Comparative Study of Cybersecurity Architecture in India’s Digital Rupee and China’s e-CNY

Dr. Harsha Patil[1], Aditi Malviya[2]

[1]Ashoka Centre for Business & Computer Studies, Nashik
Harshap.acbcs[at]aef.edu.in

[2]IGNOU, Delhi, India
malviyaaditi18[at]gmail.com

Abstract: ***Central Bank Digital Currencies (CBDCs) are becoming a major innovation in global finance, and India’s Digital Rupee marks an important step toward secure, government-backed digital payments. As CBDCs grow, cybersecurity becomes an increasingly important concern due to risks such as identity theft, privacy breaches, fraud, and assaults on digital wallets or transaction systems. This study examines the cybersecurity architecture of India's Digital Rupee and compares it with that of China's e-CNY. The purpose is to determine India's CBDC cybersecurity strengths, weaknesses, and areas for improvement.***

Keywords: Digital Currency, e-rupee, Cybersecurity, Economy, digital wallet

1.Introduction

The rapid digitalization of the global economy has fundamentally transformed how individuals, businesses, and governments conduct financial transactions. The growing adoption of real-time payment systems, mobile banking, and fintech platforms has prompted central banks worldwide to explore Central Bank Digital Currencies (CBDCs) as the next stage of monetary evolution. CBDCs aim to provide a secure, sovereign-backed digital alternative to physical cash while enhancing payment efficiency, transparency, and financial inclusion

A Central Bank Digital Currency is a digital representation of a nation’s fiat currency issued and regulated by its central bank. It is fully backed by the government and has the same legal status as physical cash. CBDCs enable secure digital payments and serve as a reliable store of value for the public. Overall, a CBDC serves as a state-backed digital alternative to paper currency, aiming to enhance payment efficiency, promote financial inclusion, and modernize national financial systems.

India entered the CBDC domain with the launch of the Digital Rupee (e₹) pilot by the Reserve Bank of India (RBI) in 2022. This initiative aligns with India’s broader Digital India vision, which has already transformed the payment ecosystem through platforms such as UPI, RTGS, and NEFT. The Digital Rupee is designed to leverage this mature digital infrastructure to enable secure, programmable, and efficient payments for both retail and wholesale use cases. Nevertheless, studies note that India faces unique challenges related to scalability, cybersecurity preparedness, and digital literacy, which could impact large-scale CBDC adoption.

However, there are additional risks associated with system resilience, privacy protection, and cyber-threat exposure when switching to a fully digital sovereign currency. These issues need to be carefully considered before being widely adopted. Any cybersecurity breach could jeopardize financial stability, interfere with national payment systems, and reduce public confidence in digital currency issued by the government.

China is selected for comparison because it operates the world’s most advanced and widely tested retail CBDC—the e-CNY. China’s e-CNY, one of the earliest and most advanced CBDC initiatives, adopts a highly centralized design emphasizing strong infrastructural control and operational security. A comparative analysis between India’s Digital Rupee and China’s e-CNY, therefore, provides valuable insights into evolving global cybersecurity practices and highlights potential strategies for strengthening India’s CBDC framework.

2.Literature Review

Studies on Central Bank Digital Currencies (CBDCs) are expanding rapidly as countries explore state-backed digital money and its implications for financial stability and cybersecurity. Foundational work by the Bank for International Settlements highlights key CBDC design principles, including token-based, account-based, and hybrid models, two-tier distribution architectures, and privacy tiers [1], [2], [3]. These studies also stress that cybersecurity, encryption, and operational resilience are essential for safe CBDC deployment. The International Monetary Fund similarly notes that CBDCs increase the national cyber-attack surface and require strong governance, secure key management, and effective incident-response capabilities [4].

Technical research adds clarity on how design choices affect security. Jin and Xia [5] argue that ledger structure, verification processes, and offline payment mechanisms directly influence scalability and vulnerability to cyber threats. Christodorescu et al. [6] highlight that secure offline transactions and hierarchical models reduce systemic risks. BIS surveys indicate that more than 80 countries are testing CBDCs using varied technological and security approaches, demonstrating wide differences in cybersecurity readiness [3].

