

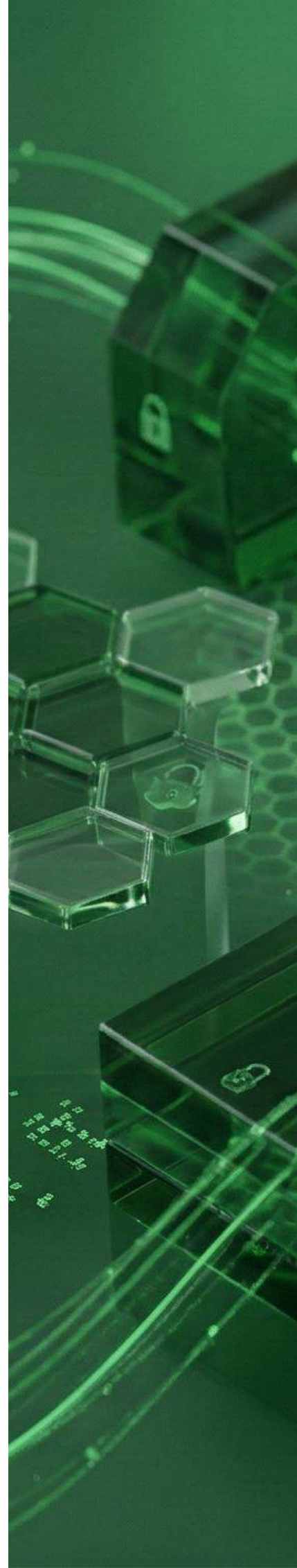
# The Future of Self-Custody: Turning Ownership Into Security

Cointelegraph Research Report



# Content

|                                                            |    |
|------------------------------------------------------------|----|
| <b>Introduction</b>                                        | 03 |
| <b>The Reckoning with Custodial Risk</b>                   | 04 |
| <b>Investor Sentiment</b>                                  | 06 |
| <b>Modern Wallet Architecture</b>                          | 10 |
| <b>Threat Modelling and<br/>Real-World Vulnerabilities</b> | 14 |
| Compromised Host Devices                                   | 14 |
| Phishing and Fake Firmware Updates                         | 15 |
| Device Trust Limits                                        | 15 |
| Theft, Temporary Access, and Evil Maid Attacks             | 18 |
| Physical Extortion and Coercion                            | 19 |
| <b>Backup and Recovery Mechanisms</b>                      | 20 |
| <b>Future Outlook</b>                                      | 23 |
| <b>Disclaimer</b>                                          | 24 |



# Introduction

---

The foundational promise of cryptocurrency is decentralized, sovereign ownership. Digital assets can be held and transferred without intermediaries, permissions, or identity-based controls. Yet, for many years, the industry operated on the implicit assumption that centralized exchanges or custodians could be trusted to safeguard assets for both retail and institutional users. A series of catastrophic collapses and high-profile security breaches over the past few years has forced a critical reckoning with this custodial risk.

Consequently, retail users and institutions alike have increasingly migrated their assets from exchanges to self-custody wallet infrastructure for greater security and control. A properly managed wallet does not require KYC to receive, hold, or transfer funds. There is no account to freeze, no counterparty to compel, and no withdrawal policy to change.

While a wide range of self-custody configurations exists, hardware wallets have emerged as the default endpoint for long-term asset storage among retail users. They strike a practical balance between security, usability, and operational simplicity, and are typically the first self-custody tool users adopt once assets leave centralized platforms.

This report examines 375 survey responses from Cointelegraph's audience to examine how investors conceive of crypto custody in 2025 and how the erosion of trust in exchanges has reshaped behavior. It examines modern wallet architectures, the threat models hardware wallets are designed to address, and the real-world failure modes that continue to cause losses even after users take custody of their keys.



# The Reckoning with Custodial Risk

The most devastating collapses, including those of FTX, Celsius Network, Mt. Gox, and QuadrigaCX, were primarily due to breaches of fiduciary trust, resulting from either internal fraud or extreme operational negligence (*Table 1*).

Mt. Gox, which once handled over 70% of all Bitcoin transactions worldwide, ceased operations in 2014 after revealing the loss of 750,000 of its customers' Bitcoin and about 100,000 of its own, totaling about 7% of the BTC supply at the time. Most or all of these funds were stolen from the Mt. Gox hot wallet over time, beginning in late 2011. These losses were due to a bug in the withdrawal mechanism, which ignored Bitcoin's transaction malleability. This collapse and the subsequent arrest of CEO Mark Karpelès for fraud and embezzlement led Japan to create the first formal regulations for cryptocurrency exchanges.

**Table 1: Crypto's Biggest Collapses: How Much Was Lost, And What Was Recovered**

| Collapse   | Approx. Loss Amount                  | Approx. Recovery by Customers                                                                                       | Recovery Status                                                                                  |
|------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Mt. Gox    | ~ 850,000 BTC<br>(~US\$450M at time) | ~ 141,000 BTC recovered<br>to distribute<br>(~US\$8-9B at current value)                                            | Recoveries are ongoing;<br>the value of BTC has<br>surged since the time<br>of loss              |
| QuadrigaCX | ~\$169M shortfall noted              | C\$902,743 (~US\$700K+) recovered<br>from hot wallets                                                               | The majority of funds<br>are inaccessible<br>(cold wallets lost)                                 |
| FTX        | ~\$8 billion customer<br>hole        | ~\$16.3 billion in assets recovered<br>reported; plan to repay most<br>customers ~118% of claim for small<br>claims | Recovery includes asset<br>value increase; full<br>repayment is still<br>contingent on processes |

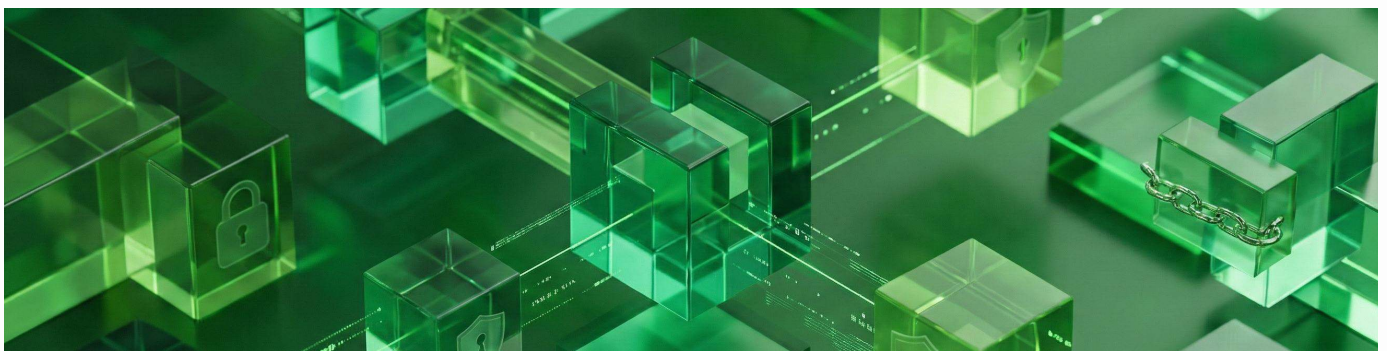
Source: Cointelegraph Research



[QuadrigaCX](#), formerly Canada's largest cryptocurrency exchange, collapsed in early 2019 after the death of its founder, [Gerald Cotten](#). The platform failed because Cotten was the only person who held the passwords to the offline cold wallets where the majority of customer funds were supposedly stored. His death in December 2018 thus rendered \$250 million inaccessible. Subsequent [review](#) by the Ontario Securities Commission concluded that Quadriga was a fraud and a Ponzi scheme. Cotten created accounts under aliases, credited himself with fictitious crypto balances, and traded them against unsuspecting clients. His subsequent trading losses were covered with deposits from new clients, resulting in a shortfall of approximately \$169 million. The company operated without internal controls or adequate books and records, which facilitated Cotten's large-scale fraud without detection.

