Digital asset custody and transaction processing leading practices using Fireblocks' MPC solution

Prepared by Ernst & Young LLP (EY) and Fireblocks

Report date: March 2023

Building a better working world

1 Introduction

EY Blockchain US Lead

Dear reader,

The objective of this document, the first in a Digital Assets Risk Management Leading Practices series, is to introduce EY's views on leading practices for institutions leveraging self-custody capabilities. It should enable custodians and other digital assets sector participants and service providers, to effectively identify and manage digital asset risks.

On January 3, 2023, the FED, OCC and FDIC issued a joint statement, titled: "Crypto-Asset Risks to Banking Organizations" based on recent industry events which highlighted a lack of risk management surrounding digital-asset services.

We, at EY, are committed to the promotion of "safe and sound business models" that allow for safer adoption of digital assets and public blockchain infrastructure. Our objective in writing this document is to discuss what we view as leading self-custody processes, procedures, policies, risk assessments, controls, gates, guardrails, and monitoring capabilities.

To provide targeted examples, we have collaborated with an industry leading self-custody provider, Fireblocks, to develop a leading practices document. We used our extensive experience integrating Fireblocks and other self-custody solutions with TradFi operations, to align our leading practice recommendations to their system's terminology, starting with and focusing on the topic of Private-Key lifecycle management. We believe that most of our recommendations, set forth in this document, apply in many ways, to general digital asset risk management regardless of the custody solution used.

To summarize, we hope this leading practices series serves as a tool to help digital assets sector participants enhance their Risk Management capabilities, as part of our mutual journey in building a better, safer, equal opportunity working world, using public blockchain technology.

I hope you find this read valuable.

Chen Zur, Principal
EY-US Blockchain Practice Leader

Fireblocks CEO

Dear reader,

Since founding Fireblocks in 2018, my co-founders and I have always believed in the power of multi-party computation (MPC) and its ability to transform the digital asset landscape. MPC has since become one of the most fundamental pieces of technology in the space, and we are proud to have played a part in this movement.

We continue to stand in our conviction that individuals and entities should have full control over their assets. We have built the Fireblocks platform entirely on this principle — delivering a specific implementation of direct custody where we seamlessly remove counterparty exposure to a party holding your assets with multiple layers of security in the highest performing manner. Now, more than ever, counterparty risk is a primary concern for market participants. In turn, market participants, including exchanges, hedge funds, and liquidity providers, are all eager to mitigate counterparty risk. As Web3 continues to grow and evolve, these conversations around custody and counterparty risk will only become increasingly important.

Fireblocks' direct custody model is based on five key principles:

1. **Provide a zero counterparty risk environment in holding your assets:** Fireblocks cannot move customer assets or block customers from accessing and releasing funds.
2. **Mitigate internal and external attack vectors:** Fireblocks deploys multi-layer security to defend against internal collusion, cyber attacks, and human error.
3. **Guarantee business continuity:** Fireblocks ensures that customers can recover from the loss of access to their keys or in the event of Fireblocks service disruptions.
4. **Ensure granular control & visibility of every transaction:** Fireblocks provides policy controls for moving funds in and out of your wallets, with audit trails for every transaction stage.
5. **Deliver high performance with ease of use:** Fireblocks provides technology for the instant transferring of digital assets between counterparties without sacrificing security.

Fireblocks has worked closely with EY to bring digital asset custody best practices to the forefront in hopes that digital asset participants can make the best decisions for themselves and their businesses. We hope that this piece of content will create informed discussions to ensure a safer and more secure future in Web3.

Michael Shaulov, Co-founder & CEO
Fireblocks

2 Overview

This artifact is intended to highlight key considerations for institutions or individuals that plan to leverage Fireblocks' Multi-Party Computational MPC wallet infrastructure. The document provides examples of leading practices that are supported by data-driven insights from the Fireblocks platform, as well as firsthand industry experiences supporting digital native and traditional institutions implementing Fireblocks' solution. This document is not intended to opine on the security or operational effectiveness of the Fireblocks solution but provide an overview of the capabilities and considerations users of the solution should assess as part of their solution implementation and design.

Users leveraging Fireblocks' MPC solution have different business requirements, risk appetites, technology infrastructures and regulatory requirements. These criteria will determine how a user may choose to leverage and configure the Fireblocks solution. Given the diversity of requirements and use cases in the digital asset space every key consideration or leading practice outlined below may not be applicable to each individual user.

3 Executive summary

Secure multi-party computational (sMPC or MPC) wallets have emerged as the leading wallet solution implemented by institutions responsible for custody of digital assets. MPC wallets allow for highly secure and scalable self-custody models, with enhanced recoverability features that allow institutions to build reliable digital asset custody workflows. Historically the most challenging aspect of digital asset custody was mitigating the single point of failure risk that private keys presented. As institutions developed enterprise grade custody solutions, they had to manage a tradeoff between security and scalability. Highly secure solutions tended to be less accessible, requiring complex storage mechanism and processes for moving assets between hot and cold storage, while highly accessible solutions often lacked the level of security institutions required. Additionally managing a large number of wallets and accurately tracking client assets and transactions was a significant hurdle, leading to robust off-chain ledger systems and omnibus wallet structures.

MPC wallets emerged as an efficient way to manage wallets and provide custody services in a way that was both secure and scalable. Instead of a single private key, that can be stolen or lost, MPC solutions leverage Threshold Signature Schemes (TSS) to create and distribute independently held "shares" of a private key, such that no one single person controls the entire private key and unilaterally make transactions. These shares are often geographically distributed, held by multiple providers and stored in hardware devices or software, such as cloud instances. Robust approval and orchestration layers, built on top of these secured key shares, combined with the use of hierarchical deterministic (HD) wallets, provide institutions with the ability to design and implement robust governance structures around the custody of digital assets, which historically was highly manual or operationally intensive. This led to an increase in the level of security, availability, and scalability of institutions key management processes and reduced the risk of a single point of failure or abuse.

