UDC 334.72:001.895(497.5)
Review Paper
https://doi.org/10.62598/JVA:12.1.6.28

Received: October 31, 2025
Accepted for publishing: April 15, 2026

COMPARISON OF CRYPTOCURRENCY STORAGE METHODS: SECURITY RISKS, COSTS AND MARKET IMPACT

Ludvig, Karlo, *M. Econ., The Faculty of Tourism and Rural Development, Josip Juraj Strossmayer University of Osijek, Croatia, karlo.ludvig@gmail.com*

Župan, Mario, *PhD, The Faculty of Tourism and Rural Development, Josip Juraj Strossmayer University of Osijek, Croatia, mzupan@ftrr.hr*

Abstract: Purpose: *This paper compares dominant cryptocurrency storage methods, analyzing their impacts on security, cost efficiency, and market dynamics. It explores how custodial and non-custodial approaches influence user behavior, institutional adoption, and regulatory frameworks in the digital asset ecosystem.*

Design: *The study uses a comparative analytical framework to assess technical, operational, and economic dimensions of hardware, software, and custodial storage models.*

Methodology: *A qualitative approach is employed, drawing on academic literature, industry reports, and case studies of major security incidents, including Mt. Gox, FTX, Bybit, and Lazarus Group attacks.*

Approach: *The research systematically contrasts custodial and non-custodial paradigms, focusing on technological foundations, risk profiles, and user control mechanisms.*

Findings: *Custodial solutions provide accessibility and compliance but carry third-party and systemic risks. Non-custodial methods offer autonomy and resilience but require technical expertise and accountability. Hybrid models effectively balance usability and security.*

Originality of the Research: *The paper synthesizes existing knowledge with recent breach analyses into a cohesive comparative framework, delivering actionable insights for investors, regulators, and developers to enhance safety and efficiency in cryptocurrency storage.*

Keywords: *Cryptocurrency; Custodial Storage; Non-Custodial Storage; Security Risks; Market Impact; Digital Asset Management; Bitcoin*

1. Introduction

The development of the cryptocurrency market over the past decades has brought significant changes to the financial system and opened up space for new forms of investment, payments, and decentralized financial services. With the growth in market value and the expansion of cryptocurrency applications, the importance of issues related to the secure storage of digital assets is also increasing. Unlike traditional financial assets, where institutions such as banks assume responsibility for their safekeeping, in the cryptocurrency ecosystem, security is often entirely in the hands of the users. This leads to specific challenges, both in terms of protection against technical threats and in the context of regulatory and economic consequences.

The method of storing cryptocurrencies is most commonly divided into custodial solutions (custodial storage), in which a third party such as exchanges or specialized service providers manages private keys on behalf of the user, and non-custodial solutions (self-custody storage), where the user assumes full responsibility for storing and using private keys through various types of wallets. Non-custodial options include hot wallets (software applications), cold wallets (hardware devices), paper wallets, and multisig solutions.

By comparing the main cryptocurrency storage methods, custodial and non-custodial, with regard to security risks, costs, and efficiency, their broader impact on the market is analyzed. Particular emphasis is placed on comparing the most commonly used wallet brands and custodial solutions, as well as presenting key incidents that have marked the development of this sector. This aims to provide an analytical framework that will enable a better understanding of the trade-offs between security, convenience, and the economic consequences of choosing a storage method.

The relevance of this topic has grown sharply in recent years. Bitcoin's price surpassing $100,000 USD in late 2024, the Bybit Ethereum wallet breach of February 2025 (one of the largest single thefts in industry history), and continuing regulatory developments worldwide, have once again placed the secure storage of digital assets at the center of investor, institutional, and policymaker attention. With institutional adoption accelerating and retail participation expanding, understanding the security risks, costs, and market impact of different storage methods is no longer a niche technical question but a core issue for the stability and trustworthiness of the entire cryptocurrency ecosystem. By analyzing the technological, economic, and regulatory dimensions of cryptocurrency storage, this paper contributes to the journal's focus on innovation and the impact of digital technologies on financial systems and sustainable economic development.

2. Classification of Cryptocurrency Storage Methods

One of the fundamental specificities of cryptocurrencies is the fact that their ownership is not tied to the owner's name but exclusively to the possession of private keys. Whoever possesses the private key also possesses the ability to dispose of certain assets on the blockchain network. As Antonopoulos explains (2014: 85), cryptocurrencies are not located in the wallet itself, but it contains private and public keys that enable access to assets recorded on the blockchain.

For this reason, the method of storing private keys is of crucial importance, and various models have been developed with the aim of reconciling two requirements: security and convenience.

The question of choosing custodial or non-custodial solutions is not only technical but also an economic issue, since the choice of storage model affects costs, the level of risk, and user trust in the entire system. In practice, it has been shown that there is no universal solution that suits all users. Beginners and small investors often prefer custodial options because they offer a simpler interface and the possibility of account recovery, while experienced investors and institutions prefer non-custodial methods for greater control and security. In addition, certain incidents such as exchange hacks or loss of private keys have shaped risk perception and led to the development of increasingly sophisticated solutions.

2.1. Custodial Storage

Custodial storage most commonly involves crypto exchanges and brokerage platforms that offer services for safeguarding digital assets. In this model, the user owns an account but not the private keys, which means they do not have full control over their cryptocurrencies. The advantage of the custodial approach is that it significantly simplifies the use of cryptocurrencies. Users do not have to worry about managing and securely storing private keys but rely on the platform's infrastructure

and security mechanisms. This model offers integration with other services, such as fast trading, conversion to fiat currencies, or the use of additional financial products. In addition, custodial systems often enable some form of account recovery, for example through multi-factor authentication, user identification, or contacting customer support.

However, the main weakness of custodial storage lies in the fact that the user has no control over their private keys. The well-known saying in the crypto community "not your keys, not your coins" warns that assets entrusted to a third party are not under the user's full control (Ledger, 2020). The history of the market records a series of significant security incidents in custodial systems, the most famous of which are the collapse of the Mt. Gox exchange in 2014, when around 850 thousand bitcoins disappeared, and the FTX collapse in 2022, which resulted in losses of several billion dollars and left a negative impact on the security of the entire market.

In addition to the risk of hacking, according to Saggese et al. (2023) additional risks include platform insolvency, poor management of user assets, regulatory interventions, or fraud. In such cases, users lose access to their assets because they have no alternative way to reach their private keys. Therefore, custodial solutions carry systemic risk that extends beyond individual users and can affect the volatility and reputation of the entire market.

Despite these risks, custodial storage remains the dominant form of cryptocurrency use among a wider circle of users. The reasons for this are simplicity and convenience, as well as the fact that an increasing number of corporate investors prefer cooperation with regulated exchanges and brokerage institutions that offer professional security standards, insurance, and regulatory oversight. This aims to mitigate the vulnerability of this model and ensure greater market stability. It is important to emphasize that there are significant differences among providers of these services. While some exchanges operate with minimal oversight and transparency, an increasing number of entities operate in accordance with financial regulations, use protection standards such as "cold storage" systems, and have contracts with insurance companies. This reduces the risk for users, although it never disappears completely. This diversity means that even within the custodial storage category there are different levels of security and reliability, which users must take into account when choosing a platform. These institutions invest considerable resources in security protocols, multi-layer encryption, and multi-authorization systems, thereby minimizing risk. Such examples show that custodial storage can function as a bridge between the traditional financial sector and the world of digital assets.

