INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMSI.com
www.isarasolutions.com

Published by iSaRa Solutions

Lessons for RBI CBDC from Various Cryptocurrency Hacks: Implications for the Security and Resilience of the Digital Rupee

Dr. Cirappa I B[1], Nagaraju V[2]

1 Professor and Chairman, Department of Studies in Commerce, Davanagere University, Tholahunase, Karnataka, India

2 Research Scholar, Department of Studies in Commerce, Davanagere University, Tholahunase, Karnataka, India. And Assistant professor, GFGC, Chikkaballapur.

Abstract

Digital currencies are no longer an experimental concept. They are rapidly becoming part of mainstream financial infrastructure. While cryptocurrencies have demonstrated the possibilities of decentralized finance, they have also revealed a darker side repeated cyberattacks resulting in massive financial losses. Some incidents involved stolen private keys. Others exploited weaknesses in smart contracts, bridges, or exchange governance. The cumulative damage has reached billions of dollars.

India's Central Bank Digital Currency (CBDC), the Digital Rupee (e₹), is being developed under the supervision of the Reserve Bank of India (RBI). Unlike cryptocurrencies, the Digital Rupee is a sovereign liability backed by the central bank. Yet the cybersecurity lessons emerging from cryptocurrency failures remain highly relevant. Ignoring them would be costly.

This study examines major cryptocurrency hacks including Mt. Gox, Coincheck, Poly Network, Wormhole, Ronin Network, WazirX, and Bybit. Using secondary data collected from central bank reports, cybersecurity databases, industry publications, and academic literature, the study identifies recurring vulnerabilities and evaluates their implications for India's CBDC framework. The findings indicate that strong governance, secure key management, continuous auditing, operational resilience, and real-time monitoring are essential for safeguarding the Digital Rupee ecosystem.

Keywords: CBDC, Digital Rupee, RBI, Cryptocurrency Security, Cyberattacks, Financial Stability, Digital Currency Governance.

1. Introduction

Money is changing.

Over the past decade, digital payments have transformed the way individuals and businesses conduct transactions. Alongside this transformation came cryptocurrencies—Bitcoin, Ethereum, and thousands of other digital assets promising decentralization and financial autonomy. The promise was compelling. The reality turned out to be more complicated. Crypto markets have witnessed some of the largest cyber thefts in financial history. Exchanges collapsed. Wallets were compromised. Smart contracts failed unexpectedly. In many cases, the technology itself

was not entirely at fault; weaknesses in governance, security practices, and operational controls often played a larger role. At the same time, central banks around the world began exploring Central Bank Digital Currencies (CBDCs). The RBI joined this movement through pilot projects for the Digital Rupee. The objective extends beyond digitizing cash. The initiative seeks to improve payment efficiency, strengthen monetary sovereignty, and support innovation within India's financial ecosystem. Yet one question remains unavoidable: What happens when digital currency infrastructure becomes a target?

The answer may already exist in the history of cryptocurrency hacks. Examining these incidents offers valuable insights into vulnerabilities that CBDC systems must avoid. This study explores those lessons and discusses how they can strengthen the security architecture of India's Digital Rupee.

2. Literature Review

Zahrashafa Putri Mahardika,a Rizky Banyualam Permana,b Nadia Maulisaa(2023): These studies show that central banks across the world are increasingly exploring the concept of Central Bank Digital Currency (CBDC) as part of the broader shift toward digital finance. CBDC is often described as a safer and more stable form of digital money, mainly because it is issued and controlled by central banks, unlike decentralized cryptocurrencies. The discussion around CBDC is not limited to developed economies anymore; emerging markets have also entered the space, making the topic more relevant than before. Yet, the academic and policy debate still feels unfinished, mostly because only a small number of countries have actually introduced CBDCs in practice. This creates a noticeable gap, especially when it comes to understanding the regulatory and legal dimensions of CBDC systems. Some scholars point out that cybersecurity risks remain one of the least explored areas, even though they could shape the success or failure of implementation. In the case of Bank Indonesia, research highlights its role in designing CBDC frameworks while dealing with technical models such as Digital Ledger Technologies (DLTs) and other electronic payment systems. What stands out is simple but critical: no matter how complex the system gets, the central bank still carries the ultimate responsibility, which makes cybersecurity resilience impossible to ignore.