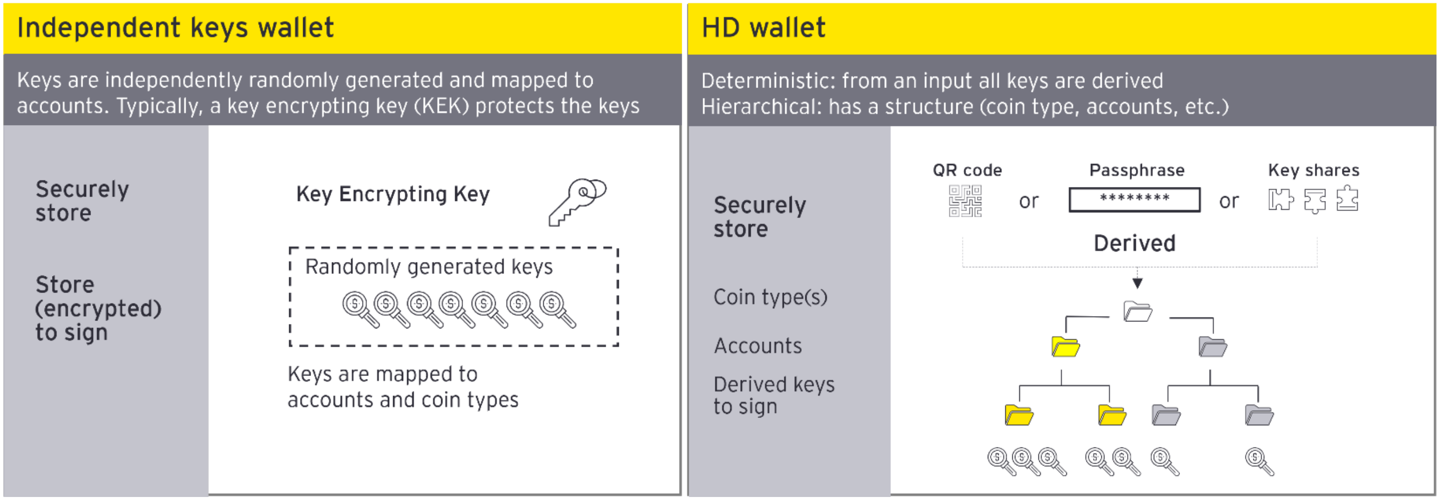
Fireblocks, a leading MPC wallet infrastructure provider, offers a self-custody MPC solution and network that allows users the ability to design and implement custody workflows with robust controls and oversight in place. The Fireblocks' MPC solution allows users to build custody workflows that have embedded maker/checker steps, enforceable trade limits, flexible authorization requirements and recovery capabilities. These capabilities serve as enablers but are generally not comprehensive enough to fully mitigate the risks associated with institutional key management. Institutions are still responsible for determining the capabilities to leverage, implementing the capabilities and ensuring they are maintained and reviewed on an ongoing basis. In addition to the Fireblocks capabilities leveraged, an institution may need to implement additional controls and procedures to effectively manage the use of the custody solution and ensure proper governance is in place.

The artifact below highlights a subset of considerations related to key management and identifies industry-leading practices based on the core capabilities that Fireblocks' offers around the governance, generation, storage and recovery of key shares, as well as the processes and controls institutions have implemented to support and govern the Fireblocks' solution.

4 Digital assets and custody

There are a variety of digital assets that exist today including fungible digital assets and non-fungible digital assets. Fungible digital assets can include assets such as native protocol assets (bitcoin or ethereum), utility tokens (Chainlink – Link tokens), governance tokens (Uniswap or Aave tokens), payment tokens (USDC or USDT tokens) and even hybrid tokens which can be a combination of asset types. Non-fungible assets on the other hand digitally represent unique, non-interchangeable assets such as music, art, real estate, and a broad range of other assets in the real (or virtual) world and may contain unique programmable contract features and rights on an individual asset by asset basis. Digital assets are effectively bearer assets where the bearer is the holder of the private key. As such, the wallet plays a critical role in safeguarding access to digital asset accounts and establishing an institution or individual's ownership and control over their digital assets.

Regardless of the classification of a digital asset, it can be held or "custodied" within some form of a digital or hareware wallet. Wallets are used to manage and prove ownerships of accounts and track account balances (in some cases unspent transaction outputs) as transactions are processed and recorded on the blockchain. The core functionality of a wallet is to store the cryptographic key material used to prove ownership of the account(s) and allow asset holders to submit valid transactions on the network (in most cases a blockchain). In the simplest form of digital wallet an account or public address has a single private key that is used to sign transactions. More complex wallet types are able to derive multiple accounts across coin types and generate an endless number of public/private key pairs; these wallets are referred to as Hierarchical Deterministic (HD) wallets. Refer to the example below for a high-level overview of the distinction between independent keys wallet and HD wallets:



Independent keys wallet

Keys are independently randomly generated and mapped to accounts. Typically, a key encrypting key (KEK) protects the keys

Securely store
Store (encrypted) to sign
Key Encrypting Key
Randomly generated keys
Keys are mapped to accounts and coin types

HD wallet

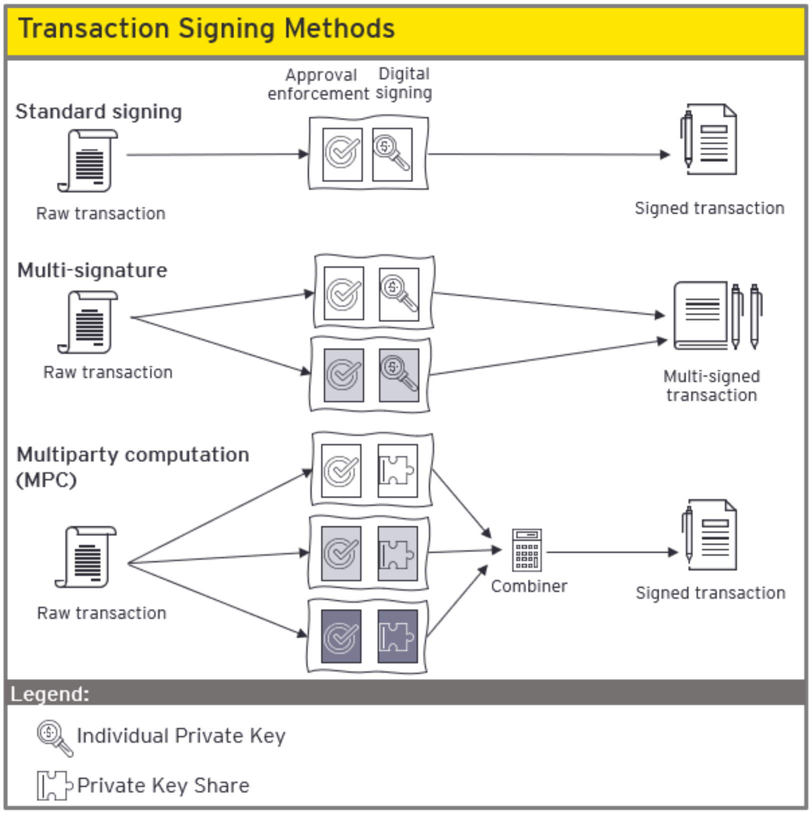
Deterministic: from an input all keys are derived
Hierarchical: has a structure (coin type, accounts, etc.)

