International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Investigating Security Flaws in Cryptocurrency Wallets and Developing Strategies to Enhance Their Security

**Deepika Sharma[1], DR. Martha Sucharitha[2]**

[1,2]Christ University, Bangalore.

**Abstract**

Cryptocurrency can be leveraged by hackers to steal funds or manipulate the system. Rug pulls are scams where inventors create a new cryptocurrency, exaggerate its price, and abandon the project, taking all invested funds. A 51% attack, which can control more than half of a cryptocurrency's mining power, could potentially disrupt the network and steal coins.

Blockchain technology's decentralized characteristics provide low susceptibility and security. This makes it vulnerable to manipulation and counterfeiting. The blockchain technology has several issues with its identity and access management system associated with the Internet of Things.

The proposed solution involves a comprehensive analysis of security threats in cryptocurrency systems, focusing on the distribution of mining power, to quantify the risk of a 51% attack.

Collect data on identity breaches, unauthorized access attempts, and other security incidents in blockchain-based IoT systems to evaluate vulnerabilities in identity and access management.

Presenting findings with comprehensive statistical evidence, such as charts, graphs, and tables, ensures a comprehensive summary of the key insights.

## Introduction

Satoshi Nakamoto initiated the cryptocurrency platform, Blockchain, in 2008. The non-centralised payment system platform. A public network, independent of any government control, creates and manages cryptocurrency, a decentralized digital money. Encryption ensures secure transactions. People can also view cryptocurrency as an entity where they can profit from changes in the currency's value. The deliberation concentrates on currency security issues, including the mining process and transactions, which are not fully secure. Users who collaborate can exploit flaws, and online digital wallet services can be targets for hacking attacks. Exchange services also pose a threat to these services, making it critical to negotiate these security concerns to preserve the safety of the virtual currency. Cryptocurrency wallets include a distinct domain that combines characteristics of password managers, banking software, and the necessity for user and transaction confidentiality. (Hauy, et al 1950)

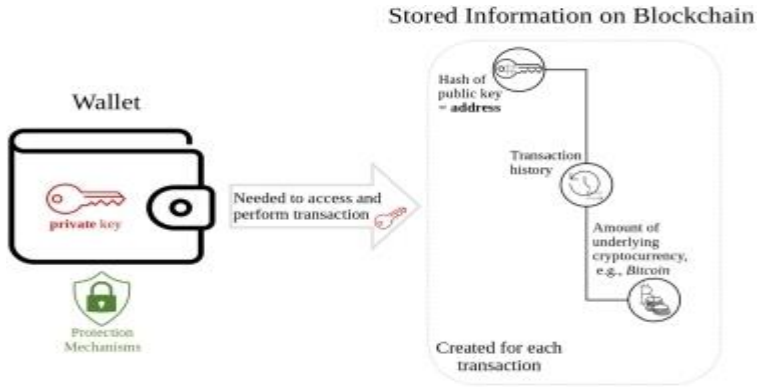



**FIG 1: The function of wallets in cryptocurrency transactions.**

Figure 1 shows a simplified representation of the essential components required for a cryptocurrency wallet transaction. Internally, the wallet contains no currency. Nonetheless, it effectively maintains and secures the private key, which is required to carry out transactions and ultimately use the coins. The digital ledger also holds extra information, such as the public key's cryptographic encode, which is often associated with the address, transaction history, and bitcoin value.

