PAPER

DEC 2024

www.RoxCustody.io

RoxCustody

# Virtual Asset Custody

*Institutional grade DeFi-MPC digital assets custody as technology*

As global investment in digital assets grows, the number of asset holders increases, and governments launch digital asset initiatives, the need to scrutinize custody services in the digital asset sector becomes more critical. It's essential for both individuals and organizations to understand how digital asset custody works, the techniques used to safeguard assets, and the potential risks involved in the digital asset ecosystem. Innovative projects are being developed and tested, and institutions that were initially hesitant are now actively participating in this dynamic area.

Although these new endeavors bring new challenges, the fundamental tasks of storing, protecting, and managing digital assets often pose the most significant hurdles. Our aim is to illuminate the world of digital asset custody, exploring its origins before the digital assets industry emerged and drawing comparisons between the custody of traditional and digital assets. Through this, we seek to demystify digital asset custody and highlight key factors to consider when assessing custody service providers.

## Understanding Traditional Custody

In financial services, "custody" refers to the safeguarding of client assets and the provision of related administrative tasks. While custody can cover a range of asset classes, it is most commonly associated with financial instruments and typically provided by custodian banks. The method of holding assets in custody depends on the type of asset. This section will describe the general administration of custody for financial instruments, referred to here as "traditional assets."

Custodians are service providers that enable institutional and retail clients to protect and manage certain assets they own. The custody market for financial instruments is largely dominated by commercial and investment banks, though some brokers also act as custodians. The market for traditional asset custodians is well-established, with a few select firms preferred by many institutions seeking custody services.

## The Importance of Custodians

Managing and protecting traditional assets presents risks and operational challenges many asset owners can't handle alone. Institutions often lack the expertise for transactions and access to necessary market infrastructure. Custodians address these challenges, providing secure asset holding and administration under regulatory protections, assuring clients of their assets' safety.

## The Range of Assets Held in Custody

Custodians are responsible for the safeguarding and management of both physical and electronic assets on behalf of their clients. The traditional assets they hold in custody encompass a diverse array of asset classes, including securities certificates (such as stocks and bonds), commodities (like gold), and other records (such as real estate documentation).

## The Role of a Custodian

**Safeguarding:** Custodians ensure the protection of their clients' legal titles by, for instance, registering assets under a nominee company's name. They also conduct reconciliation processes to maintain consistency between the assets they are expected to hold for clients, as recorded in their books, and their actual holdings. This includes ensuring alignment with the records of a central intermediary, like a Central Securities Depository (CSD), when applicable.

**Settlement:** Custodians manage the settlement of transactions for their clients. This could involve processing settlements through a CSD's central register for dematerialized traditional assets, such as publicly listed company shares. For other types of regulated traditional assets, custodians handle any additional required formalities.

**Asset Services:** Custodians may provide an array of services that enable clients to exercise their rights and meet obligations related to the traditional assets they own.

## Traditional Asset Custody Methods

Digital asset custody employs two main models: omnibus (commingled assets) and segregated (separate assets). Effective custody requires robust policies, controls, and procedures to ensure accurate trade execution, record-keeping, and asset segregation, protecting client holdings. Secure authorization processes, often via dedicated platforms, are crucial for preventing unauthorized transactions and ensuring compliance with client instructions.

A custodian mitigates risks by Implementing clear policies and procedures, often supported by specific platforms or portals, to ensure secure operations related to who can authorize transactions for custodied assets. This helps prevent unauthorized actions and ensures compliance with client directives.

## Differences in digital asset custody

Before exploring the specific features of digital asset custody, it's important to clarify some key concepts related to digital assets that are central to the rest of this paper. Understanding the terminology used to describe digital asset custody services is essential for comprehending the nature of digital asset custody.

The classification of digital assets is evolving with new regulatory frameworks emerging worldwide, and it varies across different jurisdictions. While international harmonization appears to be a long-term goal, global regulators increasingly recognize the need for consistency.

**Public** Key and Public Address: Public keys are data strings similar to bank account numbers. They can be shared publicly and are used by third parties to send transactions. When sending digital assets, the sender uses the recipient's public key. A public address is a hashed version of the public key, which can be quickly generated and used for transactions in place of the public key itself. This is akin to creating and using disposable virtual debit cards for a limited number of transactions.