The evolution of institutional self-custody

Self-custody solutions were initially developed for retail users, which is why single signature hardware wallets and browser-based wallets were the most highly adopted wallets in the digital asset space. These wallets may have been sufficient for individual users, but institutions that require using several wallets (sometimes thousands), with significant transaction volumes and sizes on a daily basis, need a more robust solution. Additionally, single signature wallets presented a single point of abuse, where any individual that gained access to a private key would be able to make unilateral transactions on the corresponding digital asset account and the assets within. Given these limitations institutions had to choose between various tradeoffs around security, recoverability, availability, and ease of usability.

This prompted the use of multi-signature wallets (multi-sig), which require multiple accounts to sign and approve transactions and secure multi-computational wallets (sMPC), which allow for the use of distributed key shares and threshold signing capabilities (m of n shares required for transaction signing).

The most significant difference between multi-signature wallets and sMPC is that in a multi-sig scheme, multiple private keys are maintained separately, and multiple signatures are required to submit a valid transaction; conversely, with sMPC the private key is broken up into shares, encrypted, and often distributed between multiple parties and locations and a valid transaction is created by bringing together a minimum number of shares to produce a single valid signature. These distinctions are outlined in the graphic below:



Fireblocks' MPC wallet infrastructure

Fireblocks is a leading MPC wallet infrastructure that provides users with institutional grade self-custody and a robust suite of capabilities that enables Fireblocks customers to manage their digital assets efficiently and securely. Fireblocks wallets are built on the MPC-CMP protocol, an internally developed advanced implementation of MPC cryptographic technology, that allows users to implement secure and flexible custody workflows.

5 Key (share) management lifecycle

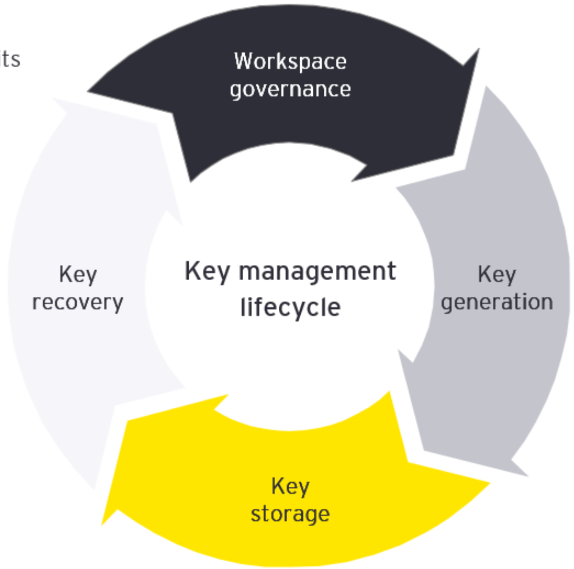
Management of keys or key shares can be broken down into a subset of components or stages that typically occur in a certain order and make up what is referred to as the key lifecycle. Each component has unique risks and considerations and is highly dependent on how an institution elects to integrate and leverage the Fireblocks' MPC solution (or other wallet service provider) and the internal processes and controls they implement to manage the solution. The following graphic provides an example of the key management lifecycle for an institution using Fireblocks and includes high-level considerations, which are discussed in more detail in the following sections.

Workspace governance

- Vault design and setup
- Transaction and approval limits
- Approval vs. signing roles
- Access and role reviews
- Vault parameter changes

Key generation

- Generation authorizations
- Key sharding methodology
- Key share generation ceremony
- Key share transmission security
- Segregation of duties



Key recovery

- Recovery authorization and approvals
- Secure recovery storage
- Secure recovery testing
- Insurance

Key storage

- Cold vs. warm vs. hot storage
- Cloud vs. hardware storage
- Geographic distribution
- Physical hardware security
- Cloud infrastructure security

Workspace governance

Understanding and properly managing the overall process of generating, storing, transacting, and recovering private keys is complex. Each step presents a unique set of risks that need to be considered and often involves multiple individuals, business lines and systems, internally and externally. Ensuring that there is proper oversight and governance of the end-to-end key management process is critical to successfully developing, implementing, and maintaining a custody solution. Even if a third-party custodian or wallet service provider is leveraged, the steps performed by the third-party should be understood and documented and any handoffs or integrations with the third-party should be reviewed and monitored to ensure proper safeguards are in place.

Fireblocks provides software and a SaaS solution that allows users to store, transact and recover their digital assets. Users can build custody workflows based on their specific use cases and business requirements using the programmable features embedded within the solution. It is important that users understand which elements within the custody workflow they are responsible for maintaining. Users have the flexibility to set parameters that the software will enforce but the parameters must be reviewed and challenged by the User on an ongoing basis. Additional checks and controls outside of the software and SaaS solution should be put in place by users to ensure the custody process is sufficiently governed.

The Fireblocks solution is comprised of the following structures: workspaces, vaults and vault accounts. A workspace is the highest level of account and for each workspace a single owner is assigned with a preset list of privileges. Within each workspace any number of vaults can be created based upon the needs of the business, client demand or regulatory requirements. Lastly, within each vault, vault accounts can be setup and each vault account can contain one

wallet for a particular asset type. There are several different ways in which vaults can be structured to ensure both internal and external requirements are met. Additionally, on top of these vault structures, Fireblocks provides an approval engine that can be used to assign and enforce user roles and transaction-related restrictions. This approval engine is frequently referred to as the orchestration layer and enables institutions the ability to implement governance processes that can be set according to an institutions needs and risk tolerances for transactions volumes and limits.

The following are example capabilities the Fireblocks' solution provides that can be leveraged to govern the key management process:

Example Fireblocks capabilities:

- Admin Quorum – a set of selected individuals responsible for approving workspace configuration changes and defining the whitelisted space to which funds can be sent outside of a user's vault(s)
- Transaction Authorization Policy (TAP) – is a rule engine that governs outgoing asset transactions to determine the appropriate action (allow, block, or require additional approval)

Examples of parameters that an end user is responsible for setting can include but are not limited to:

- Determining the number of workspaces
- Determining the number of vaults
- Assigning access to vaults and workspaces
- Determining which assets are acceptable for the user
- Adding or removing whitelisted addresses
- Determining which users have signing capabilities
- Setting the user roles
- Defining the number of approvals required for transactions
- Defining number of signors required for transactions
- Setting transaction limits

The following table outlines a list of critical considerations, related to the governance of the key management process, that intuitions leveraging Fireblocks MPC solution should consider. For each critical consideration a leading practice example is provided. The leading practice may be an incremental business operation a user has implemented, an internal technical capability a user has developed, or an existing capability provided by the Fireblocks MPC solution, which is denoted within the table.