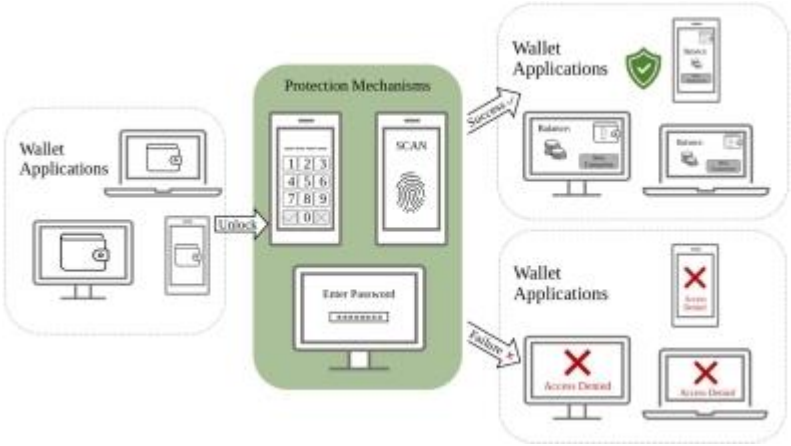



**FIG 2 : Security measures for accessing wallet applications.**

Passwords, biometric authentication, such as fingerprints, and Personal Identification Numbers (PINs) work together to limit unlawful transactions and prevent unintentional access. The process of encrypting data to guarantee its safekeeping is known as encryption. We encrypt the data to ensure that only authorized individuals can access it. To decode and access the data, the program needs a password, PIN, or some other kind of authentication. Figure 2 provides a brief summary of some protective measures. For instance, we can use the stored Personal Identification Number (PIN) to carry out financial transactions and obtain full wallet permission.

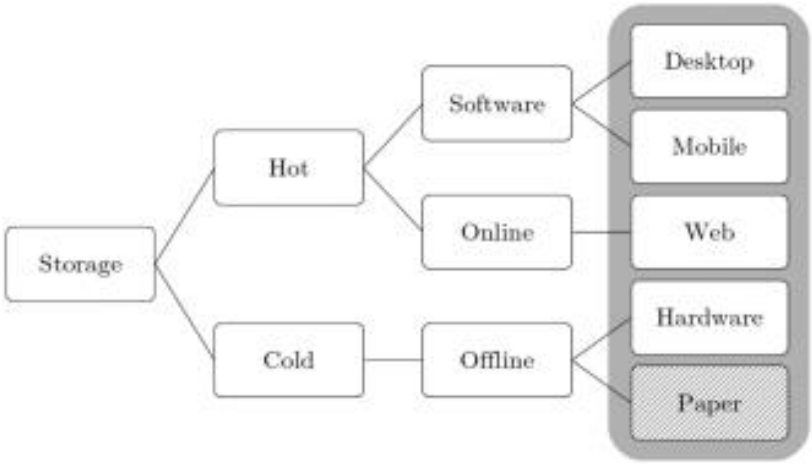



**FIG 3 : Types of wallets**

Cryptocurrency wallets are categorized based on network access, storage medium, chain storage, and key storage.

- **Hot wallets** necessitate a continuous internet connection and can be installed on smartphones or desktops. They have the capability to function as either online or web wallets, as well as software wallets.
- **Cold wallets**, also known as hardware wallets, function exclusively without internet connectivity. Non-technological implementations, like paper wallets, need the act of writing down private keys. Many people view cold wallets as more secure because they don't require internet connectivity.
- **Desktop wallets** installed on a PC provide users with full authority over their cryptographic keys and funds. Local files serve as a repository for storing and safeguarding confidential information, which makes it imperative to create backups in order to avoid any potential loss or harm.
- **Mobile wallets,** similar to desktop wallets, are software applications installed on mobile devices. Regular backups are essential because of the possibility of security breaches. Web wallets, which involve third-party ownership, are the least secure option. However, their use benefits include easy access from anywhere. Nevertheless, in the event that you misplace your login credentials, you would permanently forfeit all of the wallet's assets.
- **Hardware wallets** offer the utmost level of protection, while they necessitate additional backups for restoration. Users frequently combine hardware wallets with software or web wallets to carry out transactions, granting them full authority over key management.

**Significant security risks and potential threats to Cryptocurrency**

**1. Analysis of Attacks on Wallet Software**

Online wallets are vulnerable to attacks, so encryption and offline backup are required. The current backup features let users recover previous wallet files and their contents. Tracing the coin's history enables the connection of user identity to the Bitcoin address. The online wallet program is vulnerable to potential Distributed Denial of Service (DDoS) attacks.

**2. Time jacking Attacks**

When an attacker connects to a node for a transaction, they sometimes send out the wrong information. The offender modifies the node's network time counter, and the tricked node may agree to a new block chain. This wastes money and time by spending them twice and not using enough computing power during

the mining process.

