iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71146

Decentralized Wallet Application: A Review

Vimal Singh[1], Yash Bhardwaj[2], Tilak Jain[3]
[1, 2, 3]Raj Kumar Goel Institute of Technology, Ghaziabad, India

Abstract: With the rise of decentralized digital currencies powered by blockchain technology, a new era of peer-to-peer transactions has emerged. The growing use of cryptocurrency wallets, which facilitate secure transactions without relying on centralized authorities, has brought about both opportunities and challenges. Despite their potential, cryptocurrency wallets are increasingly targeted by hackers, exposing users to risks such as theft, fraud, and data breaches. Blockchain's immutability and cryptographic techniques provide robust solutions to these issues, yet security concerns persist due to vulnerabilities in wallet design and implementation. This paper reviews the current state of cryptocurrency wallets, highlighting the critical security risks associated with their use. It introduces a multi-dimensional taxonomy for classifying wallet designs and evaluating their security implications. We identify common vulnerabilities and map them to corresponding defense strategies. The paper also explores the role of key management, security vulnerabilities in blockchain protocols, and the need for continuous improvements in wallet architecture. We propose a decentralized, secure, and user-friendly digital wallet solution built on Ethereum's distributed ledger, ensuring privacy, transaction transparency, and eliminating third-party intermediaries. The research also discusses the potential for integrating blockchain wallets with decentralized applications (dApps) to enhance functionality and user control.

Keywords: Blockchain, Cryptocurrency Wallet, Wallet Security, Key Management, Attacks, Defense Mechanisms, Smart Contracts, Decentralized Applications (dApps), Ethereum, Private Key, Public Key, Decentralization.

I. INTRODUCTION

Blockchain is a decentralized, immutable digital ledger that records verifiable transactions across a distributed peer-to-peer network. Designed with Byzantine fault tolerance and cryptographic security at its core, blockchain ensures that data, once validated and linked via cryptographic hashes, cannot be altered without affecting the entire chain [6]. This tamper-proof structure enables trust less interactions and forms the backbone for decentralized applications (dApps), decentralized finance (DeFi), and cryptocurrencies.

Cryptocurrency wallets (crypto wallets) serve as the primary interface for users to access and interact with blockchain networks. Unlike physical wallets or centralized banking systems governed by institutions such as the RBI or FDIC, cryptocurrencies are not stored in any single location or physical form. Instead, they exist as transaction data stored on the blockchain. Wallets manage public-private key pairs that authorize the transfer of assets on-chain. As Suratkar et al. [2] explain, wallets do not hold actual coins but rather facilitate ownership proofs via cryptographic signatures. According to Suratkar et al. [2], wallets are broadly categorized into hot (internet-connected) and cold (offline) types. Hot wallets—such as browser-based and mobile wallets—offer accessibility but are more vulnerable to network-based attacks. Cold wallets—such as hardware or air-gapped wallets—prioritize security, storing private keys offline and reducing risk [6]. However, each wallet type comes with trade-offs in usability, security, and recovery.

Despite their critical role in decentralized finance, wallets face numerous challenges that impede broader adoption. As He et al. [1] note, key management remains a major issue, with users struggling to store, protect, and recover private keys effectively. Choudhary et al. [3] further highlight the lack of unified security frameworks in decentralized wallet applications, emphasizing the need for improved authentication and backup mechanisms. Erinle et al. [4] stress the risk posed by private key leakage and software vulnerabilities, which can lead to irreversible financial losses. In addition, Popchev and Radeva [5] observe that wallets are essential gateways for interacting with smart contracts, tokens, and dApps in the Web3 ecosystem, and their reliability is crucial for enabling trust less user interaction.

As blockchain systems continue to evolve, the development of secure, user-friendly, and interoperable decentralized wallets is essential. This paper proposes a decentralized cryptocurrency wallet solution that improves private key security, simplifies user onboarding, and enhances integration with blockchain-based services. The design draws on best practices from existing literature and proposes a balance between usability and strong cryptographic protections, contributing to the next generation of decentralized financial tools.

II. EXISTING SYSTEM

Decentralized wallets, while offering significant advantages in privacy and security, still face several usability and functional challenges that hinder widespread adoption. A major drawback lies in the complex process of private key management. As emphasized by Lehto et al. [6], the secure handling of private keys is critical, and losing them results in permanent loss of access to digital assets. Unlike traditional banking systems that offer account recovery options, decentralized wallets lack such mechanisms, as also noted by Suratkar et al. [2].