**Private Keys:** These are data strings that have a unique mathematical relationship with the public key, where the ownership of digital assets is recorded on a distributed ledger. They are used to sign or authenticate transactions from the holder's public address to another person's public key. Private keys are essential for establishing and exercising ownership rights over digital assets.

**Distributed Ledger Technology (DLT):** This technology allows for the operation and use of a digital information or data store that is shared across a network of computers (nodes) and may be accessible to other participants. Participants use a consensus mechanism to validate and synchronize additions to the ledger.

**Digital Assets:** Often called "cryptoassets" or "virtual assets," digital assets generally refer to digital representations of value or rights recorded to a public address on a distributed ledger, as part of a DLT system or similar technology. This is meant to be a broad term, and in this paper, we use "digital assets" as an umbrella term to include all types of digital assets, such as stablecoins, security tokens, utility tokens, and even non-fungible tokens to some extent.

**Wallet:** Wallets are the systems and processes responsible for storing and managing private keys, which are used to operate a person's public address. Essentially, a wallet is the technology through which these keys are handled, making it a crucial component of any digital asset custody service.

## Digital vs. Traditional Asset Custody

Digital assets have become a prominent asset class, especially from the 2010s onward. Many digital assets have evolved beyond speculative investments to become integral to a tokenized economy that recently, albeit briefly, exceeded a market value of US $3 trillion.

This asset class is distinct from traditional assets because ownership of a digital asset relies on cryptographic techniques and often (though not always) depends on an underlying infrastructure known as DLT. In contrast, traditional financial instruments often have a tangible form (like a share certificate), even if they are immobilized and dematerialized. When we talk about digital assets, we are essentially referring to intangible data represented on a DLT system in encrypted form, with ownership demonstrated and transferred through private keys associated with the DLT system.

The widespread adoption of digital assets has led to a growing demand for effective digital asset custody solutions. Digital asset custody is essential; every user, whether existing, new, institutional, or retail, requires a secure method to store and manage their digital assets. However, this asset class is not one that traditional custodians are accustomed to safeguarding or managing for clients.

Traditional custodians facilitated connections with various stakeholders in the conventional financial markets, but digital asset markets involve a different range of stakeholders and institutions connected in new ways.

Traditional custodians are making strides in technology, yet they still rely on risk management frameworks grounded in traditional regulated custody standards to operate in the digital asset market. Some custodians, such as Standard Chartered Bank and Bank of New York Mellon, have set up subsidiaries specifically to offer custody services for digital assets.

For institutions looking to launch digital asset projects, selecting a custodian that meets the institutional standards associated with traditional asset custody is often the initial hurdle. This presents a significant challenge for institutions entering the digital asset space.

## Understanding Digital Asset Custody

In this paper, when we talk about digital asset custody from a technical standpoint, we mean the custody or storage of the private key or keys linked to the public addresses where the client's digital assets are recorded. This also encompasses the ability to manage the client's wallet by executing transactions on the distributed ledger, following the client's instructions. Essentially, we refer to the custody and controlled deployment of private keys when discussing digital asset custody.

A distinction exists between a third party that stores and manages the private key (true or direct custodians, as referred to in this paper) and services that may be better described as technology providers, where the client holds the private key to authenticate transactions.

It's important to distinguish between custodial wallet services and full digital custody services. Custodial wallet services are generally simpler and designed for ease of access for users. In contrast, digital custody services are more institutionally focused, allowing multiple users to access private keys, such as when a corporation or institution requires multiple personnel to have access, and they often emphasize institutional-grade security.

## Methods for Securing Digital Assets

In any digital asset custody arrangement, securing the private key is crucial. Key decisions must be made regarding how the private key is stored and the processes and timelines for using it to authenticate transactions. Generally, there are two options for storing the key:

(a) By the client, known as "self-custody" or a "non-custodial" arrangement; or
(b) By a custodian, in a "custodial" arrangement.