**3. '>50%' Attack**

Hacking the mining process poses a significant threat to the Bitcoin network. The mining process becomes vulnerable when a group of users collaborates to obtain over half of its computational power. Then, this individual or organization has the ability to exclude, modify, or reverse transactions and stop mining some or all legal blocks for their own benefit. Recent research has shown that attackers can get past a 6-deep approved transaction with only about 40% of the computer's resources, and they have a 50% chance of succeeding.

**Reasons for the unresolved issues**

1. **Complexity and Diversity of Wallets:** Cryptocurrency wallets encompass a diverse range of options, including hardware wallets, software wallets, web wallets, and mobile wallets. Each category possesses its own unique structure, characteristics, and possible weaknesses, which complicates the development of a universally applicable security solution.
2. **Sophisticated Attack Methods:** The techniques used by cybercriminals to take advantage of weaknesses in bitcoin wallets are constantly becoming more complex. These encompass phishing, malware, social engineering, and zero-day assaults. Staying informed of these ever-changing dangers necessitates continual watchfulness and ingenuity.
3. **User Behaviour and Awareness:** User conduct raises a wide range of security concerns, including inadequate password administration, vulnerability to phishing schemes, and failure to adhere to optimal security protocols. Improving security also entails instructing users and advocating for better security practices.
4. **Rapidly Evolving Technology:** Cryptocurrency technology is constantly evolving, with new wallets, protocols, and features being introduced frequently. This rapid development can outpace the ability to fully understand and secure every aspect of the technology.
5. **Regulatory and Legal Challenges:** The absence of uniform security standards and regulations across many jurisdictions poses a significant obstacle in the development of internationally recognized security solutions.
   Uncertainty and flaws in security protocols result from the legal and regulatory frameworks' incomplete alignment with the technology.
6. **Ecosystem Complexity:** Further security issues arise when cryptocurrency wallets have to interface with other platforms like blockchain networks, decentralized apps (dApps), and exchanges. Dependence on unsecure third parties for services and libraries may lead to vulnerabilities.

## RESEARCH OBJECTIVE

The aim of this study is to determine and examine common security flaws in bitcoin wallets, encompassing both hardware and software variations. With an emphasis on issues including user authentication, transaction signing, and private key management, this study attempts to investigate the fundamental origins of these errors. The research also aims to create and suggest sophisticated security measures, such as multi-factor authentication, encryption methods, and safe backup plans, to mitigate the discovered dangers. The objective is to increase the general resistance of bitcoin wallets against assaults, boosting user confidence and guaranteeing safer digital asset transmission and storage.

## LITERATURE REVIEW

1. Houy, et al (2023) narrated Cryptocurrency wallets include a distinct domain that combines characteristics of password managers, banking software, and the necessity for user and transaction confidentiality.
2. M. Elrayah and A. S. Juhari (2023) narrated cryptocurrencies into e-commerce platforms, focusing on consumer satisfaction. It surveyed 231 cryptocurrency wallet owners and found that integrating a wallet can enhance the user experience by offering a streamlined payment method, attracting tech-savvy users, and speeding up checkouts.
3. W. B. Sentana, M. Ikram, and M. A. Kaafar (2023) narrated Cryptocurrency wallet apps handle sensitive financial information, making them attractive targets for criminals seeking to steal assets and invade privacy. The investigation reveals significant security weaknesses, such as the unsecured use of HTTP for transaction processing, highlighting critical privacy concerns.
4. Y. Yu, T. Sharma, S. Das, and Y. Wang (2024) narrated A significant number of individuals refrain from using hardware wallets due to concerns related to usability and security, namely regarding the key recovery services offered by manufacturers and the risk of phishing attacks.
5. J. M. Kizza (2024) narrated A decentralized network of servers maintains the blockchain, and every transaction using the data in these blocks requires consent from a majority of the network servers via reliable and verifiable protocols.
6. Ngozi Samuel (2024) narrated The lack of regulatory monitoring, as well as the frequency of fraud, hacking, and market manipulation, make it difficult for customers to seek justice.
7. S. Raveenthiren (2024) narrated The paper introduces the Enhanced Elliptic Curve Digital Signature Algorithm (EECDSA), which combines advanced ECDSA, blockchain technology, Golang programming language, and JSON data interchange.
8. H. Qin (2024) narrated This research investigates the process of refining and utilizing language models (LLMs) to cater to the particular requirements of the bitcoin industry.
9. Soni and S. Maheshwari (2024) narrated Demonstrate the crucial role these attacks play for the perpetrators in obtaining unjust rewards or deceiving the honest users through fraud and focus on developing new protocols as defensive countermeasures against attacks.
10. M. Bartoletti (2023) narrated One major obstacle to the widespread use of Bitcoin in point-of-sale (POS) situations is the lengthy waiting time for the network to verify the validity of transactions.
11. U. Agarwal (2024) narrated The study investigates fraudulent cryptocurrencies and proposes a method that combines artificial intelligence and blockchain technologies to deter such occurrences. The random forest classifier exhibited exceptional performance, with an accuracy rate of 97.5%.
12. T. Thomas (2020) narrated Our examination uncovered significant data in the RAM that is valuable to forensic investigations. This includes transaction history, extended public keys, passphrases, and unique device identifiers.
13. (2024) The findings show that technologies like Proof of Stake, zero-knowledge proofs, and multi-signature wallets significantly improve security and examines protocols like Bitcoin, Ethereum, Zcash, and Monero, revealing varying levels of effectiveness in addressing security issues.
14. (2024) The research concludes that the existing fraud triangle is insufficient and proposes the fraud scale and triangle of fraud action as more effective frameworks. Inadequate understanding of technology, the decentralized structure of blockchain, and the lack of regulations all play a role in the commission, concealment, and legitimacy of fraudulent activities.