Another key concern is the scalability of blockchain platforms, which directly impacts wallet performance. He et al. [1] have discussed how scalability bottlenecks can lead to high transaction fees and slower processing times, reducing the efficiency and attractiveness of blockchain-based wallets. Users may experience delayed transaction confirmations and increased costs, particularly during network congestion.

Managing multiple wallets for different cryptocurrencies adds to the complexity. Choudhary et al. [3] highlight this as a significant concern, noting that users are often forced to maintain separate wallets for each token or coin, which not only complicates user experience but also raises security risks. This fragmentation arises due to the lack of interoperability and standardization across platforms.

The absence of centralized customer support is another limitation. Since decentralized wallets operate without an intermediary, users encountering issues have limited recourse. Erinle et al. [4] point out that this can be particularly problematic for beginners or non-technical users who may find the system unforgiving when mistakes occur.

Moreover, the immutable nature of blockchain transactions presents additional challenges. As described by Popchev and Radeva [5], transactions made on the blockchain are irreversible, meaning that mistakes such as sending funds to an incorrect address cannot be rectified. This irreversible design, while promoting trust lessness and transparency, introduces risk for users who are unfamiliar with the technology.

Regulatory uncertainty surrounding blockchain technologies also complicates the use of decentralized wallets. Inconsistent legal frameworks across countries make it difficult to ensure compliance and trust for broader use. These legal ambiguities, combined with usability and technical issues, limit the mainstream integration of decentralized financial tools.

To overcome these obstacles, improvements are needed in wallet design to enhance security, user-friendliness, and support. Future solutions must focus on standardizing wallet architecture, improving recovery options, and incorporating user-centric features that promote accessibility without compromising decentralization. Lehto et al. [6] suggest that combining robust security measures with simplified user interfaces will be key to making decentralized wallets more practical and widely accepted.

III. LITERATURE REVIEW

Cryptocurrency wallets are fundamental to blockchain infrastructure, serving as tools for managing, storing, and transacting digital assets through cryptographic key pairs. He et al. [1] introduced a decentralized wallet management model using multi-constrained derangement for better security and usability. Suratkar et al. [2] provided a comprehensive review of cryptocurrency wallets, categorizing them into hot (internet-connected) and cold (offline) wallets, each offering different trade-offs in security and convenience. Choudhary et al. [3] proposed a decentralized wallet application leveraging blockchain, highlighting its benefits in eliminating intermediaries and offering improved privacy.

Erinle et al. [4] conducted a Systematization of Knowledge (SoK) study that outlined wallet vulnerabilities such as poor key management and phishing attacks, emphasizing the need for more robust authentication and user education. Popchev and Radeva (2024) further demonstrated the development and implementation of decentralized applications (dApps), positioning wallets as key interfaces for smart contract interaction and asset control.

From a security perspective, Lehto et al. [6] introduced CryptoVault, a hardware wallet designed to secure decentralized key storage with physical safeguards. Kirobo [7] conducted a systematic review identifying common wallet vulnerabilities like replay attacks, malware threats, and private key leakage. These studies suggest that secure wallet design must include seed phrase protection, cryptographic hashing, and optional hardware support. The user experience is also evolving; decentralized wallets now offer real-time market data, seamless dApp connectivity, and transparent transaction histories enabled by blockchain's immutable ledger. These innovations empower users with self-custody, lower transaction fees, and censorship-resistant finance. Despite advancements, gaps remain in user-centric design, secure key recovery mechanisms, and education for mass adoption, which this current work aims to address.

A. Hot vs. Cold Wallets

Cryptocurrency wallets can be broadly categorized into hot wallets and cold wallets based on their connection to the internet. Hot wallets are connected to the internet, enabling easy access to cryptocurrency assets and quick transactions. They are typically used for frequent transactions, but they are more vulnerable to hacking and other security threats. For instance, Suratkar et al. [2] discuss how web wallets are convenient and accessible but are more prone to cyberattacks due to the storage of private keys on third-party servers.

Some wallets like Jaxx and Guarda enhance security by letting users manage their private keys themselves, reducing dependency on centralized services.