This paper focuses on custodial arrangements provided by third-party custodians to clients. Two common types of institutional custody offerings are Multi-Party Computation (MPC) solutions and Hardware Security Module (HSM) solutions. The primary difference between these two offerings often lies in the cryptographic standards applied to the private key and the storage solution for the private key or its shards.

## Wallet types

Regardless of the chosen custody model, there are various methods for storing private keys in both non-custodial and custodial wallet arrangements. Private keys can be stored in either a physical or digital environment.

When private keys are stored physically, such as in purpose-built hardware wallets, they are kept offline, disconnected from the internet—this is known as a "cold" wallet. This method is often considered a "long-term" storage solution. However, there are hardware solutions that allow for offline storage with very low latency, referred to as "warm wallet" solutions.

If private keys are stored digitally in an online environment, they are kept in a "hot" wallet, meaning the wallet is connected to the internet.

Another type of wallet to consider is the "warm" wallet, where private keys are stored in a secure enclave separate from the online environment. Users can access the private keys using hardware intermediary devices that transfer data packets between environments, allowing for reconstruction without an online connection to the storage environment.

## Key sharding and multisignature wallets

To minimize operational and cybersecurity risks associated with digital assets, various technical mechanisms have been developed. Sharded environments and multi-signature user policies are two examples often used to mitigate the risk of a single point of failure.

Key features of any sharding plan include encryption standards, the security of physical shard artifacts, geographic distribution, redundancy, and secure access and deployment protocols.

Multi-signature wallets work similarly by requiring multiple signatures before a transaction is approved and a client's digital assets are transferred.

## Centralized Custody

Centralized custody involves the storage and management of digital assets by a third-party provider, such as a cryptocurrency exchange or custodian service. In this arrangement, the custodian holds the private keys associated with the digital assets and is responsible for securing and managing these assets on behalf of the users.

Centralized custody services are typically user-friendly and offer a straightforward interface for managing digital assets.

- Risk of Centralization: The primary risk is the concentration of assets, which can make them susceptible to hacking, fraud, or regulatory challenges. If the custodian is compromised, all assets under their management are at risk.
- No Direct Control: Users do not have direct control over their private keys, which means they are entirely dependent on the custodian for access and security.

Centralized custody wallets are provided by centralized businesses, such as cryptocurrency exchanges, offering less user control but increased convenience and security measures.

## Self-Custody and Hardware Wallet

A self-storage hardware wallet is a physical device designed to securely store and manage private keys for cryptocurrencies. These devices remain offline when not in use, which significantly reduces the risk of hacking and unauthorized access.

Users maintain full control over their private keys since they are stored directly on the hardware wallet, eliminating the need to rely on a third party.

Self-storage hardware wallets are considered among the most secure methods for storing digital assets because they are disconnected from the internet when not in use, making them less susceptible to online threats.

However, managing a self-storage wallet requires a certain level of technical knowledge, and users must be diligent in safeguarding their seed phrases (private keys). While self-storage offers complete control and high security, it demands more technical understanding and careful management.

## Multi Party Computation (MPC) wallet

Multi-Party Computation (MPC) in the realm of cryptocurrency is a cryptographic technique that enables multiple parties to collaboratively perform computations on their data without exposing the data itself. This approach is particularly valuable for enhancing the security and privacy of digital assets.

In MPC, private keys or other sensitive information are divided into multiple parts (shards) and distributed among different parties. Each party holds a piece of the data, ensuring that no single party has sufficient information to reconstruct the entire key or data.

MPC is employed to securely manage private keys by splitting and distributing them, thereby minimizing the risk of theft or loss.

The challenge with Multi-Party Computation (MPC) custody is that, despite private keys being distributed across multiple servers, the custody provider still owns these servers. This ownership gives the provider significant control and influence over the custody process, effectively maintaining a centralized role.

Even though MPC distributes private keys across multiple servers, the fact that the custody provider owns these servers allows them to manage and control the assets centrally, leading to centralization issues similar to traditional custody solutions.

The aim of MPC custody solutions is to enhance security by distributing control and eliminating single points of failure. However, if the custody provider retains ownership of the servers, this undermines decentralization, as the provider can still exert control over the assets and operations.