15. (2024) Criminals utilize these services to conceal illicit gains and make secure payments through bitcoin exchanges for untraceable transactions. The volatility and lack of transparency surrounding Bitcoin make it appealing to individuals with dubious motives, such as those who seek to aid insurgents or engage in illicit drug transactions.
16. H. Byun (2024) narrated "The study introduces a technique for managing private keys and creates a password verification oracle to defend against brute force attacks."

**Research Methodology**

**1. Data Collection**

**Academic Literature:** publications, and conference proceedings related to bitcoin wallets, blockchain technology, and cybersecurity.

**Case Studies:** Analysis of previous attacks on cryptocurrency wallets, such as phishing, malware, or key management failures.

**Government and Regulatory Reports:** Documents addressing security standards and regulations inside cryptocurrency systems.

**Inclusion Criteria:**

- Examine studies and publications released during the last 3 to 5 years to guarantee pertinence.
- The Details on various types of wallets, including hot, cold, mobile, and hardware wallets.
- The study concentrates on common and advanced security flaws such as private key management, phishing attacks, 51% attacks, and hardware vulnerabilities.

**Exclusion Criteria:**

- The reports are outdated and do not accurately reflect the current state of wallet technology.
- The information highlights aspects of cryptocurrencies that are not related to security, like transaction efficiency and usability.

**2. Data Evaluation**

**Credibility:** Articles subjected to expert review, reliable reports, and publications by esteemed security professionals.