Sehgal, S., Yasir, M., & Kour, S. (2024): Existing literature examines digital currency by drawing a clear line between digitization and digitalization, showing how both shape the financial ecosystem in different ways. Researchers often divide digital currencies into two broad forms—centralized and decentralized—and this distinction matters more than it first seems. A growing body of work pays close attention to Central Bank Digital Currencies (CBDCs), with particular interest in India's e₹ (Digital Rupee) as an evolving model of sovereign digital money. These studies suggest that CBDCs could expand financial inclusion, speed up transactions, and even reshape how monetary policy works in practice, though the outcomes are still somewhat uncertain. At the same time, the conversation is not all optimistic; cyber threats, privacy concerns, regulatory confusion, and possible financial instability keep surfacing as major concerns. Some scholars argue that without strong frameworks for risk management and constant oversight, digital currencies may create more operational vulnerabilities than expected.

Interestingly, recent discussions connect this transformation with the Fourth Industrial Revolution, where digital technologies are not only changing banking but also sectors like agriculture through smart farming and precision-based systems. Frameworks such as the National Institute of Standards and Technology Risk Management Framework and the Committee on Payments and Market Infrastructures principles are often cited as practical guides to manage these risks and strengthen digital currency systems.

Kesavaraj, S. V., Jakhiya, C. M., & Bhandari, C. N. (2022): This literature on India's digital currency initiative highlights the introduction of the Digital Rupee as a major step in the country's push toward digital transformation. Many researchers connect this move with the broader technological shift, including the rollout of 5G, suggesting that India is trying to position itself strongly in the global digital economy. Studies examining the Reserve Bank of India's CBDC framework point out both opportunities and uncertainties, mainly because the official design details remain somewhat limited. On one side, the Digital Rupee is expected to improve payment efficiency and expand the role of the central bank beyond traditional monetary functions; on the other, concerns around cybersecurity like hacking, privacy breaches, and state surveillance—keep showing up in the discussion. Some authors have suggested cryptographic tools such as hashing and tokenization as possible safeguards, though whether they can fully solve these issues is still debatable. Another important point in the literature is the question of interest: whether the Digital Rupee should carry interest or not, because that small design choice could significantly affect banking behaviour and monetary policy. Existing FinTech and mathematical models often predict that CBDCs may reshape the banking sector, but not overnight. Most scholars agree that replacing physical cash in India is unlikely in the short run, largely due to low financial literacy and weak technological infrastructure, though the long-term outlook appears much more promising.

CA Umesh Kumar Bhavsar (2024): Present study identifies the introduction of India's Digital Rupee as a major development in the country's financial modernization journey, especially at a time when digital payments and cryptocurrencies are rapidly reshaping global finance. Scholars often describe it as more than just another payment tool; it signals a structural shift in how money may circulate in the economy. Studies focusing on the Reserve Bank of India note that the Digital Rupee, built on blockchain-based systems, combines transparency and traceability with centralized control, which gives the regulator stronger oversight. This balance between innovation and control is seen as one of its defining features. A good share of the literature argues that CBDCs could widen financial inclusion by reaching people who remain outside traditional banking systems, while also making transactions quicker and less dependent on physical cash. Still, the story is not entirely smooth issues like weak digital infrastructure, privacy worries, and cybersecurity threats continue to raise questions that researchers have not fully answered. Some studies also point out that the Digital Rupee may give the RBI sharper tools for monetary policy, which sounds promising, but the long-term effects on banking behaviour and economic stability are still being figured out. Taken together, the literature

suggests that while the Digital Rupee carries strong transformative potential, its success depends heavily on how these practical and regulatory challenges are managed.