The most disastrous exchange collapse was the [downfall of FTX](#) in November 2022, which exposed an \$8 billion hole in its accounts. FTX was the third-largest exchange by volume at the time. Executives, led by [CEO Sam Bankman-Fried](#), lent more than half of their customers' funds to their affiliated trading firm, [Alameda Research](#), which explicitly violated FTX's terms of service. Following an [article published by CoinDesk](#) that exposed the financial relationship and holdings of FTX's proprietary token (FTT) on Alameda's balance sheet, customer withdrawals spiked, which led to a liquidity crisis that ultimately contributed to FTX's bankruptcy.

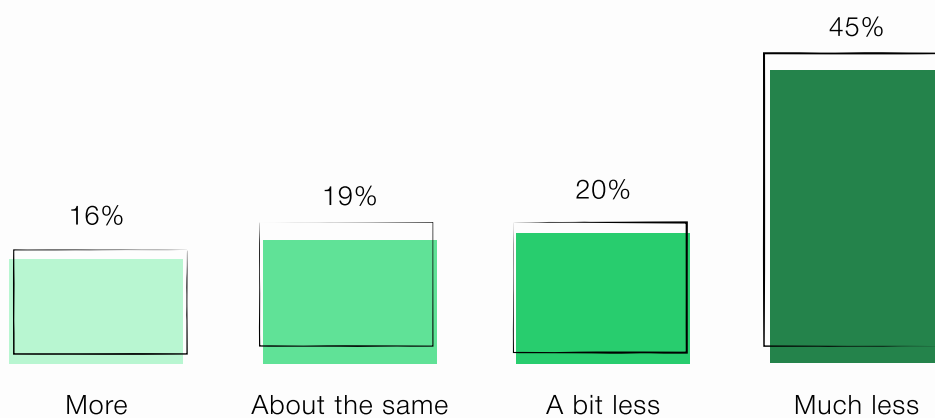
Similar incidents have continued to surface across both large and mid-sized exchanges because centralized custodians are structurally attractive targets. They aggregate vast pools of liquid assets behind a small number of operational, administrative, and key-management control points. For attackers, the payoff profile is asymmetric. A single successful breach can yield hundreds of millions of dollars, while targeting individual self-custody users is slower, more fragmented, and far less predictable. As long as custody remains concentrated at scale, centralized exchanges remain rational, high-value targets for sustained and well-resourced adversaries.



# Investor Sentiment

These repeated failures have fundamentally altered how investors perceive custodial trust. When respondents were asked to define custody in 2025, their answers reflected a pronounced erosion of confidence in centralized entities. A majority reported trusting centralized exchanges either much less (45%) or a bit less (20%) than they did ~4 years ago.

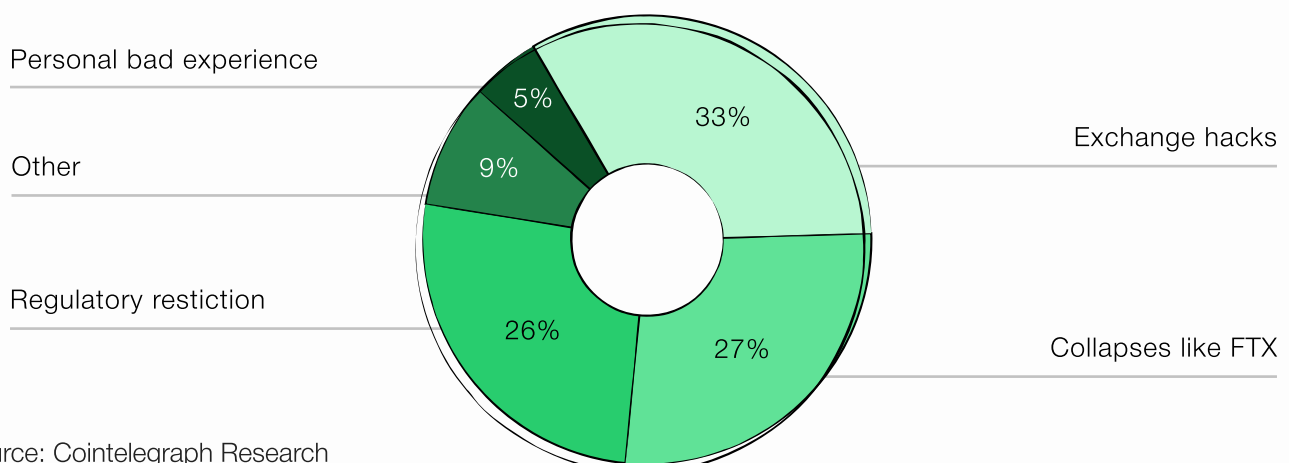
**Figure 1: Change In Trust In Centralized Exchanges Since 2022**



Source: [Cointelegraph Research](#)

The three primary catalysts behind this shift in user psychology were exchange hacks (33%), regulatory restrictions (26%), and major collapses such as FTX (27%).

**Figure 2: What Has Been The Biggest Catalyst For A Decrease In Your Trust In Centralized Exchanges?**



Source: [Cointelegraph Research](#)



Concerns that future regulation, compliance, and enforcement could restrict access to funds remain a salient threat. When authorities instruct exchanges to suspend withdrawals, restrict access, or impose compliance measures on custodial platforms, users recognize that their ability to move their own funds is contingent on external decisions as long as they are on an exchange. The more tightly custodial services are governed, the more users confront the reality that they do not control their keys unless they take self-custody.