Critical consideration	Leading practice	Internal business operation	Internal technical capability	Fireblocks enabled capability	Fireblocks or Industry Insight
1. Has a process been established for determining vault owners and access rights to the vaults within the Fireblocks' solution or applications with access to the Fireblocks' solution been established?	✓ Workspace access and permissions align to current roles and requirements across business lines, operations and audit functions and are set up to proactively enforce segregation of duties.	X		X	***Fireblocks Capability:*** *Fireblocks provides customers with seven different roles to choose from with varying degrees of functionalities and access*
	✓ Clearly defined process for making changes to user roles is in place and aligns with or is integrated into the existing access management program.	X			
2. How has the institution leveraged the user roles within the Fireblocks' solution to ensure sufficient segregation of duties and reviews?	✓ User roles within the workspace are based on specific business line requirements, access requirements and are clearly documented and where possible separation of signing and submission are in place.	X		X	***Fireblocks Insight:*** *On average Fireblocks users have 3.5 administrators per workspace*
3. How frequently are the user roles and permissions in the Fireblocks' platform or the applications connected to Fireblocks reviewed?	✓ Ongoing reviews of vault owner(s) and user permissions align with existing access management review cadences and are incorporated into existing access management program.	X		X	
4. How are the vault parameters and rules configured and who approves parameter configurations?	✓ A policy is in place to outline vault parameter configurations including documentation of thresholds set and rational, frequency of ongoing reviews and roles and responsibilities across business lines.	X		X	***Fireblocks Capability:*** *There are 16 unique rule parameters that can be leveraged that can be combined and customized based on business requirements*
	✓ Regular reviews of the vault parameters are integrated into the existing change management programs. If no change management program is currently in place, then a robust vault parameter review process is created and performed on a regular basis.	X		X	***Fireblocks Insight:*** *Fireblocks users on average set 9 rules with retail and traditional financial institutions that require more robust rule sets setting on average 12+ rules*

Critical consideration	Leading practice	Internal business operation	Internal technical capability	Fireblocks enabled capability
5. Is there proper governance surrounding the management of wallets and key share(s) and is this sufficiently documented?	✓ A Digital Asset Steering Committee is established that meets on a reoccurring basis to discuss major industry updates, strategy decisions and any recent security or operational incidents that occurred. The committee includes executive leadership and the necessary stakeholders across the various functional areas such as technology, cybersecurity, compliance, etc.	X		
6. How is the institution planning to monitor or review transactions?	✓ Clear processes are in place for review and approval of transactions prior to signing. Approval workflows within the Fireblocks' solution may be leveraged to enforce transaction limits and create tiered approval structures for transactions based on size and volume.	X		X
	✓ Automated reviews and monitoring capabilities are in place based on real-time reconciliations, pre-set monitoring rules, whitelisting checks, etc.		X	X
	✓ Limiting the transactions with "one-time addresses" and leveraging the whitelisting capability in addition to setting sufficient approval or blocking limitations allows for more secure transactions.	X		X
7. What controls are in place to prevent a single point of abuse with the workspace owner?	✓ Workspace owners should not be allowed to submit transactions and perform administrative functions such as generating a new vault or new key share(s).	X		X
	✓ Robust monitoring controls are in place to detect and alert of any suspicious activity such as large trades, vault permission changes or new key generation events.		X	

Fireblocks or Industry Insight

Fireblocks Capability: *Signing capabilities are limited to Owner, Admin and Signer roles within the workspace*

Fireblocks Capability: *Fireblocks offers a list of vetted counterparties operating on the Fireblocks network*

Key share generation

The generation of the private key shares is one of the most important steps within the key management lifecycle, if not securely performed it can jeopardize the security of any assets subsequently held within associated wallets. At no point during the key generation ceremony should the key shares be brought together or should a single individual have access to all the key shares and there should be strictly enforced controls around monitoring the generation process to ensure compliance. Subsequent to the initial generation, strict segregation of duties and access controls should also be in place between individuals who are able to access the initial key shares, who is able to submit and sign transactions, and who is able to recover or generate new key shares.

There are two distinct types of key share generations that occur on the Fireblocks' platform. The first is the initial generation of the key shares related to the setup of a workspace. This is a highly secure ceremony conducted by Fireblocks with robust controls in place around ensuring segregation of duties. This process and the associated controls are reviewed by an independent third party and adheres to leading international security standards. As part of this ceremony a workspace owner, selected by the institution, will have to set a secure passphrase and setup an initial account. The second key share generation ceremony relates to the setup of any additional users that require signing capabilities within the workspace (admins or signers). This process is highly automated and requires the workspace owner to approve the requests prior to the new MPC shares being generated. A clearly defined policy should be in place around obtaining proper approvals and tracking users with MPC shares and signing capabilities on an ongoing basis.

The following table outlines a list of critical considerations, related to the generation of private key shares, that institutions leveraging Fireblocks' MPC solution should understand and assess. For each critical consideration a leading practice example is provided. The leading practice example may be an incremental business operation a user has implemented, an internal technical capability a user has developed, or an existing capability provided by the Fireblocks' MPC solution, which is denoted within the table.