Sabine Houy, Philipp Schmid, and Alexandre Bartel. 2023:

This research paper shows that the rise of cryptocurrencies has pushed the demand for cryptocurrency wallet applications, making them a central part of digital financial transactions. These wallets come in many forms—mobile apps, hardware devices, and web-based systems and each carries its own strengths and weak points. What makes them especially interesting is that they are not just payment tools; in many ways, they act like a mix of password managers, banking apps, and privacy-preserving systems all at once. That complexity creates problems. Studies reveal that cryptocurrency wallets are exposed to a wide range of security threats, and attackers often exploit vulnerabilities to gain unauthorized access and steal funds. Existing research has mapped these threats into several layers, including memory and storage, operating systems, software layers, network infrastructure, blockchain protocols, and other less predictable risks. One thing becomes clear pretty fast: while there are plenty of technical countermeasures available, their actual implementation remains uneven and, honestly, sometimes surprisingly weak. The literature also points to a noticeable gap between proposed security solutions and real-world adoption, which suggests that wallet security is still evolving and far from settled.

Weichbroth, P.; Wereszko, K.; Anacka, H.; Kowal, J(2023): In this research paper Authors studies on cryptocurrency security underline that the main purpose of security is simple but critical: protecting digital assets, devices, and services from theft, disruption, or misuse. Even though cryptocurrencies have been around since the launch of Bitcoin in 2009, the volume of research focused specifically on their security remains surprisingly limited. A number of scholars have tried to bridge this gap by examining both the technical side and the human side of cryptocurrency security, because, honestly, one without the other does not tell the full story. Their reviews show that security is not just about stronger encryption or better protocols. It is also about people—how much they know, how they respond, and whether they can recognize threats before it is too late. Findings from the literature suggest that effective protection against cyberattacks depends on a mix of advanced technical defences and continuous education, training, and skill development among users. This becomes even more important when social engineering attacks are considered, since they remain one of the easiest ways attackers break into systems. Current discussions are now slowly shifting toward how these security models can be adapted for Central Bank Digital Currencies (CBDCs), which opens up a whole new set of challenges and research questions.

3. Research Objectives

Primary Objective

To identify critical lessons from major cryptocurrency hacks and evaluate their relevance to the RBI's CBDC ecosystem.

Specific Objectives

1. To examine major cryptocurrency hacks and their causes.
2. To assess the financial impact of these incidents.

3. To identify vulnerabilities relevant to CBDC infrastructure.
4. To evaluate implications for the Digital Rupee.
5. To develop recommendations for enhancing CBDC security and resilience.

4. Research Gap:

Many studies have examined cryptocurrency hacks and their financial losses. Most of this research focuses on technical issues like wallet breaches, smart contract failures, and exchange security. At the same time, CBDC research mainly discusses financial inclusion, payment efficiency, and monetary policy. However, very few studies connect cryptocurrency hack lessons with CBDC security design. This creates an important research gap. There is limited research on how past crypto security failures can help improve CBDC systems. This gap is especially important for India because the Reserve Bank of India is developing the Digital Rupee. Even though CBDCs are centrally controlled, they still use wallets, key systems, and digital infrastructure that may face similar risks. Current studies do not provide enough practical frameworks linking crypto hacks to CBDC risk management. This study aims to fill that gap by analysing major crypto hacks and identifying lessons for the security and resilience of RBI's Digital Rupee.

5. Research Methodology

This study follows a descriptive and exploratory research design to examine the security challenges associated with digital currencies and their relevance to the RBI's Central Bank Digital Currency (CBDC) initiative The study relies entirely on secondary data collected from multiple credible sources. Information was gathered from publications issued by the Reserve Bank of India (RBI), reports published by the Bank for International Settlements (BIS), cybersecurity databases, industry reports, academic journals, and news investigations covering major cryptocurrency security breaches. Bringing together evidence from these diverse sources allowed for a broader understanding of both technical and governance-related risks in digital currency systems.

To analyses the data, the study uses a combination of case study analysis, comparative assessment, descriptive statistical techniques, and policy evaluation. Individual hacking incidents were examined to understand their causes and consequences, while comparisons across cases helped identify common security weaknesses. Statistical analysis was used to classify and interpret patterns in the recorded attacks, and policy evaluation was applied to assess how the identified lessons could strengthen the RBI's CBDC framework.