Cold wallets, in contrast, are offline storage solutions (e.g., hardware wallets) that are more secure due to their isolation from online threats. He et al. [1] propose a decentralized multi-constrained derangement-based wallet management scheme that enhances cold wallet security, making it more robust against key exposure.

These wallets are preferred for long-term storage due to their low attack surface, though usability remains a trade-off. Erinle et al. [4] highlight that both hot and cold wallets often rely on seed phrases for recovery, introducing risk if the user mismanages them. They emphasize that while cold wallets offer better security by being offline, the user is solely responsible for safeguarding recovery data.

Table 1 compares hot and cold wallets, focusing on differences in internet connectivity, usage, security, key management, recovery mechanisms, user experience, vulnerabilities, and advanced security features, supported by relevant literature.

B. Security Challenges

Security is a prominent concern in wallet design. Kirobo [7] provides a systematic review of vulnerabilities in cryptocurrency wallets. His study identifies phishing attacks, weak password protocols, and compromised third-party key services as primary threats. The review also outlines how software bugs and implementation flaws in hot wallets increase attack vectors.

In response to such vulnerabilities, Lehto et al. [6] introduce *CryptoVault*, a secure hardware wallet with decentralized key management, designed to enhance physical and logical security. This system is focused on secure key storage and mitigates risk through encrypted communication and hardware isolation.

Erinle et al. [4] further classify wallet vulnerabilities into design-related and operational flaws and advocate for strategies like two-factor authentication, multi-signature schemes, and hardware wallets to counteract them. Despite these measures, the human factor—misplacing seed phrases or falling victim to scams—remains a major vulnerability.

C. User Experience

The usability of cryptocurrency wallets often conflicts with security requirements. Suratkar et al. [2] explain that hot wallets are generally more user-friendly and suitable for new users due to their simplified UI and fast access. However, this ease of use often compromises security when wallets are hosted online, or keys are stored in the browser.

Choudhary et al. [3] propose a decentralized wallet application that integrates a user-friendly interface while enhancing trust via blockchain-based transaction validation. The application removes intermediaries and facilitates peer-to-peer asset management, highlighting a shift toward user-empowered financial systems. Popchev and Radeva [5] analyse how decentralized applications (dApps) integrate wallet functionality for identity management and transaction approval. While this provides transparency and user autonomy, it introduces complexity that may hinder mainstream adoption. Their work suggests that better UX design and onboarding tutorials could improve adoption among non-technical users.

D. Gaps Addressed by This Work

While the existing literature explores various wallet types and their associated challenges, several research gaps remain. Most notably, few studies address the balance between ease of use and robust security in practical wallet applications. For example, while hardware wallets are secure, they may alienate less tech-savvy users. Similarly, while hot wallets offer convenience, they often compromise on privacy and security.

This work addresses these challenges by proposing a hybrid wallet framework that merges the best aspects of hot and cold wallets—providing both user-friendliness and strong security protocols. It introduces backup mechanisms that reduce human error and emphasizes user education as a first-class component of wallet design.

Table 1: Comparison of Hot Wallet and Cold Wallet

Criteria	Hot Wallets	Cold Wallets
Internet Connection	Always connected to the internet	Remain offline, no direct internet connection
Usage	Suitable for frequent transactions and daily use	Ideal for long-term storage and large holdings
Security	More vulnerable to cyberattacks (e.g., phishing, compromised key services)	Highly secure due to physical isolation from online threats
Examples	Jaxx, Guarda (with user-controlled keys), Web wallets	Hardware wallets (e.g., Ledger, Trezor), paper wallets
Key Management	Often stored online or in browsers; some wallets allow local key control	Keys stored offline; secure against online exposure
Recovery Mechanism	Seed phrases commonly used; vulnerable if mishandled	Also use seed phrases; complete user responsibility for secure storage
User Experience (UX)	More user-friendly, fast access, suitable for beginners	Less intuitive, slower access; may be difficult for non-technical users
Vulnerabilities	Susceptible to software bugs, third-party server breaches, weak password protocols	Physical damage, loss, or mismanagement of recovery phrase
Advanced Security	May include 2FA, multi-signature support	Supports secure hardware isolation, encrypted storage, and decentralized key management (e.g., CryptoVault)
Literature Support	Suratkar et al. [2], Erinle et al. [4], Kirobo [7]	He et al. [1], Erinle et al. [4], Lehto et al. [6]

IV. BASIC THEORY

Cryptocurrency wallets are software platforms designed to enable users to interact with blockchain networks, facilitating transactions and storing digital assets. These wallets manage two key elements: a public address and a private key. The public address, which is a hexadecimal string, is used to receive cryptocurrencies, while the private key, also a hexadecimal string, is kept secure and is required to sign transactions on the blockchain.