2.2. Non-custodial storage

Unlike the custodial model, in non-custodial storage the user manages their own private keys and has full control over the digital assets, meaning no intermediary can block, restrict, or misuse the funds. However, if the user loses the private key, they also lose access to the assets (Clarke, 2023). For this very reason, the non-custodial approach is often considered the only option that truly realizes ownership of cryptocurrencies in line with the principles of decentralization.

One form of non-custodial storage is hot wallets, software applications that remain constantly connected to the internet (Ledger, 2025a). They earned the name "hot" because they are active and ready for use at any moment. They most commonly come as mobile or desktop applications, though web wallets accessed through browsers also exist.

The advantage of hot wallets lies in their convenience. Users enjoy fast and simple access to their funds, which is essential for daily transactions, trading, and interaction with decentralized applications (dApps). Integration with DeFi services (decentralized finance protocols such as lending and swapping), NFT marketplaces, or decentralized exchanges is usually available immediately and without additional setup. The main drawback of hot wallets stems from their constant online status. Being always connected makes them more vulnerable to cyberattacks, phishing campaigns,

malicious browser extensions, and malware. Attacks aimed at stealing private keys or seed phrases represent the greatest threat to this type of storage. For this reason, hot wallets are recommended primarily for smaller amounts used in everyday activities, while larger holdings should be kept in more secure storage forms.

Cold wallets represent another type of non-custodial solution that is not permanently connected to the internet. The most common form is hardware devices that store private keys on an isolated chip; transactions are signed inside the device, and the private key never leaves the hardware (BitPay, 2022). The advantage of cold wallets is their high level of security. Since they are not continuously accessible online, they are virtually immune to remote attacks. This approach makes cold wallets ideal for long-term storage of significant amounts. Drawbacks include higher purchase costs compared to software options, the need for regular firmware updates, and reduced convenience for frequent use. For users who trade often, cold wallets can be impractical because they require physical connection of the device and extra steps for every transaction.

A paper wallet originally meant simply printing the private and public keys on paper. Today, however, the term is often applied to other physical media that store keys, including metal plates, plastic cards, or other durable materials. In recent years, metal versions have gained popularity for their resistance to moisture, fire, or physical damage. The advantage of paper wallets is complete isolation from network threats, since the private key exists only in non-digital form that cannot be hacked. Antonopoulos (2014: 106) similarly describes paper wallets as a form of cold (offline) storage and backup, useful for protection against technical failures or data loss, yet vulnerable to theft or physical access by third parties. Today, paper wallets are used far less frequently than in the market's early days, but they still have a place among users seeking ultimate simplicity and long-term storage without reliance on technology.

Multisig (multi-signature) solutions are systems that require multiple private keys to sign a transaction. Typical configurations are two-of-three (2/3) or three-of-five (3/5). This means funds cannot be moved without the consent of multiple parties. The advantage of these systems is that compromise of a single key does not result in loss of control over the assets, though the complexity of coordination among key holders and the possibility of losing one key increase risk (Goel et al., 2023). Coordination between multiple parties is required, and losing one key can complicate or even prevent access to the assets, depending on the configuration. Multisig solutions also demand detailed planning and technical implementation, making them unsuitable for beginners.

2.3. Advantages and Disadvantages of Custodial and Non-Custodial Storage

Choosing between custodial and non-custodial storage goes beyond technical differences in private-key management; it involves broader economic, regulatory, and practical implications. While one model offers greater convenience and support, the other emphasizes autonomy and long-term security. According to Seymour and Goodell (2024), assets stored in a non-custodial wallet cannot be easily blocked or frozen by regulatory decision, which has proven critical for users in countries with unstable financial systems or restrictive capital controls. However, assets in custodial storage are usually more liquid and immediately available for trading, enabling active investors to react quickly to market shifts. In non-custodial models, assets are often held in safer but less liquid forms, which can slow response to rapid price changes. This dynamic also affects overall market liquidity: the larger the share of assets locked in non-custodial wallets, the lower the volume available on exchanges, which can increase volatility.

From a trust perspective, both models carry distinct implications. In custodial storage, trust rests on the reputation and regulatory status of the service provider. Any incident undermines confidence not only in that platform but in the market as a whole. In non-custodial storage, trust is internal; the user

relies on their own discipline and the technical solutions they employ. In the long run, both models appear likely to coexist. Custodial systems provide liquidity, institutional capital, and regulatory acceptance, while non-custodial solutions ensure decentralization, resilience, and preservation of the core idea of cryptocurrencies. The balance between these two approaches will shape the future structure and stability of the market.

3. Methodology

This study uses a qualitative comparative analytical framework. This approach is appropriate for systematically examining the complex trade-offs between security risks, costs, and market impact of cryptocurrency storage methods when primary data collection is not required. The chosen methodology enables a desk-based synthesis of existing knowledge, recent industry developments, and real-world cases. It provides a comprehensive overview suitable for an emerging and rapidly evolving field such as digital asset management.

The research strategy consists of a systematic contrast between custodial and non-custodial paradigms, focusing on technological foundations, risk profiles, and user control mechanisms. Custodial and non-custodial solutions are compared across three core dimensions: security risks, cost efficiency, and market dynamics including liquidity, volatility, and user behavior. This comparison uses a structured analytical procedure based exclusively on secondary sources.

Data were drawn from academic literature (primarily peer-reviewed articles from arXiv and other databases), official industry reports and documentation from wallet and exchange providers, and publicly available Google Trends data. To ensure representativeness, purposive sampling was applied for the selection of specific solutions and cases. Non-custodial cryptocurrency storage solutions were divided into hot and cold wallets. In the hot wallet category, MetaMask, Trust Wallet, and Exodus were selected because they rank among the most commonly used in practice. In the cold wallet category, Ledger, Trezor, and SafePal were chosen for the same reason. Custodial solutions were represented by the major platforms Coinbase, Binance, and Kraken.

Four major security incidents (Mt. Gox, FTX, Bybit, and Lazarus Group attacks) were purposively sampled based on their scale, illustrative value for different types of risk (hot wallet misuse, internal fund mismanagement, internal transfer vulnerabilities, and state-sponsored bridge attacks), and their documented market-wide consequences.

User interest in both non-custodial and custodial solutions was analyzed using Google Trends data as a proxy indicator. Searches for the selected wallet and exchange brands were measured over the five-year period from 2020 to 2025, with an additional focused analysis of interest in “hardware wallet” during the FTX collapse period. The collected information was synthesized into a cohesive comparative framework. This approach ensures transparency and reproducibility through full citation of sources and explicit documentation of selection criteria.

4. Comparison of Non-Custodial Solutions

Non-custodial cryptocurrency storage solutions are typically divided into hot and cold wallets, with each approach carrying its own advantages and limitations. These examples provide insight into key functionalities, security features, and user experiences, thereby offering a representative picture of the trade-offs between security and convenience within the non-custodial model.

4.1. Comparison of Cold (Hardware) Wallets

4.1.1. Ledger (Nano S Plus, Nano X, Stax)

Ledger is one of the most well-known hardware wallet manufacturers and has long been considered an industry standard. Their devices use a secure element chip, a special security processor also found in bank cards and passports, designed to protect sensitive data and prevent extraction even when physical access to the device exists (Ledger, 2019).

The primary Ledger application is Ledger Live, a software interface for managing cryptocurrencies and installing applications for various blockchain networks. A large number of networks and tokens are supported, with integration into decentralized applications made possible through WalletConnect (a standard that connects wallets and dApps via QR code or link).

