
21ST CAPITAL

# BITCOIN VAULTS FOR ORGANIZATIONS

Nov. 2024

## Enhancing Organization Security with Bitcoin Vaults

Author: Ziya S.
Date: November 29, 2024
Email: contact@21stcapital.com

www.21stcapital.com

# Enhancing Organization Security with Bitcoin Vaults

## Introduction

Securing Bitcoin assets within an organization poses unique challenges. Traditional methods like single-signature (single-sig) and multi-signature (multi-sig) wallets have inherent risks that can make it nearly impossible to establish a truly secure setup. However, with the advent of Bitcoin vaults employing multi-layered architectures, organizations can now implement more flexible and robust security policies enforced by the Bitcoin network itself.

## Challenges with Traditional Methods

Single-sig wallets rely on one private key to access and manage funds. In an organizational context, this approach is fraught with risks. If the individual holding the key passes away unexpectedly, the organization may permanently lose access to the funds. A single point of failure makes it easier for malicious actors to steal the key and, consequently, the organization's assets. Relying on one person requires immense trust, which can be problematic if that trust is broken.

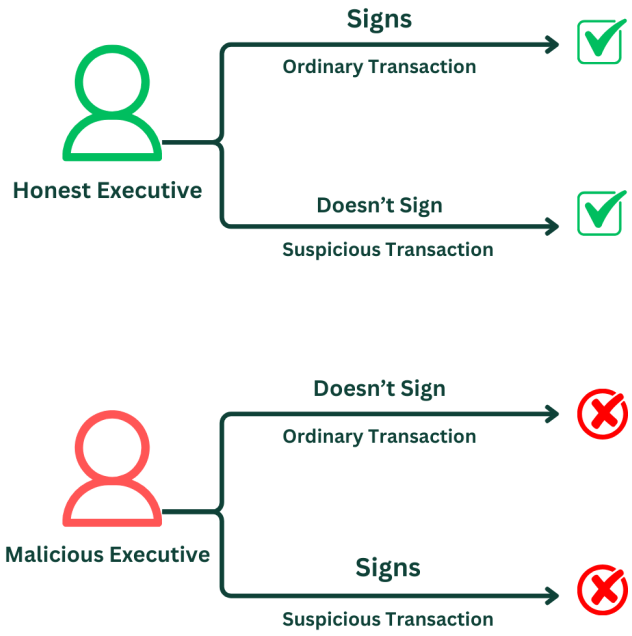
- **Death of Key Holder**: If the individual holding the key passes away unexpectedly, the organization may permanently lose access to the funds.
- **Theft**: A single point of failure makes it easier for malicious actors to steal the key and, consequently, the organization's assets.
- **Trust Issues**: Relying on one person requires immense trust, which can be problematic if that trust is broken.

Multi-sig wallets require multiple keys to authorize transactions, distributing control among several parties. While this improves security, it introduces other issues. Co-signers may refuse to sign transactions, either maliciously or due to internal conflicts, effectively blocking access to funds. If one or more co-signers lose their keys and the required signing threshold cannot be met, the funds become irretrievable. Without a recovery mechanism, lost or inaccessible keys can render the wallet unusable.

- **Key Withholding**: Co-signers may refuse to sign transactions, either maliciously or due to internal conflicts, effectively blocking access to funds.
- **Loss of Keys**: If one or more co-signers lose their keys and the required signing threshold cannot be met, the funds become irretrievable.
- **Unrecoverable Wallets**: Without a recovery mechanism, lost or inaccessible keys can render the wallet unusable.

## Cosigners as Policies

In traditional multi-sig setups, cosigners (human beings) effectively act as policies. They can choose to sign (approve) or not sign (deny) transactions. By refusing to sign suspicious transactions, they help prevent theft. However, cosigners might become uncooperative or act against the organization's interests, leading to blocked transactions or unauthorized actions. This reliance on human behavior introduces unpredictability and potential vulnerabilities. To mitigate these risks, organizations need security policies enforced by the Bitcoin network itself, reducing dependence on individual actions.