**Table 2: Historical Precedents Of Custodial Access Restrictions Triggered By Regulation Or Enforcement**

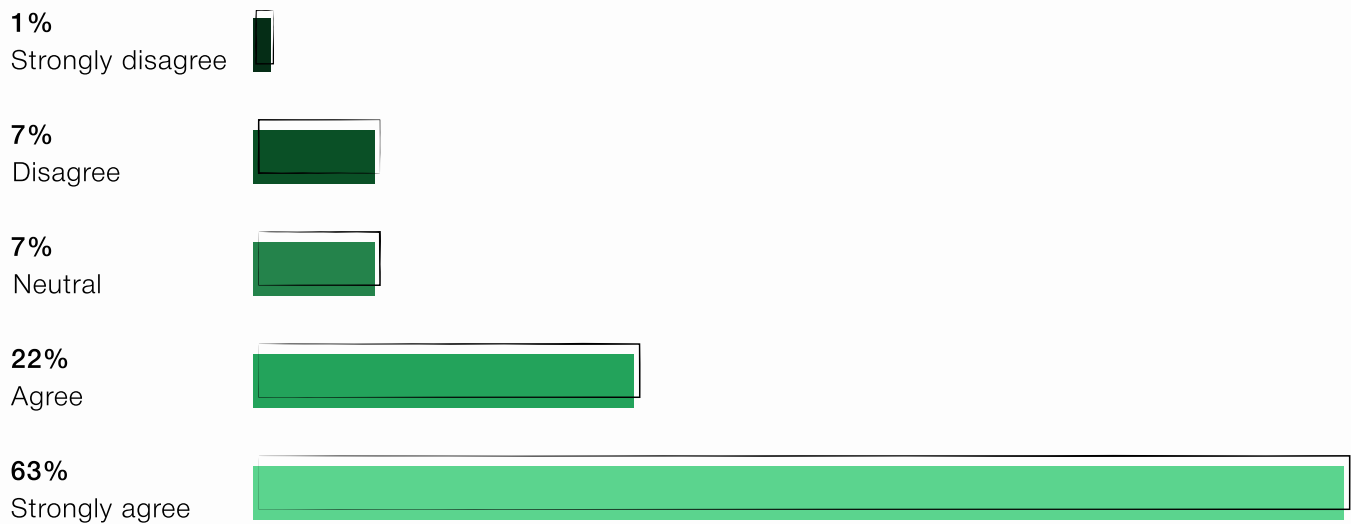
| Year | Jurisdiction               | Authority action                                                                                                                                                       | Custodial constraint                                                                                                                           |
|------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 2013 | United States              | U.S. authorities obtained a <u>seizure warrant</u> and seized funds tied to Mt. Gox's U.S. payment rails ( <u>Dwolla/Mt. Gox-linked accounts</u> ) under an AML theory | Disrupted ability to move funds through regulated rails                                                                                        |
| 2017 | China                      | <u>Chinese authorities ordered Beijing-based crypto exchanges to halt trading and notify users of closure</u>                                                          | Forced platform shutdown and user migration; custodial services become non-operational under policy pressure (cold wallets lost)               |
| 2018 | India                      | RBI circular prohibited regulated entities <u>from providing services to virtual-currency businesses</u>                                                               | Fiat on/off ramps for exchanges cut off by regulator order                                                                                     |
| 2022 | Canada                     | <u>Emergency Economic Measures Order</u> expanded AML/ATF obligations and enabled financial restrictions during the <u>Emergencies Act period</u>                      | Financial institutions could restrict/freeze access to funds linked to designated activity; crypto explicitly within scope (cold wallets lost) |
| 2022 | European Union             | <u>EU sanctions package extended restrictions to crypto wallets/deposits; exchanges required to enforce measures</u>                                                   | Exchanges restricted or deactivated accounts and limited services in line with sanctions (cold wallets lost)                                   |
| 2022 | Bahamas / global spillover | <u>FTX suspended withdrawals</u> "until further notice" as the collapse unfolded                                                                                       | Users lost the ability to withdraw on demand; access became contingent on the bankruptcy proceedings (cold wallets lost)                       |
| 2024 | Canada                     | <u>Canadian authorities seized TradeOgre as part of a law-enforcement action</u>                                                                                       | Exchange operations halted; users lost access to custodial accounts pending legal proceedings                                                  |

Source: Cointelegraph Research



This crisis of confidence has reinforced the fundamental ethos of cryptocurrency: “Not your keys, not your coins.” The vast majority of respondents either strongly agreed (63%) or agreed (22%) with this principle, which signals a decisive return to the ideals of self-sovereignty.

**Figure 3: Do You Agree With The Phrase “Not Your Keys, Not Your Coins”?**



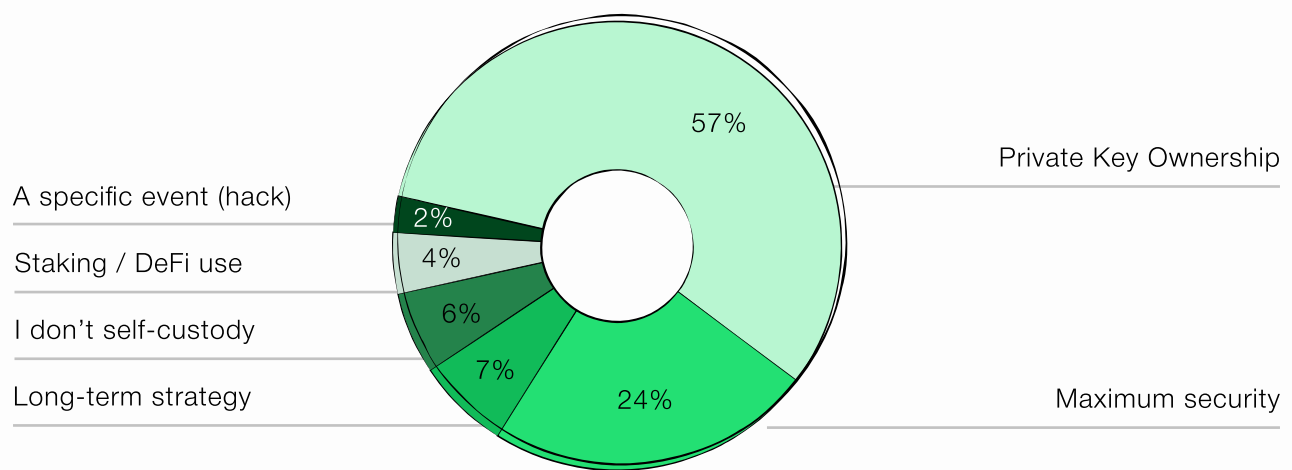
Source: [Cointelegraph Research](#)

Frameworks such as the [EU's Markets in Crypto-Assets Regulation \(MiCA\)](#) may improve operational standards for custodial service providers, but they do not change the underlying structure of custody. Consequently, retail users have increasingly migrated their assets from exchanges to self-custody wallet infrastructure to gain greater security and full control of the funds.

In our survey, a majority of respondents cited the direct ownership of private keys as their primary motivation (57%), followed by the pursuit of maximum security and reduced counterparty exposure (24%).