This centralization can lead to transparency and trust issues. Users may lack full visibility into the operations and security measures implemented by the provider, which can be concerning for those seeking a truly decentralized and transparent solution.

In summary, while MPC custody seeks to improve security by distributing private keys across multiple servers, the custody provider's ownership of these servers means they still play a centralized role. This centralization can result in dependence on third parties, a lack of true decentralization, and potential transparency and trust issues.

## Decentralised Multi Party Computation (DeFi MPC) wallets

Multi-Party Computation (MPC) is a cryptographic technique that enables multiple parties to collaboratively perform computations on their data without exposing the data itself. In Decentralized Finance (DeFi), MPC is essential for enhancing security, privacy, and efficiency. MPC wallets distribute the private key across multiple parties while ensuring that the vault owner retains control and oversight, significantly reducing the risk of theft or loss of digital assets.

The vault owner, often an institution or a group of individuals, holds a share of the private key, which is vital for signing transactions and managing the vault. When a transaction is needed, multiple parties work together to reconstruct the private key. The transaction is then signed and executed on the blockchain, ensuring that no single party can act independently.

By distributing the private key and requiring multiple signatures for transactions, MPC wallets offer increased security and privacy. This approach is particularly advantageous in DeFi, where the risk of hacks and fraud is high.

In summary, an MPC wallet in DeFi with a vault owner ensures secure transactions, enhanced privacy, and robust compliance, making it a preferred choice for managing digital assets in the decentralized finance ecosystem.

## Regulation

The right of self-custody in cryptocurrency regulations refers to the ability of individuals to hold and manage their own cryptocurrency wallets and assets without depending on third-party services or intermediaries. This means users have complete control over their private keys and can conduct transactions directly from their wallets.

However, regulations regarding self-custody can vary widely depending on the jurisdiction. For instance, the European Union's new Anti-Money Laundering laws have introduced measures affecting self-custody wallets. These regulations require identity verification for transactions above a certain threshold and prohibit anonymous transactions. While the EU initially proposed a $1,000 limit on self-custody transactions, this was later removed.

Overall, the right of self-custody is considered a fundamental aspect of financial privacy and independence, but it also presents regulatory challenges aimed at preventing illicit activities. This aligns with the core principles of Distributed Ledger Technology (DLT) and regulatory frameworks.

Regarding Multi-Party Computation (MPC) custody, even though private keys are distributed across multiple servers, the custody provider owns these servers. This ownership means the provider maintains significant control and influence over the custody process, effectively playing a centralized role.

## The Right of DeFi MPC custody in Crypto Regulations

DeFi custody, like self-custody, does not inherently demand regulation. DeFi MPC wallets enable users to control their private keys and assets without relying on centralized intermediaries. This decentralization grants users complete control over their funds, reducing the need for regulatory oversight typically required for centralized custodians.

While some jurisdictions have introduced regulations to tackle issues such as money laundering and illicit activities, these often focus on transactions rather than the custody of assets. For instance, the European Union's Anti-Money Laundering laws require identity verification for transactions above a certain threshold but do not specifically regulate DeFi custody.

In summary, DeFi custody does not necessitate regulation because it empowers users to independently manage their assets, aligns with the decentralized nature of blockchain, and preserves financial privacy and control without requiring identity verification or other regulatory measures.

## Rox Custody, DeFi MPC

Revolutionizing Security for Institutional digital Assets safeguarding. Rox Custody is carefully designed with a robust framework built on three foundational layers to ensure comprehensive security, governance, and policy adherence.

- **Security Layer:**Utilizes advanced encryption and access controls to safeguard assets from unauthorized access and cyber threats.
- **Governance Layer:** Establishes clear protocols and oversight mechanisms to ensure transparency and accountability.
- **Policy Layer:** Incorporates regulatory compliance and best practices to align activities with legal standards and ethical guidelines.

Rox's multi-layered security approach integrates DeFi-MPC and hardware security to minimize the risk of breaches and create a trusted environment for managing digital assets.

Rox Custody focuses on decentralization and control by giving the vault owner 50% of the private key, ensuring RoxCustody does not have access to that part, as Rox Custody does not retain a copy of it. This setup requires the vault owner's explicit approval for outgoing transactions.

