DOI: 10.20535/kpisn.2025.1.309585
UDC 004.056

Oleg Boiko[*]
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
[*]Corresponding author: o.a.boiko@kpi.ua

A METHOD FOR PROTECTING DIGITAL ASSETS FROM PERMANENT LOSS IN THE EVENT OF PRIVATE KEY LOSS

Background. Cryptocurrencies have introduced a decentralized and secure way to transfer value, with private keys playing a crucial role in authorizing transactions and verifying ownership. However, the loss or destruction of private keys leads to permanent asset loss, presenting a significant risk to users and hindering broader adoption.
Objective. This paper presents a smart contract-based method to mitigate the risk of losing digital assets in the event of permanent private key loss, providing an automated recovery procedure without compromising the security of digital assets.
Method. The proposed solution leverages smart contract technology to create an automated recovery process. Key components include a protected address (Address A), a predefined recovery address (Address B), and a specified time interval (Period T). If no outgoing transactions are registered during Period T, the smart contract transfers assets from Address A to Address B.
Results. The proposed method ensures that in the event of private key loss, assets are automatically transferred to a backup address after Period T. This process ensures users maintain full control over their assets, allowing adjustments to Period T and Address B as needed.
Conclusions. The smart contract-based recovery method provides a reliable and user-friendly solution to address the consequences of possible permanent private key loss. It complements existing solutions, offering an additional layer of security and enhancing user confidence in decentralized financial systems. Future research might focus on improving the security and reliability of the backup address.
Keywords: information security; cryptocurrency; private key; smart contract; asset recovery; digital assets.

Introduction

Cryptocurrencies have revolutionized the financial landscape by introducing a decentralized and secure means of transferring value. At the heart of this revolution is the concept of private keys, used for authorizing transactions and verifying ownership within cryptocurrency systems, ensuring that only the rightful owner can access and transfer their assets.

Despite their crucial role, private keys come with inherent risks. The most significant of these is the potential for permanent asset loss if the private key itself is lost or destroyed. Unlike traditional financial systems where numerous recovery methods can be employed to regain access to accounts, the decentralized nature of cryptocurrencies means that once a private key is lost, the corresponding digital assets become irretrievable. This presents a substantial risk to asset holders and poses a barrier to the broader adoption of cryptocurrencies.

A poignant example is the 2018 case of QuadrigaCX, a Canadian cryptocurrency exchange. Its founder, Gerald Cotten, who solely owned the private keys to the exchange's cold wallets, passed away unexpectedly. This leftover $130 million in assets locked with no way to recover them [1].

Another example is the story of Bitcoin developer Stefan Thomas, who had three backups of his wallet – an encrypted USB stick, a Dropbox account, and a Virtualbox virtual machine. However, he managed to erase two of them and forgot the password to the third, forever losing access to 7,000 BTC (worth $125,000 at the time) [2].

The most straightforward solution to this user experience problem is to create a custodial service that manages keys and handles transactions. This is the method used by major centralized exchanges

Пропозиція для цитування цієї статті: О.А. Бойко, "Метод захисту цифрових активів від незворотної втрати у випадку втрати приватного ключа", *Наукові вісті КПІ*, № 1, с. 63–68, 2025. doi: 10.20535/kpisn.2025.1.309585

Offer a citation for this article: Oleg Boiko, "A method for protecting digital assets from permanent loss in the event of private key loss", *KPI Science News*, no. 1, pp. 63–68, 2025. doi: 10.20535/kpisn.2025.1.309585

and custodial wallets, allowing for traditional access mechanisms and features like password recovery. However, this approach introduces significant centralization risks and conflicts with one of the fundamental principles of web3/crypto: “Not your keys, not your coins”.

On the non-custodial side, there are some interesting modern solutions and proposals, such as hardware, multi-signature, and social recovery wallets, as well as some biometric authentication ideas. While these solutions offer valuable improvements in user experience and risk reduction, they still have their challenges, described further in this research.

This paper proposes a relatively simple solution, designed to mitigate the risk of losing digital assets in the event of permanent private key loss. The described approach aims to provide an automated smart contract-based recovery procedure without compromising the underlying security of digital assets.