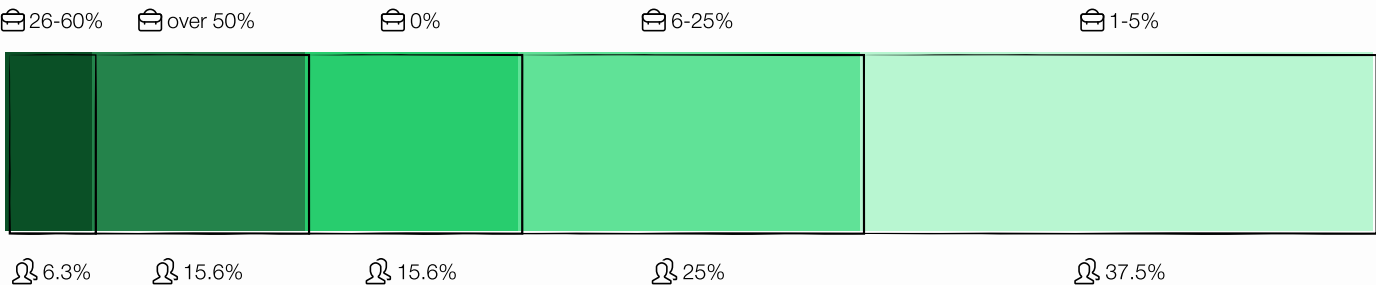
Figure 4: If You Use Self-Custody, What’s The Main Reason?



Source: [Cointelegraph Research](#)

This preference translates into concrete risk tolerance, as most respondents reported that they would not leave their portfolio on a custodial exchange for longer than one month, even in the absence of immediate distress.

Figure 5: What % Of Your Portfolio Would You Leave On An Exchange For More Than 1 Month?



Source: [Cointelegraph Research](#)



# Modern Wallet Architecture

---

Once assets leave custodial platforms, responsibility for key management is entirely with the user. Modern wallets can be classified along several dimensions, but for practical purposes understanding the distinction between hot wallets and cold wallets is most important.

A hot wallet is a setup in which private keys are stored in software running on a general-purpose device, such as a smartphone or personal computer, that is designed to run many different applications and is directly connected to the internet. They are most convenient for moving small balances or making frequent interactions. A cold wallet, on the other hand, features a separate key storage and signing device that is not connected to the internet. For the retail use case, this device is usually a hardware signer, commonly called a hardware wallet. As off-the-shelf consumer hardware, these devices trace back to 2014, when Trezor introduced its first product, the [Model One](#), to the market. The product interaction model it established quickly became the inspiration for an entire industry, as hardware wallets are better suited for serious, long-term custody, particularly for larger balances. Survey data shows that 36% of respondents report active hardware wallet usage, indicating that a substantial share of users already treat hardware-enforced key isolation as the baseline for asset protection.

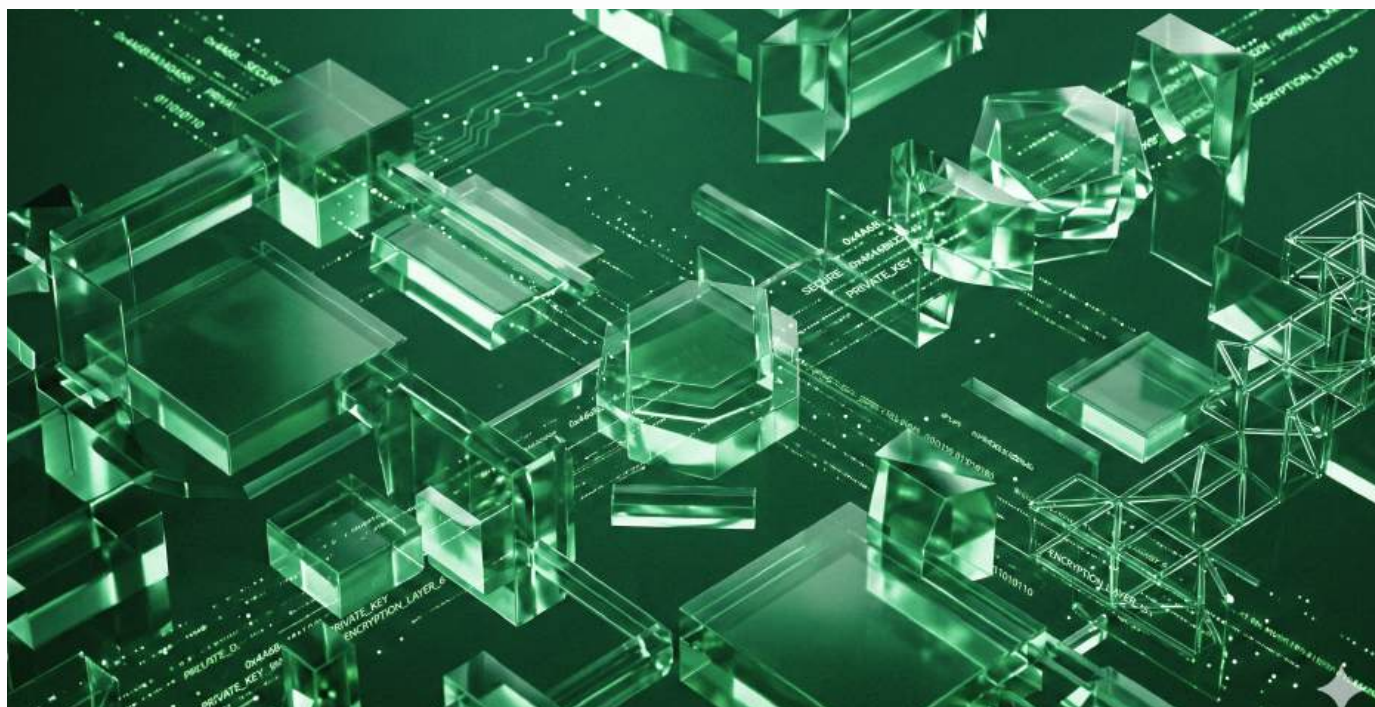
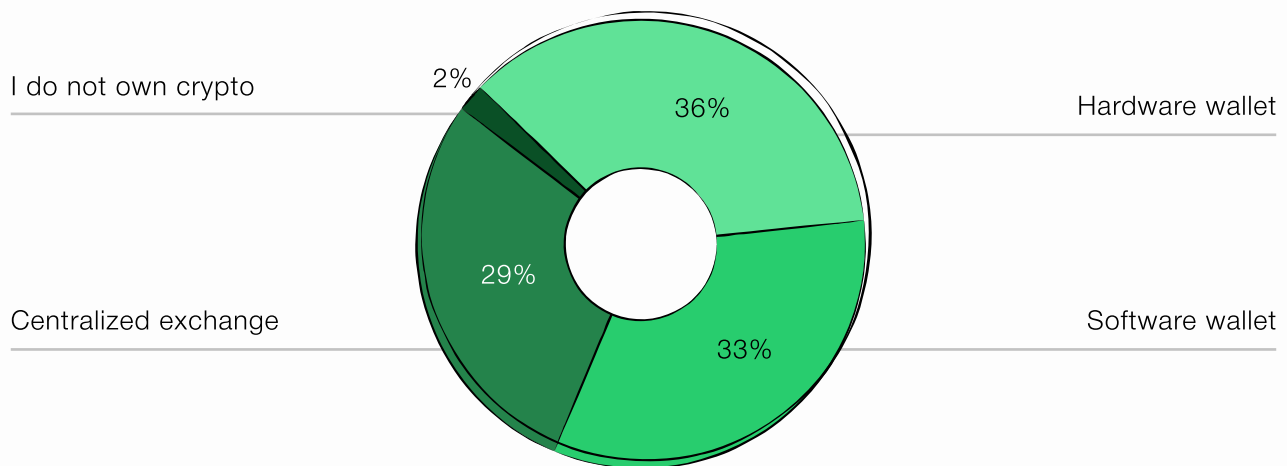