Suratkar et al. [2] explain that wallets are client software for blockchain platforms, enabling transactions through the use of stored public and private keys. Most modern wallets are Hierarchical Deterministic (HD) wallets, which allow users to restore their balance and full transaction history using a mnemonic phrase if the wallet is lost or compromised. This structure makes cryptocurrency wallets similar to online banking accounts, where the public address acts as an account number and the blockchain serves as the ledger. Additionally, custodial wallets, which are managed by third parties, resemble traditional banking systems where custodians manage transactions on behalf of users.

He et al. [1] emphasize the importance of private key management, where private keys (sk) are encrypted and stored securely in the wallet. The security of a wallet heavily depends on its infrastructure, whether it is software-based (e.g., desktop, mobile, or browser wallets) or hardware-based (e.g., using a secure element like a microcontroller). While software wallets are more vulnerable to security risks due to their internet connectivity, hardware wallets offer greater protection by keeping private keys offline, reducing exposure to cyber threats.

In addition, Kailun Yan, Jilian Zhang, and Xiangyu Liu [12] discuss the decentralized nature of ecosystems in the blockchain context, emphasizing how decentralized services, including cryptocurrency wallets, operate without the control of centralized entities.

Their research suggests that while decentralized platforms promise verifiable, self-governing, and permissionless services, some wallets may still rely on centralized components like RPC services and third-party SDKs, introduce potential security risks. They argue that such centralization contradicts the foundational principles of decentralization and exposes users to risks which like data theft or unauthorized access, thus threatening the security of users' assets.

Moreover, Suratkar et al. [2] and Yan et al. [12] highlight the variety of wallet functionalities such as multicurrency support, token conversion, and integration with crypto exchanges. They also note the importance of encryption and secure key management practices to safeguard the wallet's integrity.

The issue of wallet anonymity is crucial, with some wallets ensuring full anonymity (requiring no personal information), while others, as pointed out by Yan et al. [12], might ask users to provide email addresses or phone numbers, compromising the privacy of the wallet. Security remains a paramount concern for cryptocurrency wallets. Yan et al. [12] identify that centralization within decentralized services, such as third-party services in wallets, exposes users to security vulnerabilities. Regular backups and using secure wallets like hardware wallets are essential to minimize these risks. Both Yan et al. [12] and He et al. [1] stress the need for robust encryption, secure key management, and awareness of potential centralization factors that may compromise the wallet's decentralized architecture.

V. METHODOLOGY

This review paper aims to analyze and compare the features, architecture, and technologies used in various decentralized cryptocurrency wallets. A systematic approach was employed to ensure a comprehensive and objective review. The methodology adopted in this survey is as follows:

A. Survey Paper and Literature Review

A thorough literature analysis of previous studies, publications, and reports on decentralized cryptocurrency wallets was part of the first phase. Key topics such as security features, wallet architecture, and integration with blockchain technology were explored. This analysis led to the selection of key papers and case studies for research, including the works of Suratkar et al. [2], who provided a comprehensive review of cryptocurrency wallets, their security challenges, and the technical details of wallet architecture. Additionally, He et al. [1] contributed valuable insights into multi-constrained wallet management and its relevance to decentralized systems. Developers and consumers of decentralized wallets were also surveyed to learn more about their preferences, real-world use cases, and difficulties. This survey aimed to gain an understanding of the practical challenges faced by users of decentralized wallets and informed the analysis of common security vulnerabilities, as discussed by Erinle et al. [4] and Choudhary et al. [3]. The characteristics and technological advancements found during the literature study were validated in part by this survey, providing a practical perspective on how existing wallets perform in real-world scenarios.

B. Selection Wallets

A total of 5 decentralized wallets were selected for evaluation based on the following criteria.