Paper ID: SC26211111618 DOI: https://dx.doi.org/10.21275/SC26211111618

Country-specific research provides deeper insights. China's e-CNY has been widely analysed for its centralized architecture, dual-tier system, and "controlled anonymity," which preserves basic user privacy while enabling law-enforcement oversight [7], [8], [9]. Studies also highlight China's focus on offline payments, secure-element chips, and strong integration with its digital payment ecosystem.

In comparison, existing literature on India's Digital Rupee focuses mostly on its hybrid architecture, RBI-led issuance, and phased pilot rollout [10], [11], [12]. However, RBI publications provide limited detail on security architecture, threat-modelling practices, or cryptographic controls. Most Indian academic work emphasizes financial inclusion, economic impact, and adoption challenges rather than cybersecurity, leaving technical security analysis underexplored.

This creates a clear research gap: India's Digital Rupee has not yet been systematically compared with established CBDC models, particularly China's e-CNY, from a cybersecurity perspective. Addressing this gap is essential for evaluating India's readiness and identifying areas requiring improvement.

3.Problem Definition

The increasing use of Central Bank Digital Currencies (CBDCs) has brought forth new cybersecurity threats that impact both financial stability and national security directly. India's Digital Rupee, currently in the pilot stage, functions within a complicated digital environment that encounters risks like wallet breaches, data exposure, fraud, and cyberattacks at the system level. Although global CBDC frontrunners such as China have established well-defined security frameworks and operational guidelines, India's cybersecurity measures for the Digital Rupee are still mostly unspecified and unexamined. Even with the rising cyber threats to digital payment systems, there is no systematic assessment of the resilience of India's CBDC framework against emerging dangers or its comparison with well-established global models. This uncertainty leads to a considerable knowledge gap when user trust, financial system stability, and the country's digital infrastructure hinge on robust cybersecurity foundations. Hence, a concentrated, comparative analysis is essential to gauge India's present preparedness and pinpoint areas that need enhancement prior to the nationwide rollout of the Digital Rupee.

4.Methodology

This study follows a qualitative, comparative research design to evaluate the cybersecurity posture of India's Digital Rupee (e₹) and compare it with China's e-CNY. The analysis is based entirely on secondary data, using credible institutional sources such as RBI publications (2022–2024), BIS technical papers, IMF Fintech Notes, publicly available CBDC architectural documents, and country-specific research reports.

The comparison is structured around five analytical dimensions that commonly determine CBDC security and performance:

1. Technical Architecture (ledger design, intermediaries, offline capability)
2. Privacy & Data Governance (anonymity levels, PII handling, data access)
3. Cybersecurity Controls (encryption, device security, key management)
4. Operational Resilience (network redundancy, scaling capacity, fault tolerance)
5. Regulatory Readiness (legal frameworks, compliance, supervisory oversight)

These dimensions were chosen because they reflect globally accepted security determinants for CBDCs and are critical to evaluating India's preparedness.

Comparative Study of India's Digital Rupee and China's e-CNY

This section presents a structured comparative analysis of India's Digital Rupee (e₹) and China's e-CNY in a structured way, focusing on things like architectural design, privacy and data governance, cybersecurity and resilience, legal and regulatory frameworks, and operational readiness. The comparison illustrates how different national priorities influence the planning of CBDC cybersecurity.

1. Technical Architecture Comparison

The management of currency issuance, distribution, transaction validation, and system governance is all determined by the technical architecture of a Central Bank Digital Currency (CBDC). These architectural choices directly affect scalability, fault tolerance, and cybersecurity resilience. While both India and China adopt a two-tier (intermediated) CBDC architecture, their implementation philosophies differ significantly.

a) India - Digital Rupee (e₹)

India's Digital Rupee adopts a hybrid architecture (2-tier architecture) that incorporates intermediaries, with the Reserve Bank of India (RBI) as the issuer of the digital currency, keeper of the core ledger, and controller of the monetary supply, while commercial banks and the authorized intermediaries are the ones who distribute the e₹ through the digital wallets, manage KYC compliance, and give customer-facing services. This model harnesses the existing banking infrastructure in India for regulatory compliance, scalability, and less disruption to the financial system.