**Relevance:** The data must focus only on bitcoin wallet vulnerabilities and corresponding security measures.

**Timeliness:** Preference for the latest data to accurately represent the dynamic nature of bitcoin technology.

**Impartiality:** Sources must remain unbiased, especially in the context of technical assessments.

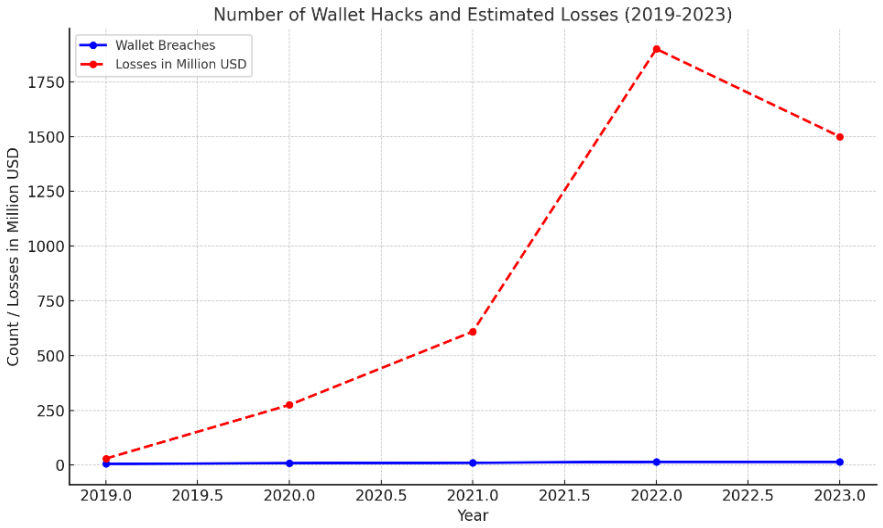
**3. Data Analysis**

**Acquaintance :** It involves reviewing selected secondary facts to gain comprehensive knowledge.

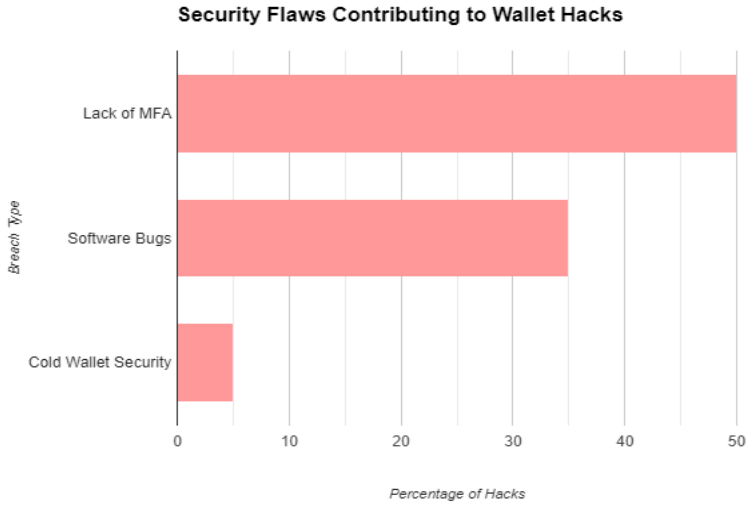
**Comparative Analysis:** Evaluate alternative solutions presented in the secondary data, emphasizing their advantages, disadvantages, and relevance in diverse contexts.

**Case Study Analysis:** Examine case studies of documented bitcoin wallet breaches to identify the underlying reasons for security failures and derive insights for future improvements.

**Graphs Analysis:**



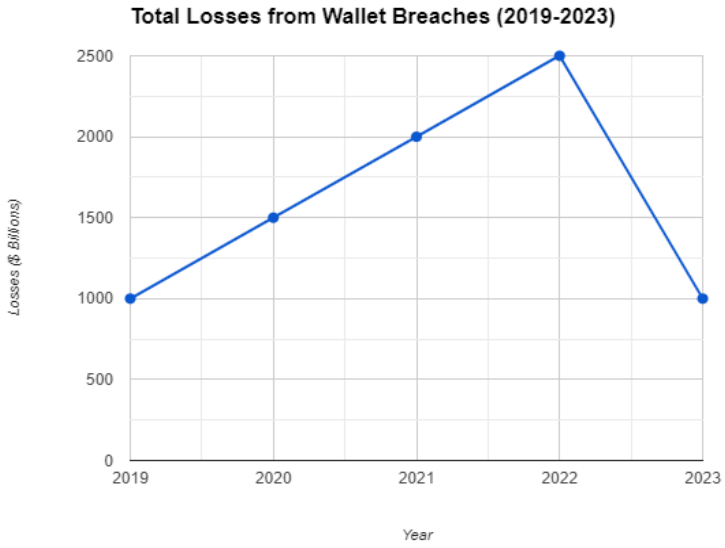

Here is the line chart showing the number of wallet hacks and estimated losses from 2019 to 2023. The blue line represents the number of breaches, and the red dashed line represents the estimated losses in millions of USD. The data highlights a sharp increase in both breaches and losses, particularly in 2022.




The graph indicates that Lack of Multi-Factor Authentication (MFA) is the most frequent cause of wallet hacks, accounting for 50% of breaches.

This highlights the critical importance of enabling strong security measures like MFA and keeping wallet software updated to minimize the risk of hacks.

While Cold Wallet Security breaches are less frequent (5%), they can result in significant losses due to the larger sums typically stored in cold wallets.