## How Vaults Offer a Superior Solution

Bitcoin vaults utilize a multi-layered security architecture that allows organizations to embed policies directly into their wallet structure, offering solutions to common challenges. By requiring all keys to sign a transaction for it to be valid, no single individual can unilaterally move funds, significantly reducing the risk of theft. For example, an organization requires signatures from all three executives to authorize any transaction, ensuring collective agreement.

To solve key withholding and loss, vaults can implement decaying or expanding multisig mechanisms. In a decaying multisig, the number of required signatures decreases after a predetermined time lock expires. This addresses situations where a cosigner becomes uncooperative or loses their key. For instance, an initial setup of a 3-of-3 multisig wallet converts to a 2-of-3 multisig after the time lock, allowing transactions to proceed with one cosigner missing. While it provides a recovery path, it can reduce security over time as fewer signatures are needed.

Alternatively, expanding multisig mechanisms add additional keys to the required signature threshold after a time lock expires, offering a recovery method without decreasing security. Starting with a 3-of-3 multisig wallet, it becomes a 3-of-4 or 3-of-5 multisig after the time lock, including new keys held by trusted parties. This maintains or enhances security while allowing access if original keys are lost or withheld.

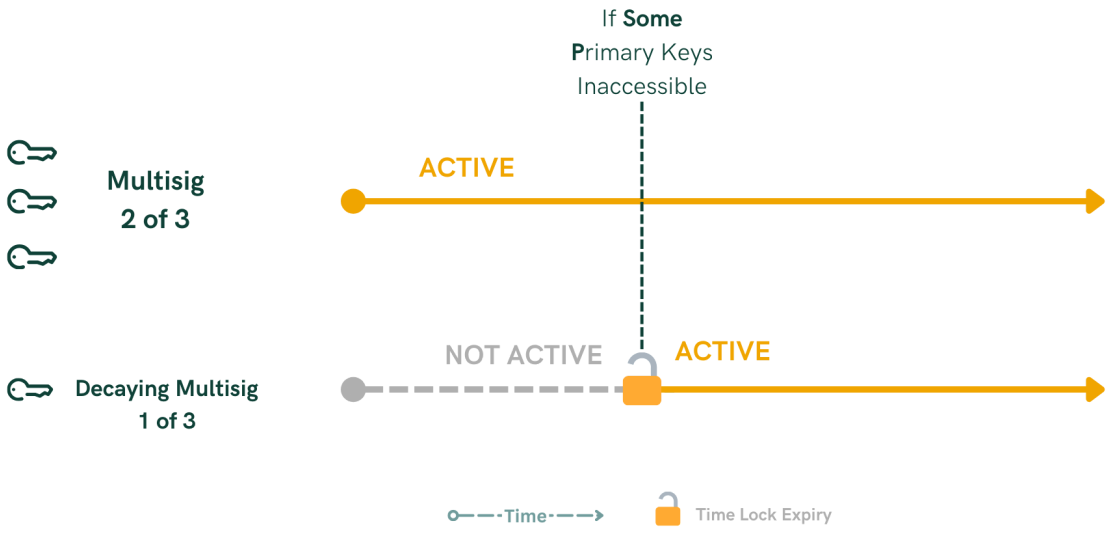
## Preventing Theft with All-Keys-Required Setup

- **Requirement**: All keys must sign a transaction for it to be valid.
- **Benefit**: No single individual can unilaterally move funds, significantly reducing the risk of theft.
- **Example**: An organization requires signatures from all three executives to authorize any transaction, ensuring collective agreement.

