21ST CAPITAL

RETHINKING BITCOIN CUSTODY

Dec. 2024

Moving Beyond the Punishing Self Custody of Bitcoin

Author: Ziya S.
Date: December 26, 2024
Email: contact@21stcapital.com

www.21stcapital.com

Moving Beyond the Punishing Self Custody of Bitcoin

Introduction of Forgiving Bitcoin Self-Custody Solutions

Punishing vs. Forgiving Self-Custody

The concept introduced here is called punishing self-custody and forgiving self-custody. It arises from comparing Bitcoin's self-custody experience to other fields, where processes that penalize small mistakes are considered punishing. In the context of Bitcoin, self-custody has traditionally been punishing. Very small and common mistakes, like losing a piece of paper or a small device, or breaking a phone, can lead to losing an entire net worth. Designing user experiences that severely penalize such ordinary errors is unusual, especially considering how, in other areas, measures are taken to prevent severe consequences from relatively minor mistakes.

In riskier fields, such as transportation or hazardous occupations, safety measures, strict instructions, and specialized tools and products help prevent extremely punishing outcomes like severe bodily harm or loss of life. Over centuries, human effort has produced numerous methods and approaches to protect individuals from losing what is valuable to them. In Bitcoin, however, the emphasis on personal control, sovereignty, and non-interference from third parties created a system granting total control but at a significant cost. Losing keys means there is no assistance available to recover coins, reflecting the concept of "not your keys, not your coins." While this principle is of utmost value, preserving sovereignty and aligning with Bitcoin's values, it also creates a scenario where losing access to keys can be devastating, and this does not necessarily need to remain the status quo for Bitcoin self custody.

A more forgiving form of self-custody is both possible and desirable. Rather than permanently losing Bitcoin due to a minor oversight, it is feasible to implement systems that maintain complete and total control while introducing mechanisms that allow for fund recovery. Such measures would not abandon the ideals of self-sovereignty, complete control, or uncensorable and unstoppable access. Instead, they would refine self-custody practices so that one small mistake no longer results in irretrievable losses.

Aspect	Punishing Self-Custody	Forgiving Self-Custody
Error Tolerance	Zero tolerance: minor mistake = loss	Built-in recovery paths for lost keys
User Experience	High stress, fear of simple errors	Reduced anxiety, safety nets available
Assistance on Key Loss	None available	Timed activation of backup keys, heirs
Alignment with Values	Sovereignty but harsh outcomes	Sovereignty plus more humane safeguards
Inheritance Planning	Not Possible without Security Compromise	Possible and Trustless execution

The Problem with Traditional Self-Custody

The current model of self-custody usually relies on a single point of access, making a misplaced key or damaged device catastrophic. The experience of our Bitcoin consultancy efforts, working with thousands of users over many years shows that human error is very common among users. People frequently lose track of small gadgets, forget about pieces of paper, or accidentally destroy or delete critical information. These scenarios highlight the need for a more forgiving user experience. Throughout history, humanity has developed forgiving approaches for valuable tools, ensuring that simple mistakes do not yield severe consequences. Bitcoin self-custody should evolve similarly.

Common Error	Frequency (Observed)	Consequence Under Punishing Model
Lost/Damaged Recovery Paper	Very Common	Total loss of all funds
Lost Hardware Wallet	Frequent	Irrecoverable coins (if Paper Recovery is Lost/Scrambled/Damaged)
Damaged Phone/Computer	Common	No method to regain access (if Paper Recovery is Lost/Scrambled/Damaged)
Forgotten Passphrase	Not Uncommon	Permanent loss of Funds
Sharing Recovery Paper	Very Common	High Compromise of Security (Theft)
Splitting Recovery Paper	Common	High Risk of Losing funds
Storing Recovery Digitally	Very Common	High Compromise of Security (Theft)
Incorrect/Incomplete Backups	Not Uncommon	Permanent inability to restore and total loss of funds
Relying Solely on Memory	Common	If user forgets even part of the phrase, permanent loss of funds
Using Non-Durable Storage for Backups	Not Uncommon	Ink fades, paper degrades, moisture damage; leads to unreadable or lost recovery
Complex Setup Without Documentation	Occasional	Multiple passphrases, hidden wallets, or derivation paths become unrecoverable
Accidentally Overwriting Backups	Occasional	Original valid backup lost; no correct data remains for wallet recovery
Using Non-Standard Seed Formats	Occasional	Seed incompatible with standard wallets, preventing proper restoration
Keeping All Backups in a Single Location	Common	Disaster (fire/flood) destroys the only backup, resulting in total loss