The line graph demonstrates a significant increase in financial losses from wallet breaches between 2019 and 2023, culminating in a peak of over $2 billion in 2022. While there have been instances of partial or full recovery, the overall trend indicates a growing vulnerability in digital wallets. This highlights the urgent need for robust security measures to protect crypto assets from theft and loss.

**Result And Discussion**

- Identify the main security weaknesses present in bitcoin wallets. Current remedies and their effectiveness.
- Existing security strategies have deficiencies that require attention.
- Proposing Innovative Strategies or revised techniques for safeguarding bitcoin wallets, like advanced encryption techniques, increased authentication protocols, or superior wallet design methodologies.

**1. Propose New Security Enhancements**

Advanced cryptographic techniques, improved key recovery methods, zero-knowledge proofs, decentralized identification solutions, behavioural analysis, cross-platform security standards, and self-destruct mechanisms are enhancing wallet security. The technologies encompass quantum-resistant encryption, zero-knowledge proofs (ZKP), decentralized identification solutions, machine learning for instantaneous transaction detection, universal security requirements for all sorts of wallets, and a self-destruct mechanism.

**2. User Education and Awareness**

Create educational resources and programs for wallet security best practices, make security features accessible to non-technical users, and implement systems to alert users about risky behaviour , such as sending funds to unknown wallets.

**3. Collaborative Efforts**

The wallet should collaborate with cybersecurity experts to stay updated on new threats, encourage open-source security reviews for community improvement, and ensure compliance with local and international laws, such as GDPR, to avoid legal vulnerabilities.

**4. Strengthening Private Key Security**

To reduce the risk of inadequate protection of private keys, especially in software wallets, one can employ multi-factor authentication, hardware wallets, and Shamir's Secret Sharing. Multi-factor authentication demands the use of biometric data, hardware tokens, or one-time passwords. On the other hand, hardware wallets securely store keys offline and possess resistance against remote hacking. Shamir's Secret Sharing algorithm divides private keys into many fragments, necessitating the use of multiple shares to reconstruct the original key.

**5. Blockchain Security Protocols**

Cryptographic wallets are vulnerable to security vulnerabilities, such as 51% attacks or double-spending. To reduce such risks, layered security protocols such as sharding and proof-of-stake can be integrated. Additionally, decentralized identification systems can improve the integrity of wallets and prevent identity theft on blockchain networks.

## CONCLUSION

The study's results show that despite significant advancements in bitcoin wallet security, both technological and human aspects still require significant attention. In order to create secure and user-friendly wallets, it will be crucial to incorporate advanced security features like multi-signature and hardware-based solutions, along with enhancing user awareness. Furthermore, as the market progresses, wallet security must advance in tandem with increasing risks and legal changes to ensure universal confidence and acceptance. In order to guarantee the safety of bitcoin wallets, it is imperative to employ a multi-faceted strategy that incorporates sophisticated cryptographic methods, secure user behaviours, and regular upgrades to address emerging risks. The research highlights the significance of cooperation among wallet developers, blockchain networks, and regulatory agencies to define security standards that apply to the entire industry while still preserving decentralization and user autonomy.

The research on examining security weaknesses in bitcoin wallets emphasizes significant vulnerabilities, such as inadequate management of private keys, poor authentication methods, and susceptibility to phishing and malware assaults. Existing mitigation measures, such as hardware wallets and encryption based on passwords, provide only a limited level of security, highlighting the necessity for more resilient solutions. Some ideas for how to fix this problem are to use complex key management systems like multi-signature and hierarchical deterministic wallets, make authentication better by using biometric or hardware-based methods, and make users more aware of security holes. To ensure the secure use of cryptocurrencies, it is essential to consistently introduce new ideas, conduct frequent examinations, and foster collaboration among developers, users, and regulatory entities in order to improve wallet security.