Combining our transaction policy engine and implementing Multi-Party Computation (MPC) within a truly decentralized system, each outgoing transaction necessitates the vault owner's consent, adhering to their detailed multi-layer transaction policies.

Our mission is to provide decentralized security combined with the ease of centralized access, empowering institutions to navigate the digital asset landscape with confidence.

## Solution

As the cryptocurrency market continues to grow, the need for secure and reliable custody solutions has become increasingly important. At Rox custody, we provide a balance between the convenience of centralised custody and the security of full self-custody.

- Simplified Complexity and Usability: Our DeFi-MPC solution removes the complexity and usability issues associated with traditional self-custody options. We provide an intuitive interface and comprehensive features, making it accessible for users of all technical levels.

- Full Control: While offering more control than fully centralised solutions, our custody-as-technology still ensures that users retain full autonomy over their cryptocurrencies, just like any self-custody solution. Users have the freedom to manage their assets as they see fit.

- Enhanced Security with MPC: We utilize Multi-Party Computation (MPC) to enhance the security of our custody-as-technology solution. MPC ensures that no single point of failure exists, and with part of the storage being cold storage and not connected to the internet, we ensure that even if the part held by the user is compromised, users' assets remain secure.

- Payment Policy for Added Security: Our solution introduces a payment policy that requires a number of transaction approvals for any outgoing transactions, customizable to different policy levels based on transaction amounts. This multi-signature approach adds an extra layer of security, preventing any unauthorized transactions.

## Rox Custody's Value proposition

**Multi-Layer Security**

- Highly secure transfers anchored by state-of-the-art Advanced DeFi-MPC, and SCM technology.
- Create wallets and permissions for different departments and users in your business
- Reliable backup storage options for vault owners, including Google Drive, Dropbox, OneDrive & AWS S3

**Direct Self-Custody**

- Complete control over your private keys, eliminating counterparty risk with Rox.
- Secure backup storage.

**Users' role and permissions**

- Manage users' roles and permissions for complete control. Grant specific access for different functionalities and maintain a client chain of command.

**Gas Station**

- Allocates gas station for your vault, and its transactions

**Governance and Policy Engine**

Create policies for granular control with our payment policy engine. Set up specific quorums, multi-tier approval flows, limits and permissions, ensuring compliance and security.

- Comprehensive transaction policies and user controls for all operations
- Streamlined automated workflow authorization and customizable admin quorums
- Detailed user roles and permissions, including 14 distinct user types

**Unified Treasury Interface**

- Manage vaults with internal, segregated, and consolidated options for your connected accounts.
- Secure wallets across blockchains

**Mobile APP for vault details, and signing**

- Leverage Rox Custody mobile application to view vaults, transactions, gas stations, and signing transaction.

**Comprehensive API Automation**

- Automate transaction authorizations and signatures through API
- Streamline transfer operations automatically

**Exchange connectivity**

·Connect your exchange accounts, sub-accounts, and monitor your exchange balance all in one place.

**Comprehensive Blockchain Support**

- Compatibility with over 30 EVM and non-EVM blockchains
- Leading support for various token types
- Custom token support available

**Deployment flexibility**

- Freedom to deploy SCM co-signer anywhere, any VM, any cloud, any machine.

## Rox Custody's Security

Rox Custody implements a robust security strategy using various modules to protect digital assets. Asymmetric cryptography ensures secure service communication and wallet key storage, while Two-Factor Authentication (2FA) provides additional access protection. Symmetric encryption secures exchange APIs and secret keys, and SHA-256 hashing protects sensitive data storage. The solution involves giving 50% encrypted private keys to vault owners, utilising cold storage with internet isolation, and Hardware Security Modules (HSM) for secure cryptographic key management.

**Asymmetric crypto graph**
Service Communication and Wallet Key Storage
Asymmetric encryption is implemented for two critical purposes in our system. First, it ensures secure communication between our services by encrypting sensitive data transmitted internally. Second, RSA encryption is used to securely store wallet private keys in our database.