In terms of cybersecurity, the distribution of operational responsibilities among several intermediaries makes it possible to avoid having a single centralized system at the core of the whole setup, thus enhancing fault tolerance and offering a greater share of the system's resilience against being taken down entirely. On the other hand, this method is also a factor that pushes the overall threat landscape higher, as the security posture of the Digital Rupee is directly correlated to the stringent application of the security measures across all the banks and intermediaries involved.

b) China – e-CNY

The e-CNY of China also follows a dual-tier model wherein the People's Bank of China (PBoC) constitutes the currency issuance and redemption, core ledger management, and technical and security standards setting. The distribution of wallets, compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, and integration with the existing payment platforms are all the responsibilities of commercial banks and authorized payment institutions.

China's architecture is highly centralized and state-controlled, designed to strengthen national digital sovereignty and reduce reliance on dominant private payment platforms such as Alipay and WeChat Pay. This centralized structure enables uniform enforcement of technical and security protocols across the entire system.

In the context of cybersecurity, the upside of centralized control is that it allows for real-time monitoring, quick threat detection, and coordinating the response to an incident. On the downside, though, it also centralizes systemic risk; thus, the central infrastructure becomes a high-value target for large-scale cyberattacks, where a single breach could have a widespread impact.

Overall, India's hybrid architecture enhances resilience by limiting single points of failure but requires strong coordination and standardized cybersecurity enforcement. In contrast, China's centralized architecture strengthens coordinated cyber defense while increasing exposure to systemic concentration risks.

2. Privacy and Data Governance Comparison

Privacy and data governance play a critical role in shaping user trust, regulatory oversight, and cybersecurity effectiveness within CBDC systems. India and China implement different privacy models that are indicative of their larger governance philosophies.

a) India- Digital Rupee (e₹)

India's Digital Rupee uses a balanced and proportional privacy framework, allowing low-value transactions to maintain token-like anonymity while subjecting higher-value transactions to regulatory scrutiny. This approach is consistent with India's democratic governance principles and data protection regime, particularly under the Digital Personal Data Protection (DPDP) Act of 2023.

From a cybersecurity standpoint, limiting centralized data collection reduces the risk and impact of large-scale data breaches while also minimizing unnecessary exposure of personally identifiable information. Higher anonymity at lower transaction levels, on the other hand, may delay the detection of sophisticated fraud or coordinated cybercrime unless accompanied by advanced monitoring and analytics capabilities.

b) China - e-CNY

China's e-CNY follows a controlled anonymity model, where small-value transactions retain limited privacy, but transaction data remains accessible to authorities for regulatory enforcement, fraud prevention, and national security purposes.

This model enhances cybersecurity resilience by enabling real-time transaction monitoring, anomaly detection, and effective AML/CFT enforcement. At the same time, centralized data storage increases the potential impact of data breaches, requiring robust data-protection and access-control mechanisms.

India's privacy model reduces centralized data exposure but requires stronger analytical tools to maintain effective cyber surveillance, whereas China's model strengthens detection and enforcement at the cost of greater data concentration and reduced individual privacy.

3. Security Controls and System Resilience Comparison

a) India - Digital Rupee (e₹)

India's Digital Rupee employs a layered cybersecurity framework, incorporating end-to-end encryption, device authentication, tiered KYC norms, and controlled wallet access. The RBI is also testing offline payment mechanisms to ensure usability in regions with limited connectivity.

This approach enhances accessibility and financial inclusion while maintaining baseline security standards. However, reliance on software-based protections increases vulnerability to emerging cyber threats if systems are not continuously updated and monitored. Offline payment functionality further introduces new risk vectors that require robust safeguards.

b) China – e-CNY

China's e-CNY security model is hardware-intensive, utilizing Hardware Security Modules (HSMs), secure-element chips in supported devices, and centralized transaction monitoring systems.