Critical consideration	Leading practice	Internal business operation	Internal technical capability	Fireblocks enabled capability
1. What documentation and processes are there around the key ceremony, transfer, and subsequent storage of shares?	✓ Within an existing key or key share management policy the key generation workflow that the institution is required to follow is defined and includes the required approvals, steps to follow and security measures that users must adhere to.	X		

Fireblocks or Industry Insight

Critical consideration	Leading practice	Internal business operation	Internal technical capability	Fireblocks enabled capability
2. Who within the organization has the authority to initiate a new key generation or setup a new workspace and what does the institution have in place for reviewing any new workspaces or changes to existing workspaces?	✓ Ensure proper segregation between individuals' that can generate new key shares, sign transactions, and initiate key share recoveries.	X		X
	✓ New key share generations or changes to existing key shares are required to be approved by the appropriately designated executive(s), on top of the workspace Owner approval, prior to initiation within the Fireblocks' solution and documentation of the approvals are retained.	X		
	✓ An automated monitoring capability is implemented by the User to monitor, flag, and record significant changes such as new key share generations or changes to existing key shares, outside of the Fireblocks' platform.	X	X	
3. How does the institution plan to securely obtain the key share(s) once generated by Fireblocks?	✓ Workspace owner passphrases used during setup are securely maintained and managed during the key generation ceremony and properly disposed of once the key share is obtained and the generation ceremony is concluded.	X		X
4. How is/are the share(s) maintained by the institution going to be received and will the transfer of the share be encrypted or sent via secure channel?	✓ Transfer of key shares are done via secure application programming interfaces[1] (APIs) or secure channels and is encrypted during transit and at rest.		X	X

Fireblocks or Industry Insight

Fireblocks Capability: *All workspace changes and transactions are recorded and are able to be exported if required*

[1] A collection of functions and procedures that allow users to interact/communicate with the data of an application or service, such as an exchange, to execute the features of the service programmatically.

Critical consideration	Leading practice	Internal business operation	Internal technical capability	Fireblocks enabled capability
5. Are there regulatory requirements or security standards that the key share generation methodology must adhere to?	✓ A regulatory mapping of cybersecurity requirements is established across multiple jurisdictions and is consistently maintained to ensure compliance with all necessary regulatory agencies.	X		
6. What processes and steps has the institution performed to review the Fireblocks' key generation ceremony?	✓ An in-depth review of the key generation process facilitated by Fireblocks and the associated controls in place to ensure the security of the generation ceremony is performed.	X		

Fireblocks or Industry Insight

Key share storage and availability

After the initial key share generation ceremony is completed, the key share(s) must be securely sent, received, and stored. The storage of the key share(s) is one of the most important and complex aspects of key management. Key shares can be stored in cloud architecture or hardware, such as the secure enclave in mobile devices. There are tradeoffs between the security and usability of the custody model based on the storage type selected in addition to significant monitoring requirements, either physical monitoring or software scanning, that institutions must implement.

Fireblocks provides users with optionality in how they wish to custody the key shares. In some cases, due to regulatory or jurisdictional requirements institutions must maintain control of all three key shares, where in other cases institutions may be able to rely on Fireblocks' to securely store some of the key shares. This decision will impact the amount of infrastructure and storage capabilities an institution will be required to have in place. As noted in the "workspace governance" section above, this should also be a consideration when assigning roles within the workspace, as certain roles may require MPC key shares to sign transactions.

Private key shares can be stored in a physical device or on cloud servers. Institutions should understand the tradeoffs when electing where and how to store their keys and ensure their solution aligns to their operational needs and security requirements. An additional consideration is whether the key shares will be stored offline, with no connection to the internet, often referred to as cold storage or whether there will be some degree of ongoing connection to the internet, referred to as warm or hot storage. Similar to the type of storage device decision, there are operational and security tradeoffs that need to be managed. Fireblocks offers cold, warm and hot storage capabilities but is not responsible for ensuring that clients maintain any predetermined balance or mix of assets in the different types of storage. Institutions should ensure they have a robust process in place for managing the availability and security of their digital assets based on the operational needs of their business.

The following table outlines a list of critical considerations, related to the storage of the private key shares, that institutions leveraging Fireblocks' MPC solution should understand and assess. For each critical consideration a leading practice example is provided. The leading practice example may be an incremental business operation a user has implemented, an internal technical capability a user has developed, or an existing capability provided by the Fireblocks' MPC solution, which is denoted within the table.

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
General storage				
1. Is there going to be diversification between the different platforms used to store key share(s) (OS, Cloud, Hardware Security Modules ((HSMs))?	✓ Key share(s) are stored across a diverse mix of storage types, such as, cloud and OS or HSM and Cloud, that achieves the desired levels of security and operational efficiency required.		X	X
2. What procedures are in place to securely store and manage the key share(s)?	✓ Key shares are automatically refreshed in preset intervals and there are scanning capabilities in place to monitor the stored key shares.			X
3. Will there be multiple internal business lines leveraging the Fireblocks' platform for digital asset transactions and will business lines require the same mix of storage and usability capabilities?	✓ The key management strategy defines expected transaction volumes across business lines and required security/vault limits that inform the wallet mix of hot/warm/cold storage.	X		
4. Is a third-party planning to be leveraged to store any of the key share(s)?	✓ Third-party storage providers that are leveraged have well defined policies and controls frameworks in place that have been tested by third parties and are subject to extensive third-party management onboarding reviews, including review by internal cybersecurity experts, prior to onboarding.	X		

Fireblocks or Industry Insight

Fireblocks Insight: *On average 39% of Fireblocks users keep some portion of their digital assets in hot wallets*

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
5. What is the current mix of cold/warm/hot storage?	✓ An analysis has been conducted by management to define the key operational requirements for the applicable digital asset product or service. A mix of hot, warm and cold wallets are used to meet the security and operational requirements of the organization.	X		X
6. How is the mix of cold/warm/hot vault wallets monitored and maintained?	✓ A robust wallet management functionality is in place to monitor the existing mix of assets between cold/warm/hot storage. A clear policy has been defined that outlines the thresholds for each wallet and asset with clear escalation and communication channels.	X	X	
Mobile storage				
1a. What procedures are in place to ensure sufficient security of any mobile devices used for storing key shares?	✓ Hardware used for hosting key share should adhere to all existing institutional hardware requirements and leading industry standards.	X		
1b. How will retirement or replacement of hardware be completed upon termination?	✓ A robust policy around retirement of mobile devices used to store key shares should be in place and in the case of lost or stolen devices there should be a clear escalation and notification channel between information security and Fireblocks to ensure a timely response.	X		
	✓ Additional safeguards are in place around the retirement of hardware owned by workspace owners' and upon notification of termination these are critically followed up on and tracked.	X		

Fireblocks or Industry Insight

Fireblocks Insight: *The most frequent driver for key share regeneration the loss or damaging of mobile devices storing key shares*

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability	Fireblocks or Industry Insight
Cloud storage					
2a. Is the share stored in the cloud encrypted at rest and during transition?	✓ Data is encrypted at rest and during transfers using industry-leading encryption[2].		X	X	
2b. Is there diversification amongst cloud providers leveraged to secure key shares?	✓ Multiple leading cloud providers are used and there is geographic distribution of data centers.		X	X	***Industry Insight:*** *Institutions should seek to comply with industry leading practices and standards, for example International Organization of standardization – Cloud ISO/IEC*
2c. Does your institution have prior experience with using and leveraging cloud technology?	✓ Internal experts are involved in the deployment of the cloud architecture, including the CISO and CTO, or external experts are leveraged to deploy and monitor the cloud architecture used to store key shares.	X			
2d. Are there existing information security or technology processes and procedures that are compatible with cloud technology?	✓ Establish robust cybersecurity and information security practices around the cloud architecture including dynamic and static scanning capabilities or identify new processes and controls and embed within the existing information security program.	X	X		
2e. How is the institution planning to manage changes to the cloud architecture?	✓ Changes to the cloud architecture are included in the existing change management program and tracked accordingly. If no program currently exists than a clear process is outlined and reviewed to ensure the appropriate reviewers are involved from information technology and information security.	X	X		

[2] Conversion of information or data into a secure code in order to prevent unauthorized access to the information or data.