The advantages of Ledger include broad network support, ease of use, and isolation of private keys. Drawbacks include the closed-source nature of the code managing the secure element, which prevents independent audits and public verification of security mechanisms. This approach creates room for potential backdoors or undetected vulnerabilities that users and the expert community cannot identify in a timely manner. Trust in Ledger was further damaged by the 2020 incident when customer addresses, names, and emails became publicly available. Although funds were not compromised, users faced heightened risk of phishing attacks (Abramova and Böhme, 2023). Despite these shortcomings, Ledger remains a solid choice for users seeking a combination of convenience and security, especially those with diverse portfolios and frequent use of DeFi protocols.

4.1.2. Trezor (Model One, Model T, Safe 3)

Trezor was the first commercially available hardware wallet, launched in 2014, and is known for its open-source philosophy. Both its devices and accompanying software are developed as open code, publicly accessible for verification and audit, contributing to transparency and user trust (Trezor, 2025). The main application is Trezor Suite, software for portfolio viewing, transactions, and connection to DeFi protocols. Trezor offers Shamir Backup (also known as Multi-Share Backup), where the seed is split into multiple parts, for example three parts requiring any two for recovery, significantly reducing the risk of full key compromise (Trezor, 2024). The advantages of Trezor lie in transparency and innovative security options. A drawback is potentially weaker protection against physical attacks (since older models lack a secure element like Ledger) and somewhat more complex operation for advanced features. It is recommended for users who value transparency and plan long-term storage of larger amounts.

4.1.3. SafePal (S1 and Newer Models)

SafePal stands out for its affordable price and focus on mobile use. The device supports an air-gapped transaction signing methodology without direct internet or computer connection, using QR codes or Bluetooth (SafePal, 2021). Management occurs through a mobile application with support for decentralized exchanges and DeFi protocols.

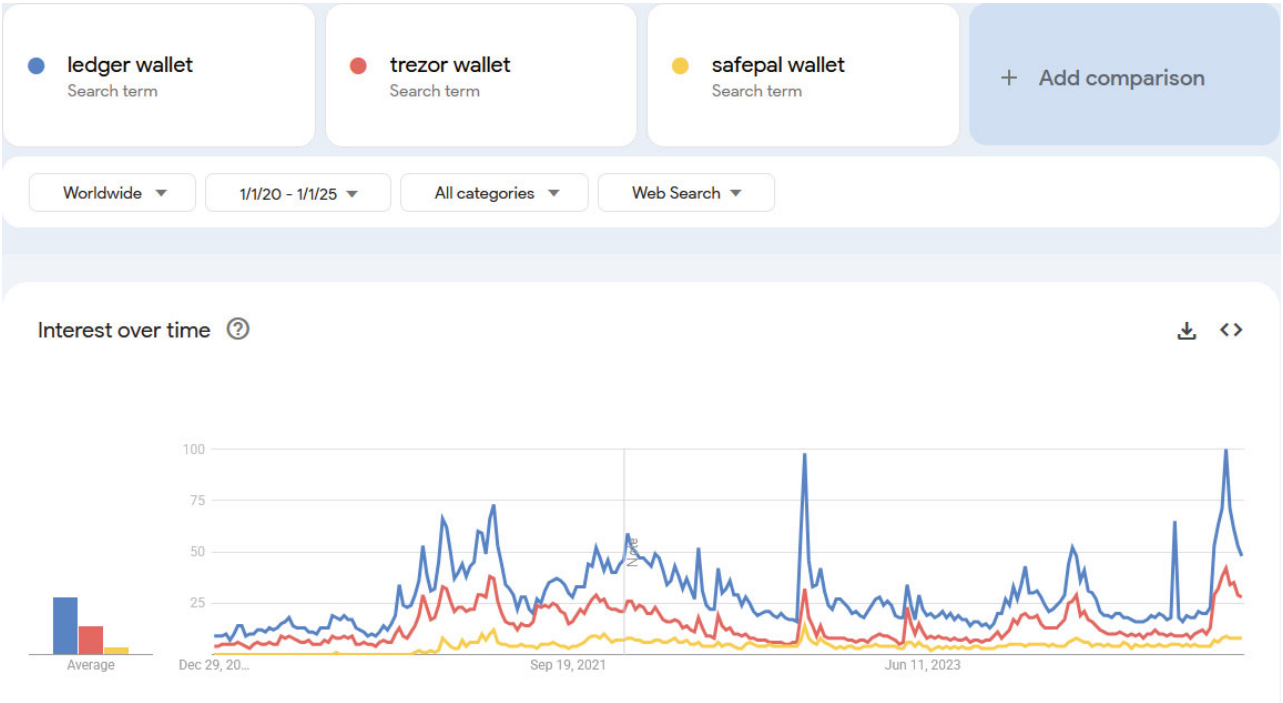
The advantages of SafePal include affordability, simple mobile integration, and broad network support. Drawbacks include a smaller reputation and community compared to Ledger and Trezor, as well as reliance on the mobile app as the primary interface. It suits users seeking a low-cost entry into hardware wallets who primarily manage assets via smartphone.

4.1.4. Analysis of Interest in Hardware Wallets

To complete the comparison of the most prominent cold wallets (Ledger, Trezor, and SafePal) beyond technical specifications, it is useful to examine the level of user interest. Google Trends data was used as an indicator, measuring the frequency of searches for terms related to these wallets over the past five years. According to Figure 1, the results show that Ledger is consistently the most searched brand, with several pronounced peaks in interest. The first significant increase occurred at the end of 2022

during the FTX collapse, when users massively sought safer storage options. The second peak appeared during the period when Bitcoin's price exceeded the $100,000 USD level, further stimulating investor interest in proven solutions. Trezor ranks second with a slightly lower volume, while SafePal records the weakest interest, although it shows gradual growth in the more recent period. Nevertheless, the movement patterns for all three wallets exhibit great similarity, as they respond to market shocks and cryptocurrency price surges almost synchronously. This indicates that user interest depends more on the overall market conditions than on differences between the brands themselves.

Figure 1 - User interest in cold wallets according to Google Trends (2020-2025)



4.1.5. Notes on Security Practices for Hardware Wallets

Regardless of the manufacturer, the seed phrase (12, 18, or 24 words representing the private key) remains the fundamental recovery mechanism. As Vohra (2025) notes, the responsibility for its safekeeping lies entirely with the user, meaning loss or destruction of the device leads to permanent loss of assets if the seed phrase is not securely stored, since entering the phrase into a new wallet is the only way to recover funds. Proper management of the seed phrase is therefore critical to security. The most important practice concerns storage method. The seed phrase should never be kept in digital form, such as on a computer, as a digital photo, or in the cloud, as such approaches open the door to cyberattacks and data theft. Instead of paper, which can be damaged by moisture or fire, metal plates resistant to external elements are increasingly used, a recommendation also provided by Ledger (2025b). It is advisable to store a copy in a secure and separate location, and for larger holdings, consider splitting the phrase into multiple parts using methods like Shamir Backup, where a specific number of parts must be combined for recovery.

Regular updates are essential to eliminate security vulnerabilities, but updates should be performed exclusively through the manufacturer's official channels. An additional layer of protection is provided by the device PIN and an optional passphrase, which acts as an extension of the seed phrase and makes funds more secure even if the base phrase is compromised. Attacks on hardware wallets are not common but can be sophisticated. Examples include supply-chain attacks, where the device is compromised

before reaching the user, or social engineering, where attackers attempt to trick the user into revealing the seed phrase on fake websites or through fraudulent support.

