Contract-based Solution for Secure Self-Custody of Blockchain Assets

R. Ayouaz

2023

Introduction

In the context of technological advancements, self-custody of digital assets on blockchains represents a significant challenge. The following text proposes a solution aimed at simplifying this self-custody while maintaining the inherent security advantages of blockchains. We introduce an innovative mechanism for managing private keys. This system allows users to have a complete control over their assets while minimizing the risks associated with the loss or theft of their private key. This approach promises a good balance between ease of use and robust security, essential in the field of blockchain transactions.

Implementation

In order to develop the proposed solution, we utilize a blockchain capable of executing smart contracts autonomously, independently of any centralized organization, and without the need for a trusted third party.

We introduce an entity responsible for securing and storing cryptographic keys for its clients. Users register with this provider through a know-your-customer procedure to obtain a pair of keys, with the option to export and keep a personal copy. Moreover, another third party supplies a digital signature device to the user, which can resemble a bank card. This device contains a private key hidden into its hardware, which is not disclosed to anyone.

Initially, the pair of keys held by the provider identifies the user's funds on the blockchain. A smart contract is then registered using this keys, stipulating that funds can only be spent via the public key of the physical device. This device can itself be protected by a password. Consequently, the spending authority is transferred from the provider's keys to that of the physical device. The contract also mention that it is possible, via the provider's keys (possibly also stored by the user), to immediately block the device, thus canceling the contract that allows it to spend the funds (A). The funds are then blocked for a predefined period. After this period, a new device linked to a similar contract can be registered. However, the simultaneous signature of the device keys and the

other keys held by the service provider can cancel this blocking request during the period in which the funds are blocked (B). Blocking requests are then no longer allowed for a certain time.

Robustness

We examine three types of possible attacks:

- Card Theft/Loss: In case of theft or loss, a request is made to the provider to block the card (A). The smart contract can include a clause delaying significant payments to provide a window for intervention in case of theft.
- Service Provider Hacking: The hacker who holds the private key but not the device may attempt to block it (A), to regain access to the funds. However, the user can cancel this blockage through access to the device's signature and the private key still held by the provider and/or the user themselves. (B)
- Malicious Provider: For users wary of the provider, keeping a copy of the private key allows countering the malicious deactivation of a card (B). This leaves time to transfer funds elsewhere if an unwanted card blockage is observed during the blockchain audit.

In the unlikely event of simultaneous hacking of the user's private key and the theft of the card, the only solution lies in the provider's commitment to reimburse losses due to its security failure.

Conclusion

The advantages of this solution are manifold. Only the actor having access to both the private key and the physical device controls their funds. This method solves the difficulty of holding funds by offering a partial key storage service, with the possibility of recovering it in case of loss. An account is created by obtaining a card similar to a bank card, linked by a smart contract, offering complete control over the funds.