**Figure 6: What Custody Methods Are You Using?**



Source: [Cointelegraph Research](#)

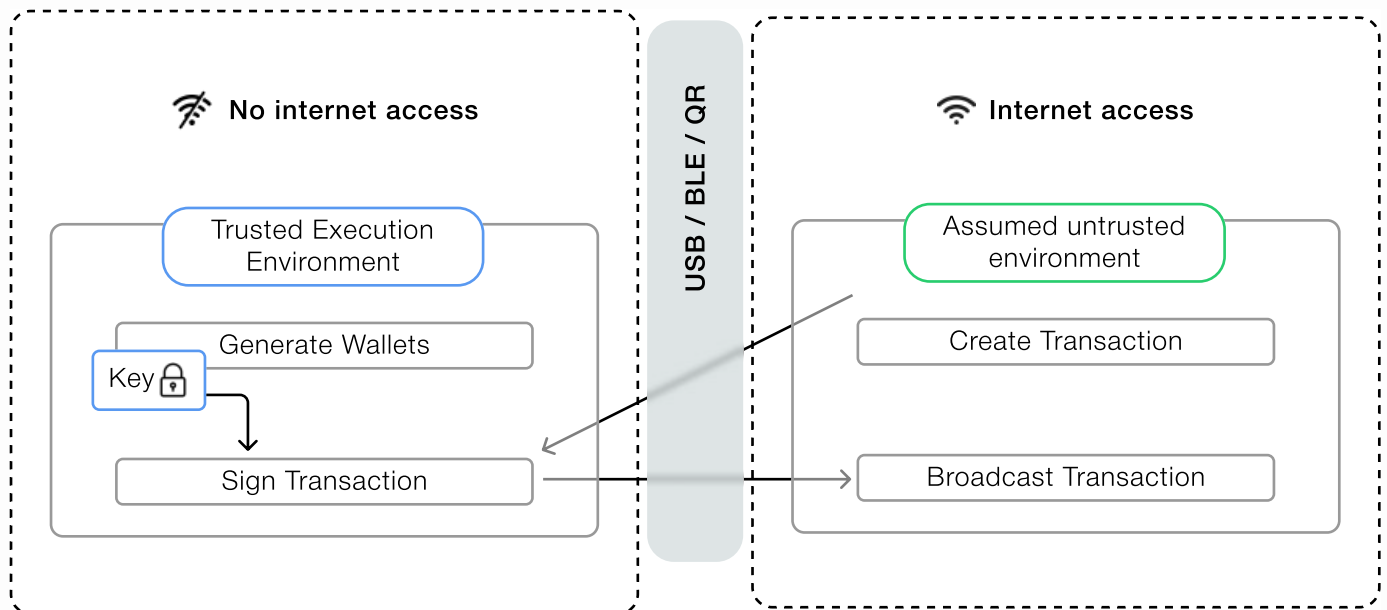
Hardware wallets split the transaction lifecycle into two distinct stages. First, the host machine assembles an unsigned transaction that specifies the intended transfer or contract interaction. The unsigned transaction is then transferred to the hardware wallet, typically via USB, Bluetooth, NFC, or QR code. The hardware wallet parses the transaction structure and displays a subset of critical fields on its own trusted screen. The user is required to physically confirm the transaction on the device before a signature is generated. Only upon explicit user approval does the hardware wallet cryptographically sign the transaction internally and return the signature to the host for broadcast.

This architecture prevents a compromised computer from directly stealing private keys, because the keys never leave the hardware wallet. It is reinforced by a Secure Element. A Secure Element is a dedicated security chip designed to protect the keys tied to wallet control. This includes the seed-phrases and the signing keys used to authorize transactions. The chip is engineered to resist invasive and semi-invasive extraction techniques that target standard microcontrollers, such as direct memory reads, probing internal buses, and fault-injection methods that try to glitch the device into revealing data.

However, it does not eliminate all risk. The protection offered by a hardware wallet depends on the user verifying that the transaction displayed on the device matches their intent, rather than blindly approving signing requests generated by an untrusted host.



**Figure 7: Basic Cold Wallet Schematic**



Source: [Cointelegraph Research](#), [Shahriar Ebrahimi Et.al](#)

The effectiveness of on-device verification varies significantly by network. Bitcoin transactions are comparatively straightforward to verify because they consist mainly of input and output addresses and amounts. A user can visually compare the address shown on the hardware wallet against the expected recipient. UTXO consolidations and self-transfer are generally recognized by the wallet as transactions that do not change the wallet balance apart from a fee.

By contrast, many Ethereum transactions authorize smart-contract interactions rather than simple ETH balance transfers. In these cases, the transaction's behavior is defined by calldata, which is binary data that encodes function calls and parameters. While hardware wallets typically display this calldata (Figure 8), it is not human-readable in raw form and does not meaningfully convey intent without additional analysis. Historically, fully interpreting calldata — and especially simulating the outcome of a smart-contract call — has been challenging for hardware wallets. Doing so would require access to contract data such as addresses, ABIs, and versioned logic, as well as the ability to reason about its execution.

Hardware wallets have focused on what they can guarantee today: signature integrity and strong key isolation. They can ensure that a transaction was authorized by the correct key, but they cannot always ensure that the user fully understands the downstream effects of a smart-contract interaction at signing time.



### Figure 8: Example Of Structured Transaction Data Displayed On A Hardware Wallet



Source: Ethereum Magicians

Generating a signature without understanding or independently verifying the smart contract call that it invokes is commonly referred to as blind signing. In early 2024, [Bybit became a victim of this](#), as its signers authorized malicious contract interactions without fully understanding the calldata they were signing, resulting in a \$1.4B loss. Mitigating this risk for Ethereum usage requires an additional verification step outside the hardware wallet. Practically, this means extracting the calldata from the software wallet, decoding it on a separate trusted device using a dedicated [decoder](#), and confirming that the decoded function calls and parameters match the intended action. [Transaction simulator tools](#) can also be used to preview execution outcomes before approval. The calldata that was fed into the decoding tool must then be cross-checked against what the hardware wallet displays at signing time. Users should also maintain a printed reference of smart contract addresses they commonly interact with and compare them directly against what the hardware wallet displays at signing time. This approach restores intent verification without relying on the compromised host.

However, this transaction verification flow is likely not a permanent limitation. Clear-signing approaches and improved transaction transparency for smart-contract interactions are an active area of development across the hardware wallet ecosystem.