6. **Scope of the Study**

This study looks closely at how security failures in cryptocurrency systems can inform the design and development of Central Bank Digital Currencies (CBDCs). At its core, the focus is simple: what went wrong in crypto, and what can central banks learn from it? The discussion mainly revolves around a few critical areas. Wallet security is one of them, because many of the largest breaches started there. Key management matters too—perhaps more than most systems realize—since compromised keys often mean compromised trust. Beyond that, the study pays attention to

operational resilience, which is really about how well a system can survive disruptions, attacks, or internal breakdowns without collapsing.

Governance is another big piece. Sometimes the problem is not the technology itself, but the way decisions are made, who controls access, and how accountability is structured. Cybersecurity architecture also comes into the picture, especially when digital currencies become part of a country's financial backbone. Risk management ties all of this together. Without it, even the strongest technical systems can fail. That said, this study stays within clear boundaries. It does not deal with cryptocurrency price movements, trading patterns, or speculative market behaviour. Those are separate debates. The concern here is narrower, but arguably more important: security, resilience, and the practical lessons they offer for CBDC systems like the RBI's Digital Rupee.

7. Limitations of the Study

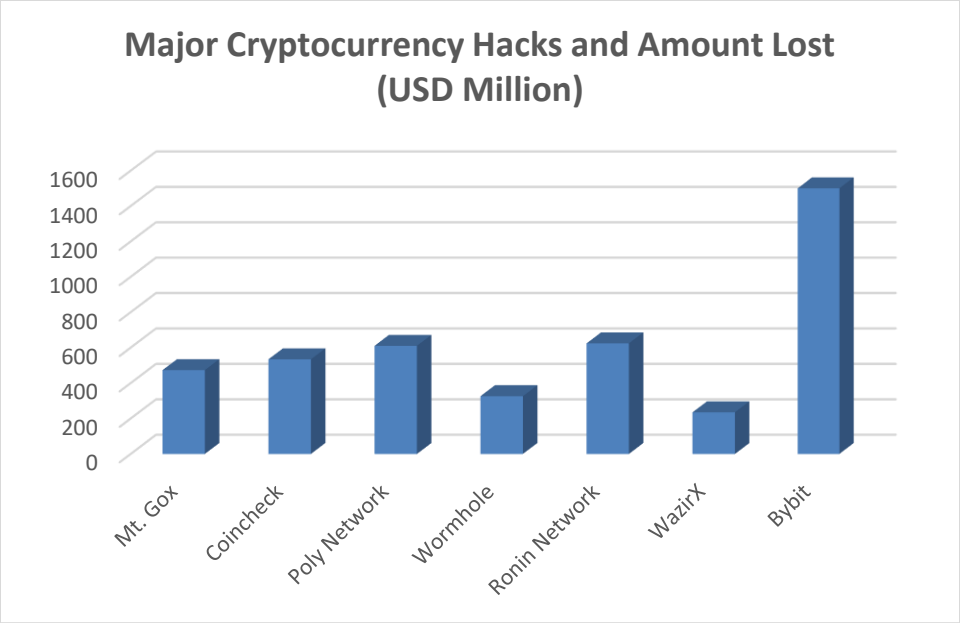
No research is without constraints. First, the study relies primarily on secondary data. Access to confidential forensic reports was limited. Second, several cryptocurrency exchanges do not publicly disclose all technical details following security incidents. Third, CBDC implementation remains an evolving field. Security frameworks continue to develop, which means future risks may differ from those observed today. Finally, India's Digital Rupee is still in the pilot stage, restricting the availability of empirical operational data.

8. Data Analysis:

Table 1: Major Cryptocurrency Hacks and Their Security Vulnerabilities

Hack Incident	Year	Amount Lost (USD Million)	Main Vulnerability	Key Lesson for RBI CBDC
Mt. Gox	2014	473	Poor internal security controls and wallet mismanagement.	Strong custody controls and real-time audit systems are essential.
Coincheck	2018	534	Hot wallet exposure and inadequate cold storage.	CBDC retail wallets should adopt hybrid custody architecture.
Poly Network	2021	610	Smart contract vulnerability in cross-chain logic.	Programmable CBDC functions require formal code verification.
Wormhole	2022	326	Bridge validation exploit.	Interoperability layers must be isolated and monitored.
Ronin Network	2022	624	Validator private key compromise.	Distributed key governance is critical for CBDC resilience
WazirX	2024	235	Multi-signature wallet compromise / custody breach.	RBI should strengthen institutional wallet governance.
Bybit	2025	1,500	Exchange wallet infrastructure compromise.	Even mature systems need adaptive, layered cyber-defence.