These safeguards significantly reduce risks like cryptographic key compromise, wallet cloning, and malware attacks. Centralized monitoring allows for rapid threat identification and containment, but the system's rigidity may limit its ability to respond to novel or evolving cyber threats.

China's hardware-based approach provides stronger baseline protection against technical attacks, whereas India's layered model is adaptable and scalable, but requires ongoing improvement to maintain long-term cybersecurity resilience.

4. Legal and Regulatory Framework Comparison

A strong legal and regulatory framework is required for enforcing cybersecurity standards, ensuring compliance, and enabling effective incident response in CBDC systems.

a) India - Digital Rupee (e₹)

India's Digital Rupee is being used through the Reserve Bank of India's (RBI) regulatory supervision and is furthermore protected by current financial regulations and the Digital Personal Data Protection (DPDP) Act, 2023. The legal setup that safeguards the Digital Rupee is changing as the pilot phases are being implemented, with the issue of a specific law for CBDC expected to occur before the nationwide launch.

The existence of powerful data protection laws significantly increases accountability and consumer confidence. Nevertheless, the lack of clear-cut incident-response mandates with respect to CBDC may result in uncoordinated actions during violent cyber incidents, unless this issue gets sorted out through the future regulations.

b) China – e-CNY

China’s e-CNY is governed by a centralized, state-centric legal framework that grants extensive authority to regulatory agencies. With this setup, compliance can be forced, enforcement made smooth, and intervening during cyber incidents can be done quickly. The law supports the authorities in prescribing common standards of security, requiring constant monitoring of transactions, and even getting the financial institutions involved immediately when there is a cyber threat.

This setup is a major boost to the system in terms of cybersecurity readiness and operational control. However, lack of legal transparency, poor user consent mechanisms, and few dispute resolution channels may negatively impact public trust and inhibit long-term acceptance. People’s and authorities’ concerns about data monitoring and privacy could be the deciding factors for users, especially in situations where cross-border or international use is involved.

The Chinese framework gives precedence to swift cyber intervention and centralized management, while the Indian framework underlines rights-based governance and gradual development of regulations, thus needing clearer operational procedures to reach similar levels of cybersecurity resilience.

Indian digital currency from future perspective

The future trajectory of India’s Digital Rupee (e₹) will be shaped by its ability to balance financial inclusion, technological innovation, regulatory compliance, and cybersecurity resilience. As the pilot phase progresses toward wider adoption, the Digital Rupee is expected to evolve from a controlled experimental framework into a critical component of India’s national payment and monetary infrastructure.

From a technological standpoint, the Digital Rupee is expected to see gradual improvements in scalability, interoperability, and programmability. Integration into the Indian digital system, including UPI, Aadhaar-based authentication, and banking systems, can increase adoption and usability significantly. However, deeper integration increases system interdependence, necessitating strong cybersecurity governance and ongoing system auditing to prevent cascading failures or coordinated cyberattacks.

In terms of cybersecurity, the future development of the Digital Rupee will necessitate a shift from pilot-level protections to national-scale defensive capabilities. This includes developing sophisticated cryptographic standards, stronger key-management protocols, real-time fraud analysis, and better incident response mechanisms. Further security measures will be required to reduce double-spending, device damage, and replay attacks as offline payment functionality expands to the rural and low-connectivity regions. As with the older models of CBDC, several specialized hardware-based security features might be included that can improve the resilience and preserve accessibility.

Privacy and data security are core components of public trust in the e-rupee. India’s model of balanced privacy allows for a limited level of anonymity in transactions with low-value transactions while providing regulator oversight for riskier transfers, which provides a strong base for adoption.

Future innovations should include the development of privacy-preserving technologies that enable effective cybersecurity monitoring without collecting too much data. Yet regulatory readiness is also essential for a full-scale rollout.

