering worldview. The pillars of Bitcoin custody and the various technical lenses, introduce a broad domain of tools and resources available to individuals, businesses, family offices, and enterprises.

Pillar take-aways:

1. **Single-Sig** remains unmatched for privacy and direct control, yet demands vigilance and user education.

2. **Multi-Sig** distributes trust by keyholder and geography, and is poised to become the de facto standard for six- and seven-figure (or greater) balances.

3. **Fully Custodial** scales user adoption but must prove reserves and maintain robust insurance to avoid FTX-style disasters.

The boundary between pillars will blur. We expect everyday wallets to embed multi-sig, privacy preserving tools, and even optional micro-insurance, making self-custody as approachable as opening a neobank app. Such tools will empower billions to hold sound money without gatekeepers and will democratize the monetary base in a truly disruptive fashion.

The core tenet of embracing solutions that uphold Bitcoin's scarcity, sovereignty, and openness, while pragmatically managing real-world risk remains as a core domain of innovation. **Whether you choose an exchange, an insured vault, or a trio of hardware devices scattered across continents, the power is now yours.**

Editor's Note

The above whitepaper is not intended as a definitive guide, but rather **a contribution to an ongoing conversation** happening in board rooms, across coffeeshop tables, and at local BitDevs. It represents one piece of signal amongst the many one should weigh when exploring solutions that best align with personal needs and circumstances. We encourage readers to treat this as a trusted and professionally reviewed input, not as an endpoint. Engage with your peers, ask questions at local meetups, and pursue independent research to develop a perspective that is both informed and personal.

Each year, as we convene at our summits, the Nashville Energy & Mining Summit, the Texas Energy & Mining Summit, the Bitcoin Payments Summit, and many more, we aim to update and refine these reports to better educate the community. **Our goal is to capture the momentum of these gatherings**, document the valuable trends and insights they surface, and to contribute to the broader effort of building resilient, practical, and forward-looking Bitcoin infrastructure.

Contributors

Thank you to our incredible Bitcoin Park community and supporters. We could not do this work without your insight and guidance. A special thank you to our expert reviewers, Steve Myers with Bitcoin Development Kit, Rob Hamilton of AnchorWatch, Tom Honzik at Unchained, Dave Schwab at Resolvr, and Brian Cubellis at Onramp.

bitcoin park

CITATIONS

1 **Allison, Ian**. "Coinbase Says It Has $255M in Insurance for Hot Wallets." CoinDesk, 2 Apr. 2019, www.coindesk.com.

2 **AnchorWatch** - "A Practical Guide to Understanding Custody Models in 2025", 2025, anchorwatch.com.

3 **ARK Invest** - "Bitcoin Custody: Securing the Future" podcast, 2023, ark-invest.com.

4 **Berwick, Angus**. "At Least $1 Billion of Client Funds Missing at FTX." Reuters, 13 Nov. 2022, www.reuters.com.

5 **Bitcoin Magazine** - Frank Corva, "Protect Your Bitcoin — And Yourself — With AnchorWatch", 28 Jan. 2025, bitcoinmagazine.com.

6 **Bitcoin Magazine** - Vivek Sen, "River Launches Proof of Reserve", 18 Sept. 2024, bitcoinmagazine.com.

7 **Bitbo** - "Unchained vs Onramp Bitcoin" comparison, 2025, bitbo.io.

8 **Blockworks - Casey Wagner**, "BitGo Broadens Insurance to Cover Over $100M", 21 Apr. 2021, blockworks.co.

9 **CoinDesk** - Anita Posch, "Best Self-Custody Lightning Wallet?", 26 Jan. 2024, coindesk.com.

10 **CoinDesk** - Frederick Munawa, "Strike Moves Custody In-House", 9 June 2023, coindesk.com.

11 **CoinDesk** - Ian Allison, "$255 Million: Coinbase Insurance Coverage", 2 Apr. 2019, coindesk.com.

12 **Corva, Frank**. "Protect Your Bitcoin—And Yourself—With AnchorWatch." Bitcoin Magazine, 28 Jan. 2025, bitcoinmagazine.com.

13 **Cubellis, Brian**. Multi-Institution Custody Explained. Onramp Bitcoin Education, 7 Feb. 2024, https://onrampbitcoin.com/education/multi-institution-custody-explained.

14 **Cubellis, Brian**. Why Multi-Institution Custody Is the Missing Piece. Onramp Bitcoin Education, 13 Feb. 2024, https://onrampbitcoin.com/education/why-multi-institution-custody-is-the-missing-piece

15 **Cubellis, Brian**. The Evolution of Bitcoin Custody. Onramp Bitcoin Education, 13 Aug. 2024, https://onrampbitcoin.com/education/the-evolution-of-bitcoin-custody.

16 **"Custody FAQ."** Coinbase, Coinbase, Inc., 2025, www.coinbase.com/en-gb/custody/faq.

17 **Fedimint** documentation and website, fedimint.org.
18 **Gemini** – Yusuf Hussain, "Gemini Launches Captive Insurance… $200M Coverage", 16 Jan. 2020, gemini.com.
19 **Honzik, Tom, and Stephen Hall**. "Bitcoin Self-Custody Approaches Compared." Unchained, Unchained Capital, Inc., 2025, www.unchained.com/features/singlesig-vs-multisig.
20 **Honzik, Tom.** "Multisig, Shamir's Secret Sharing, & MPC Compared." *Unchained*, Unchained Capital, Inc., 2025, www.unchained.com/features/mpc-vs-multisig-vs-sss.
21 **Honzik, Tom**. "Multisig, Shamir's Secret Sharing, & MPC Compared." Unchained, Unchained Capital, Inc., 2025, www.unchained.com/features/mpc-vs-multisig-vs-sss.
22 **Hussain, Yusuf**. "Gemini Launches Captive Insurance Company to Increase Digital-Asset Coverage." Gemini Blog, 16 Jan. 2020, www.gemini.com.
23 **Mikalic, Jackson**. How Does Multi-Institution Bitcoin Custody Work? Onramp Bitcoin Education, 14 May 2025, https://onrampbitcoin.com/education/how-does-multi-institution-bitcoin-custody-work.
24 **Munawa, Frederick**. "Strike Brings Custody In-House After Prime Trust Issues." CoinDesk, 9 June 2023, www.coindesk.com.
25 **Nunchuk**. Miniscript 101: A Technical Guide. Nunchuk Blog, 19 Mar. 2023, https://nunchuk.io/blog/miniscript101.
26 **Reuters** – Angus Berwick, "At least $1 billion of client funds missing at FTX", 13 Nov. 2022, reuters.com.
27 **Sen, Vivek**. "River Financial Introduces Monthly Proof-of-Reserve Audits." Bitcoin Magazine, 18 Sept. 2024, bitcoinmagazine.com.
28 **Shapiro, Zack, and Zack Cohen**. State-Level Strategic Bitcoin Reserve Toolkit. Bitcoin Policy Institute – Future of Money Series, 9 July 2025, https://www.btcpolicy.org/articles/state-level-strategic-bitcoin-reserve-toolkit.
29 **The Data Accuracy Flywheel: How Chainalysis Consistently Identifies and Verifies Blockchain Entities**. Chainalysis Blog, 16 Jan. 2024, Chainalysis Team, chainalysis.com/blog/chainalysis-data-accuracy/.
30 **Wagner, Casey**. "BitGo Broadens Insurance Coverage to $700 Million." Blockworks, 21 Apr. 2021, blockworks.co.