For each corporate account, we generate a unique key pair comprising a public key and a private key. The private keys of wallets are encrypted with the corporate's public key before being stored. To enhance security further: The encrypted private key is divided into two parts: one part is securely stored in our database, and the other is sent to a secure configuration management (SCM) system. The private key required for decryption is stored in an isolated private server that is not connected to the internet.

This setup ensures that even if a corporate exits our system, we can securely provide their private key pair, along with the private keys required for decryption, while maintaining the highest level of security.

**Symmetric Encryption**
Exchange API and Secret Keys
We use symmetric encryption to store sensitive information such as exchange API keys and secret keys. Symmetric encryption is chosen for its efficiency in encrypting and decrypting data with a single shared key. The decryption key is stored in a highly secure and isolated manner on our private server, ensuring that it is only accessible by authorized processes. This method provides both confidentiality and speed, making it ideal for frequently accessed sensitive data.

**Multi Party Computation (MPC)**
Shared private key with vault owner & their backup storage
In a shared private key system, half of the key is kept safe in Rox Custody's cold storage, while the other half is encrypted and stored on the vault owner's private server, with a backup. This dual storage approach enhances security by avoiding a single point of failure and ensures only authorized access to sensitive data through encryption.

**Cold Storage (Isolated from internet)**
Cold storage involves keeping sensitive data or digital assets offline, away from the internet, to enhance security. Commonly used for cryptocurrencies and confidential information, it protects against hacking and malware by isolating data from online threats, ensuring safety and integrity.

**Hardware Security Modul (HSM)**
A Hardware Security Module (HSM) is a secure device that protects and manages digital keys for strong authentication and cryptographic processes. Used in sectors like finance and healthcare, HSMs provide a tamper-resistant environment to safeguard sensitive data. They securely generate, store, and manage cryptographic keys, playing a vital role in preventing data breaches and ensuring robust security.

**ERC-4337**
enhances security by replacing traditional accounts with programmable smart contract wallets, enabling features like multi-sig, social recovery, and custom security rules to reduce reliance on vulnerable private keys and improve protection against attacks, though careful development and auditing are crucial to mitigate new potential vulnerabilities.

**Hashing - SHA-256**
Sensitive data Storage
We utilize the Secure Hash Algorithm 256 (SHA-256) for storing user passwords. SHA-256 is a cryptographic hash function designed to produce a fixed-size, unique, and irreversible hash for any input data. This makes it an ideal choice for storing passwords securely, as the process is one-way and ensures that passwords cannot be retrieved even by us. By hashing passwords, we safeguard user authentication data against unauthorized access or breaches.

**JWT**
JWT security relies on cryptography to ensure message integrity and authenticity. This method verifies that the token hasn't been tampered with. Upon receiving a JWT, the recipient uses the same algorithm and corresponding key to recalculate the signature and compare it to the provided one. A match confirms the token's validity.

**2 Factor Authentication (2FA)**
Two-factor authentication (2FA) enhances security by requiring two forms of verification: something you know (like a password) and something you have (such as a smartphone app or fingerprint). This extra step ensures that even if a password is compromised, unauthorized access is prevented, significantly boosting account security.

## Conclusion

In conclusion, the right of self-custody within the evolving framework of crypto regulations is a pivotal characteristic of financial privacy and independence, allowing individuals to control and secure their cryptocurrency wallets and assets without reliance on centralized services.

With the advent of new technologies, self-custody has become a cornerstone of decentralized finance (DeFi), embodying the principles of financial autonomy and privacy. DeFi custody, particularly through Multi-Party Computation (MPC) wallets, exemplifies the potential for users to maintain control over their assets without the need for centralized intermediaries. This decentralization not only aligns with the ethos of blockchain technology, thereby reducing or eliminating the necessity for regulatory oversight typically associated with centralized custodians. While some jurisdictions have introduced regulations to combat illicit activities, these measures primarily target transactions rather than the custody of assets themselves.

The DeFi MPC Custody solution stands out in this context, offering a multi-layered security approach that combines decentralized MPC with hardware security to protect digital assets. By implementing advanced encryption, governance protocols, and policy adherence, it ensures a trusted environment for managing digital assets.