## REFERENCE

1. S. Houy, P. Schmid, and A. Bartel, “Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review,” *ACM Comput. Surv.*, vol. 56, no. 1, p. 4:1-4:31, Aug. 2023, doi: 10.1145/3596906.
2. W. B. Sentana, M. Ikram, and M. A. Kaafar, “An Empirical Analysis of Security and Privacy Risks in Android Cryptocurrency Wallet Apps,” in *Applied Cryptography and Network Security*, M. Tibouchi and X. Wang, Eds., Cham: Springer Nature Switzerland, 2023, pp. 699–725. doi: 10.1007/978-3-031-33491-7_26.
3. H. Byun, J. Kim, Y. Jeong, B. Seok, S. Gong, and C. Lee, “A Security Analysis of Cryptocurrency Wallets against Password Brute-Force Attacks,” *Electronics*, vol. 13, no. 13, Art. no. 13, Jan. 2024,

doi: 10.3390/electronics13132433.
4. M. Elrayah and A. S. Juhari, "Exploring the Impact of Cryptocurrency Integration on E-Commerce Platforms: A Framework for Marketplace Integration," *Przestrzeń Społeczna (Social Space)*, vol. 23, no. 4, Art. no. 4, 2023.
5. "Cryptocurrency May Prove Financial Crime: A Conceptual Analysis: Business & Management Book Chapter | IGI Global." Accessed: Sep. 05, 2024. [Online]. Available: https://www.igi-global.com/chapter/cryptocurrency-may-prove-financial-crime/321792
6. "Cryptocurrency Fraud: Strategies for Investigators - ProQuest." Accessed: Sep. 05, 2024. [Online]. Available: https://www.proquest.com/openview/5d905e7f8df92fe46be0edf20fb461f1/1?pq-origsite=gscholar&cbl=18750&diss=y
7. "Cryptocurrency Security Challenges: Innovations in Blockchain Protocols to Mitigate Risks | Journal of Advanced Technological Innovations." Accessed: Sep. 05, 2024. [Online]. Available: https://www.novadatatech.com/index.php/jati/article/view/30
8. T. Thomas, M. Piscitelli, I. Shavrov, and I. Baggili, "Memory FORESHADOW: Memory FOREnSics of HArDware CryptOcurrency wallets – A Tool and Visualization Framework," *Forensic Science International: Digital Investigation*, vol. 33, p. 301002, Jul. 2020, doi: 10.1016/j.fsidi.2020.301002.
9. U. Agarwal, V. Rishiwal, S. Tanwar, and M. Yadav, "Blockchain and crypto forensics: Investigating crypto frauds," *International Journal of Network Management*, vol. 34, no. 2, p. e2255, 2024, doi: 10.1002/nem.2255.
10. M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, "Cryptocurrency Scams: Analysis and Perspectives," *IEEE Access*, vol. 9, pp. 148353–148373, 2021, doi: 10.1109/ACCESS.2021.3123894.
11. Soni and S. Maheshwari, "A survey of attacks on the bitcoin system," in *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, IEEE, 2018, pp. 1–5. Accessed: Sep. 05, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8546925/
12. H. Qin, "Revolutionizing Cryptocurrency Operations: The Role of Domain-Specific Large Language Models (LLMs)," *International Journal of Computer Trends and Technology*, vol. 72, pp. 101–113, Jun. 2024, doi: 10.14445/22312803/IJCTT-V72I6P114.
13. S. Raveenthiren and S. Peraisoody, "A novel approach to secure IoT cryptocurrency wallets based on Enhanced ECDSA algorithm," in *2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)*, Mar. 2024, pp. 1–6. doi: 10.1109/ICITIIT61487.2024.10580090.
14. Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu, and Adefolake Olachi Adewusi, "Enhancing consumer protection in cryptocurrency transactions: Legal strategies and policy recommendations," *Int. J. Sci. Res. Arch.*, vol. 12, no. 1, pp. 520–532, May 2024, doi: 10.30574/ijsra.2024.12.1.0801.
15. J. M. Kizza, "Blockchains, Cryptocurrency, and Smart Contracts Technologies: Security Considerations," in *Guide to Computer Network Security*, J. M. Kizza, Ed., Cham: Springer International Publishing, 2024, pp. 575–600. doi: 10.1007/978-3-031-47549-8_26.
16. Y. Yu, T. Sharma, S. Das, and Y. Wang, "'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*, in CHI '24. New York, NY, USA: Association for Computing Machinery, May 2024, pp. 1–17. doi: 10.1145/3613904.3642534.