(Source: Reuters (2025): Crypto's biggest hacks and heists after Bybit theft, CoinMarketCap Academy (2024): Largest crypto heists in history.)



Analytical Interpretation

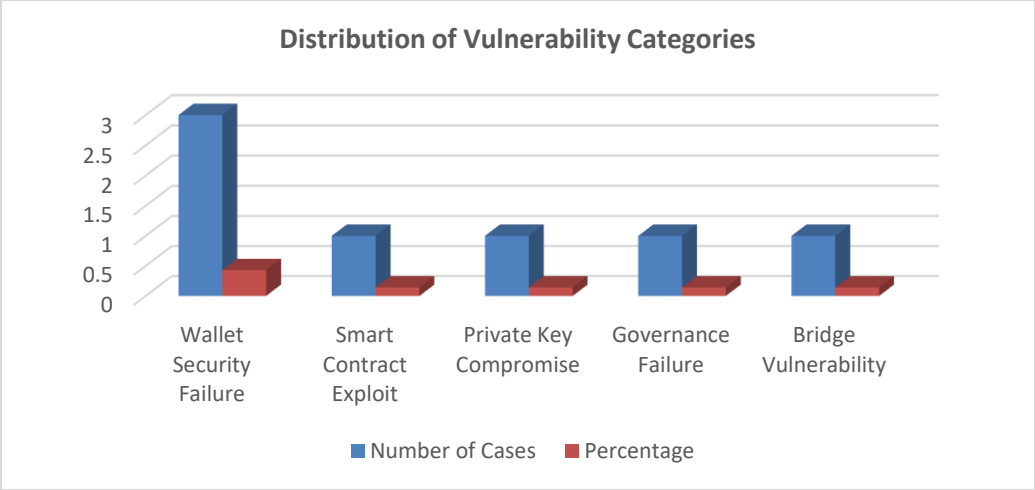
The revised table shows that the largest concentration of losses occurred between 2021 and 2025, reflecting the increasing scale and sophistication of attacks in modern digital asset ecosystems. The Bybit incident alone accounts for nearly 35% of total losses, indicating that exchange-level vulnerabilities remain the most severe systemic risk. Wallet-related breaches (Mt. Gox, Coincheck, WazirX, and Bybit) collectively represent over 63% of the total losses, reinforcing the argument that digital custody infrastructure is the weakest link in financial digitization.

From a CBDC perspective, the RBI must recognize that while the Digital Rupee operates within a centralized framework, many vulnerabilities observed in cryptocurrency systems particularly at the wallet, governance, and interoperability layers remain transferable. In practical terms, the lesson is clear: the success of CBDCs will depend less on blockchain innovation and more on institutional security design.

Table 2: Distribution of Vulnerability Categories.

Vulnerability Type	Number of Cases	Percentage
Wallet Security Failure	3	42.86%
Smart Contract Exploit	1	14.29%
Private Key Compromise	1	14.29%
Governance Failure	1	14.29%
Bridge Vulnerability	1	14.29%

(Source: Reuters (2025): Crypto's biggest hacks and heists after Bybit theft, CoinMarketCap Academy (2024): Largest crypto heists in history.)



Interpretation

The table shows a clear pattern. Wallet security failures appear most often 42.86% of the total cases. That is almost half of all the major hacks considered in this study. It says something important wallets continue to be the weakest point in digital asset systems, even when the underlying blockchain remains secure. The other vulnerabilities, such as smart contract exploits, private key compromise, governance failure, and bridge vulnerabilities, each account for 14.29%. On paper, the numbers look evenly spread. But in practice, each of these failures exposes a very different type of risk. A smart contract flaw points to coding weaknesses. A private key compromise raises concerns about access control. Governance failure often reflects poor decision making or weak oversight, which can sometimes be more dangerous than technical issues.