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
Hardware storage				
3a. Are any key shares planning to be stored in physical hardware devices such as a hardware security module (HSM)?	✓ All hardware used to store key shares adheres to leading industry standards and a review is performed by the information security team on a reoccurring basis to ensure the hardware is still in line with leading industry guidance.	X		
3b. What physical access controls will the institution have in place to securely protect the key share(s)?	✓ Access to physical HSMs is restricted to only approved individuals and there should be surveillance and multi-party access requirements in place to avoid a single point of abuse.	X		
3c. Are HSMs containing key share materials geographically disbursed?	✓ HSMs used to store key material are geographically disbursed with robust security and disaster recovery procedures in place.			

Fireblocks or Industry Insight

Industry Insight: *Entities using HSMs to store cryptographic key shares should ensure the modules are compliant with existing cyber standards such as FIPS 140-2 issued by the National Institute of Standards & Technology (NIST)*

Key share backup and recovery

The ability to securely recover digital assets in the event a private key is lost or stolen is one of the most important aspects of digital asset custody. A key backup can be a password or mnemonic, written on paper and securely stored, or copies of private key shares stored on air gapped hardware security modules or secure cloud environments. How these backups are stored and accessed is equally as important as how the existing key shares are stored.

The storage of the backup warrants the same level of security as the keys or shares used in the day-to-day operations, which is often overlooked or not assessed as part of the initial setup. No matter how secure a solution design and storage, there will always be human elements and unforeseen events that can occur, which can lead to the need for recovery. Two critical components that institutions should consider when assessing their key recovery processes related to Fireblocks are:

1) **Storage:** Institutions should review how the backup material is stored and understand the security measure taken such as encryption techniques or access limitations, whether the backups are geographically disbursed and, in the event, a third party is being leveraged, what ongoing procedures are performed.

2) **Testing:** Institutions should perform ongoing testing of the recovery capabilities and process leveraging a simulation environment to test that the backups are not corrupted and ensure the responsible parties understand the necessary steps to be taken.

Fireblocks allows institutions to perform two types of recovery procedures, soft recovery or hard recovery, depending on if a single signing device (hosting a key share) is lost or if access to all signing devices is lost at the same time.

- Soft Recovery: Recover a specific devices key share but requires that the institution still have access to at least one other MPC share related to that workspace. The most common causes for a soft recovery are loss of the mobile device, inability to access the device's MPC key share, or migration to a new device. Soft recovery creates a new set of MPC key shares on the newly paired device once completed. [3]
- Hard Recovery: Reconstruction of the entire private key seed of a workspace vault. All operations are halted while the wallet structure is restored or migrated, and it requires the workspace owner's recovery passphrase.

The Fireblocks' MPC solution is designed to avoid a single point of compromise by distributing the private key shares and signing capabilities but if a hard recovery is required, this risk may be reintroduced if not performed in a secure manner, due to the generation of the extended private key in a single location. Institutions are directly responsible for ensuring the security of the hardware, software and passwords used to facilitate a hard recovery. This allows institutions the ability recover their digital assets even if the Fireblocks' platform is unavailable. Due to the need for secure testing and storage, developing a safe and repeatable key recovery testing methodology remains challenging. Even if institutions elect to outsource this responsibility assessing the process and security measures the third party takes to store and test the recovery functionality is an important consideration.

The following table outlines a list of critical considerations, related to the recovery of the private key shares, that institutions leveraging Fireblocks' MPC solution should understand and assess. For each critical consideration a leading practice example is provided. The leading practice example may be an incremental business operation a user has implemented, an internal technical capability a user has developed, or an existing capability provided by the Fireblocks' MPC solution, which is denoted within the table.

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
General				
1. Are the backups sufficiently encrypted?	✓ All backups or offline devices used in a key recovery process are encrypted at rest and stored in either cloud architecture, secured data centers or physical locations that have sufficient cyber and physical security in place.	X	X	

Fireblocks or Industry Insight

[3] If an Owners key share is lost incremental steps are required, such as a video call, due to the increased security requirements and the previous MPC key shares stored on the Owner device are paired to the new device, unlike with the Signor recovery which creates new MPC key shares all together.

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
Soft key recovery				
2. How are the recovery passphrases for Owners or Signors stored?	✓ If physically maintained, access controls are in place to ensure unauthorized individuals cannot gain access. If not physically stored, an industry-leading or internally approved password protection application is leveraged. In both cases a passphrase rotation requirement is in place.	X	X	
	✓ The auto-passphrase feature provided by Fireblocks is setup for users storing key shares on their mobile devices, reducing the likelihood of losing or leaking the passphrase.			X
3. How will the institution ensure that there will always be a way to perform soft key recovery in the case a soft key recovery passphrase is lost?	✓ A minimum of two signing devices are set up on a workspace to ensure that soft recoverability is possible.	X	X	
	✓ A static signing devices with an MPC key share is setup and securely stored to ensure that soft key recovery can always be performed. The passphrase and device are stored separately and require separate individuals to access them.	X		X
4. What are the procedures for ensuring that devices previously holding key shares are properly discarded?	✓ A clearly defined process is in place for secure disposal of all devices hosting key shares upon termination or role change. Deletion of private key shares on new devices when new MPC key shares are generated for signors.			X
Hard key recovery				
4. How will the institution test the recovery functionality on an ongoing basis in a secure manner?	✓ Backup and recovery procedures are routinely tested in a simulation environment, using temporary MPC key shares, to ensure that all components are operating properly, and assets can be recovered by the institution.	X	X	