The following sections will explore the problem statement, review recent relevant research and publications, examine existing key management options, and finally present the design of the proposed solution, analysing its potential benefits and drawbacks.

Problem Statement

Securing private keys is a complex and non-trivial problem because it requires balancing two conflicting goals: ensuring uncompromisable non-custodial control of digital assets and minimizing the respective management risks (along with the associated significant emotional pressure) for users, especially those who are not tech-savvy.

The goal of this article is to propose a simple, transparent and user-friendly method that allows cryptocurrency users to have a “Plan B” for the possible scenario of private key loss, without sacrificing the fundamental security of non-custodial ownership of the respective digital assets.

Analysis of Recent Research and Publications

In 2021, the Austrian Institute of Technology (AIT) conducted an online survey to understand the preferences of the general audience regarding the handling of private keys for blockchain-based applications. About 80 % of participants preferred the direct variant, which requires users to store the private key themselves, while around 60 % opted for a hybrid variant where an external manager is responsible for the backup. This indicates that participants value data sovereignty more than the risk of losing money or other digital assets. Approximately half of the survey participants would prefer to record the access code on paper, while others would store it on their mobile phone, in a password manager, or by printing it [3].

Various methods have been developed to enhance the security and recoverability of private keys. One of the most prominent is **Hardware wallets**, which were thoroughly analyzed in a 2019 research paper by Edinburgh Napier University [4]. Hardware wallets are devices designed to store private keys offline in what is known as “cold storage”. They connect to a computer via USB or Bluetooth for transaction signing, but the keys never leave the device, reducing exposure to internet-based attacks. Although secure against online threats, hardware wallets are vulnerable to physical damage or loss, which, in the context of this paper, is technically equivalent to private key loss.

Another significant concept is **Multi-signature wallets**, which allow multiple configurations of keys to authorize a transaction, thereby reducing the risk of losing one of these keys [5]. One of the main challenges with this approach is reduced usability, as each transaction requires confirmation from at least two different key holders. Therefore, this concept is better suited for businesses, organizations, or group-owned digital assets.

Several recovery mechanisms have been proposed to mitigate the consequences of key loss, including the **Social recovery wallet** concept. This type of digital wallet enables the recovery of private keys and digital assets through a user’s social network, utilizing guardians (trusted individuals or devices) to aid in the recovery process [6]. Under normal circumstances, a social recovery wallet functions like a regular wallet, requiring only a single confirmation click for transactions. If the user loses their signing key, the social recovery feature is activated, allowing the user to request their guardians to sign a transaction that updates the wallet’s signing key to a new one [7]. It’s worth noting that getting a social recovery system right is a complex engineering challenge. Implementing it reliably and transparently can be difficult and poses its own security risks.

Another approach is utilizing **Biometric authentication** to enhance key recovery processes, as explored in a recent (2023) paper from Kharkiv Polytechnic Institute [8]. Biometric authentication is a security process that verifies a person’s identity based on their unique physiological or behavioural traits, such as facial features, fingerprints, or handwriting patterns. The main challenge is processing biometric data accurately across varied conditions and datasets.

Additionally, there is an inherent risk in trusting the numerous actors involved in the design, production, and shipment of the authentication devices.

This paper proposes a method to address these gaps by leveraging simple and transparent smart contract technology to provide a reliable and automated recovery procedure.

Design Principles

The proposed method is based on the following design principles:

Security: Ensure that the respective architecture does not compromise the fundamental security of the digital assets.

Automation: Implement an automated process to minimize human intervention and reduce the risk of errors.

Flexibility: Allow for customizable parameters to address different user needs and preferences.

Transparency: Maintain clear and auditable processes to build trust and accountability.

Simplicity: The less complex the system, the more reliable and resilient it is.

Ergonomics and UX: The system should be intuitive and straightforward and should not require any additional training for any relevant user.

Proposed Solution

The core concept of the proposed protection method is the establishment of an automated, smart contract-based system based on three key components:

Address A – the protected address (the private key for which may be lost).