Why a Forgiving Approach Is Needed

Implementing multiple layers of recovery and rescue, combined with time boundaries and multisignatures for enhanced security, can achieve this goal. Multisignature wallets require multiple authorizations, deterring attackers, while layered recovery paths enable users to regain access to their Bitcoin if primary keys are lost. Although self-custody should remain under the owner's sole authority, it does not need to be a solitary endeavor in practice. Incorporating trusted parties or entities under certain conditions can create a safer environment. For example, extra sets of keys can remain inactive at first by a time boundary condition in the Bitcoin network called Timelocks and the keys will only become available after a very long period of time, offering a means of regaining access without compromising the original owner's supreme decision-making power.

Key Activation Timeline

Time 0 (Vault Initialization)

Primary keys are active, backup keys dormant

After 3 Month of Fund Inactivity

If primary keys lost, first layer of backup keys become available

After 9 Month of Fund Inactivity

If still no keys found, secondary backup keys or heirs' keys activate

After 15 Months of Fund Inactivity

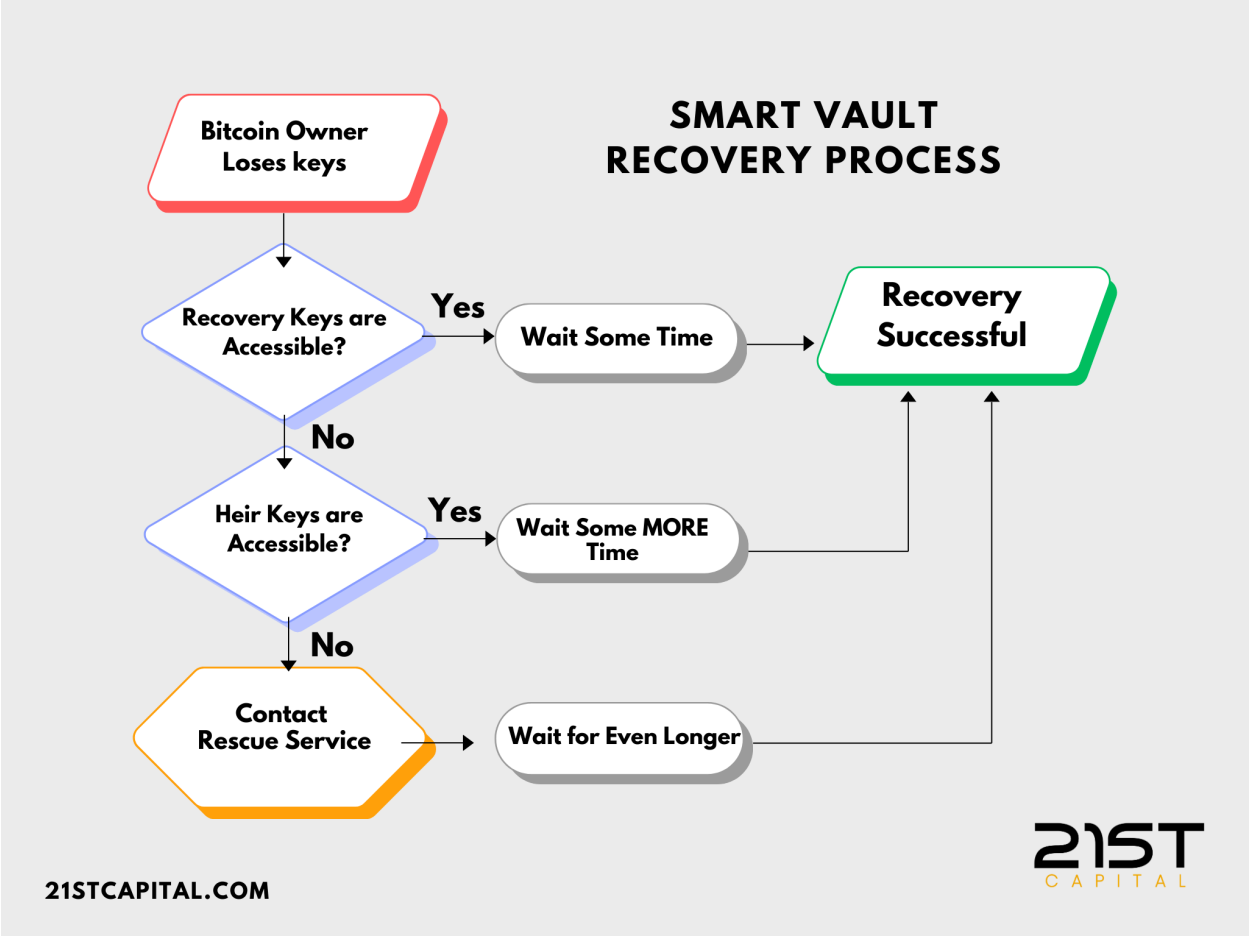
In extreme scenario, expert recovery keys activate as a last resort for fund rescue

