21ST
CAPITAL

BITCOIN WALLET RECOVERY

Nov. 2024

Understanding Complexities and Future Directions

Author: Ziya S.
Date: November 14, 2024
Email: contact@21stcapital.com

www.21stcapital.com

Bitcoin Wallet Recovery: Understanding Complexities and Future Directions

Introduction

Recovering a Bitcoin wallet is a topic that encompasses several important aspects. While it might seem straightforward, there are underlying complexities that users should be aware of. In this article, we aim to address some key points that can help answer common questions related to wallet recovery.

Bitcoin Wallet Recovery and BIP39 Standard

Generally, when recovering a wallet using recovery words, there is no need to worry excessively. Most wallets are compatible with the **BIP39** standard, which means recovery is often successful without much hassle. Occasionally, you might need to adjust a couple of options during the recovery process, but overall, it tends to work smoothly.

Limitations of Recovery Words Alone

However, something that is less frequently discussed is that in certain situations, recovery words alone are not sufficient for recovery. The reason is that some wallets—either due to being very old or because they are new and different—are not compatible with standard protocols. In such cases, recovery becomes more complicated.

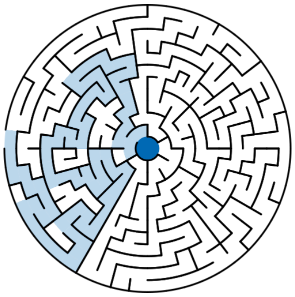
Importance of Open-Source Wallets

One factor that can almost always ensure successful recovery is if the wallet is **open-source**. If a wallet has implemented unique or unusual features, having access to its code allows us to examine what has been done and how we can resolve any issues. Open-source wallets provide the transparency needed to troubleshoot and recover funds effectively.

Detailed Requirements for Wallet Recovery

For a successful recovery, we need to use the following information and follow the specific paths that will reach our target of generating the specific private keys accessing the coins:

- **Recovery words**
- **Address derivation paths**
- **Passphrase** (if any)
- **Compatible Software**



This means that, strictly speaking, we need more than just the recovery words. However, since most wallets perform address generation and the use of recovery words according to the BIP39 standard, we usually do not need to go through additional steps.

Case Studies: Electrum and Samourai Wallets

What is the story with Electrum? The developers of **Electrum** use a separate standard, which they—and many others—believe is even better than BIP39. Their goal with this difference was to reduce some of the prerequisites and embed them within the recovery words themselves. For example, the address generation method is included in the seed itself. This is why when you enter an Electrum seed, you don't need to choose your address standard; it understands it automatically. This can be considered an upgrade over BIP39. Although we recognize this method as a better effort, still, practically the user is limited to using electrum for recovering coins because almost no other wallets support their format. Furthermore, there is a significant chance that in the future, individuals and even wallets will not be heavily involved with address derivation paths and will instead use **descriptors** which we will discuss later in this article.

What about Samourai Wallet? **Samourai Wallet** is one of those wallets that operates in a somewhat advanced manner. It essentially creates four or five, (let's say), wallets within itself, using different paths. Although the address derivation paths are documented beforehand, recovering it on most other wallets isn't as simple as just entering the recovery words. You need to create, for example, three separate wallets with different standards and maybe another two or more wallets for some custom paths that the Samourai wallet software creates. The reason for this complexity was that Samourai Wallet offered privacy features that utilized various address standards and paths.

Recovery Words
Derivation Paths
Software

The Broader Discussion on Wallets and Recovery Methods

The discussion around wallets and their recovery methods is quite interesting overall. Many developers have their own ideas on this subject, and some have even implemented and standardized their ideas. There are always concerns regarding all the information needed to recover a wallet, and everyone has their own ideas for solving these issues, each with its own trade-offs.

Future of Wallets and Recoverability

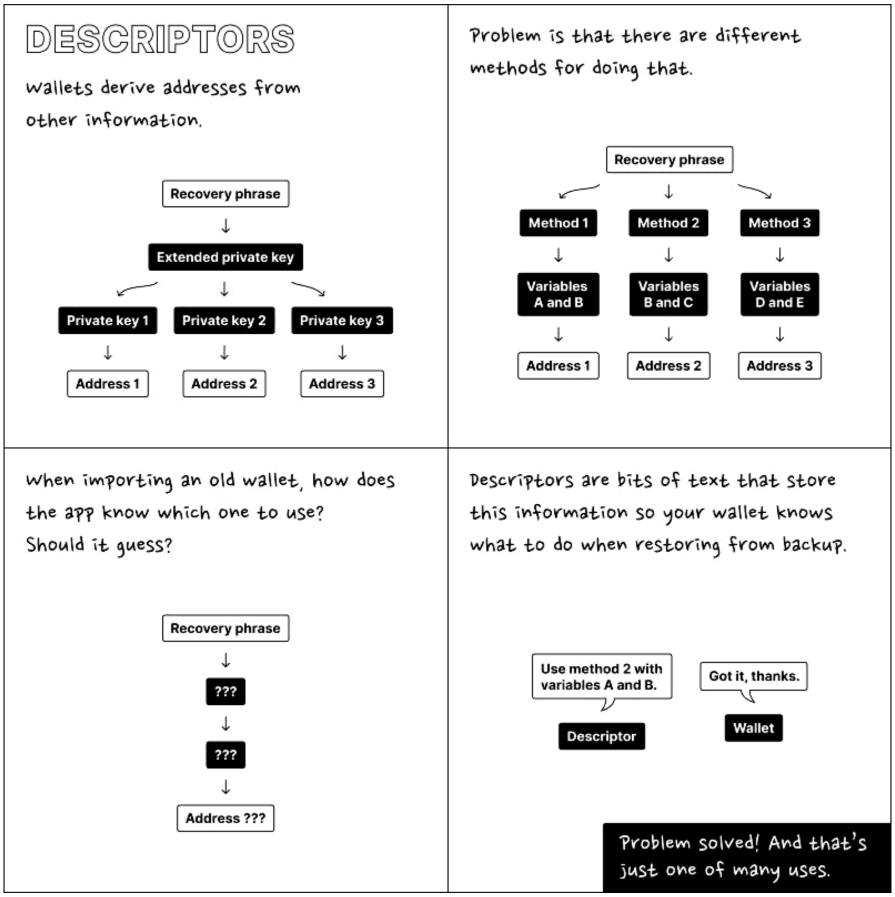
What will be the situation with wallets and their recoverability in the future? We need to think about this subject in a way that considers future applications of Bitcoin. Wallet developers must consider how Bitcoin will be used moving forward.

We think that the most solid and comprehensive method that has been proposed and implemented so far—and will likely become more widespread in the future—is the use of **descriptors**. The reason is that we produce certain information after generating the seed, and no matter what we do, we cannot add this information into the seed itself, unless our applications are limited to one of a few simple standards like Electrum.

Descriptors: A Comprehensive Solution

For this reason, the approach has been to gather the additional wallet information all in one place and standardize how we record this information. This data is not sensitive in terms of accessing the wallet—for example, it doesn't contain private keys. You can store this information separately and even digitally with ease, significantly reducing the chance of losing it. Moreover, in hardware wallets, these descriptors are planned to be registered in the future.

Descriptors can be thought of as a map for finding your addresses and how to spend from your wallet. They also have very advanced capabilities where you can define various spending conditions and other parameters in this map for more advanced or improved applications in the future. Remember the Taproot upgrade? To utilize Taproot's interesting capabilities, we need a place to store a lot of information for more advanced Bitcoin transactions—something akin to smart contracts—which is facilitated by these descriptors.


DESCRIPTORS
wallets derive addresses from other information.
Recovery phrase
Extended private key
Private key 1
Private key 2
Private key 3
Address 1
Address 2
Address 3
Problem is that there are different methods for doing that.
Recovery phrase
Method 1
Method 2
Method 3
Variables A and B
Variables B and C
Variables D and E
Address 1
Address 2
Address 3
When importing an old wallet, how does the app know which one to use? Should it guess?
Recovery phrase
???
???
Address ???
Descriptors are bits of text that store this information so your wallet knows what to do when restoring from backup.
Use method 2 with variables A and B.
Got it, thanks.
Descriptor
Wallet
Problem solved! And that's just one of many uses.

In light of these challenges, it's evident that future recovery methods should not mirror the current approaches. Recovery solutions should be **integrated directly into the wallet**, offering **flexibility** to accommodate users with diverse requirements. This integration allows for customizable security features that go beyond simple recovery seeds, providing robust protection without adding complexity for the user. By building recovery mechanisms into the wallet, users can benefit from **layered security architectures** that automatically adapt to different scenarios, reducing the reliance on external tools or detailed technical knowledge.

One innovative approach to this is the implementation of a **multi-layer security architecture**, as seen in solutions like Smart Vaults. In this setup, the wallet employs multiple layers of security:

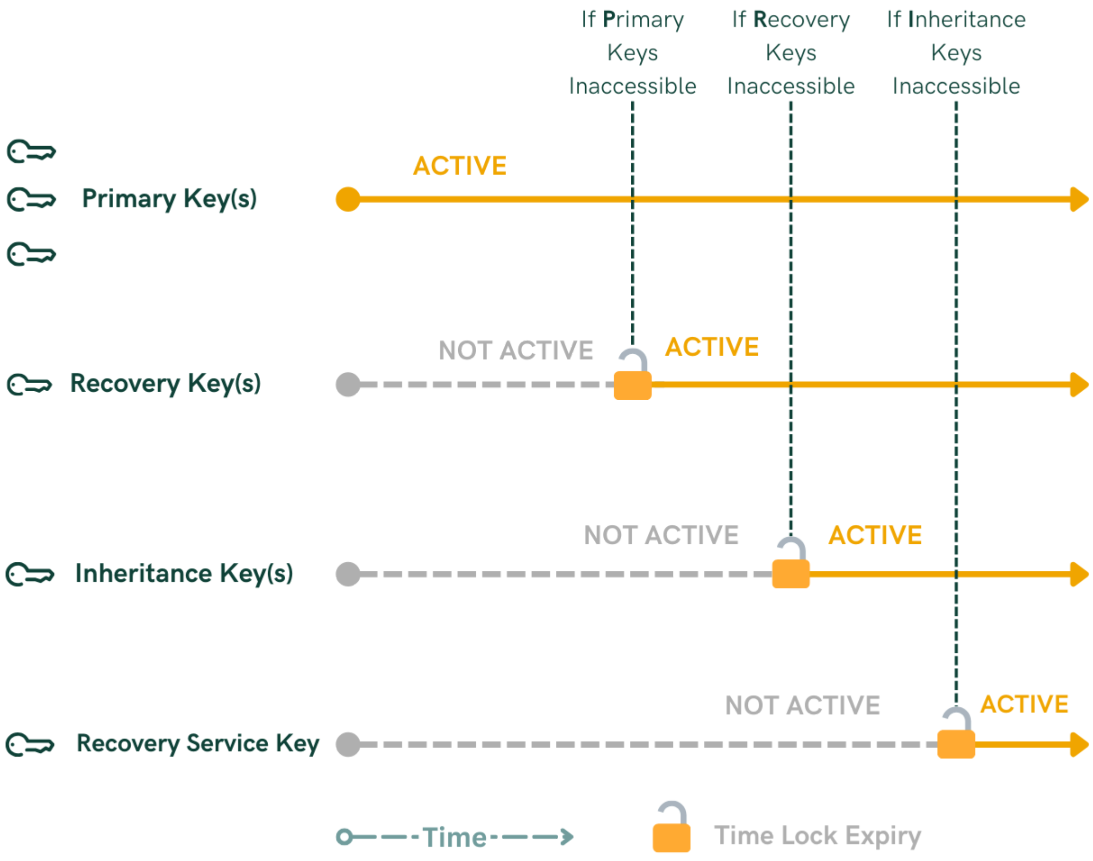
- **Primary Layer**: The user holds multiple keys (e.g., in a 2-of-3 multi-signature configuration) for regular transactions.
- **Recovery Layer**: Additional keys that activate after a period of inactivity, allowing the user to regain access if primary keys are lost.
- **Inheritance Layer**: Keys held by designated heirs, which become active under predefined conditions, ensuring seamless transfer of assets.
- **Recovery Service Layer**: An ultimate fail-safe managed by a trusted recovery service that can assist in fund retrieval with the user's consent.

For example, a user might hold two keys for daily use, while a third key is held securely by a recovery service to assist in emergencies. If the user loses access to their primary keys, the recovery layer activates after a set time, enabling them to restore access without compromising security. This layered approach provides a **flexible and secure framework**, tailored to individual needs, and addresses many of the shortcomings of current recovery methods by ensuring that users maintain control over their assets in various unforeseen circumstances.

Adding an Inheritance Layer

Layered security architectures also allow for the addition of an **inheritance layer**, which acts as a recovery method for your heirs rather than yourself.

- **Heirs' Keys**: You provide trusted heirs with keys that are inactive and secured behind time locks.
- **Activation Conditions**: These keys become active only after a significant period of inactivity, indicating that you're no longer able to manage your funds.
- **Secure Transfer**: This ensures that your Bitcoin can be passed on securely without compromising your control during your lifetime.



By incorporating an inheritance layer, you can have peace of mind knowing your assets will be accessible to your loved ones in the future without exposing yourself to additional risks now.

Check Out Our Layered Recovery Solution: The Smart Vault

With Smart Vault, you can set up multiple recovery options, automate inheritance planning, and make sure you never lose your Bitcoin again. Book a Demo on 21stcapital.com/demo

Conclusion

Understanding the complexities of Bitcoin wallet recovery is essential for anyone involved in cryptocurrency. While recovery words and the BIP39 standard provide a solid foundation, there are limitations and exceptions that users should be aware of. Open-source wallets offer transparency and a higher chance of successful recovery. As we look to the future, descriptors present a promising solution that addresses many of the current shortcomings, offering advanced capabilities and better adaptability for future applications.