1) Usage and Popularity: The wallets included are well-regarded and frequently utilized within the cryptocurrency community. They represent a mix of both well-established wallets and newer, emerging ones, ensuring a broad spectrum of user preferences and experiences.
2) Open-source Availability: Wallets with open-source code were preferred to ensure transparency and accessibility.
3) Compatibility with Ethereum and Bitcoin Transactions: Wallets supporting Ethereum and Ethereum-compatible blockchains (e.g., Binance Smart Chain, Polygon) were prioritized, as these networks are popular in decentralized finance (DeFi) and other decentralized applications (dApps).

The selected wallets span a wide range of use cases and target audiences, from mobile-first wallets to full-featured desktop solutions, to ensure a diverse and representative evaluation.

C. Evaluation Criteria

The evaluation of the selected decentralized wallets was based on the following criteria, along with other key factors.

1) Security Features: This includes the management of private keys, use of encryption mechanisms (e.g., AES, RSA), cryptographic hashing (e.g., SHA-256), multi-signature support, and the implementation of additional security features such as two-factor authentication (2FA) and biometric authentication.
2) Blockchain Integration: An assessment was conducted on the wallet’s integration capabilities with various blockchain platforms, including major networks like Ethereum and Bitcoin. The evaluation emphasized the wallet’s effectiveness in enabling seamless cross-chain interoperability.
3) Smart Contract Compatibility: The analysis explored the wallet’s capabilities in interacting with blockchain-specific functionalities, particularly its integration with Ethereum smart contracts such as ERC-20 tokens and DeFi platforms. Key areas included support for contract execution, token transfers, and operations on decentralized exchanges (DEXs). Additionally, the wallet’s compatibility with Bitcoin was assessed, focusing on its ability to manage transactions, support SegWit addresses, and interact with Bitcoin-based services where applicable.

4) Back and Recovery Options: The wallet's provisions for securing and recovering funds, including backup options like seed phrases, private key exports, and multi-factor authentication for recovery.
5) Performance and Scalability: An evaluation of the wallet's performance and scalability was conducted, focusing on its responsiveness during both typical usage and high-traffic scenarios. Key factors included transaction processing speed, memory usage, and the system's capacity to efficiently handle a growing user base and increased blockchain activity.
6) Support for Additional Features: This includes features such as token swapping, staking, decentralized application (dApp) integration, and multi-chain support.

D. Data Collection

To ensure a comprehensive and accurate evaluation, data was gathered from multiple sources. Official documentation provided in-depth information on the wallet's features, architecture, and security measures as outlined by the development teams. Additionally, GitHub repositories were examined to assess the quality of the wallet's code, the libraries used, and the level of community contributions. Developer forums, including Stack Overflow, Reddit, and official platform threads, were reviewed to understand common user challenges and gather valuable feedback. Whitepapers detailing the wallet's design philosophy and security protocols were thoroughly studied, along with academic research related to wallet security, user experience, and blockchain integration.

For Bitcoin-specific data collection, transaction data was reviewed using public Bitcoin block explorers to evaluate how well the wallet manages Bitcoin transactions, supports SegWit, and handles address compatibility. The Bitcoin protocol and its security mechanisms were also analysed to assess the wallet's adherence to these standards. Finally, hands-on testing was conducted on various wallets across both desktop and mobile platforms to assess their practical performance, user-friendliness, and security features. Transaction simulations on test nets were carried out to validate the wallets' functionality, including token transfers, smart contract interactions, and Bitcoin transaction handling.

E. Analysis Approach

The data collected from various sources was analysed using the evaluation criteria to identify key strengths, weaknesses, and common patterns across the wallets.

Strengths: Wallets were noted for unique features such as cross-chain interoperability (Ethereum, Bitcoin, Polkadot, Solana), strong smart contract support (ERC-20 tokens, DeFi protocols), and excellent scalability under load. Security features like multi-signature, biometric authentication, and advanced cryptographic protocols (AES, RSA) were highlighted as major strengths. User-friendly interfaces and performance optimization for fast transaction speeds were also identified.

Weaknesses: Common weaknesses included poor UI design, limited blockchain support, security vulnerabilities (e.g., weak encryption, lack of multi-factor authentication), and slow transaction processing during high-load conditions. Some wallets also lacked advanced features like staking or token swapping.