# Threat Modelling and Real-World Vulnerabilities

---

Hardware wallets are widely regarded as one of the strongest security models available for self-custody. However, self-custody by definition places ultimate responsibility with the user. No device can remove that entirely. This section, therefore, maps the remaining risk surface: which threats hardware wallets are designed to mitigate, where their protections are strongest, and where user discipline and operational practices remain essential.

## Compromised Host Devices

The primary threat hardware signers were built to confront is a compromised desktop or mobile device. A software wallet running on a computer or phone can be emptied if an attacker gains remote access, installs a keylogger, or tampers with local files. Careless users sometimes even store recovery phrases in plain text, which makes theft trivial once the system is breached. Browser-based wallets can be vulnerable to JavaScript exploits and compromising a browser may at times be easier than taking over the entire operating system. Hardware wallets address most vulnerabilities associated with personal computers by confining the private keys and signing operations to a dedicated device that cannot be accessed directly through the host.

A securely designed hardware wallet prevents keys from being exported through USB or other interfaces, and the device's screen allows the user to verify recipient addresses independently of what the compromised computer displays. This neutralizes the majority of risks from remote compromise. However, if a user copies a spoofed deposit address for an exchange from a phishing page or a man-in-the-middle proxy, the hardware wallet will display the identical address and allow the user to sign the transaction. Nothing about the recipient address, per se, can indicate that it is fraudulent.



# Phishing and Fake Firmware Updates

Adversaries impersonate hardware wallet manufacturers with emails that closely resemble legitimate communications, using subtly altered domains, misspellings, or cloned interfaces to appear authentic. The objective is to induce urgency and trick users into revealing their recovery phrase. Typical messages will claim that a device requires an immediate security update, that funds are at risk, or that a wallet must be “verified” following a breach. These prompts often redirect users to fake apps or websites that request recovery seeds. Legitimate support workflows never request recovery seeds, passphrases, or private keys. Firmware updates do not require entering a seed into a website, email form, or third-party application. Any prompt that asks for recovery material outside of the device itself is malicious. Firmware updates should only be initiated through the official companion application and sourced directly from the manufacturer. Users should independently verify domains, avoid links embedded in emails or social media messages, and treat unsolicited update prompts as hostile by default.

## Device Trust Limits

Users who think adversarially tend to want to minimize trust not only in software but also in the hardware wallet manufacturer, the firmware distribution process, and the shipping and supply chain. From this perspective, the goal is not to eliminate trust entirely, but reduce how much trust must be placed in any single actor. This is why some users prefer designs that allow for inspection, verification, and independent scrutiny where feasible.

Meaningful verification is far more achievable at the software layer than at the hardware layer. At the software layer, open-source firmware allows independent experts to inspect how keys are generated, stored, and used, rather than relying solely on vendor assurances. However, source availability alone is insufficient. If firmware builds are not reproducible, most users must still trust that the manufacturer compiled and distributed the correct code, since compiling locally will produce a binary with a different hash and no vendor signature.

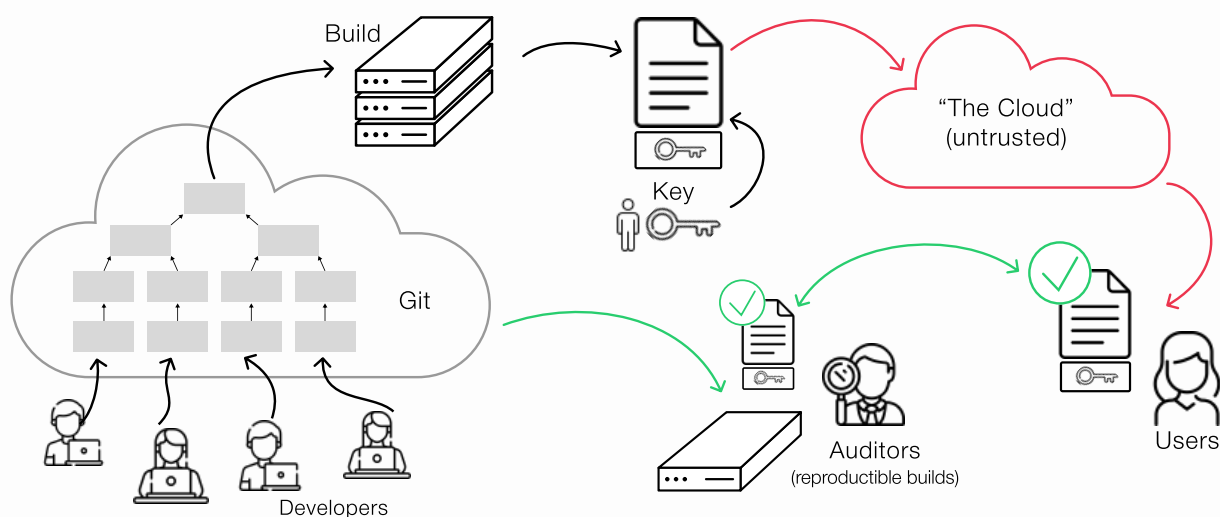
When a firmware build process is reproducible, third parties can independently compile the firmware and confirm that the resulting binary matches the hash of the manufacturer-distributed release.



This significantly reduces software supply-chain risk by making it far more difficult to introduce malicious code during compilation or distribution without detection. In practice, only a small subset of users will perform this verification themselves, but the existence of reproducible builds enables independent auditors and security researchers to do so on behalf of the wider user base.

These mechanisms primarily address software supply-chain risk. They help reduce the chance that malicious code is introduced during development, compilation, or distribution. They do not, however, guarantee that a physical device corresponds exactly to its published specifications, nor can they fully secure the manufacturing and delivery process end to end. This distinction between software trust and hardware trust is often blurred, but it is critical (*Figure 9*).

**Figure 9: The Trust Gap In Software Verification**



Source: [Can We Build Trustable Hardware?](#) — Andrew Huang

Hardware verification presents a fundamentally different problem. Even when hardware designs are published openly, users have limited ability to confirm that the device they receive was fabricated, assembled, and delivered exactly as intended. Hardware supply chains involve many independent actors — including chip manufacturers, PCB assemblers, distributors, and logistics providers — each of which introduces additional attack surface.

This asymmetry between software and hardware verification has been emphasized by [Andrew Huang](#), a hardware hacker and security researcher best known for [his work on hardware trust](#), reverse engineering, and supply-chain risk. [Huang argues](#) that while software can be verified cryptographically, hardware verification relies on physical inspection, simplicity, and tamper evidence rather than formal proofs.



There are efforts that move closer to this ideal. For example, [Foundation devices](#) allow users to source components or assemble parts of the device themselves. Other research efforts, including [Huang's work with programmable FPGA-based systems](#), explore designs that reduce reliance on opaque silicon. More recently, Trezor Safe 7 integrates the [TROPIC01](#) secure element, which is designed to be auditable at the design level and improves verifiability deeper in the hardware stack, including at the secure element layer. However, these approaches do not eliminate trust in semiconductor fabrication, nor have they been widely adopted in consumer hardware wallets due to cost, complexity, and usability constraints.

