A COMPARATIVE ANALYSIS OF OFFLINE WALLETS AND THEIR INTEGRATION WITH NFC FOR PRACTICAL OFFLINE PAYMENTS

Nexhibe SEJFULI-RAMADANI[1], Florim IDRIZI[2], Valentina ANGELKOSKA[3], Aleksandar RISTESKI[4]

[1]*Department of Informatics, Faculty of Natural Sciences and Mathematics, MK
2 Department of Informatics, Faculty of Natural Sciences and Mathematics, MK
3 Faculty of Economics, MK
4 Faculty of Electrical Engineering and Information Technologies, MK
*Corresponding Author: e-mail: nexhibe.sejfuli@unite.edu.mk

Abstract

In this paper, we conduct a comparative examination of offline (cold) wallets that are designed for storing cryptocurrency. Our analysis focuses on security, usability, and accessibility, with specific attention given to popular solutions like Ledger and Trezor. We evaluate these wallets based on how practical they are to use without compromising security and efficiency. Furthermore, we explore the integration of Near Field Communication (NFC) technology into offline wallets. This approach aims to make cryptocurrency transactions more secure, convenient, and user-friendly, especially in Electric Vehicle (EV) charging stations. By envisioning a future where transportation infrastructure and cryptocurrency security intersect, our research seeks to advance technologies that balance security with the demands of modern payment systems. Through this effort, we aim to provide valuable insights to stakeholders in the cryptocurrency ecosystem, informing strategic decisions and driving the development of secure, user-centric financial technologies. By shortening the gap between theoretical security concepts and real-world operational needs, our work aims to help other researchers and stakeholders create a future where blockchain-based currencies can be just as practical as efficient.

Keywords: blockchain, NFC, electric vehicles, Safepal, Cypherock X1, Ellipal Titan 2, Onekey, D'CENT, Tangem, Keystone 3 Pro, Trezor Safe 3, SecuX V20, Ledger Nano X, Ryder One

1. Introduction

Cryptocurrencies have revolutionized the financial landscape by providing decentralized, digital alternatives to traditional currency systems. As the adoption of cryptocurrencies continues to grow, the need for secure and efficient methods of managing digital assets has become increasingly critical. Offline wallets, also known as cold wallets, play a vital role in this ecosystem by providing a high level of security through their isolation from internet connectivity. This paper focuses on a comparative analysis of various offline wallets, specifically examining their security features, usability, supported cryptocurrencies, and unique functionalities. By evaluating popular solutions like Ledger and Trezor, among others, this paper seeks to inform strategic decisions and drive the development of secure, user-centric financial technologies. Through hands-on testing and detailed technical analysis, this study aims to offer a comprehensive comparison that will assist users in choosing the most suitable cold wallet for their needs, ultimately contributing to a future where blockchain-based currencies are as practical and efficient as traditional financial systems.

2. Advantages of using offline wallets

An offline wallet, also known as a cold wallet, is a physical device designed to store cryptocurrency private keys securely offline. This isolation ensures that private keys remain secure from unauthorized access or cyberattacks. Offline wallets are typically used for long-term storage of digital assets, providing a highly secure environment where private keys are never exposed to potential online vulnerabilities. The primary advantage of a cold wallet is its ability to provide maximum security for storing large amounts of cryptocurrency over long periods, as the lack of internet connectivity minimizes the risk of unauthorized access [1].

During the setup process, most offline wallets generate a so-called seed backup, which is a recovery phrase, a generated sequence of words. This phrase serves as a backup mechanism that allows users to recover their wallet and its contents in case the wallet is lost, damaged, or reset. An additional feature that cold wallets should ideally offer is an air-gapped design, which refers to a security measure used in cryptocurrency wallets where the device is completely isolated from any form of network communication [1]. This means the wallet does not connect to the internet, Wi-Fi, Bluetooth, or any other wireless network. Transactions are typically signed offline, often using QR code scanning to transfer data between the air-gapped device and an online device. This design significantly enhances security by preventing remote attacks and unauthorized access. Air-gapped wallets are ideal for users who prioritize security and want to minimize the risk of their private keys being exposed to potential online threats.

Methodology

This paper conducts a comparative analysis of various cold wallets through a combination of hands-on testing and examination of technical specifications. By directly interacting with each wallet, we were able to evaluate user experience factors such as setup processes, interface design, and ease of use. This practical approach provided insights into the day-to-day functionality and user-friendliness of each device, highlighting how these aspects can impact the overall effectiveness of the wallets in real-world scenarios. In addition to hands-on testing, the paper examines the technical specifications of each cold wallet, including security features, supported cryptocurrencies, and unique functionalities.