Fireblocks or Industry Insight

***Fireblocks insight:** The most common cause of soft recovery is due to loss of mobile device; institutions should ensure they properly plan and setup workspaces to allow for proper recovery capabilities*

***Industry insight:** Current recovery testing approaches for MPC solutions may create significant security vulnerabilities if they require recreating the extended private keys as part of the recovery test. Institutions should ensure any recovery testing are secure and that appropriate controls are in place*

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
5. How is the institution planning to test the backups to ensure that they operate as intended?	✓ Establish a secure periodic recovery testing procedure to ensure the recovery mechanism operates as intended without consolidating all key shares in a single location. Testing occurs at a minimum on an annual basis.	X	X	X
	✓ The recovery ceremony has a robust set of controls and procedures to ensure the safety of the backup including physical access controls, multi-step approvals, and in some cases third parties or auditors present.	X		
	✓ Operational drills are performed to ensure that all participants have a clear understanding of roles and responsibilities in the recovery process.	X		
6. How are the backup components planning to be securely stored?	✓ Backup devices, passphrases and backup files are stored in diversified geographic locations and if leveraging a third-party service for storage, different providers as well.	X		X
7. How are the RSA passphrases and Owner passphrases used during recovery secured?	✓ If physically maintained, access controls are in place to ensure unauthorized individuals cannot gain access. If not physically stored, an industry-leading or internally approved password protection application is leveraged.	X		
8. Is the institution planning to store the backups themselves or leverage a third-party provider to store the backup?	✓ Institutions leverage industry-leading data centers or providers to store hardware containing backup key information and restrict the access to each recovery component to separate individuals or parties.	X		
9. Who will have access to the backups and what controls are in place to ensure a single point of failure?	✓ Access to the backup(s) should be restricted to a few key individuals and any recovery functionality should require multiple parties and involve physical access restrictions and monitoring procedures.	X		
10. Is the institution planning to leverage a third-party to assist with facilitating the recovery procedures?	✓ Institutions assisting with or governing the recovery procedures adhere to leading industry standards and are subject to review by well-known third parties, such as audit firms.	X		

Fireblocks or Industry Insight

Additional considerations

In addition to the specific Fireblocks' capabilities and considerations around custody and governance of the wallet and key shares there are additional operations and processes that institutions should assess and understand to effectively transact and service digital assets. This can include the ability to independently confirm transactions, maintain a connection to the various networks, transaction fee monitoring, reconciliations, and a number of other capabilities. These considerations may vary greatly depending on the design of the custody solution but in most cases are applicable to any institution implementing a self-custody solution.

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
Transaction signing and availability				
1. How will transactions be drafted and submitted to the network?	✓ Use of API co-signor functionality to achieve scalable transaction volumes.			X
2. Does the entity plan to have the ability and personnel to submit transactions 24/7 and 365 days a year?	✓ Use of shard replication and a "follow the sun" model allowing for 24/7 access to make and submit transactions.	X	X	
3. Has the institution assessed how the proposed business model would be impacted by traditional business models and requirements and clearly outlined each parties requirements within service level agreements?	✓ Policies and terms of service with clients clearly demonstrate any limitations that traditional business models or working hours may incur on accessibility and the responsibility that the institution has for providing the service.	X		
Reconciling and reporting				
4. How would an institution reconcile balances if they use the Fireblocks' self-custody solution?	✓ Three-way reconciliations between Fireblocks, internal ledgers, and the public blockchain are completed on a transactional basis.		X	X

Fireblocks or Industry Insight

Industry insight: *Traditional business models and operations are often challenged by the global reach and continuous availability of digital assets. Institutions should proactively assess and determine if incremental processes or support is needed to sufficiently address these challenges*

Critical consideration	Leading practice	Internal business operation	Internal Technical capability	Fireblocks enabled capability
5. Is the institution planning to independently obtain blockchain data for account balances and transactions?	✓ Blockchain data is either independently obtained or sourced from a third party provider with sufficient controls in place and reconciled against internal ledgers.	X	X	
6. How are the institutions planning to integrate data from the Fireblocks' platform into existing applications?	✓ API end points are used for recording transactions sent through the Fireblocks' solution network and automated data pulls are set up and integrated with accounting applications daily.		X	
Connectivity and transaction confirmation				
7. How will the institution independently confirm if transactions have been processed?	✓ Independent transaction confirmation and recording processes are built and integrated with the Fireblocks' solution and the blockchain on a real-time basis using the available APIs.		X	
8. How is the institution planning to connect to the network (third party, self-host, etc.)?	✓ Independently run nodes or a node service provider that is well known in the industry and has a SOC report or other documentation available demonstrating information security practices and controls are in place.		X	
9. Is the institution able to monitor the gas[4] fees being charged and submitted to the network?	✓ Gas fees are monitored using built in limit checks during transaction creation. Acceptable gas fee ranges are defined within a procedural document for operations staff or embedded within an internally controlled front-end application.	X	X	

Fireblocks or Industry Insight

[4] The pricing mechanism employed on the native blockchains to calculate the costs of smart contracts operations (if applicable) and transaction fees.

6 How can EY teams help

EY teams have extensive knowledge and is considered a “world leader” in developing and promoting cutting-edge blockchain technology. EY operates a seamless cross service line team including strategists, engineers, risk managers and tax professionals that allows it to build and offer digital asset services that are of industry-leading quality and meet the level of security and operational soundness enterprise-grade systems and processes require. We seek to be a critical strategic collaborator in an institution’s digital asset journey, starting with helping implement secure and scalable custody capabilities and business process.

We have assisted highly regulated global financial institutions as well as digital natives, such as crypto exchanges, in developing and implementing digital asset custody capabilities to meet regulatory and assurance standards over the past five plus years.

We have also provided a broad array of blockchain services including:

- Design and help implement custody solutions, including wallet, key, and storage considerations
- Provide guidance and develop tokenization capabilities
- Design, develop, and review smart contracts
- Develop policies and controls frameworks specific to digital assets
- Design and integrate digital asset systems into existing architecture
- Perform attestations and audits of digital assets
- Perform due diligence assessments of digital assets
- Provide guidance on tax implications and filings
- Provide guidance to establish blockchain and cryptocurrency product strategy

For further information on digital asset services that EY or Fireblocks can support please reach out to brian.stern@ey.com or ahart@fireblocks.com.