While there are no confirmed cases of successful compromises occurring upstream at major hardware wallet manufacturers, attacks at the distribution stage are well documented across multiple brands. In one widely reported [case covered by CoinDesk](#), scammers sent fake Ledger devices that included modified hardware and instructions prompting users to enter their 24-word recovery phrase into malicious software. Kaspersky also [documented](#) similar counterfeit activity where attackers sold Trezor devices that had been modified to leak recovery material after setup. More commonly, users have been scammed by purchasing devices from secondary marketplaces that arrived with pre-generated seed phrases, a known attack vector highlighted repeatedly by [Ledger](#) after victims unknowingly restored wallets already controlled by attackers.

These incidents buttress the fact that the final link in the supply chain, from manufacturer to end user, remains a critical attack surface. However, modern hardware wallet designs have introduced stronger countermeasures via the aforementioned secure elements that authenticate firmware cryptographically, and make firmware-level counterfeiting significantly more difficult than in earlier hardware iterations. While this does not eliminate distribution-stage risk, it raises the technical bar for attackers and shifts most observed exploits toward social engineering rather than silicon-level compromise.

Operational guidance, therefore, remains that devices should be sourced directly from the manufacturer or from [officially recognized distribution channels](#). Any device that arrives with a pre-generated seed phrase, altered packaging, or irregular setup flow should be treated as compromised. Users must generate recovery material themselves during device initialization and never input an existing seed phrase provided by a third party.



# Theft, Temporary Access, and Evil Maid Attacks

This class of threats involves theft or temporary access without the owner's knowledge. Device-level PINs are designed to prevent unauthorized access to the wallet interface and signing functionality, and most hardware wallets enforce exponential back-off or data wipes after repeated failed attempts. These controls make casual brute-force attacks impractical, but their protection should not be viewed as absolute. In devices without a Secure Element, PIN protections have been bypassed through hardware extraction and fault attacks, and even hardened designs may degrade over time as techniques improve. Wired reported such a vulnerability for the KeepKey hardware device in 2020. In these cases, side-channel and fault-injection techniques allowed attackers to recover PINs without breaking the underlying cryptography. For this reason, loss or theft of a hardware wallet should always be treated as a security incident, and funds should be migrated to a new seed as soon as possible.

Crucially, the device PIN protects access to the hardware, not the recovery seed. Anyone in possession of the recovery seed can restore the wallet on another device regardless of the PIN, which means the PIN mitigates physical access risk but does not secure funds independently of backup material.

A different and more subtle risk arises when an attacker gains brief access while the owner is absent but does not appear to steal the device. This is commonly referred to as an evil maid attack. In this scenario, the adversary tampers with the device or replaces it with a facsimile designed to capture PINs or the passphrase to the wallet at a later time. Some hardware wallets implement mitigations against this class of attack. For example, the Coldcard Q displays anti-phishing words derived from the device and the first half of the PIN, allowing the user to detect device substitution before entering the full PIN. Trezor also allows visual personalization, such as custom boot screens, to help users recognize their own hardware.



# Physical Extortion and Coercion

Break-ins, physical coercion, and kidnappings have increasingly targeted crypto holders because transferring funds onchain does not involve the oversight and friction of bank transfers. [Publicly documented cases](#) show 74 publicly reported physical attacks in 2025 alone, with at least 9 incidents already recorded in January 2026. The number of incidents that have not circulated through the press is likely higher.

Both figures should be treated as lower bounds, as many attacks across multiple jurisdictions are never reported, and the dataset is non-exhaustive. However, visibility consistently appears as a risk amplifier. The presence of a hardware wallet, its packaging, or public disclosures of holdings, whether on social media or within friend groups, can mark someone as a target.

Some wallets attempt to mitigate coercion risk through BIP-39 passphrases. A BIP39 passphrase is an optional, user-defined word or phrase added to the 12 or 24-word mnemonic seed phrase to create a completely separate "hidden" wallet. Entering the seed without the correct passphrase reveals only the decoy wallet with a small amount of funds. When such passphrases are used, backups should be stored across multiple locations and recorded on durable media. However, passphrases introduce an additional secret that must be preserved perfectly. Forgotten, misrecorded, or inadequately backed-up passphrases result in irreversible loss even when the seed phrase itself is intact, and are therefore discouraged by several researchers who track real-world loss data.

Other devices also attempt to mitigate coercion risk through explicit duress controls, such as duress PINs or “brick” functions that either reveal a low-balance wallet or render the device temporarily unusable. This approach was first formalized in consumer hardware wallets by [Coldcard](#), but other hardware wallet platforms, including Trezor, have increasingly supported the feature.

Duress PINs can provide plausible deniability for the existence of further funds, but they also introduce a darker game-theoretic problem: If an attacker suspects hidden wallets exist, they may escalate pressure indefinitely. When the device becomes unusable through a brick pin and no backup is accessible on-site, the attacker may be convinced that immediate access has been lost. Depending on situational context, this could thwart the attack or create an incentive for prolonged coercion or hostage taking. In practice, discretion about holdings remains the strongest defense against physical extortion.



# Backup and Recovery Mechanisms

---

Loss of access to a hardware wallet does not occur only through theft. Loss and theft are common, but they are not the only failure modes. Hardware wallets are electronic devices, and like all electronics, they degrade. Exposure to moisture, dust, physical stress, and repeated thermal cycles weakens solder joints and electrical components over time. Because the current generation of hardware wallets has not existed long enough, the typical time-to-failure for devices purchased today remains unknown. Environmental events such as fires, floods, storms, and earthquakes can also permanently destroy a device and any keys stored on it.

A substantial portion of the cryptocurrency supply has already been lost due to inadequate backup practices. According to [data from Bitbo](#) and [Glassnode](#), coins not moved in over ten years sit near roughly 15–18% of supply. An estimated 5–7% percentage of this is attributable to the original coins mined by Satoshi Nakamoto. Even after excluding those coins, it is likely that around 10% of the circulating supply has been lost, primarily because users lost recovery seeds or failed to maintain durable backups.

Recovery seeds exist as a last line of defense in the event that a hardware wallet is lost, damaged, or destroyed. They are not meant to be used routinely, but they must work reliably when needed. Users should familiarize themselves with the recovery process and perform a dry run before trusting a backup. At the same time, a recovery seed should not automatically grant full access in all cases.