This adjustment naturally extends to inheritance planning, a notoriously difficult aspect of Bitcoin self custody. By involving trusted individuals or designated heirs, and by employing time-delayed activation of backup keys, it becomes possible for heirs to access Bitcoin after a certain period, honoring the owner's wishes. At the same time, the use of Bitcoin technologies like Multisignature, Miniscript, Time locks, and Descriptors ensures that no extra keys can perform unauthorized actions. These trustless rules, enforced by the Bitcoin network itself, remove dependency on external custodians or custodial solutions and preserve the spirit of trustless and decentralized Bitcoin ownership.

Recovery and Rescue Experts

Considering external assistance, such as Bitcoin experts or security teams, can further enhance resilience. These parties' keys would remain dormant for an extended time and only activate if every other safeguard has failed. Such extreme conditions are difficult to imagine, as they require every participant, including the owner and heirs, to lose their keys simultaneously. If, against all odds, this occurs, the long-inactive key from a recovery service provider, such as a reputable Bitcoin security team, can finally activate. In doing so, what would have been permanently lost coins can be saved, converting what was once a final death sentence for one's Bitcoin holdings into a last resort recovery—a kind of rescue rather than a mere recovery.

This refined approach moves away from punishing self-custody and toward a more forgiving model. Instead of one small error condemning valuable assets, the presence of layered security, time locks, trusted parties, and carefully arranged protocols ensures that a mistake or an unforeseen tragedy does not permanently separate owners or their heirs from the wealth they intended to protect. As a result, Bitcoin custody becomes more aligned with intuitive and human-friendly designs found in other parts of life, where multiple safety nets and fallback measures stand ready to prevent a single misstep from erasing everything.



Smart Vaults

For those interested in exploring a more forgiving approach to self-custody, solutions like 21st Capital's Smart Vault provide a structured, secure, and flexible way to safeguard Bitcoin holdings. The Smart Vault incorporates multi-layered keys, time locks, and carefully enforced conditions on the Bitcoin network that preserve sovereignty while allowing recovery paths tailored to unique circumstances. Book a demo for an opportunity to see how Smart Vaults work in practice.