4.2. Comparison of Hot (Software) Wallets

4.2.1. MetaMask

MetaMask is the most well-known hot wallet in the Ethereum ecosystem and networks using the Ethereum Virtual Machine (He et al. 2023). It is available as a browser extension and mobile application. Its strength lies in direct integration with decentralized applications (dApps), making it a standard tool for DeFi protocols and NFT marketplaces.

The advantage of MetaMask is its broad support and active community, but due to its high popularity, it is a frequent target of phishing attacks. He et al. (2023) points out that MetaMask provides signing APIs that, in phishing scenarios, can be exploited to trick users into unintentionally granting a dApp excessive permissions over tokens. In practice, this means a user can lose funds if they fail to verify what permissions they are approving in the MetaMask interface. MetaMask is ideal for advanced users who actively engage with DeFi and NFT markets but requires a high level of discipline in reviewing permissions and security settings.

4.2.2. Trust Wallet

Trust Wallet is a mobile hot wallet supporting hundreds of blockchain networks and thousands of tokens, owned by Binance. Its user interface is simple and beginner-friendly, with a built-in dApp browser enabling direct access to decentralized applications within the wallet (Changelly, 2025).

Unlike MetaMask, which focuses solely on Ethereum and EVM (Ethereum Virtual Machine) networks, Trust Wallet offers broader support, making it more attractive to users seeking a single solution across multiple blockchain ecosystems. The main risk of this approach lies in the security of the device itself. If the phone is compromised by malware or lost without a seed phrase backup, funds can be permanently lost. Trust Wallet is a good choice for users wanting a mobile, multifunctional, and straightforward solution without complex configurations.

4.2.3. Exodus

Exodus is a desktop and mobile hot wallet recognized for its visually appealing and intuitive interface. It is particularly popular among users who want a clear portfolio overview and integrated features like in-app cryptocurrency exchange. It supports hundreds of different cryptocurrencies and can connect to hardware wallets like Trezor, enhancing security.

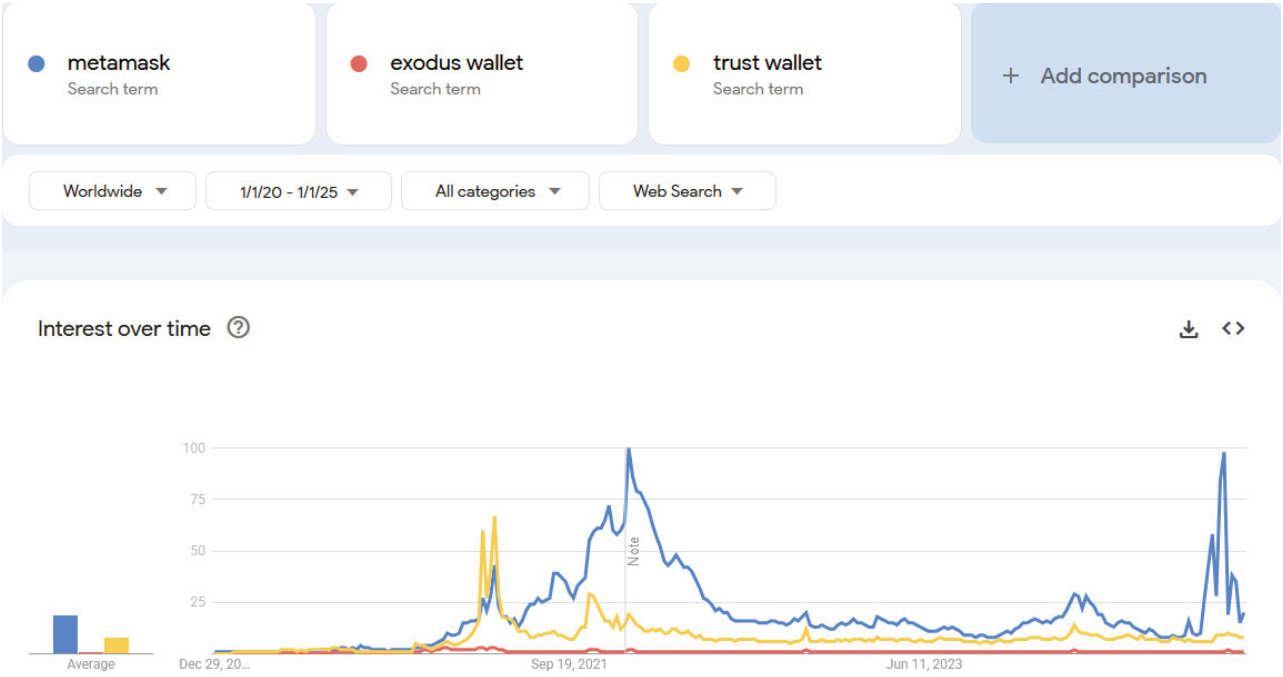
The main advantage of Exodus is its simplicity and multifunctionality, making it suitable for users who want clear asset management without delving into complex DeFi protocols. A drawback is its closed-source code, meaning users must trust the developer that the application has no security flaws, without the possibility of independent verification.

4.2.4. Analysis of Interest in Hot Wallets

User interest in hot wallets is shown through Google Trends data for MetaMask, Trust Wallet, and Exodus over the past five years. According to Figure 2, MetaMask far leads in search volume and serves as the primary indicator of trends in this category, while Trust Wallet records occasional spikes, and Exodus remains at lower levels. Pronounced peaks in interest occur during major market events, such as the FTX collapse at the end of 2022 and the period when Bitcoin surpassed the $100,000 USD. A

similar pattern was observed with hardware wallets, confirming that demand for non-custodial solutions intensifies both in crisis situations and during phases of strong market optimism.

Figure 2 - User Interest in Hot Wallets According to Google Trends (2020-2025)



4.2.5. Security Notes for Hot Wallets

The greatest security challenge for hot wallets stems from their constant internet connection. This exposes them to phishing attacks, fake websites, and malicious extensions attempting to access private keys or seed phrases. One common attack method is token approval phishing, where a user unintentionally grants a smart contract permanent permission to control their tokens.

An additional issue is the security of the device running the wallet. If the computer or mobile device is compromised by malware, private keys can be endangered. It is therefore recommended to use dedicated devices for larger amounts or combine a hot wallet with a hardware wallet, where transactions are signed in an offline environment.

Users should always verify the permissions requested by dApps, download applications only from official sources, and regularly update software. It is also advised to separate funds: smaller amounts for daily use can remain in a hot wallet, while larger holdings should be stored in more secure cold wallets. This combination achieves a balance between convenience and security.

5. Comparison of Custodial Solutions

Custodial solutions offer simplicity, liquidity, and integration with a range of additional services. A particularly important advantage of the custodial model is the availability of fiat on/off ramps, allowing users to easily convert traditional currencies like euros or dollars into cryptocurrencies (on-ramp) and withdraw funds from cryptocurrencies back to bank accounts (off-ramp). In this way, custodial solutions bridge the world of digital assets with the traditional financial system. This model shifts key security and operational risk from the user to the service provider. The quality of custodial solutions in practice

depends on the regulatory oversight to which they are subject, including licensing requirements and mandatory user identity verification (KYC - Know Your Customer), a process that verifies personal data to reduce the risk of fraud and other illegal activities. According to Bappy, Cheon, and Islam (2025), such regulatory mechanisms are critical because they compel custodial platforms to verify identity before granting access to services, thereby increasing platform accountability and reducing the risk of misuse. In addition to regulatory requirements, internal controls, system technical architecture, business transparency, and risk management policies all play important roles in determining the level of security and trust in a given platform.

