



TRUSTLESS COSIGNING RESCUE

Dec.
2024

New Paradigm of Trustless Cosigning as Rescue Services for Bitcoin Custody

Author: Ziya S.

Date: December 16, 2024

Email: contact@21stcapital.com

www.21stcapital.com

New Paradigm of Trustless Cosigning as Rescue Services for Bitcoin Custody

When it comes to safeguarding Bitcoin, the principle of self-custody is paramount. However, recovery options for lost keys often force users to compromise this sovereignty. Collaborative custody companies offer one solution, but their approach inherently relies on trust and shared control. In contrast, Vault Software introduces a groundbreaking recovery service that upholds user independence, providing a robust safety net while maintaining full self-sovereignty.

The Collaborative Custody Model: A Trust-Based Approach

Collaborative custody companies aim to bridge the gap between self-custody and custodial solutions by allowing users to maintain partial control over their Bitcoin. However, in the event of key loss, these companies act as custodians, capable of signing on behalf of the user to regain access. This process requires users to trust the company's intentions, operational security, and regulatory compliance.

Moreover, collaborative custody solutions often require users to retain at least some of their keys. If all keys are lost, the company cannot assist because their role as "collaborators" inherently depends on co-signing with the user. This limitation creates vulnerabilities that can leave users unable to recover their funds, exposing them to potential key withholding or restrictions due to regulatory changes.

Risks and Limitations of Collaborative Custody

<p>TRUST DEPENDENCY</p> <p>In collaborative custody, if users lose access to their keys, they must rely on the company to act as a custodian. This places immense trust in the company's intentions, operational security, and adherence to regulatory norms.</p>	<p>CUSTODIAL CONTROL RISKS</p> <p>Collaborative custody companies can potentially misuse their authority or withhold access due to regulatory changes, internal policies, or malicious intent.</p>
<p>INCOMPLETE RECOVERY OPTIONS</p> <p>These services often require users to retain at least one key. If all keys are lost, the collaborator cannot assist, as their role is inherently dependent on co-signing with the user</p>	<p>REGULATORY RISKS</p> <p>Collaborative custody companies are susceptible to regulatory pressures that may restrict or modify their recovery operations</p>
<p>KEY WITHHOLDING</p> <p>Companies could potentially withhold keys, leaving users without access to their funds</p>	<p>COLLABORATION LIMITATIONS</p> <p>By definition, collaborative custody requires the user to participate in the recovery process. If the user loses all keys, the system fails, leaving funds inaccessible.</p>

Vault Software Recovery: Independence Above All

Vault Software takes a completely different approach, ensuring users retain full control of their Bitcoin while offering a safety net for worst-case scenarios. With Vault services, users hold the recovery keys, enabling them to stay self-sovereign. Recovery does not require compromising independence or relying on a third party. Instead, users can regain access to their Bitcoin on their own, using a system designed to be more robust than collaborative custody recovery solutions.

In scenarios where all other wallets or methods would deem Bitcoin irretrievable, Vault Software steps in to save what might otherwise be considered "dead Bitcoins." Unlike collaborative custody or semi-custodial methods, Vault's recovery service does not require users to share custody with the provider. Users maintain full ownership and control of their assets, relying on Vault only for essential assistance to regain access.

BITCOIN VAULTS

SELF-SOVEREIGN RECOVERY

Vault users retain the recovery keys, ensuring they remain independent. Recovery is designed to empower users rather than transfer control to a third party

NO CUSTODIAL COMPROMISE

Unlike collaborative custody solutions, Vault recovery does not involve sharing custody with the service provider. Users maintain full control of their Bitcoin at all times

RESCUE-FIRST PHILOSOPHY

Vault recovery services act as a safety net for worst-case scenarios. Even in situations where users lose access to all keys—circumstances that would render their Bitcoin irretrievable with traditional wallets—Vault can help recover access without compromising ownership

SAVING "DEAD" BITCOINS

Vault's innovative approach provides a lifeline for Bitcoin that would otherwise be considered lost. It revives the concept of Bitcoin self-sovereignty by enabling recovery without reliance on external custodians

INHERITANCE CAPABLE

Unlike custodial inheritance protocols reliant on cosigners, vault setups are non-custodial and enforced trustlessly, keeping users in full control until activation.

A Rescue Service, Not Just Recovery

The unique strength of Vault Software's recovery service lies in its rescue-first philosophy. This service acts as a last-resort safety net, designed to operate in scenarios where other methods fail completely. It ensures users can revive their Bitcoin without relinquishing control or relying on collaborators.

Vault's approach is particularly vital in extreme cases. In collaborative custody, if a user loses all their keys, the company cannot act unilaterally to recover the funds. By contrast, Vault Software enables recovery even in these dire circumstances, making it possible to bring Bitcoin back to life. This capability makes Vault a rescue service rather than a mere recovery tool—a service that protects users' sovereignty while providing peace of mind.

No Compromise on Self-Custody

Vault Software's recovery service is not a compromise on self-custody. It does not depend on shared control, trust-based agreements, or third-party interventions. Instead, it offers users a robust, reliable fallback mechanism that preserves their autonomy. Whether users lose access due to mistakes, unforeseen circumstances, or complete loss of keys, Vault can help them recover without compromising their independence.

Check Out Our Smart VaultWith the Smart Vault, you can set up multiple recovery options, automate inheritance planning, and make sure you never lose your Bitcoin again. [Book a Demo](#)

Conclusion

Vault Software redefines recovery services by prioritizing self-sovereignty and independence. Unlike collaborative custody solutions, which require trust and shared control, Vault empowers users to stay in control of their Bitcoin while offering a reliable safety net for the worst-case scenarios. By preserving ownership, eliminating custodial risks, and providing a rescue-focused service, Vault Software ensures that Bitcoin users can confidently secure their assets without compromising the principles of self-custody. This innovative approach marks a significant step forward in safeguarding Bitcoin's core ethos of financial freedom and independence.