Bridge vulnerabilities are also worth noting. They may only show one case here, but the scale of losses in such attacks is usually massive because bridges connect multiple systems. That makes them attractive targets. What stands out is this: not all risks are equally frequent, but all of them can be severe. For the RBI's CBDC framework, the message is quite direct. Strengthening wallet security should be the first priority, but focusing only on wallets would be a mistake. The broader system code, governance, keys, and interoperability needs equal attention if resilience is the goal.

Table 3: Lessons from Cryptocurrency Hacks and Implications for RBI CBDC

Lesson from Crypto Ecosystem	Implication for Digital Rupee
Hot wallets are vulnerable	Secure custody architecture
Private keys can be compromised	Threshold signature systems
Smart contracts contain coding risks	Mandatory code audits
Bridges create attack surfaces	Controlled interoperability
Insider threats are real	Multi-level authorization
Delayed detection increases losses	Real-time monitoring

(Source: BIS Project Polaris Report, BIS CBDC Operational Risk Report)

9. Findings

Several findings emerged from the above analysis.

1. Technology alone does not guarantee security. Most major hacks involved operational or governance weaknesses rather than failures of blockchain consensus mechanisms.
2. Digital asset custody remains the most vulnerable component within the ecosystem.
3. Cross-chain infrastructure introduces substantial risks and requires stricter controls.
4. Private-key management remains one of the most critical cybersecurity challenges.
5. CBDCs require stronger security standards than conventional crypto platforms because they support sovereign monetary systems and public trust.

10. Suggestions

The lessons are clear.

i. **Strengthen Key Management:** Threshold signatures and distributed custody arrangements should replace centralized key storage wherever possible.

ii. **Conduct Continuous Audits:** Security reviews should be frequent, independent, and mandatory.

iii. **Deploy Real-Time Monitoring:** Suspicious activities must be detected immediately rather than after losses occur.

iv. **Build Resilient Offline Payment Systems:** Offline functionality should incorporate secure hardware and anti-double-spending safeguards.

v. **Improve Governance Structures:** Technology controls are important. Governance controls are equally important.

vi. **Stress-Test the System:** Regular cyber resilience exercises can expose weaknesses before attackers do.

vii. **Limit Exposure to External Networks:** Interoperability should be carefully controlled and continuously monitored.

viii. **Protect User Privacy:** Privacy-enhancing technologies should be embedded from the design stage rather than added later.

11. Scope for Further Research.

Future studies on the Reserve Bank of India's Digital Rupee can go in many directions, especially when we look at the lessons hidden in cryptocurrency hacks. One important area is comparing India's CBDC system with models like People's Bank of China's digital yuan or the eNaira, because each system handles security in its own way. There's also room to study how AI could catch fraud before it spreads something that feels almost necessary now. User behaviour matters too; sometimes the weakest point isn't the system itself, but the people using it. A deeper look at how centralized CBDC models differ from decentralized networks like Bitcoin could reveal some uncomfortable but useful truths. Then there's the quantum computing problem still distant, maybe, but not something central banks can ignore forever. Cross-border payments and privacy concerns will also need closer attention, since both bring their own risks and trade-offs. At the end of it all, future research has to connect technology, regulation, and public trust, because one without the others rarely works well.

12. Conclusion

The cryptocurrency sector has effectively become a global cybersecurity laboratory. Some lessons were expensive. Others were catastrophic. From Mt. Gox to Bybit, the recurring message is remarkably consistent: security failures rarely arise from a single weakness. They emerge when technical vulnerabilities intersect with weak governance, poor operational controls, inadequate monitoring, or flawed risk management. The Digital Rupee enters this landscape with an advantage. It can learn from a decade of cryptocurrency successes and failures without repeating the same mistakes.

For the RBI, the challenge extends beyond building a functional CBDC. The real challenge is building one that citizens trust. Security, resilience, privacy, and accountability will determine whether that trust is earned and sustained. A secure CBDC is not simply a technological achievement. It is a foundation for the future of digital money in India.