5.1. Coinbase

Coinbase is a cryptocurrency exchange founded in 2012 in San Francisco, often highlighted as one of the most accessible platforms for entering the world of cryptocurrencies. Its popularity among beginners stems partly from a simple user interface, with additional credibility provided by a strong focus on regulatory compliance, especially in the U.S., where it is publicly listed on the Nasdaq exchange (Barker, 2024). Accounts are integrated with fiat deposits and withdrawals, while storage is organized in a hybrid manner, with most assets in cold storage and a smaller operational portion in hot vaults (Coinbase, n.d.). Users benefit from an additional layer of protection, particularly through multi-factor authentication, as well as a clear and intuitive interface that simplifies daily use. Coinbase stands out for having built a reputation as a reliable and transparent platform over the years, clearly communicating its rules and processes. This approach instills confidence in users, who know that a stable system and consistent security and risk management practices stand behind the service. The main limitation for Coinbase users arises from the custodial model itself, as they lack access to private keys and depend on platform availability and its policies. Additional drawbacks include occasional technical outages or temporary trading restrictions during periods of heightened activity. For some users, strict verification procedures and transaction monitoring are also limiting; while they enhance security and regulatory compliance, they reduce flexibility and anonymity.

5.2. Binance

Binance was founded in 2017 and within less than a year grew into the world's largest cryptocurrency exchange by trading volume (Binance, n.d. a). It is known for low fees, rapid listing of new tokens, and an extremely wide range of products, from DeFi options to its own blockchain (BNB Chain). Binance is often perceived as innovative but also riskier due to regulatory challenges it faces in various markets (Reuters, 2025a). To increase user trust and mitigate this perception, Binance publicly discloses wallet addresses and uses cryptographic proof-of-reserves methods, claiming full coverage of all user assets (Binance, n.d. b). For users, it is crucial to understand that greater functionality increases the attack surface and operational complexity, thereby heightening the importance of personal discipline in account protection.

5.3. Kraken

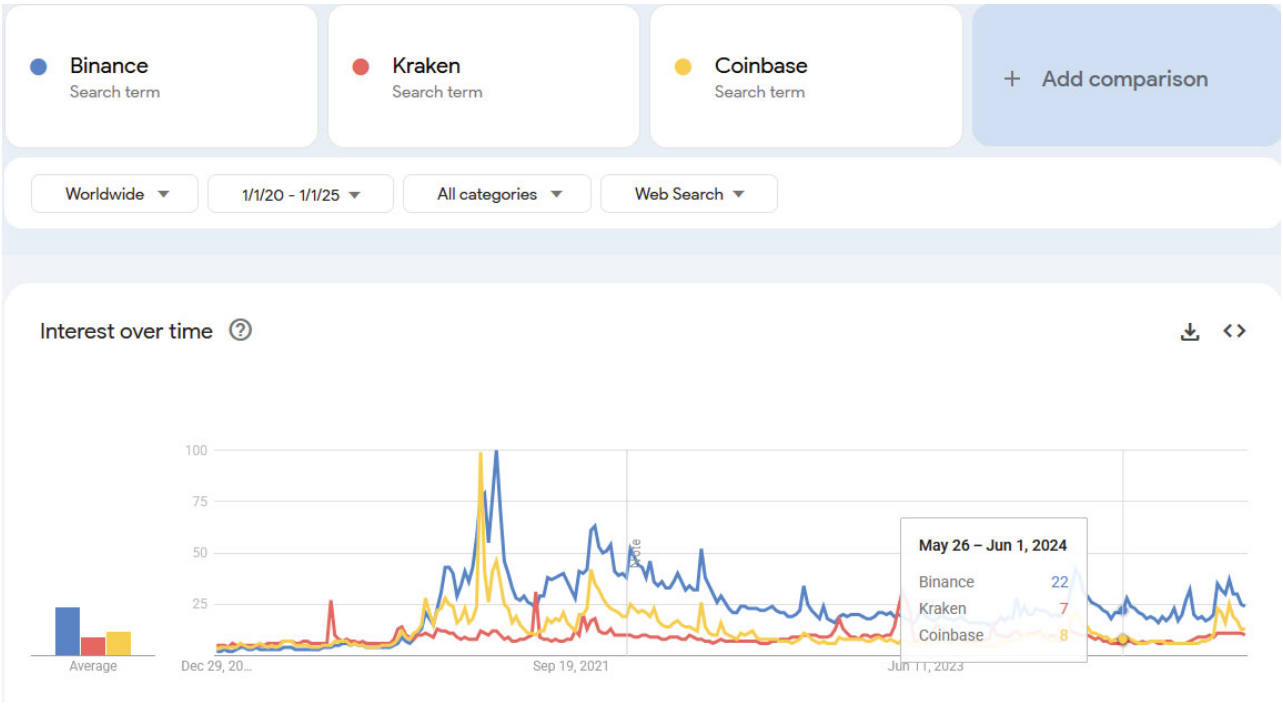
Kraken is one of the oldest and most well-known cryptocurrency exchanges, founded in 2011 in San Francisco. It emphasizes rigorous internal controls, transparent communication, and careful introduction of new features. It has built a reputation as a reliable and secure platform through a focus on protecting user assets and regulatory compliance (Gong, 2024). Over the years, Kraken has positioned itself as a platform primarily attracting serious investors and professional traders. It places special emphasis on security procedures related to transactions and user accounts, for example requiring multiple confirmations via email and additional authentication layers for sensitive actions. This level of operational detail slows processes compared to competitors but provides investors with confidence that transactions occur in a

highly controlled and secure environment. Gong (2024) also notes that Kraken was the first exchange to obtain a special banking license (Special Purpose Depository Institution) in the U.S., enabling greater independence from traditional banks and the development of its own infrastructure. Over years of operation, Kraken has avoided major security incidents, further solidified its reputation and distinguished it as a more conservative alternative to competitors who prioritize innovation over stability.

5.4. Analysis of Interest in Custodial Platforms

Unlike non-custodial solutions, where interest growth is mainly tied to security and asset control concerns, patterns for custodial platforms are linked to broader market and institutional events. According to Figure 3, the largest search peak occurred in early 2021, when Binance and Coinbase became primary entry points for a massive wave of new investors. This surge was associated with institutional Bitcoin inflows, price increases to then-record levels, and Coinbase's Nasdaq listing, which further boosted its visibility. A second peak was observed in August 2025, when French authorities opened an investigation into Binance over suspicions of money laundering and tax irregularities (Reuters, 2025b). The news sparked broader discussions about the reliability of global exchanges and drew public attention to regulatory oversight, reflected in increased searches for the largest platforms. This dynamic shows that interest in custodial services primarily rises during periods of market expansion and regulatory uncertainty, rather than as a direct result of security incidents.

Figure 3 - User Interest in Exchanges According to Google Trends (2020-2025)



5.5. Key Security and Operational Elements of Custodial Solutions

Although different custodial solutions vary in details, several common elements determine their quality and reliability. The cold and hot storage policy dictates what portion of assets is offline and thus more resistant to attacks, while the method of transaction authorization and key fragmentation affects system resilience to individual failures. Transparency through reserve disclosures and independent audits increases confidence in platform solvency, and the quality of operational security and response speed are

critical in crisis situations. Ultimately, the legal framework in which the platform operates determines how assets are treated in extreme events such as insolvency.