## Solving Key Withholding and Loss with Decaying or Expanding Multisig

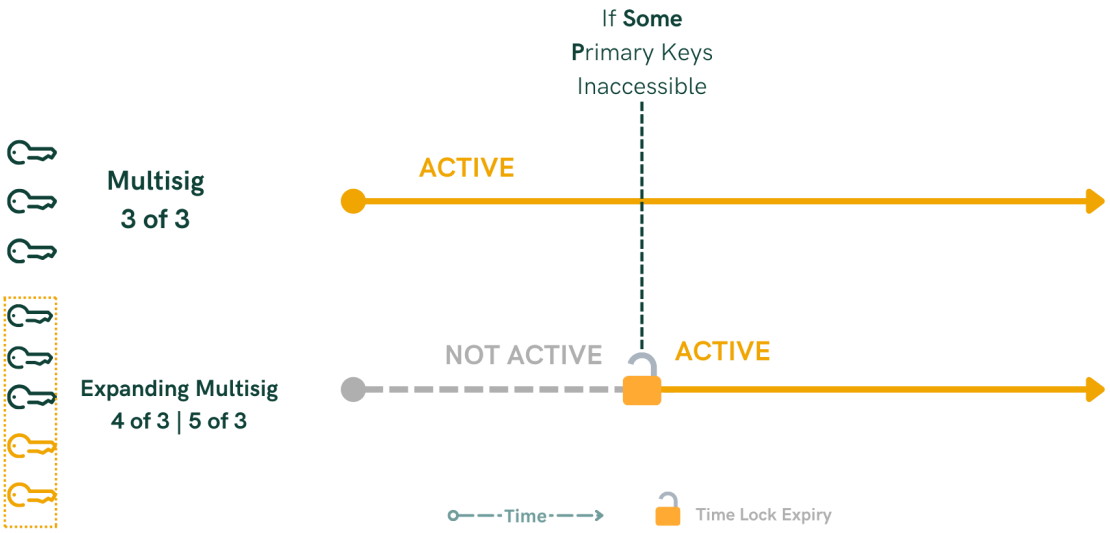
### Decaying Multisig

- **Mechanism**: The number of required signatures decreases after a predetermined time lock expires.
- **Usage**: Addresses situations where a cosigner becomes uncooperative or loses their key.
- **Example**:
  - Initial Setup: A 3-of-3 multisig wallet.
  - After Time Lock: Converts to a 2-of-3 multisig, allowing transactions to proceed with one cosigner missing.
- **Consideration**: While it provides a recovery path, it can reduce security over time as fewer signatures are needed.



**Expanding Multisig**

- **Mechanism**: Additional keys are added to the required signature threshold after a time lock expires.
- **Usage**: Offers a recovery method without decreasing security.
- **Example**:
  - Initial Setup: A 3-of-3 multisig wallet.
  - After Time Lock: Becomes a 3-of-4 or 3-of-5 multisig, including new keys held by trusted parties.
- **Benefit**: Maintains or enhances security while allowing access if original keys are lost or withheld.