7 Appendix A

Glossary of terms

Admin quorum	A preset threshold of how many Admin users must approve administrative actions or activities in a workspace.
Air gapped	Air-gapped wallets are crypto wallets that are completely disconnected from the internet and any form of wireless communication. This generally means that they are disconnected from both traditional internet connections as well as Bluetooth, WiFi, NFC (near-field communication). Transacting often requires the use of USBs.
Application Programming Interfaces (APIs)	An application programming interface, or API, enables computer programs to communicate. APIs are used to extract and share data either internally or externally.
Approval engine	Fireblocks' approval engine, referred to as the transaction authorization policy (TAP), serves as the governance and oversight layer on top of the custody solution. TAP is a set of rules that can be leveraged to dictate limits and approvals for transactions or the movement of funds.
Bearer instrument	A bearer instrument is an instrument that entitles the holder of the document to the underlying asset and acts as the sole proof of ownership.
Browser-based wallets	Browser-based wallets are a type of digital wallet that is accessed and managed through a web browser. These wallets are often hosted on a centralized platform or server, and do not require users to download or install any additional software or apps. Popular examples include Metamask and Coinbase wallet.
Cold storage	The private keys stored completely offline on a device that is not connected to the internet. Signing of transactions occurs in an offline device prior to be sent to the public network.
Fungible digital assets	Fungible digital assets are cryptographic assets on a blockchain where all instances of that token or asset are identical and interchangeable. Two different fungible assets serve the same purpose even when they are divided or exchanged with other fungible assets of the same type.
Governance tokens	A governance token is a smart contract-based token that can be used to participate in the governance of a protocol by serving as a voting mechanism.
Hard recovery	Hard recovery consists of a complete reconstruction of the extended private key of the Fireblocks' vault. All operations are halted while the wallet structure is restored or migrated, and it requires the workspace owner's recovery passphrase.
Hierarchical deterministic (HD) wallets	HD Wallets are a type of digital wallet that can generate a hierarchical structure of public and private addresses from a single master seed using a derivation method.
Hot storage	Hot wallets are connected to the internet, so the private keys required to sign transactions are always online.
Hybrid tokens	Hybrid tokens refer to tokens that fit into more than one existing classification (utility, governance, payment).
Key shares	A key share is a component of the computational data required to generate a private key. A combination of key shares can be used to regenerate the extended private key or sign transactions.
Mnemonic	Mnemonics is a group of words, usually 12, 18 or 24 words, that a digital wallet relies upon to generate a private key when a new digital asset wallet is created.
Multi-party computation (MPC)	MPC is a cryptographic protocol used to sign and validate transactions that distributes a computation across a set of parties where no individual party has access to other parties' computation.
MPC-CMP protocol	MPC-CMP is an open, free-to-use MPC protocol developed by Fireblocks' research and development team, that reduces the transaction signing up processes required by historical MPC solutions.
Multi-signature wallets	A multi-signature wallet ("multisig" for short) is a cryptocurrency wallet that requires two or more private keys to sign a transaction.

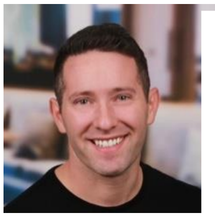
Native protocol assets	Native protocol assets are digital assets that are built into and operate on the underlying blockchain, such as Bitcoin and Ethereum, that are used to pay for network fees or facilitate consensus.
Non-fungible digital assets	Non-fungible digital assets are cryptographic assets on a blockchain where each individual asset or token is unique from every other form or version of the asset.
Omnibus wallet structures	Omnibus wallet structures are digital asset wallet structures that combine clients' digital assets into single wallets, often by asset type (i.e., BTC, ETH, SOL, etc.) to maintain custody of digital assets more efficiently. Offline ledgers are used to track existing customer balances in and out of the wallets.
Payment tokens	A payment token is a digital representation of value, often pegged to a fiat currency value, that is used as a means of payment.
SaaS solution	A SaaS solution is a software service that can be directly accessed and used by clients over the internet and involves storing the application.
Self-custody solutions	A self-custody wallet solution is a solution where the owner of the digital wallet holds and maintains the cryptographic private key material.
Single point of failure	A single point of failure refers to a person, entity, technology or application that if inaccessible would inhibit or limit the ability to continue operations.
Single signature wallets	A wallet solution that has a single public address paired with a single private key. The private key is required to sign transactions.
Soft recovery	Soft recovery involves regenerating key shares from the same master seed but requires that the institution still have access to at least one other MPC share related to that workspace. Soft recovery creates a new set of MPC key shares on the newly paired device once completed.
Threshold Signature Schemes (TSS)	Threshold Signature Scheme (TSS) is a cryptographic method for generating keys and signing transactions among a distributed group of parties. These signature schemes allow users to set a threshold of required users, often referred to as "t of n", where n is the total number of participants and t is the threshold of parties required to be met.
Transaction Authorization Policy (TAP)	TAP is the transaction approval layer of the solution. Within the TAP are a set of rules that dictate the limits and boundaries around the movement of assets.
Utility Tokens	A utility token is a smart contract-based token that can be exchanged for a service provided by a protocol, for example obtaining pricing data for a service provider.
Vault	Within each Fireblocks workspace any number of vaults can be created with based upon operational requirements or client segregation. Within a vault, vault accounts that related to various types of digital assets can be setup.
Vault Account	A Fireblocks vault account contains a digital wallet for a particular asset type.
Warm Storage	Warm wallets are connected to the internet and transactions can be created automatically, but human involvement is needed to sign the transaction and send it to the blockchain.
Whitelisted Addresses	A whitelisted address is an individual public address that an administrator or user with the proper privileges trusts and elects to transact with on the Fireblocks network.
Workspaces	A workspace is the highest level of account and for each workspace a single owner is assigned with a preset list of privileges. Within each workspace administrators can set up any number of vaults.

Primary Authors

Chen Zur

US Blockchain Practice Leader

chen.zur@ey.com



Brian Stern

Blockchain Consulting
Digital Asset Strategy & Risk
brian.stern@ey.com

Aaron Stafford

Blockchain Consulting
Digital Asset Strategy & Risk
aaron.stafford@ey.com

Additional Key Contributors

Arwin Holmes

Global Blockchain
Chief Technology Officer

arwin.holmes@ey.com

Yair Frankel

Blockchain Cybersecurity and Custody Expert

yair.frankel@ey.com

David Byrd

Blockchain Strategy Leader for Assurance

david.byrd@ey.com

Yaniv Sofer

Blockchain Technology Lead

yaniv.sofer@ey.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of
Ernst & Young Global Limited operating in the US.

2301-4169080
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice

ey.com