6. Costs and Trade-offs by Storage Method

6.1. Custodial Costs and Trade-offs

One of the less obvious costs of custodial solutions arises from the regulatory framework. Platforms operating in strictly regulated jurisdictions often pass compliance costs to end users. This includes identity verification procedures (KYC), transaction monitoring, and tax authority reporting. While it provides users with additional legal protection, this framework can reduce privacy and freedom in asset management. In practice, users must accept extra administrative steps and potentially higher fees to legally use the platform.

Custodial platforms also impose opportunity costs by restricting access to certain features. For example, a user holding funds on an exchange may be prevented from using them in some DeFi protocols or transferring them to unsupported networks. This limits opportunities available in a non-custodial environment. Another form of opportunity cost relates to reaction time: during technical issues or congestion, users may temporarily lose access to their assets and miss market opportunities.

6.2. Non-custodial Costs and Trade-offs

In non-custodial solutions, a significant cost lies in education and the time required to acquire knowledge. Managing private keys, configuring multisig solutions, understanding backups, and using advanced options demand technical expertise that most average users must still develop. The cost here is not measured directly in money but in the time and effort needed for proper technology use.

There are also psychological costs to the non-custodial approach. Full responsibility for security can be a source of constant concern, especially for users with larger holdings. Fear of losing the seed phrase or entering a transaction incorrectly can lead to delayed activity or excessive caution. In some cases, users choose custodial platforms precisely because of these psychological factors, even while aware of increased third-party risk (Delfabbro, King, and Williams, 2021).

Another trade-off involves inheritance and legal aspects. In custodial systems, platforms sometimes offer procedures allowing family or heirs to access funds upon the user's death. In non-custodial models, this is much harder to achieve, as everything depends on whether the user has pre-planned a system for sharing or transferring the seed phrase. The lack of institutional support means assets can remain permanently locked.

6.3. Implications of Custodial and Non-Custodial Models

At the macroeconomic level, differences in costs and trade-offs between custodial and non-custodial models also impact market liquidity. Custodial platforms concentrate large amounts of assets on centralized addresses, increasing available trading volume and reducing transaction costs. At the same time, this concentration creates systemic risk, as an attack or collapse of a major platform can shake the entire market.

Non-custodial solutions disperse assets across millions of addresses under individual and institutional control. This strengthens system resilience but reduces exchange volume and can heighten volatility. In other words, the choice of storage model affects not only the user but also the dynamics of the entire market.

Hybrid approaches often attempt to reconcile these opposites. A common practice is to allocate funds by purpose: a smaller portion in custodial accounts for trading and conversion, while the majority of capital

is held in cold wallets for security. This simultaneously minimizes operational costs and reduces loss risk. However, even such a strategy carries its own challenges, including more complex management, the need for additional knowledge, and greater logistical demands.

7. Impact of Security Incidents on the Market

Security incidents in the crypto sphere act as stress tests that evaluate technology, operational controls, and market structure resilience. When an attack or platform collapse occurs, the first minutes and hours typically bring sudden pressure on liquidity (Umar, 2025). Prices then react with rapid shifts, first in directly affected tokens and then, through correlations and arbitrage links, across the broader market. Short-term volatility spikes are often amplified by technical factors such as automatic liquidations and withdrawal limits on exchanges, further deepening price movements. After an incident, participant behavior often changes: users reduce exposure to custodial platforms and move funds to non-custodial environments, while exchange traffic temporarily shifts to those with higher trust and stronger risk controls.

The regulatory environment reacts more slowly but with lasting effects. Major incidents prompt tighter rules on asset custody, segregation of user funds, reporting, and transaction forensics. This increases operating costs for custodial entities but also raises industry standards. At the same time, some users avoid additional regulation by turning to non-custodial solutions, altering liquidity distribution between centralized and decentralized channels. Four cases that marked different phases of market development and demonstrate recurring patterns: hot wallet misuse at Mt. Gox, opaque management at FTX, Ethereum wallet compromise at Bybit, and years-long attacks by the Lazarus group on exchanges and bridges.

7.1. Mt. Gox: Prolonged Theft from Hot Wallet

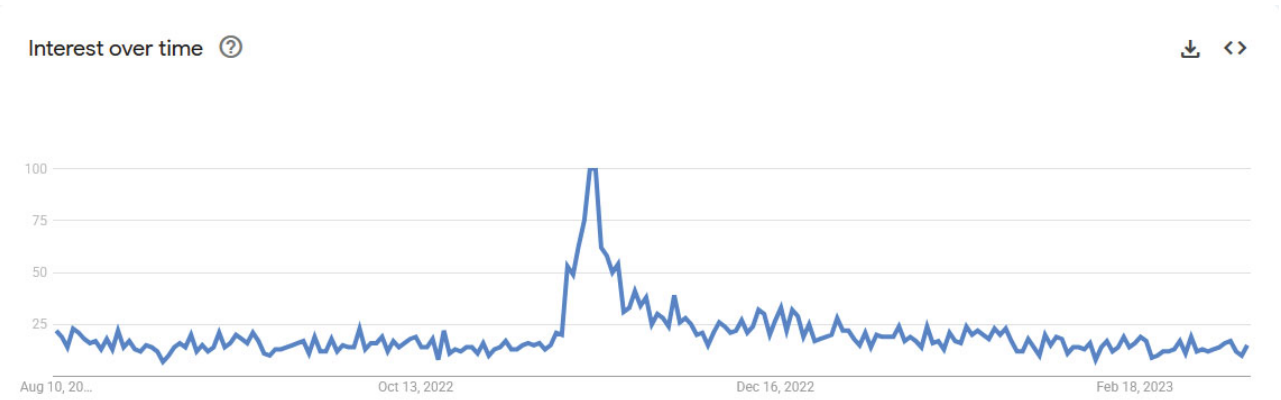
Mt. Gox, founded in 2010 in Japan, quickly became the world's largest Bitcoin exchange and by early 2014 processed over two-thirds of all global transactions. Its central role in the market gave it an almost monopolistic position but also meant the entire market was exposed to risk if serious problems arose. According to Decker and Wattenhofer (2014), Mt. Gox suspended Bitcoin withdrawals in February 2014, citing the "transaction malleability" problem as the main reason—a situation where attackers can alter a transaction's signature to make it appear unconfirmed. It was announced that approximately 850,000 bitcoins were missing, then worth over half a billion U.S. dollars. Later, about 200,000 BTC were found in an old wallet, reducing the final shortfall to roughly 650,000 BTC. Subsequent technical analysis revealed the loss was not from a single major breach but years of continuous draining from a hot wallet compromised as early as 2011. In other words, Mt. Gox was unaware that funds were disappearing over multiple years, indicating severe deficiencies in internal controls and oversight. The market consequences were dramatic. In the weeks around the collapse, Bitcoin's price plummeted, and the shock spread to other exchanges. Trust in crypto exchanges was severely damaged and took years to recover. Mt. Gox thus became a symbol of the early risks in the crypto ecosystem: technical vulnerabilities, poor management, and lack of regulatory frameworks.

7.2. FTX: Misuse of Customer Funds

In early November 2022, one of the largest crises in crypto industry history erupted. On November 2, CoinDesk published a report showing that Alameda Research, an investment firm closely tied to FTX, largely based its balance sheet on FTT, an internal token issued by FTX itself. This structure indicated strong interdependence between the two companies and significant vulnerability in the event of an FTT value drop. The news triggered a wave of customer fund withdrawals, which in just a few days exposed a liquidity shortfall of approximately $8 billion USD.