CBDC-specific laws that clarify and account for the ownership of data, its liability, and cybersecurity issues must be created. Also, new cross-border CBDC proposals provide the potential to speed and improve payments but also have complex security and jurisdictional risks and must conform to international security and interoperability norms. Overall, a gradual, security-first expansion supported by robust governance and regulatory clarity will be essential to the Digital Rupee’s long-term success.

5.Conclusion

The Central Bank Digital Currencies represent a revolutionary change in the way modern money is managed, and cybersecurity is important to trust and stability. This comparison between the digital rupee of India’s and China’s e-CNY shows how the design architecture, privacy, security, and regulatory systems function on the cybersecurity resilience of CBDCs.

While the two economies have two-tiered regimes, India adopts an intermediated hybrid model concerned with financial inclusion and system stability, while China maintains centralized policies for security and responds rapidly to threats. China's experience will inform India's decision to adopt cybersecurity protocols among intermediaries, real-time surveillance of transactions, and to seek out more secure devices for wallets and keys with embedded hardware.

India has a comprehensive privacy framework, addressing the downsides of centralized data, but this should be complemented by robust analytics to detect fraud. But, as the Digital Rupee gains momentum, it will be crucial to capitalize on China's strength in coordinated processes and stress-tested implementation while also respecting India's focus on privacy and inclusion in order to build a strong and reputable CBDC environment.

References

[1] BIS. (2021). *Central Bank Digital currencies: System Design and Interoperability*. https://www.bis.org/publ/othp42_system_design.pdf

[2] Central bank digital currency (CBDC) information security and operational risks to central banks. (2023). *Www.bis.org*. https://www.bis.org/publ/othp81.htm

[3] Illes, A., Kosse, A., & Wierts, P. (2025, August 22). *Advancing in tandem—results of the 2024 BIS survey on central bank digital currencies and crypto*. Bis.org. https://www.bis.org/publ/bppdf/bispap159.htm

[4] *Cyber Resilience of the Central Bank Digital Currency Ecosystem*. (2024, August 27). IMF. https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/27/Cyber-Resilience-of-the-Central-Bank-Digital-Currency-Ecosystem-554090

[5] Jin, S. Y., & Xia, Y. (2022). CEV Framework: A Central Bank Digital Currency Evaluation and Verification Framework With a Focus on Consensus Algorithms and Operating Architectures. *IEEE Access*, *10*, 63698–63714. https://doi.org/10.1109/access.2022.3183092

[6] Christodorescu, M., Gu, W. C., Kumaresan, R., Minaei, M., Ozdayi, M., Price, B., Raghuraman, S., Saad, M., Sheffield, C., Xu, M., & Zamani, M. (2020). Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies. *ArXiv:2012.08003 [Cs]*. https://arxiv.org/abs/2012.08003

[7] Deutsche Bank. (2021, July 14). *Digital yuan: what is it, and how does it work? – Deutsche Bank*. Www.db.com. https://www.db.com/news/detail/20210714-digital-yuan-what-is-it-and-how-does-it-work

[8] Mu, C. (2023). Theories and practice of exploring China's e-CNY. *Data, Digitalization, Decentralized Finance and Central Bank Digital Currencies*, 179–190. https://doi.org/10.1515/9783111002736-013

[9] Rbi.org.in. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CONCEPTNOTEACB531172E0B4DFC9A6E506C2C24FFB6.PDF

[10] Reserve *Bank of India*. (2024). Rbi.org.in. https://www.rbi.org.in/commonman/English/scripts/FAQs.aspx?Id=3686

[11] *Central Bank Digital Currency (CBDC) pilot launched by RBI in retail segment has components based on blockchain technology*. (2022). Pib.gov.in. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883&reg=3&lang=2

[12] Central *Bank Digital Currencies (CBDCs) and democratic values*. (2023). https://doi.org/10.1787/f3e70f1f-en

[13] National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1). https://doi.org/10.6028/nist.cswp.04162018

[14] 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*.