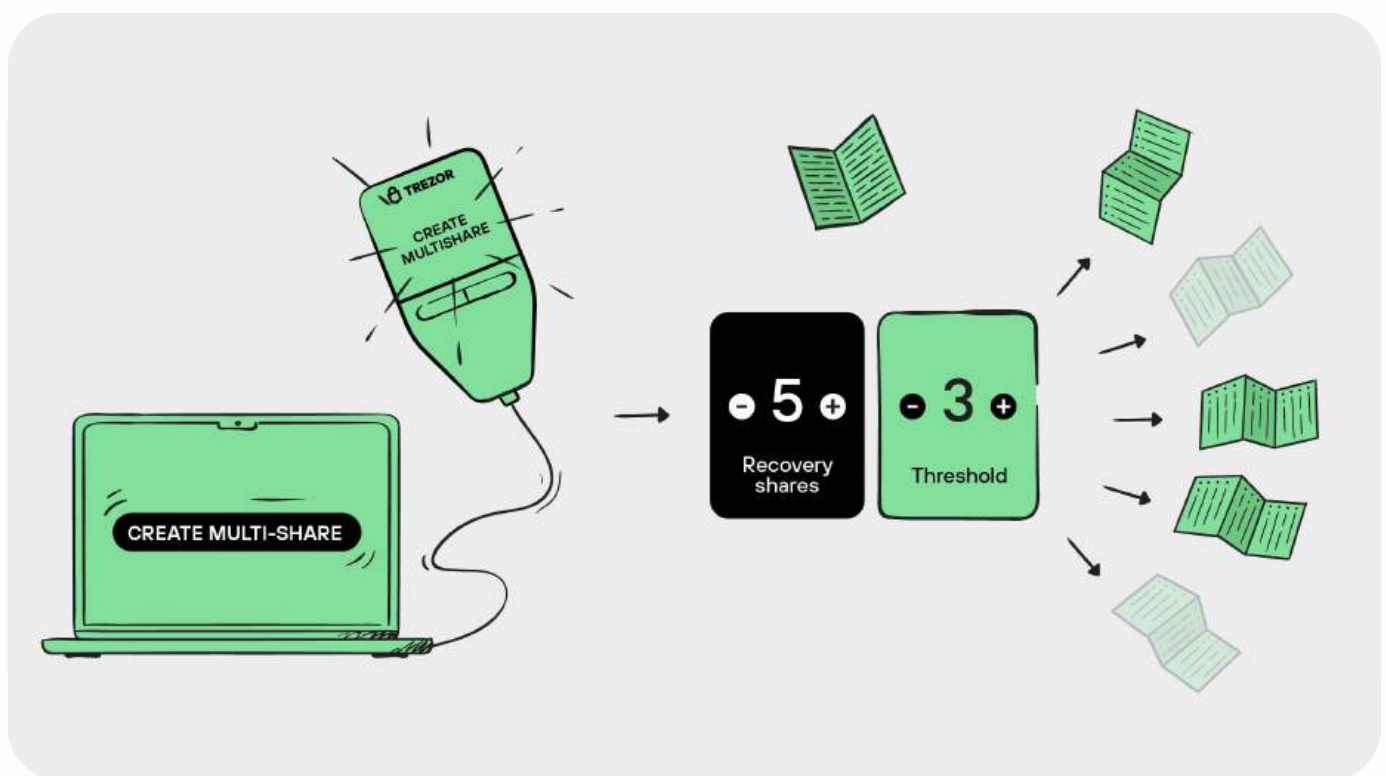
However, funds are protected only by possession of the recovery seed; backups can become a liability rather than a safeguard. Secure elements, tamper-resistant enclosures, and other device-level protections provide little value if the recovery seed is stored in the same location as the hardware wallet and no additional authentication is required. This is where additional access controls, such as BIP-39 passphrases, play a role. When such passphrases are used, backups of the passphrase should be stored across multiple locations and recorded on durable media.



However, this added protection could increase complexity and complicate inheritance or emergency recovery. For some users, especially those prioritizing simplicity or estate planning, storing an unencrypted seed in a secure, insured location such as a bank deposit box may represent a more appropriate balance between security and accessibility. There is no universally “safe” technical response once physical control is lost.

An alternative approach is SLIP-39, commonly referred to as Shamir Backup. SLIP-39 splits the wallet backup into multiple shares and requires a threshold (for example, 3-of-5) to restore access. Individual shares can be geographically distributed, reducing the risk that any one compromise results in total loss or unauthorized access. SLIP-39 was introduced into consumer hardware wallets by Trezor and has since been adopted more broadly as a recovery standard precisely because it protects against physical theft without increasing the probability of user-induced loss.

**Figure 10: Trezor's SLIP-39**



Source: [Trezor](#)

Regardless of the access model chosen, the physical durability of the backup remains non-negotiable. [James Lopp](#), a long-standing Bitcoin developer and security advocate, conducted an [extensive study](#) on how common backup methods fail under realistic disaster conditions, including fire exposure, prolonged water submersion, corrosion, and mechanical stress. Paper, ink, and laminated formats consistently degraded or became unreadable. Many consumer metal products failed as well when markings were shallow, stamped, or assembled from multiple parts (*Figure 11*).

**Figure 11: Metal Seed Phrase Backup Devices**



Source: [Jameson Lopp](#), Trezor

Backups that survived reliably shared the same properties. They used solid titanium or stainless steel to resist heat and corrosion, and they recorded seed words through deep physical modification — either center-punching or electrochemical etching — so that information remained legible even after deformation or surface damage. Round and single-piece designs are also favoured, as Lopp's testing shows that they are more resistant to bending, torsion, and edge deformation under extreme force. Commercial products that follow these constraints exist, and equivalent durability can be achieved through simple open designs using basic tools that can be found at the local stores.

# Future Outlook

---

Our survey of 375 Cointelegraph readers show that self-custody remains a strong trend in spite of the recent rise of ETFs and other TradFi wrappers. It is the marker of a seasoned crypto user to avoid keeping funds in the hands of others for longer than is necessary.

When assets are held in self-custody, control can be exercised without identity checks, account closures, or permissioned withdrawal. For most users, single-signature hardware wallets will remain the baseline custody model because they strike a workable balance between security, usability, and operational burden. They meaningfully reduce exposure to custodial failure and remote compromise while remaining accessible to non-expert users.

More advanced setups, such as multisignature wallets, can mitigate several trade-offs inherent in single-signature designs. However, these benefits come at the cost of increased complexity. When implemented without sufficient expertise, multisig setups can introduce new failure modes. For this reason, multisig remains best suited to power users and institutions with the operational discipline to manage it correctly.

Ultimately, the strength of self-custody does not hinge on ever more complex hardware or future cryptographic breakthroughs alone. It depends on how consistently users apply basic security practices, understand their threat models, and maintain their setups over time. Turning ownership into security is not a static property of a device. It is a behavioral practice maintained over time.



# Disclaimer

---

This document is for information only and does not constitute investment advice, an investment recommendation, or a solicitation to buy or sell — it is merely a summary of key aspects of the Cointelegraph Report. In particular, this document is not intended to replace individual investment or other advice.

The information contained in this publication is based on the knowledge available at the time of preparation and is subject to change without notice. The authors were diligent with their selection of information but assume no liability for the accuracy, completeness or timeliness of the information provided.

Past performance is not a guide to future performance. Values may fall or rise, and you may not get back the amount you invested. Income from investments may fluctuate.

Cointelegraph does not endorse and is not responsible for or liable for any content, accuracy, quality, advertising, products or other materials on this page. Readers should do their own research before taking any actions related to the company.

Cointelegraph is not responsible, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of or reliance on any content, goods, or services mentioned in this publication.

## Author



**Kyrian Alex**  
Research Analyst