By November 11, 2022, FTX and over a hundred affiliated entities filed for bankruptcy, while the market reacted with panic and a sharp drop in confidence. In a U.S. criminal trial, founder and former CEO Sam Bankman-Fried was convicted of fraud and embezzlement and sentenced to 25 years in prison in March 2024, with an order for forfeiture of criminal proceeds worth about $11 billion USD.
According to Vidal-Tomás et al. (2023), the FTX collapse in 2022 was not caused by an external hacker attack but by a combination of internal fund misuse and opaque risk management. Their analysis proved that these factors began affecting market liquidity and behavior even before the formal bankruptcy. Nevertheless, the market effects resembled a major security incident: a sudden surge in volatility, mass withdrawals from other exchanges, and a strengthening preference for non-custodial solutions, which return full control over funds to users. This trend is confirmed by Google Trends data in Figure 4, which recorded a significant increase in searches for "hardware wallet" during that period. The rise in interest suggests users actively sought safer storage solutions, with a particular focus on devices enabling full control over private keys and reducing dependence on centralized exchanges.

Figure 4 - User Interest in "Hardware Wallet" According to Google Trends During the FTX Collapse Period



7.3. Bybit: Compromise of Hot Wallet and the Largest Single Theft

On February 21, 2025, Bybit announced that an unknown attacker had seized control of the exchange's Ethereum wallet during a routine internal transfer and transferred approximately 400,000 ETH, which at the time amounted to about $1.5 billion USD. This is one of the largest single thefts in the history of the cryptocurrency industry. The attack was carried out by manipulating the transaction signing interface (multi-signature process), enabling unauthorized transfers of funds, which were then distributed across thousands of different addresses (Rivas, Santos, and Sanz, 2025). Although Bybit stated that it could absorb the loss and that customer funds were not at risk, there was a temporary surge in withdrawal requests and delays in transaction processing. Such a reaction is typical of short-term consequences in similar security incidents but also highlights a broader issue: the vulnerability of centralized exchanges and the reputational risk that can have a domino effect on the entire market. This attack further confirmed the importance of security issues in the cryptocurrency asset industry: it demonstrated how a single compromise can shake user trust, spark regulatory discussions, and accelerate the shift of parts of the market toward safer, non-custodial solutions.

7.4. Lazarus Group: Attacks on Bridges

The Lazarus Group has been operating for years as one of the most active hacking organizations in the cryptocurrency sector. According to Di Santo (2025), it is a group funded by North Korea that

conducts long-term and targeted operations against exchanges, blockchain bridges, and other critical system points. Their typical approach often involves social engineering, such as through fake job offers or malicious files that compromise computer systems and gain access to private keys. After a successful attack, stolen funds are quickly moved through a series of transactions on various blockchain networks, making tracking difficult and enabling their monetization.

The most significant financial blows have occurred on cross-chain bridges, infrastructural points that enable value transfers between different networks and where substantial liquidity is concentrated. For example, in March 2022, approximately $620 million USD was stolen from the Ronin Bridge (a bridge between Ethereum and the Ronin chain). According to Chainalysis analysis, funds stolen from the Ronin Bridge were moved through tens of thousands of addresses, representing a typical money laundering pattern for the Lazarus Group (Plante, 2022). Additionally, the FBI confirmed that the Lazarus Group was behind the attack on the Horizon Bridge, in which about $100 million USD was stolen, with funds transferred through complex transaction chains to cover tracks (FBI, 2023). Such events caused an immediate drop in trust in bridge security, temporarily reduced transaction volumes, and increased volatility in tokens associated with those ecosystems.

On a broader scale, the consequences of such attacks spilled over to the entire market. Institutional capital became more cautious toward investments in projects relying on cross-chain solutions, while individual investors withdrew their funds to safer storage forms, most commonly cold wallets. Periodic liquidity withdrawals from exchanges and bridges caused price oscillations and reduced capital availability for trading. In the long term, these incidents spurred discussions on the sustainability of current bridge models and accelerated the development of safer alternatives, such as multi-signature signing, key fragmentation, and more complex transaction approval procedures.

7.5. Common Patterns and Risk Mitigation Measures

All four cases reveal the same breaking point: concentration of authority over keys and insufficiently granular operational controls. In the Mt. Gox case, the hot wallet compromise lasted for years because there was no clear separation between operational and long-term storage, nor independent monitoring of outflow streams, allowing theft to go unnoticed until the scale of losses became obvious. FTX showed how, even without a classic hacker attack, inadequate management and opaque transfers can produce effects identical to a major security incident. Bybit illustrated the risk of short exposure windows during internal movements, when the hot component temporarily holds significant amounts. Lazarus operations reveal that attacks often begin with social engineering targeted at developers and staff, followed by seizure of signing authority or compromise of bridges where liquidity and trust converge.

Risk mitigation measures can be divided into technical, organizational, and financial-legal categories. At the technical level, it is crucial to clearly separate operational funds from long-term storage, so that only the portion of assets needed for daily operations is kept online. Larger amounts should remain in a safer, offline environment. Using systems where multiple people or devices are required to sign a transaction reduces the chance that a single compromise leads to total loss. It is also useful to monitor transaction patterns and block unusual amounts or destinations before they are executed.

Organizationally, discipline and clear procedures are essential. The most sensitive actions should not depend on a single person but require approval from at least two individuals. All exceptions and manual solutions must be recorded and justified to ensure transparency and an audit trail. When an incident occurs, it is key to communicate quickly and clearly with users—explaining what happened, which addresses were affected, and what measures have been taken. Such an approach reduces panic and strengthens long-term trust.

Financially and legally, the most important is to ensure that customer funds are segregated from the platform's own assets, so that in the event of insolvency, the property is protected. Independent reserve

audits should cover not only assets but also liabilities, so users know if funds are truly covered. Insurance can provide additional protection, although with limitations, as policies often do not cover internal failures. At the market level, pre-arranged liquidity maintenance arrangements can help mitigate sudden disruptions after major incidents.

Technological solutions, operational discipline, and legal-financial structure must work together. If any one of them is too weak, a single incident can escalate into an event with market-wide consequences. But when they complement each other, even serious attack attempts usually end with limited damage and a quick restoration of trust.

8. Conclusion

The analysis of different cryptocurrency storage methods has shown that the choice between custodial and non-custodial approaches is never a simple decision but a complex balance between security, convenience, costs, and control. Custodial solutions offer accessibility, regulatory compliance, and integration with traditional finance, while non-custodial solutions provide genuine autonomy and resilience against third-party risk. In practice, hybrid strategies have become the most common solution among both retail investors and institutions.

Security incidents have repeatedly acted as powerful stress tests for the entire ecosystem. They expose weaknesses in key management and operational controls while simultaneously accelerating innovation in technical safeguards and stricter regulatory frameworks. As the cryptocurrency market continues to mature, the ability to combine user control with institutional-grade protections will determine long-term stability and mainstream trust.

The security and efficiency of cryptocurrency storage methods cannot be viewed in isolation but always within the context of market dynamics, regulatory trends, and technological innovations. The storage question directly impacts volatility, liquidity, and trust in the entire market. As users and institutions navigate between different solutions, one thing remains clear: the future of the cryptocurrency industry will largely be defined by the balance between security standards, regulatory adaptation, and innovations that allow users to simultaneously retain control over their assets and enjoy the convenience of modern financial services.