The wallets examined for this paper are Safepal, Cypherock X1, Ellipal Titan 2, Onekey, D'CENT, Tangem, Keystone 3 Pro, Trezor Safe 3, SecuX V20, Ledger Nano X, and Ryder One.

3. Security Features

Security is a paramount concern for cryptocurrency users, as it ensures the safety and integrity of their digital assets. Hardware wallets are designed to provide an additional layer of security compared to software wallets, primarily by isolating the private keys from potential online threats [2]. Each of the wallets reviewed has a combination of physical security measures, innovative key management techniques, and isolation from network threats to ensure the highest possible security for their users. Depending on individual needs and risk tolerance, users can choose a wallet that best fits their security requirements. In this section, we list the wallets reviewed and the security measures that they offer.

Table 1. Important security features of the cold wallets listed in the paper

Wallet	Features	Description
Safepal S1 Pro	Air-Gapped and Seed Phrase Recovery	Uses QR code scanning for transactions, isolating it from network-based threats. Utilizes seed phrases for recovery
Cypherock X1	Key Splitting	Private key is split into five parts, stored across four cards and one vault device, with only one part needed for recovery.
	PIN Protection	Each part is protected by an additional PIN code
	Non-Updatable Firmware	Cards' firmware cannot be updated, preventing backdoor hacks
Ellipal Titan 2	Anti-Disassembly and Anti-Tampering	Features strong physical security measures to prevent tampering
	Air-Gapped and Seed Phrase Recovery	Uses QR code scanning for transactions, isolating it from network-based threats. Utilizes seed phrases for recovery
Keystone 3 Pro	Multiple Security Chips	Utilizes three security element chips for enhanced protection
	Biometric authentication	Includes biometric authentication for an extra layer of security
Tangem	Card-Based System	Uses cards that do not require charging or connectivity, activated by tapping against a smartphone.
	Non-Updatable Firmware	Avoids firmware updates to eliminate risks of backdoor hacks
	Physical Durability	Waterproof and physically durable, providing excellent protection against damage and environmental hazards
Ledger Nano X	Connection via Cable	Connects to PC or laptop via cable for secure transactions
	Past Security Issues	Despite being popular, has faced security breaches, notably a hack in 2023 compromising its connect kit
Onekey	Open Source	Both software and hardware are open source, ensuring transparency and trust
	Cross-Chain Swap	Features a cross-chain swap with a low fee, enhancing security during transactions
D'CENT	Biometric Authentication	Features biometric authentication directly on the wallet
	Not Open Source	Unlike some competitors, D'CENT is not fully open source.
SecuX V20	Biometric Authentication	Includes biometric authentication for enhanced security

	Bluetooth Connection	Connects to a smartphone via Bluetooth, which may introduce additional security risks compared to air-gapped options
Trezor Safe 3	Open Source	Fully open source, providing transparency and trust
	Connection via Cable	Connects to a PC or laptop via cable, ensuring secure transactions
Ryder One	Key Splitting	Splits the private key onto a recovery tag, eliminating the need for seed phrases
	Offline Operation	100% offline, ensuring maximum security against online threats
	Physical Durability	Waterproof and dustproof

4. Ease of use

Usability is a critical factor for cryptocurrency wallets, as it directly impacts the user experience and the ability to efficiently manage digital assets. A user-friendly wallet can significantly enhance the overall experience by making it easier to set up, navigate, and perform transactions. This section highlights the user-friendliness of various wallets, focusing on setup processes, interface design, and overall usability. Factors such as how intuitive the interface is, how quickly users can get started, and the ease with which they can manage their assets play a crucial role in determining the practicality of a wallet.

Tangem's User-Friendliness and Rapid Transaction Setup

Out of the wallets reviewed for this paper, Tangem came first in terms of usability, primarily because of its simplicity and rapid transaction setup. Tangem's design is particularly appealing to beginners due to its straightforward and user-centric approach. Tangem offers three different setup methods: the traditional seed phrase method, the ability to import other wallets, and their innovative method where additional cards function as backup cards without using seed phrases. This flexibility allows users to choose the method that best suits their preferences and security needs.
Moreover, Tangem's cards do not require charging, Bluetooth, or any other form of connectivity. Users simply touch the card against their phone, and the wallet sets up and signs transactions within seconds. This ease of use is unparalleled, making Tangem an excellent choice for users who prioritize simplicity and speed in managing their cryptocurrency.

Usability vs. Security: The Case of Tangem and Ledger Nano X

While Tangem excels in usability, it's important to consider the trade-offs between ease of use and security. The Ledger Nano X, despite being one of the most popular cryptocurrency wallets, has faced significant security challenges. In 2023, Ledger experienced security breaches involving third-party integrations, leading to a cautious approach to adopting new technologies [3][4][6]. As a result, Ledger has refrained from using third-party integrations like those employed by Tangem to ensure maximum security for its users.
This contrast between Tangem and Ledger Nano X highlights the ongoing equilibrium problem between ease of use and security in cryptocurrency wallets. While Tangem prioritizes user-friendliness and rapid setup, Ledger emphasizes stringent security measures to protect users'

assets. Users must weigh these factors according to their individual needs and risk tolerance, selecting a wallet that strikes the right balance for their specific requirements. Some Ease of Use features for the other wallets are noted below:

5. Supported Coins and Networks

The range of supported coins and networks is a crucial factor when selecting a cryptocurrency wallet, as it directly affects the wallet's versatility and utility. This section summarizes the supported coins and networks of the wallets reviewed in this study.

Safepal S1 Pro, Ellipal Titan 2, and Tangem
Safepal S1 Pro supports over 10,000 cryptocurrencies, including major ones like Bitcoin (BTC), Ethereum (ETH), and Binance Coin (BNB), along with numerous ERC-20 tokens. It supports a wide range of blockchain networks and allows users to manually add custom tokens. Ellipal Titan 2 also supports over 10,000 cryptocurrencies and natively supports 41 blockchains, enhancing its versatility. It enables direct interaction with decentralized finance (DeFi) applications. Tangem supports a wide range of cryptocurrencies, is compatible with multiple blockchain networks, and features a user-friendly, card-based system that does not require charging or connectivity.

Cypherock X1 and Keystone 3 Pro
Cypherock X1 supports over 3,000 cryptocurrencies [4] and is compatible with multiple blockchain networks, although it lacks the capability to manually add custom tokens. Keystone 3 Pro offers extensive support for numerous cryptocurrencies and integrates with major blockchain networks. It supports direct interaction with decentralized applications through QR code transactions and has direct integration with Metamask and other software wallets.

Ledger Nano X and Onekey
Ledger Nano X supports over 1,800 cryptocurrencies [5], including major coins and numerous ERC-20 tokens, and integrates with the Ledger Live program for enhanced user experience. It can connect with various software wallets to expand its support for additional coins and networks. Onekey supports a vast array of cryptocurrencies and tokens, is compatible with numerous blockchain networks, and offers a cross-chain swap feature with a low fee, enhancing security and convenience during transactions.

D'CENT, SecuX V20, and Trezor Safe 3
D'CENT provides extensive support for multiple cryptocurrencies and integrates with several blockchain networks and Metamask, making it useful for DeFi applications [7][8]. SecuX V20 supports a broad range of cryptocurrencies, is compatible with various blockchain networks, and allows the manual addition of coins for flexible asset management. Trezor Safe 3 supports over 1,000 cryptocurrencies, integrates with several blockchain networks, and can connect to software wallets for broader support. Its open-source nature ensures transparency and trust.

Users should consider their specific needs, including the types of cryptocurrencies they own and the networks they interact with, to select the most suitable wallet for their purposes. Understanding the supported coins and networks of each wallet helps users make informed decisions to manage their digital assets securely and efficiently.

6. Unique Features

Some of the wallets analyzed offered unique features that set them apart by catering to specific user needs, enhancing security, or providing additional utility. These distinctive functionalities can significantly influence a user's choice of wallet, depending on their specific requirements and priorities [9]. This section highlights these unique features, illustrating how each caters to different aspects of cryptocurrency management and user preferences.

Safepal S1 Pro: Comprehensive DeFi Utilities

The Safepal S1 Pro stands out due to its integration of swapping and buying features directly within its app. Users can choose between several decentralized exchanges or centralized exchanges like Binance without incurring additional fees, providing flexibility and cost-efficiency [10]. The wallet also supports cross-chain bridging, facilitating seamless transfers between different blockchain networks. Additionally, Safepal's app includes farming, earning, and staking features, making it a comprehensive DeFi tool that enables users to earn passive income directly within the app.

Cypherock X1: Innovative Key Management

Cypherock X1 employs a unique key management system by splitting the private key into five parts stored across four cards and one vault device [11]. This method ensures that losing multiple parts does not compromise the wallet's security, as only one part is needed for recovery. Each part is protected by a PIN code, adding an extra layer of security. The cards' firmware is non-updatable, preventing potential vulnerabilities from being introduced through firmware updates, and ensuring the wallet remains secure over time.

Onekey: Cross-Chain Swap and NFT Display

Onekey offers a cross-chain swap feature with a low fee of 0.3%, enhancing security during transactions by minimizing the need to move funds between different wallets or exchanges [12]. The touch wallet can display NFTs, making it convenient for collectors to view and manage their digital art directly on the device. Both software and hardware are open source, ensuring transparency and trust by allowing the community to audit the code.

D'CENT: Metamask Integration and Extensive Coin Support

D'CENT features biometric authentication directly on the wallet, adding an extra layer of security and convenience by using fingerprint recognition [7][8]. The wallet integrates directly with Metamask, enhancing usability for DeFi applications and allowing seamless interaction with decentralized apps. D'CENT supports a wide range of blockchain networks and coins, with the ability to manually add coins, providing flexibility and broad support for various assets.

Conclusions

In conclusion, the comparative analysis of offline wallets conducted in this study highlights the diverse approaches to securing and managing digital assets in the cryptocurrency space. Each wallet examined offers unique features and varying levels of security and usability, catering to different user needs and preferences. From the physical security measures of the Ellipal Titan 2 to the innovative key management system of the Cypherock X1, these wallets demonstrate significant advancements in ensuring the safety and accessibility of cryptocurrency.
The integration of NFC technology into offline wallets represents a promising development for enhancing the practicality of cryptocurrency transactions, particularly in scenarios such as EV charging stations. By maintaining a balance between security and user-friendliness, this integration has the potential to make cryptocurrency transactions more convenient and widespread.
This research provides valuable insights for stakeholders, helping them make informed decisions about the adoption and development of secure, user-centric financial technologies. As

the cryptocurrency ecosystem continues to evolve, the findings of this study can guide further advancements in wallet design and functionality, ultimately contributing to a more secure and efficient future for digital currencies.

References

[1] S. T. Bukhari, M. U. Janjua and J. Qadir, "Secure Storage of Crypto Wallet Seed Phrase Using ECC and Splitting Technique," in IEEE Open Journal of the Computer Society, vol. 5, pp. 278-289, 2024, doi: 10.1109/OJCS.2024.3398794. keywords: {Blockchains;Security;Elliptic curve cryptography;Cryptocurrency;Encryption;Bitcoin;Peer-to-peer computing;Seed phrase storage;crypto wallets;blockchain;security;mnemonic phrase;master phrase}.

[2] Homoliak, I., & Perešíni, M. (2024). SoK: Cryptocurrency Wallets--A Security Review and Classification based on Authentication Factors. arXiv preprint arXiv:2402.17659.

[3] Strasser, B. P. (2024). Secure and Usable Decentralized Web Wallet (Doctoral dissertation, University of Applied Sciences).

[4] Yu, Y., Sharma, T., Das, S., & Wang, Y. (2024, May). " Don't put all your eggs in one basket": How Cryptocurrency Users Choose and Secure Their Wallets. In Proceedings of the CHI Conference on Human Factors in Computing Systems (pp. 1-17).

[5] Ledger supported Coins & Tokens (2024) Ledger. Available at: https://www.ledger.com/supported-crypto-assets

[6] Kim, J., Kim, P., Lee, Y., & Choi, D. (2024). Key Backup and Recovery for Resilient DID Environment. Mathematics, 12(6), 830.

[7] Margret, M. K., & Julie, E. G. (2024). Smarter and resilient smart contracts applications for smart cities environment using blockchain technology. Automatika, 65(2), 572-583.

[8] Rezazadeh, A., & Bohnsack, R. Value Creation and Value Capture in Polyadic Business Models: A Multiple Case Study of Blockchain Nft Ventures. Available at SSRN 4807858.

[9] Bukhari, S. T., Janjua, M. U., & Qadir, J. (2024). Secure Storage of Crypto Wallet Seed Phrase Using ECC and Splitting Technique. IEEE Open Journal of the Computer Society.

[10] SafePal crypto hardware wallet (official): The best wallet to protect your assets (no date) SafePal Crypto Hardware Wallet (Official) | The best wallet to protect your assets. Available at: https://www.safepal.com/en/ .

[11] Cypherock X1 (no date) Cypherock X1 – Cypherock Shop. Available at: https://www.cypherock.com/product/cypherock-x1/.

[12] Open source crypto wallet trusted by millions. (no date) OneKey Wallet | Open source crypto wallet trusted by millions. Available at: https://onekey.so/