Common Patterns: Across most wallets, security protocols (AES encryption, SHA-256 hashing), multi-chain compatibility, and DeFi integration were standard. A focus on user-friendly design, mobile and desktop synchronization, and decentralized finance services (e.g., DEX integration, staking) emerged as common industry trends.

To provide a clear and structured overview of the findings, Table 2 presents a detailed comparative analysis of the five wallets based on the evaluation criteria discussed earlier.

This table serves as a visual representation of the analysis, highlighting key features such as security, ease of use, seed phrase recovery, smart contract compatibility, and platform support. It offers a concise summary of each wallet's performance in critical areas like private key management, backup and recovery processes, and access to real-time market data. By transforming qualitative observations into a direct side-by-side comparison, Table 2 simplifies the decision-making process, allowing for a quick assessment of the strengths and weaknesses of each wallet.

Additionally, the table includes details on supported assets, associated costs/fees, user anonymity, and blockchain compatibility, providing a comprehensive look at the functionalities of each wallet. Overall, Table 2 aligns with the approach used throughout the paper, reflecting the extensive evaluation process and acting as a useful tool for comparing wallets based on real-world user needs and preferences.

Table 2: Comparison of multi-currency web wallets based on various features

Features / Wallet	MetaMask[9]	Trust Wallet	Coinbase[8]	MyEtherWallet (MEW)[11]	Electrum[10]
Security	High (private key local)	High (private key local)	High (private key local)	High (private key local)	Very High (local key + encryption)
User-Friendliness	Very User-Friendly	Very User-Friendly	Easy to Use	Moderate (for crypto enthusiasts)	Basic but powerful
Seed Phrase Recovery	Yes	Yes	Yes	Yes	Yes
Supported Assets	Ethereum + EVM chains + Tokens	160K+ assets on 70+ blockchains	Ethereum, Solana, and many tokens	Primarily Ethereum and ERC-20	Bitcoin only
Built-in Exchange	Yes (Swaps integrated)	Yes (DEX integration)	Yes (DEX + NFT marketplace)	No (uses third-party services)	No (manual exchange integration)
Private Key Handling	Local storage	Local storage	Local storage	Local storage	Local device storage
Smart Contract Support	Yes	Yes	Yes	Limited	No (BTC only)
Real-time Market Data	Limited (via integrations)	Yes	Yes	Limited	Limited
Blockchain Compatibility	Ethereum, BSC, Polygon, etc.	Multiple blockchains	Multiple blockchains	Ethereum focused	Bitcoin only
Backup & Recovery	Manual (write down seed phrase)	Manual	Manual	Manual	Manual
Cost / Fees	Gas fees + swap fees	Gas fees	Gas fees	Gas fees	BTC network fees
Open Source	Partially Open Source	Partially Open Source	Closed Source	Open Source	Open Source
Key Management	User-controlled (non-custodial)	User-controlled (non-custodial)	User-controlled (non-custodial)	User-controlled (non-custodial)	User-controlled (non-custodial)
Platform Support	Browser Extension, Mobile	Mobile (iOS/Android)	Mobile, Browser Extension	Web-based, Mobile	Desktop (Windows, macOS, Linux)
Anonymity	Medium (depends on use)	High (no personal info needed)	Low (tied to Coinbase account)	Medium	High (no account needed)
Fiat Currencies Supported	No direct fiat support	Yes (via providers like MoonPay)	Yes (via Coinbase account)	Limited (via 3rd-party integrations)	No
Supported Coins & Tokens	ETH, BNB, MATIC, USDT, DAI, etc.	160K+ including BTC, ETH, SOL, ADA	ETH, SOL, MATIC, AVAX, DAI, USDC	ETH, ERC-20 tokens	BTC only

VI. FUTURE SCOPE

The advancement of cryptocurrency wallets remains a vital domain for continued innovation and scholarly investigation. One significant trajectory involves designing hybrid wallet models that unify the usability of hot wallets with the high-level security of cold storage. Such models could feature hardware-based key protection and multi-factor authentication to counter threats such as phishing and private key leakage, as emphasized by Kirobo [7] and Erinle et al. [4].

Furthermore, as decentralized applications (dApps) and smart contracts become more intricate, future efforts should prioritize simplifying user interaction without compromising on security. Researchers like Choudhary et al. [3] have already proposed user-centric decentralized wallet solutions. Building on this, subsequent work might incorporate gamified security modules and interactive onboarding experiences to facilitate wallet recovery and safe seed phrase handling.