References:

1. Mahardika, Z., Permana, R. B., & Maulisa, N. (2023). GOING DIGITAL RUPIAH: SOME CONSIDERATIONS FROM SOVEREIGNTY AND CYBERSECURITY PERSPECTIVES. *Journal of Central Banking Law and Institutions*. https://doi.org/10.21098/jcli.v2i1.42
2. Sehgal, S., Yasir, M., & Kour, S. (2024). E-Rupee: Unlocking India's Digital Economy, Challenges, and Opportunities. *South Asian Journal of Social Studies and Economics*. https://doi.org/10.9734/sajsse/2024/v21i8860
3. Kesavaraj, S. V., Jakhiya, C. M., & Bhandari, C. N. (2022). A Study on Upcoming Central Bank Digital Currency: Opportunities, Obstacles, and Potential FinTech Solutions using Cryptography in the Indian Scenario. *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-10. https://doi.org/10.1109/icccnt54827.2022.9984539
4. Bhavsar, C. U. K. (2024). THE RISE OF DIGITAL RUPEE: INDIA'S LEAP INTO THE FUTURE OF CURRENCY. *BSSS Journal of Commerce*. https://doi.org/10.51767/joc1602
5. Saleem, S., & S. (2024). Digital rupee: Benefits and risks. *Science Talks*. https://doi.org/10.1016/j.sctalk.2024.100371
6. Weichbroth, P., Wereszko, K., Anacka, H., & Kowal, J. (2023). Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. *Sensors (Basel, Switzerland), 23*. https://doi.org/10.3390/s23063155
7. Krause, D. S. (2025). Crypto Security in the Aftermath of the Bybit Hack: Evaluating Risk Management Strategies for Digital Assets. *International Journal of Cryptocurrency Research*. https://doi.org/10.51483/ijccr.5.1.2025.92-101
8. Elessawy, ً., Gad, I., Abdelkader, H., & Haroun, A. (2023). Double Spending Attacks in Decentralized Digital Currencies: Challenges and Countermeasures. *IJCI. International Journal of Computers and Information*. https://doi.org/10.21608/ijci.2023.236377.1140.
9. Bank for International Settlements. (2023). *Project Polaris: A security and resilience framework for CBDC systems*. Retrieved from BIS Project Polaris Report

10. Bank for International Settlements. (2023). *Central bank digital currency information security and operational risks to central banks*. Retrieved from BIS CBDC Risk Report
11. Bank for International Settlements. (2023). *Lessons learnt on CBDCs*. Retrieved from BIS Lessons Learnt on CBDCs
12. Reuters. (2025). *Crypto's biggest hacks and heists after Bybit theft*. Retrieved from Reuters Crypto Hacks Report
13. Reuters. (2024). *Losses from crypto hacks jump to $2.2 billion in 2024*. Retrieved from Reuters Chainalysis Report
14. CoinMarketCap. (2023). *Largest crypto hacks in history*. Retrieved from CoinMarketCap Crypto Hacks Study
15. Abdelrahman, M., et al. (2025). *Threshold Signatures for Central Bank Digital Currencies*. Retrieved from ArXiv Threshold Signatures Study
16. Zarifis, A., & Cheng, X. (2023). *The six ways to build trust and reduce privacy concern in a CBDC*. Retrieved from ArXiv CBDC Trust Study
17. Guiraud, D. A., et al. (2025). *Objectives and design principles in offline payments with CBDC*. Retrieved from ArXiv Offline CBDC Security Study

Websites:

- https://www.reuters.com/technology/cybersecurity/cryptos-biggest-hacks-heists-after-15-billion-theft-bybit-2025-02-24/
- https://coinmarketcap.com/academy/article/largest-crypto-heists-in-history-have-exchanges-learned-anything-from-their-mistakes
- https://www.bis.org/publ/othp70.htm
- https://www.bis.org/publ/othp81.htm

AUTHOR CONTRIBUTIONS

Conceptualization, Methodology, Formal Analysis, Resources, Writing – Original Draft Preparation, Writing – Review & Editing, Both Authors have read and agreed to the final published version of the manuscript.

CONFLICT OF INTERESTS

Both the authors of this research paper confirm that there is no conflict of interest for this publication.

FUNDING

Author of this research paper confirms that no financial support or funding was provided for this research from any funding agency in the public, commercial, or not-for-profit sectors.

ACKNOWLEDGEMENT

The authors would like to express sincere gratitude for giving us support throughout the work. We also thank the editors, readers, reviewers and critics for spending time for reviewing this paper.

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM