DOI 10.34185/1562-9945-5-162-2026-13
UDC 004.056.5:004.41

I.V. Ponomarev

ARCHITECTURE OF A SECURE CRYPTOCURRENCY WALLET BASED ON AIR-GAP AND MULTISIGNATURE MECHANISMS

Abstract. The study addresses the vulnerabilities of cryptocurrency wallets to network attacks. A secure cross-platform architecture is proposed, integrating Air-Gap, PSBT, and M-of-N multisignature mechanisms. The solution implements isolated online and offline modules with transaction data exchange via QR codes. Results demonstrate that this architectural approach effectively ensures private key isolation and enhances the security of digital asset transactions.
Keywords: cryptocurrency wallet, Air-Gap, cold storage, multisignature, PSBT, QR code, blockchain, offline signing, cross-platform application.

Problem statement. The rapid growth in cryptocurrency transaction volumes has intensified the focus on secure asset storage and protection mechanisms. Cryptocurrency wallets constitute a fundamental component of blockchain infrastructure, enabling user interaction with decentralized networks. However, they also represent a critical vulnerability within this ecosystem. Unlike traditional financial systems, where security is enforced by centralized regulatory entities, decentralized architectures transfer full responsibility for asset protection to individual users.

Cryptocurrency wallets are generally classified into two categories: hot wallets and cold wallets, distinguished primarily by their connectivity to the Internet and corresponding security characteristics. Hot wallets operate on devices with continuous network access, offering high usability for routine transactions. This category encompasses software solutions such as Trust Wallet and MetaMask, as well as mobile and web applications provided by cryptocurrency exchanges. Nevertheless, persistent connectivity significantly increases exposure to cyber threats. Common attack vectors include phishing, malware (e.g., spyware and clipboard hijackers), and exploitation of zero-day vulnerabilities in operating systems such as Android, iOS, and Windows. According to Chainalysis, a substantial proportion of cryptocurrency asset losses result from compromises of hot wallets through browser extensions and mobile platforms [1].

Conversely, cold wallets are designed to maintain complete isolation from online environments, prioritizing maximum security. This class includes paper wallets and hardware wallets. Paper wallets provide full offline storage but are susceptible to physical damage, loss, or destruction, rendering them impractical for frequent use.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Hardware wallets, exemplified by Ledger and Trezor, secure private keys within dedicated hardware modules, thereby mitigating remote compromise risks. However, these devices exhibit functional limitations and remain vulnerable to specific threats, including supply chain attacks, partial opacity of source code, and risks associated with physical connectivity via USB, Bluetooth, or NFC, which introduce additional attack surfaces.

To increase the security of transactions in the blockchain, a multi-signature mechanism is used, which requires several independent signatures to confirm the operation. Instead of a single private key, the M-of-N rule is used, where N is the total number of owners and M is the minimum number of signatures required to complete a transaction. This approach prevents unauthorized access, as compromising a single key does not allow the transaction to be completed. In the Bitcoin blockchain, multi-signature is implemented through scripts (e.g., P2WSH) and the BIP-174 Partially Signed Bitcoin Transaction (PSBT) format [2], and in the Ethereum blockchain, through smart contracts such as Safe with threshold and permission logic [3].

A common cybersecurity practice to protect critical data, such as private cryptographic keys or confidential transactions, is the use of air-gapped devices. These are computers or hardware systems that are physically isolated from any network connections, including the Internet, local networks, and wireless interfaces. Such isolation means that the device has no active network ports or radio channels, making it inaccessible to remote attacks. Interaction with such devices is carried out via offline data transfer methods, such as QR codes or USB media, which allows you to maintain isolation and minimize the risks of compromise.

Thus, it is relevant to consider a combination of several technologies for ensuring the security of cryptocurrency wallets.

Analysis of the latest research and publications. The security of cryptocurrency wallets remains a key topic of current research. The paper by Guri et al. [4] addresses the problem of private key leakage even from isolated (air-gapped) systems. The authors demonstrate the possibility of attacks through side channels (electromagnetic, acoustic), which calls into question the absolute security of offline devices.

The study by Homoliak et al. [5] proposes the concept of SmartOTPs, a two-factor authentication mechanism for smart contracts that uses QR codes and hash chains to transmit signatures offline. This solution increases the security of transactions without losing convenience.

Another important direction is the standardization of the transaction signing process. Homoliak et al. (2024) review modern approaches to multi-signature and PSBT, which allow for collective control of assets [6]. CertiK [7] analyzes PSBT vulnerabilities in DeFi projects and offers recommendations for secure implementation, including SIGHASH verification and avoiding UTXO dust.

The study by Das et al. [8] focuses on threshold signatures, which provide compactness and efficiency for multi-party protocols. This is especially relevant for cold wallets, where minimizing the risk of compromise is important.

Special attention is paid to hardware wallets. Dabrowski et al. [9] showed architectural shortcomings of popular solutions (Ledger, Trezor), in particular supply chain risks. Šorf et

al. [10] performed a large-scale analysis of 17 hardware wallet models, revealing implementation problems, although the cryptographic algorithms remain robust.

Comparative studies (Haryadi et al. [11], Lim et al. [12]) demonstrate a trade-off between the convenience of hot wallets and the security of cold wallets. Hybrid solutions are considered a promising direction that combines the advantages of both approaches.

In general, current work emphasizes the need for a comprehensive approach: a combination of Air-Gap, multi-signature, PSBT and cryptographic protection of local data to create secure and convenient cryptocurrency wallets.

Purpose of the research. The aim of the research is to develop an architecture and create a cross-platform cryptocurrency wallet that provides:

1) physical isolation of private keys (Air-Gap) during the signing process;

2) use of the PSBT standard for secure data exchange between online and offline modules;

3) integration of the QR process for transferring transaction data between isolated environments, which eliminates direct network connection and increases resistance to attacks;

4) implementation of a multi-signature mechanism for collective control of assets;

5) use of cryptographic algorithms to protect the local database.

Presentation of the main research material. When developing a cross-platform wallet application, cold storage technologies, air-gapped devices, data transfer using QR codes and multi-signatures are combined in a single architecture.

To achieve maximum security, the wallet is divided into two physical modules: the online Watcher module and the offline Signer module.

In addition, the system is structured according to the principle of a three-level architecture: Core, Transport, UI.

The Core level includes cryptographic primitives, key management and multi-signature logic. The Transport level implements Air-Gap, PSBT exchange between modules via QR codes. The UI interface level is responsible for transaction management, address book and credential verification (Fig. 1).

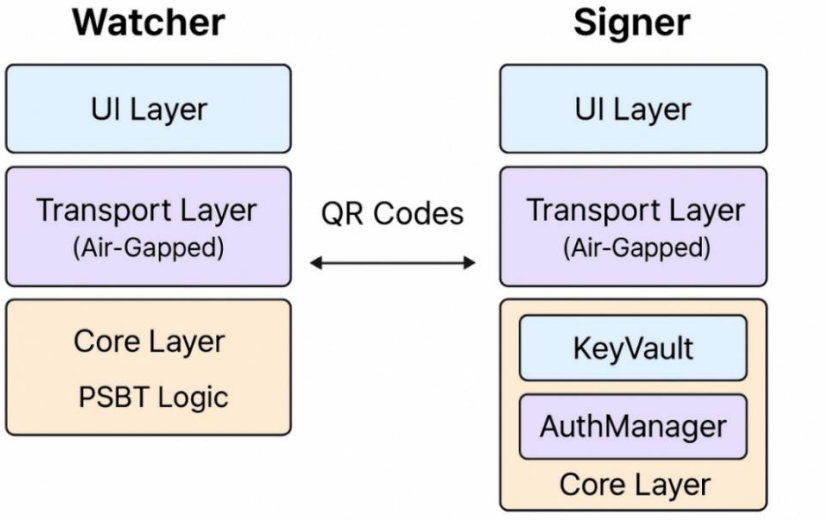

Figure 1 - Architecture of a two-module wallet with a three-tier structure

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

The online Watcher module is installed on the user's main smartphone with network access. It connects to blockchains (Bitcoin, Ethereum) to obtain balances and transaction history. It stores only the extended public key (xPub), which allows generating all wallet addresses for receiving funds, but does not allow spending them. It forms the initial transaction structure (UTXO for BTC, Nonce for ETH) and visualizes it in the form of a QR code. It accepts the signed transaction from the offline module and sends it to the blockchain network.

The offline Signer module is installed on an isolated device (without a SIM card, Wi-Fi and Bluetooth). It generates the Seed phrase and private keys, encrypts them and stores them in the database. Then, it reads the QR code from the Watcher module, checks the user's parameters and applies a digital signature in an isolated environment.

The wallet initialization process is critical and occurs exclusively in the offline Signer module. A cryptographically stable random number generator (CSPRNG) is used to generate a 256-bit sequence. A checksum is added to it, after which the data is divided into groups of 11 bits. Each group corresponds to a word from the BIP-39 dictionary, which results in a 24-word seed phrase that is used to restore the wallet. The seed phrase is converted to 512-bit binary data (seed) using the PBKDF2 function with 2048 iterations of HMAC-SHA512. According to the BIP-44 standard, a hierarchical derivation structure is used, which determines the order of key and address generation [14]. This approach allows one wallet to manage multiple cryptocurrencies (Bitcoin, Ethereum) and different types of addresses.

Key storage is implemented using the built-in SQLite database, while encryption is used to protect confidential information, where the user's password serves as the basis for generating the encryption key. The PBKDF2 function is used to convert the password to a 256-bit AES key, and all data in the keys table, including the seed phrase and private keys, are encrypted using the AES-256-CBC algorithm before being written to the database. This approach guarantees that even in the event of theft of the device and gaining access to the file system, the attacker will not be able to read the keys without knowing the password.

The algorithm for working with a multi-signature wallet via the Air-gap interface consists of the following stages.

First, in the Watcher module, the user forms a transaction, specifying the recipient's address and the amount. The application receives current data from the blockchain, creates a PSBT package and displays it as a QR code.

Next, each of the M signature participants opens the Signer module on their offline device and scans this code. After that, Signer module decrypts the transaction, shows the details ("Sending 1.0 BTC to bc1q... Fee: 0.0005 BTC"), and the user physically verifies the information. For authorization, a password is entered, based on which the private key is decrypted. Then the module digitally signs the transaction, clears the memory and generates a new QR code with a partially signed transaction.

Watcher module sequentially scans all signed codes from M offline modules, checks their validity and forms the final PSBT with the M-of-N threshold. When the number of signatures reaches the threshold, the transaction becomes valid and is broadcast to the blockchain network.

The client-level implementation of the wallet modules is made using modern cross-platform technologies. The mobile interface is built on Vue.js in combination with the Quasar Framework, which provides adaptive design and component architecture. Apache Cordova is utilized to access the device's hardware capabilities, such as the camera and file storage, by integrating native APIs into the web application.

The desktop implementation is based on Electron, enabling the application to run as a native app on Windows, macOS, and Linux while maintaining a unified codebase. In parallel, the Progressive Web App (PWA) mode is supported for working in a browser with offline caching and push notifications.

Specialized libraries are used to work with blockchains:

• bitcoinjs-lib — for generating and processing PSBT, generating keys, signatures and working with the UTXO model.

• ethers.js — for interacting with Ethereum-compatible networks, including generating transactions, calculating EIP-712 hashes, verifying signatures and calling smart contracts.

Conclusions. The proposed two-module architecture ensures private key isolation within an offline environment, eliminating network-based compromise risks. By integrating Air-Gap, PSBT, and M-of-N multisignature with robust AES-256 encryption, the system achieves high security without sacrificing usability. The cross-platform implementation provides a unified user experience across mobile and desktop devices. Ultimately, the developed solution effectively balances hardware-level protection, cryptographic transparency, and functional accessibility.

REFERENCES

1. Chainalysis. (2025). 2025 Crypto Crime Mid-Year Update. Retrieved January 8, 2026, from https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/

2. Bitcoin Improvement Proposal 174 (BIP-174): Partially Signed Bitcoin Transaction Format. Retrieved January 8, 2026, from https://bips.dev/174/

3. Safe Foundation. (n.d.). Safe {Core}: Contracts Architecture. Retrieved January 8, 2026, from https://docs.safe.global/docs/contracts_architecture/

4. Guri, M. (2018). BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. arXiv. Retrieved January 8, 2026, from https://arxiv.org/pdf/1804.08714

5. Homoliak, I., Breitenbacher, D., Hujnak, O., Hartel, P., Binder, A., & Szalachowski, P. (2018). SmartOTPs: An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets (Extended version). arXiv. https://doi.org/10.48550/arXiv.1812.03598

6. Homoliak, I., & Perešíni, M. (2024). SoK: Cryptocurrency Wallets – A Security Review and Classification based on Authentication Factors. In 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).
https://doi.org/10.1109/ICBC59979.2024.10634439

7. CertiK. (2024, December 17). Exploring PSBT in Bitcoin DeFi: Security Best Practices. CertiK Blog. Retrieved January 8, 2026, from
https://www.certik.com/resources/blog/exploring-psbt-in-bitcoin-defi-security-best-practices

8. Das, S., Camacho, P., Xiang, Z., Nieto, J., Bünz, B., & Ren, L. (2023). Threshold signatures from inner product argument: Succinct, weighted, and multi-threshold. In Proceedings

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23) (pp. 356–370). https://doi.org/10.1145/3576915.3623096
9. Dabrowski, A., Pfefer, K., Reichel, M., Mai, A., Weippl, E. R., & Franz, M. (2021). Better keep cash in your boots – Hardware wallets are the new single point of failure. In Proceedings of the 2021 ACM CCS Workshop on Decentralized Finance and Security (DeFi '21) (pp. 1–8). https://doi.org/10.1145/3464967.3488588
10. Šorf, M., Švenda, P., & Chmielewski, Ł. (2025). Large-scale security analysis of hardware wallets. In Lecture Notes in Computer Science (Vol. 15995, pp. 360–377). Springer. https://doi.org/10.1007/978-3-032-00633-2_21
11. Haryadi, G. A., Rahaman, M. F., Subhan, M. R., Lee, J. M., & Kim, D.-S. (2022). Comparative study of cryptocurrency wallet security: A hybrid, hot, and cold wallet approach. ResearchGate. Retrieved January 8, 2026, from https://www.researchgate.net/publication/375187201_Comparative_Study_of_Cryptocurrency_Wallet_Security_A_Hybrid_Hot_and_Cold_Wallet_Approach
12. Lim, H.-J., Lee, S., Kim, M., & Lee, W. (2025). Comparative analysis of security features and risks in digital asset wallets. Electronics, 14(12), 2436. https://doi.org/10.3390/electronics14122436
13. National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard (AES). https://doi.org/10.6028/NIST.FIPS.197-upd1
14. Bitcoin Improvement Proposal 44 (BIP-44): Multi-Account Hierarchy for Deterministic Wallets. Retrieved January 8, 2026, from https://bips.dev/44/

Received 09.01.2026.
Accepted 15.01.2026.

Архітектура безпечного криптогаманця на основі механізмів Air-Gap та мультипідпису

Сучасний стан кібербезпеки в галузі цифрових активів свідчить про критичну вразливість гаманців до мережевих атак та шпигунського ПЗ. Наукові розробки підтверджують, що навіть ізольовані системи можуть бути скомпрометовані через побічні канали, що вимагає впровадження багаторівневих методів захисту. Актуальними напрямками досліджень є використання стандарту PSBT для уніфікації передачі даних та протоколів мультипідпису для усунення єдиної точки відмови. Аналіз існуючих апаратних рішень вказує на ризики закритих архітектур, що робить затребуваним створення відкритих систем із фізичною ізоляцією ключів.

Метою роботи є проєктування та реалізація архітектури кросплатформного криптогаманця, що поєднує метод Air-Gap для фізичної ізоляції приватних ключів, стандарт PSBT для безпечного обміну даними та механізм мультипідпису M-of-N для колективного управління активами.

Запропонована архітектура базується на розділенні системи на два функціональні модулі: онлайн-модуль Watcher та офлайн-модуль Signer. Модуль Watcher відповідає за моніторинг блокчейну та формування транзакцій, зберігаючи лише публічні ключі. Модуль Signer функціонує на пристрої без мережевих інтерфейсів, забезпечуючи генерацію та зберігання приватних ключів у зашифрованій базі даних SQLite. Взаємодія між модулями здійснюється через візуальний інтерфейс QR-кодів,

що виключає прямий цифровий контакт між середовищами. Програмна реалізація виконана на стеку Vue.js та Quasar, що разом із Cordova та Electron забезпечує роботу застосунку на Android, iOS, Windows та Linux з єдиною кодовою базою.

Розроблена дворівнева архітектура ефективно ізолює приватні ключі від мережевих загроз, забезпечуючи високу стійкість до віддалених атак. Використання стандартів PSBT та мультипідпису гарантує прозорість транзакцій та можливість колективного контролю над коштами. Кросплатформний підхід дозволяє масштабувати рішення на різні типи пристроїв, зберігаючи баланс між безкомпромісною безпекою та зручністю для кінцевого користувача.

Пономарьов Ігор Володимирович – к.т.н., доцент кафедри електронних обчислювальних машин факультету фізики, електроніки та комп'ютерних систем Дніпровського національного університету ім. Олеся Гончара.
ORCID: https://orcid.org/0009-0009-7139-2885

Ponomarev Igor Volodimirovich – candidate of technical sciences, associate professor of the department of electronic computers of the faculty of physics electronics and computer systems of the Oles Honchar Dnipro National University.
ORCID: https://orcid.org/0009-0009-7139-2885

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)