Backup Address B – a predefined restoration address (explained in detail further below).

Period T – a predefined time interval during which no outgoing transactions (explicitly signed by the owner) are registered in the blockchain. This criterion can serve as a reliable confirmation for the private key loss event.

The idea in a nutshell: the smart contract will send assets from protected Address A to the backup Address B in case of no signed transactions during period T (see Fig. 1).

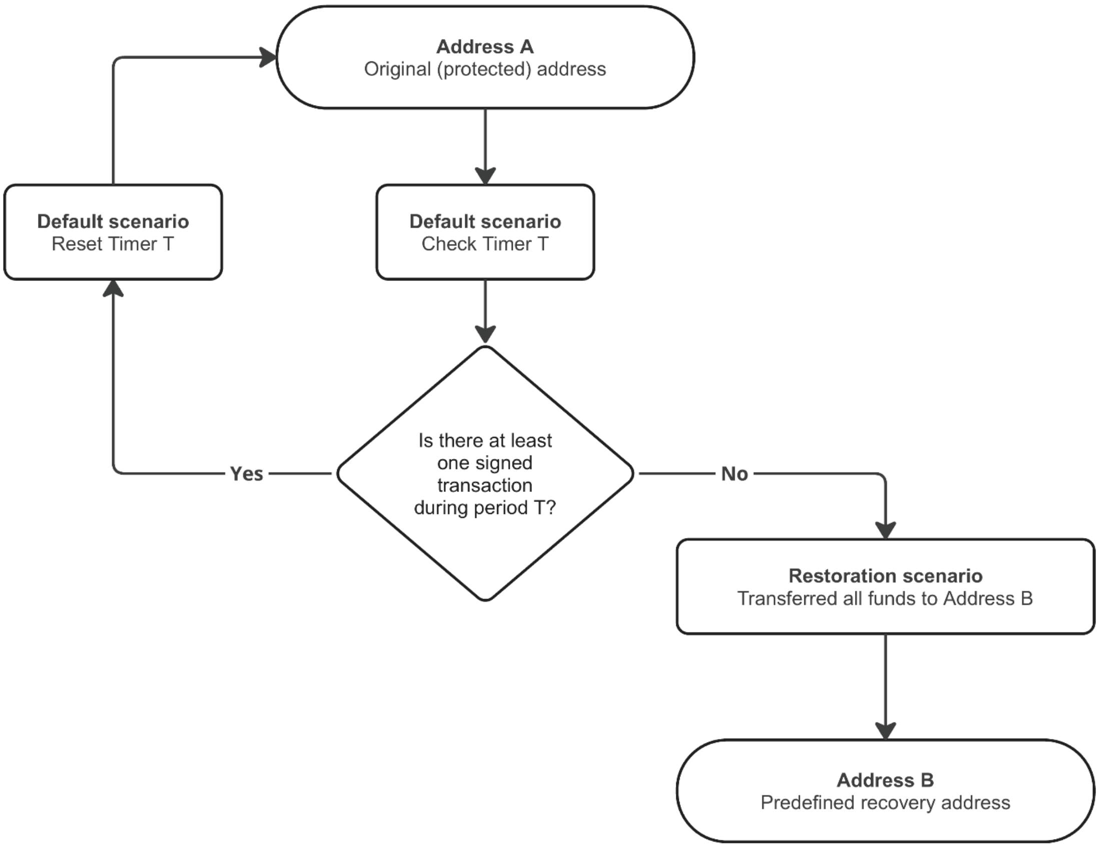
Address A
Original (protected) address
Default scenario
Reset Timer T
Default scenario
Check Timer T
Is there at least one signed transaction during period T?
Yes
No
Restoration scenario
Transferred all funds to Address B
Address B
Predefined recovery address

Fig. 1. Principle schema of the proposed solution

Address B can be:

1. **One's own backup storage** with a different private key or different access principle (e.g. custodial or social recovery wallet).

2. **The heir's wallet** (children, grandchildren, spouse, relatives, business partners, etc.) – an automated classical inheritance.

3. **A wallet of a trusted institution**, that upon the event of smart contract execution, will be able to use the positive human factor to perform reliable, rational, and legally transparent verification and transfer of funds to the legitimate addressee.

Any authorized outgoing activity, such as sending funds or any other signed operation, will reset the countdown (timer) of period T. Thus, in the case of regular active Address A usage, the timer will be regularly reset and the funds will stay in place. Also, it should be relatively easy to develop an application that will listen to the relevant blockchain information and send a reminder (e.g. one month before period T ends) with an offer to sign an empty "signal" transaction to reset period T.

The period T itself can be set to any comfortable value, from more dynamic, e.g. 1-2 weeks (for institutions with a lot of operations and a high responsibility level), to more conservative, like 2-5 years (for individual long-term investments). In any case, once the smart protection contract is activated, the owner of the funds (or their heir) might feel significantly better protected from the irretrievable loss of the assets as a result of a wide range of unsuccessful circumstances, such as storage device mechanical damage, loss or destruction of the recovery phrase, death or disappearance of the sole owner, and so on. Obviously, the described method will not be able to protect assets in case of private key theft.

Examples

Scenario 1: "Simple Plan B".

Alice stores some digital coins in her blockchain wallet (Address A) with the private key's mnemonic written down on a piece of paper. She assigns a restoration address (Address B) to her account on the centralized exchange Coinance, which is secured by email-password access. She sets the restoration period (T) to 6 months.

Alice retains full and exclusive control of her funds. However, if she loses access to both her wallet and the private key mnemonic, she simply needs to wait 6 months from the date of the last transaction. The smart contract will then transfer her funds to the Coinance account. In case she forgets or loses her Coinance password, she can recover it using Coinance's email-based recovery procedure.

Scenario 2: "Digital Will Protection".

Bob stores some digital coins in his blockchain wallet (Address A) with the private key secured in multiple software and hardware storages, but in a way that only Bob can access them. He assigns a restoration address (Address B) to the account of his legal advisory firm Satoshi & Partners, and sets a restoration period (T) to 1 year.

Bob retains full and exclusive control of his funds. However, in the event of his death, incapacity, or other unforeseen circumstances, his heirs only need to wait 1 year from the date of the last transaction. The smart contract will then transfer the funds to Satoshi & Partners, where the firm can distribute the assets to Bob's heirs, based on legal agreements and/or instructions Bob has provided.

Advantages

1. While maintaining control over the private key, its owner still retains full control over their assets and, at any time, will be able to:

a. disable/suspend the execution of the security smart contract;

b. sign any transaction (including an empty one) to reset the timer counting the period T;

c. change period T;

d. Change Address B.

2. In case of private key loss, the assets will not be irretrievably lost. The owner (or the relevant applicant) will only need to wait until the end of period T, after which the assets will be transferred to the reserved address.

Disadvantages

1. The need to occasionally sign at least one transaction to reset the count of the period T.

2. The need to maintain the reliability of Address B and/or redefine this address in case of concerns.

Conclusions

The management of private keys in the cryptocurrency and digital assets ecosystem is one of the critical research areas due to the inherent risks associated with key loss. Existing solutions, such as hardware wallets, multi-signature wallets, social recovery wallets, and biometric authentication, have provided various methods to enhance security and recoverability. However, each of these solutions presents its own set of challenges, including engineering complexity and reliance on third-party hardware.

This paper proposes a new method that leverages automated smart contract technology to address the consequences of possible event of permanent private key loss. Unlike existing solutions, this approach provides a time-based automated transfer system that activates upon detecting the absence of outgoing transactions over a predefined period. This method offers some valuable advantages, including high transparency, minimal human intervention, and enhanced flexibility in setting recovery parameters. The proposed solution maintains the fundamental security of non-custodial ownership while introducing a practical "Plan B" for asset recovery.

Importantly, the smart contract-based protection method proposed in this paper is not intended to replace existing solutions but to augment and complement them, by providing an additional layer of backup and problem-solving opportunities.