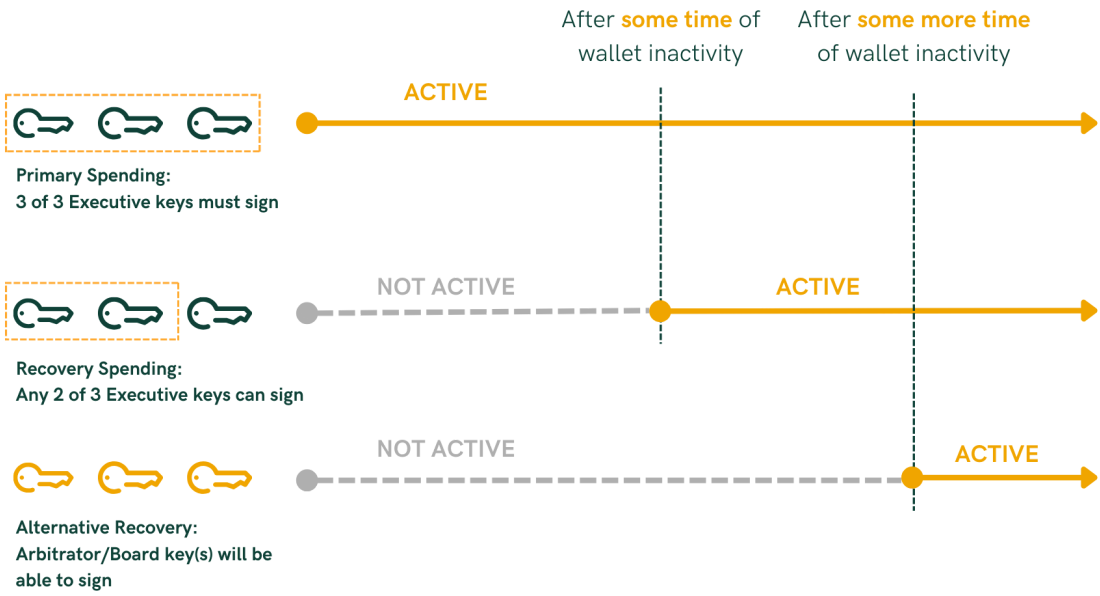



Another strategy is the use of third-party cosigner swapping to enhance security and ensure continued access to funds. In this setup, the organization includes a trusted third-party cosigner—such as a security firm—in the initial multisig configuration to provide an extra layer of security. Recognizing that this cosigner might, for various reasons, refrain from signing or withhold their key, the wallet is designed so that after a predetermined time lock expires, a secondary third-party cosigner becomes active in the next layer. This allows the organization to bypass the uncooperative primary cosigner without compromising security, as the secondary cosigner takes over their role. This mechanism ensures that reliance on external cosigners does not become a single point of failure and enhances the resilience of the organization's Bitcoin holdings by embedding a policy enforced by the Bitcoin network itself.

## Arbitration for Conflict Resolution

Organizations may face internal conflicts where key holders refuse to cooperate. After a time lock, a new layer activates, enabling the board of directors or an appointed arbitrator to access the funds. Arbiter keys are held by neutral parties within the organization or trusted external entities like law firms. For example, if executives are in disagreement and refuse to sign off on critical transactions, after the specified time lock, the board's keys become active, allowing them to override the impasse and manage the funds per organizational policies.

Extended applications include integrating external arbitrators such as courts or regulatory bodies into the setup to address legal disputes or compliance issues.




## Policies Enforced by the Bitcoin Network

By embedding these policies into the wallet's structure and utilizing Bitcoin's scripting capabilities, policies are enforced automatically by the network, reducing reliance on individual discretion. Time locks and multi-layered keys protect against unauthorized access and internal malfeasance. Organizations can customize the vault to fit specific needs, adjusting time locks, signature requirements, and arbitration protocols.

## Benefits of Multi-Layered Vaults for Organizations

Combining multiple security layers mitigates various risks, from theft to internal conflicts. Automated enforcement lessens the need to rely solely on the trustworthiness of individuals, reducing dependence on trust. The following are all the benefits of utilizing vaults for organizations:

- **Robust Security**: Combining multiple security layers mitigates various risks, from theft to internal conflicts.
- **Reduced Dependence on Trust**: Automated enforcement lessens the need to rely solely on the trustworthiness of individuals.
- **Improved Recoverability**: Mechanisms like expanding multisig ensure that lost or withheld keys don't permanently lock funds.
- **Conflict Resolution**: Arbitration layers provide structured methods for resolving internal disputes without compromising asset security.
- **Adaptability**: Vaults can be tailored to organizational changes, scaling with growth or adapting to new regulatory environments.

At **21st Capital**, we provide organizations with advanced Bitcoin vault solutions that incorporate multi-layered security architectures, including time locks and arbitration layers. Our expertise allows us to embed your specific policies directly into the wallet structure, ensuring robust security against theft, key loss, and internal conflicts. By partnering with us, you can benefit from automated enforcement of security measures, reduced dependence on individual trust, and customized setups tailored to your organizational needs. We invite you to book a demo with us so we can demonstrate how our **Smart Vault** works and help you implement a solution that secures your assets effectively.

## Conclusion

Traditional single-sig and multi-sig wallets present significant challenges for organizations seeking to secure their Bitcoin assets effectively. Human factors like trust, cooperation, and the potential for malfeasance introduce vulnerabilities that are difficult to manage. Bitcoin vaults with a multi-layered security architecture offer a superior solution by embedding policies directly into the wallet's structure, enforced by the Bitcoin network itself. By requiring all keys to sign, incorporating time locks, and adding arbitration layers, organizations can safeguard against theft, key loss, and internal conflicts. This approach not only enhances security but also provides the flexibility needed to adapt to different scenarios, ensuring that organizational assets remain secure and accessible when needed. As Bitcoin and blockchain technologies continue to evolve, such advanced security measures will become increasingly vital for organizations managing digital assets.