9. List of References

1. Abramova, S. i Böhme, R. (2023) Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case. arXiv. URL: https://arxiv.org/abs/2308.00375 (Accessed: 11th April 2026)
2. Antonopoulos, A. M. (2014) Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1. izd. O'Reilly Media.
3. Bappy, F. H., Cheon, E. & Islam, T. (2025) Centralized Trust in Decentralized Systems: Unveiling Hidden Contradictions in Blockchain and Cryptocurrency. arXiv. URL: https://arxiv.org/abs/2505.06661 (Accessed: 11th April 2026)
4. Barker, J. (2024) Coinbase Review: Features, Regulation & More. Datawallet. URL: https://www.datawallet.com/crypto/coinbase-review (Accessed: 11th April 2026)
5. Binance (n.d. a) About Binance. Binance. URL: https://www.binance.com/en/about (Accessed: 11th April 2026)
6. Binance (n.d. b) Transparency of Funds. Binance. URL: https://www.binance.com/en/about-legal/transparency-of-funds (Accessed: 11th April 2026)

7. BitPay (2022) Hardware Wallets Explained: How They Work & How to Secure Your Crypto. BitPay. URL: https://www.bitpay.com/blog/hardware-wallets-explained (Accessed: 11th April 2026)
8. Changelly (2025) Trust Wallet Review 2025: Is Trust Wallet Safe? URL: https://changelly.com/blog/is-trust-wallet-safe/ (Accessed: 11th April 2026)
9. Clarke, A. (2023) Non-Custodial Wallets and the Decentralization of Crypto Ownership. Nasdaq. URL: https://www.nasdaq.com/articles/non-custodial-wallets-and-the-decentralization-of-crypto-ownership (Accessed: 11th April 2026)
10. Coinbase (n.d.) What Does Coinbase Do with My Digital Assets? Coinbase Help Center. URL: https://help.coinbase.com/en/coinbase/other-topics/legal-policies/what-does-coinbase-do-with-my-digital-assets (Accessed: 11th April 2026)
11. Decker, C. i Wattenhofer, R. (2014) Bitcoin Transaction Malleability and MtGox. arXiv. URL: https://arxiv.org/abs/1403.6676 (Accessed: 11th April 2026)
12. Delfabbro, P., King, D. & Williams, J. (2021) The psychology of cryptocurrency trading: Risk and reward. Addictive Behaviors, 114, 106741. URL: https://www.researchgate.net/publication/352574339_The_psychology_of_cryptocurr ency_trading_Risk_and_protective_factors (Accessed: 11th April 2026)
13. Di Santo, A. (2025) Lazarus Group Targets Crypto-Wallets and Financial Data while employing new Tradecrafts. arXiv. URL: https://arxiv.org/abs/2505.21725 (Accessed: 11th April 2026)
14. FBI (2023) FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft. FBI. URL: https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft (Accessed: 11th April 2026)
15. He, B., et al. (2023) TxPhishScope: Towards Detecting and Understanding Phishing Contracts on Ethereum. ACM CCS 2023. URL: https://dl.acm.org/doi/10.1145/3576915.3623210 (Accessed: 11th April 2026)
16. Gong, J. (2024) Kraken Company Research Profile. Contrary Research. URL: https://research.contrary.com/company/kraken (Accessed: 11th April 2026)
17. K. Goel, V. S. Bisht and S. Chaudhary, "Multisignature Crypto Wallet Paper," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023. URL: https://ieeexplore.ieee.org/document/10192591 (Accessed: 11th April 2026)
18. Ledger (2019) The Secure Element Chip: How It Keeps Your Ledger Secure. Ledger. URL: https://www.ledger.com/academy/security/the-secure-element-whistanding-security-attacks (Accessed: 11th April 2026)
19. Ledger (2020) Not Your Keys, Not Your Coins: Explained. Ledger. URL: https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters (Accessed: 11th April 2026)
20. Ledger (2025a) What Are the Different Types of Crypto Wallets? Ledger Academy. URL: https://www.ledger.com/academy/topics/crypto/types-of-crypto-wallets (Accessed: 11th April 2026)
21. Ledger (2025b) Seed Phrase Storage. Ledger. URL:https://shop.ledger.com/pages/seed-phrase-storage (Accessed: 11th April 2026)
22. Plante, E. (2022) $30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit. Chainalysis. URL: https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure (Accessed: 11th April 2026)

23. Rivas, M., Santos, R. i Sanz, J. (2025) In-Depth Technical Analysis of the Bybit Hack. NCC Group. URL: https://www.nccgroup.com/research/in-depth-technical-analysis-of-the-bybit-hack/ (Accessed: 11th April 2026)
24. Reuters (2025a) Australia watchdog orders Binance unit conduct audit over money laundering. Reuters. URL: https://www.reuters.com/sustainability/boards-policy-regulation/australia-watchdog-orders-binance-unit-conduct-audit-over-money-laundering-2025-08-22/ (Accessed: 11th April 2026)
25. Reuters (2025b) French investigators open fraud probe against crypto platform Binance. Reuters. URL: https://www.reuters.com/technology/french-investigators-open-money-laundering-probe-against-crypto-platform-binance-2025-01-28/ (Accessed: 11th April 2026)
26. SafePal (2021) Air-gapped Signing Mechanism. SafePal. URL: https://safepalsupport.zendesk.com/hc/en-us/articles/360061264971-Air-gapped Signing-Mechanism (Accessed: 11th April 2026)
27. Saggese, P., et al. (2023) Assessing the Solvency of Virtual Asset Service Providers: Are Current Standards Sufficient? arXiv. URL: https://arxiv.org/abs/2309.16408 (Accessed: 11th April 2026)
28. Seymour, T. i Goodell, G. (2024) Custodial and Non-Custodial Wallets. arXiv. URL: https://arxiv.org/abs/2409.15389 (Accessed: 11th April 2026)
29. Trezor (2024) What is Shamir Backup? Trezor. URL: https://trezor.io/learn/advanced/standards-proposals/what-is-shamir-backup (Accessed: 11th April 2026)
30. Trezor (2025) Trezor Fundamentals. Trezor. URL: https://trezor.io/guides/trezor-devices/trezor-fundamentals/trezor-fundamentals (Accessed: 11th April 2026)
31. Umar, M. (2025) The impact of cyber-attacks on different dimensions of cryptocurrency markets: price, return, and liquidity. Technology in Society. URL: https://www.sciencedirect.com/science/article/abs/pii/S0160791X25000557 (Accessed: 11th April 2026)
32. Vidal-Tomás, D., Briola, A. i Aste, T. (2023) FTX's Downfall and Binance's Consolidation: The Fragility of Centralised Digital Finance. arXiv. URL: https://arxiv.org/abs/2302.11371 (Accessed: 11th April 2026)
33. Vohra, S. (2025) Singularity Blockchain Key Management via non-custodial key management. arXiv. URL: https://arxiv.org/abs/2506.02282 (Accessed: 11th April 2026)

10. List of Figures

Figure 1. User Interest in Cold Wallets According to Google Trends, Period 2020-2025.

Source: Google Trends. URL: https://trends.google.com

Figure 2. User Interest in Hot Wallets According to Google Trends, Period 2020-2025.

Source: Google Trends. URL: https://trends.google.com

Figure 3. User Interest in Exchanges According to Google Trends, Period 2020-2025.

Source: Google Trends. URL: https://trends.google.com

Figure 4. User Interest in "Hardware Wallet" According to Google Trends During the FTX Collapse Period.

Source: Google Trends. URL: https://trends.google.com