The proposed solution can be applied in various scenarios, from individual long-term investments to high-responsibility institutional operations. It provides a reliable and transparent method for asset recovery without compromising security. The smart contract-based approach ensures that users or their designated heirs can retrieve assets even in cases of key loss, device damage, or owner incapacity.

Despite its advantages, the proposed solution also identifies new challenges and areas for further research. Perhaps most important is enhancing the security and reliability of the backup address.

The practical implementation of the proposed method will not only mitigate the risk of asset loss but also support the broader adoption and confidence in decentralized financial systems.

References

[1] N. De and A. Baydakova, "The collapse of QuadrigaCX: What we know (and what we don't)", CoinDesk, 2019. [Online]. Retrieved from: https://www.coindesk.com/markets/2019/02/06/the-collapse-of-quadrigacx-what-we-know-and-what-we-dont/

[2] V. Buterin, "Bitcoin Self-Defense, Part I: Wallet Protection", 2013. [Online]. Retrieved from: https://bitcoinmagazine.com/culture/bitcoin-self-defense-part-i-wallet-protection-1368758841

[3] C. Brunner *et al.*, "Who Stores the Private Key? An Exploratory Study about User Preferences of Key Management for Blockchain-based Applications", 2021. [Online]. Retrieved from: https://www.researchgate.net/publication/349402052_Who_Stores_the_Private_Key_An_Exploratory_Study_about_User_Preferences_of_Key_Management_for_Blockchain-based_Applications. DOI: 10.5220/0010173200230032.

[4] B. Mackay, "Evaluation of Security in Hardware and Software Cryptocurrency Wallets", 2019. [Online]. Retrieved from: https://www.researchgate.net/publication/338054399_Evaluation_of_Security_in_Hardware_and_Software_Cryptocurrency_Wallets. DOI: 10.13140/RG.2.2.31686.29768.

[5] Investopedia, "Multi-signature wallets: Definition and use cases", 2023. [Online]. Retrieved from: https://www.investopedia.com/multi-signature-wallets-definition-5271193

[6] A.B. Pedin IV *et al.*, "Smart Contract-Based Social Recovery Wallet Management Scheme for Digital Assets", 2023. [Online]. Retrieved from: https://www.researchgate.net/publication/371515274_Smart_Contract-Based_Social_Recovery_Wallet_Management_Scheme_for_Digital_Assets. DOI: 10.1145/3564746.3587016.

[7] V. Buterin, "Why we need wide adoption of social recovery wallets", Jan 2021. [Online]. Retrieved from: https://vitalik.eth.limo/general/2021/01/11/recovery.html

[8] S. Datsenko and H. Kuchuk, "Biometric Authentication Utilizing Convolutional Neural Networks", *A.I.S.*, Jun. 2023, vol. 7, no. 2, pp. 87–91. [Online]. DOI: 10.20998/2522-9052.2023.2.12

О.А. Бойко

МЕТОД ЗАХИСТУ ЦИФРОВИХ АКТИВІВ ВІД НЕЗВОРОТНОЇ ВТРАТИ У ВИПАДКУ ВТРАТИ ПРИВАТНОГО КЛЮЧА

Проблематика. Технологія блокчейну і криптовалют запровадила можливість безпечного і децентралізованого передавання цінності, де приватні ключі відіграють ключову роль в авторизації транзакцій і перевірці права власності. Утім, втрата або знищення приватних ключів призводять до незворотної втрати активів, що становить значний ризик для користувачів і заважає ширшому впровадженню технології.

Мета дослідження. У цій статті запропоновано метод на основі смарт-контрактів, що допомагає знизити ризик втрати активів у разі втрати приватного ключа, забезпечуючи автоматизовану процедуру відновлення зі збереженням рівня безпеки цифрових активів.

Методика реалізації. Запропонований метод використовує технологію смарт-контрактів для забезпечення автоматичного відновлення активів. Ключові компоненти включають захищену адресу (Адреса А), заздалегідь визначену адресу відновлення (Адреса В) і визначений часовий інтервал очікування (Період Т). Якщо протягом Періоду Т не зареєстровано вихідних транзакцій, смарт-контракт автоматично переводить активи з Адреси А на Адресу В.