Exploration into advanced cryptographic methods, including threshold cryptography and multi-party computation, also presents a compelling direction for enhancing decentralized key recovery systems. These methods aim to eliminate single points of failure while offering users better command over their private credentials, aligning with work by Lehto et al. [6].

Additionally, incorporating real-time market analytics and AI-driven threat detection mechanisms could empower users to take pre-emptive actions against suspicious activities. Addressing global blockchain interoperability, including cross-chain asset management and multi-currency support, will also be essential as wallets transition into comprehensive financial platforms—a challenge noted by Popchev and Radeva [5].

Altogether, the proposed future directions address existing limitations in security and usability while laying a foundation for scalable, resilient wallet architectures in the growing decentralized finance landscape.

VIII. CONCULSION

Cryptocurrency wallets play a vital role within the blockchain ecosystem, acting as the core interface through which users manage digital assets and interact with decentralized finance platforms. Existing literature highlights a persistent tension between usability and security. While intuitive, user-friendly wallets can accelerate adoption by lowering entry barriers for both novice and experienced users, they often expose users to significant risks—including those stemming from poor key management and susceptibility to cyberattacks.

This paper has examined a range of wallet frameworks and shed light on recurring security flaws, such as improper seed phrase handling and insufficient authentication mechanisms, that threaten asset safety. It has also assessed emerging solutions that aim to merge the convenience of hot wallets with the enhanced protection typically associated with cold storage. In particular, hybrid models that leverage hardware-level key storage, advanced cryptographic tools, and interactive user guidance present a promising path forward.

By integrating conceptual insights with practical implications, this research underscores the need to approach wallet development through both technological and human-centred lenses. The path toward more secure and accessible wallets lies in addressing the intricacies of user behaviour, improving interface design, and embedding advanced security measures. Continued innovation in real-time threat detection, multi-factor and multi-signature verification systems, and decentralized recovery protocols will be instrumental in shaping the next generation of cryptocurrency wallet solutions.

VIII. FUNDING DECLARATION

The authors declare that no funding was received for this study.

REFERENCES

[1] X. He, J. Lin, K. Li, and X. Chen, "A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement," IEEE Access, vol. 7, pp. 185250-185263, 2019.

[2] S. Suratkar, M. Shirole, and S. Bhirud, "Cryptocurrency wallet: A review," 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), IEEE, 2020.

[3] K. Choudhary, A. Dhanse, M. Dubey, Y. Kushwaha, and A. Ingle, "Decentralized Wallet Application using Blockchain," International Journal of Innovative Science and Research Technology), 2024.

[4] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu, "Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets," arXiv preprint arXiv:2307.12874, 2023.

[5] I. Popchev and I. Radeva, "Decentralized Application (dApp) Development and Implementation," Cybernetics and Information Technologies, vol. 24, no. 2, pp. 122-141, 2024.

[6] N. Lehto, K. Halunen, O. M. Latvala, A. Karinsalo, and J. Salonen, "CryptoVault-a secure hardware wallet for decentralized key management," 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS), pp. 1-4, 2021.

[7] A. R. Kirobo, "Security vulnerabilities in cryptocurrency wallets: A systematic review," International Journal of Cybersecurity, vol. 9, no. 3, pp. 74-89, 2024.

[8] Coinbase Exchange Review',2018. https://www.finder.com/in/coinbase exchange-review. [Accessed: 22- Jan- 2020].

[9] Lee, W. M. (2023). Using the MetaMask crypto wallet. In Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript (pp. 111-144). Berkeley, CA: Apress.

[10] Turuani, M., Voegtlin, T., & Rusinowitch, M. (2016, February). Automated verification of electrum wallet. In International Conference on Financial Cryptography and Data Security (pp. 27-42). Berlin, Heidelberg: Springer Berlin Heidelberg.

[11] Mackay, B. (2019). Evaluation of security in hardware and software cryptocurrency wallets. School of Computing Edinburgh, Napier University Edinburgh, Scotland.

[12] Yan, K., Zhang, J., Liu, X., Diao, W., & Guo, S. (2023, April). Bad apples: Understanding the centralized security risks in decentralized ecosystems. In Proceedings of the ACM Web Conference 2023 (pp. 2274-22