CENTRAL BANK DIGITAL CURRENCY (CBDC) & PRIVACY: THE LEGAL STATUS OF THE E-RUPI AND THE CONFLICT BETWEEN "PROGRAMMABLE MONEY" AND CONSTITUTIONAL PRIVACY RIGHTS IN INDIA

Gunda Dinesh, Alliance School of Law, Alliance University

ABSTRACT

This paper focuses on CBDC E-Rupi often referred as digital currency. E-Rupi is India's official legal tender currency launched by RBI and it can be used for everyday transactions. The main question is whether the E-Rupi can be considered as programmable money and It's legal status and conflict with the fundamental right to privacy under Article 21 of the Indian Constitution. This paper uses doctrinal legal research approach it examines primary legal sources, including the RBI Concept Note on CBDC (2022), the Finance Bill 2022 amendments to the Reserve Bank of India Act, 1934 (expanding "bank note" to digital form), the Digital Personal Data Protection Act, 2023, and constitutional jurisprudence. It integrates policy and governance analysis from global CBDC literature. The key findings of the paper includes clear legal status as legal tender of E-Rupi, backed by the RBI's balance sheet and statutory recognition, positioning it as sovereign money equivalent to physical cash while enabling direct, intermediary-free transfers. While the e-Rupee strengthens monetary sovereignty and financial inclusion, its programmable features risk transforming money from a tool of individual freedom into an instrument of state control, undermining the right to privacy and democratic trust.

Keywords: (Central Bank Digital Currency) CBDC, E-Rupi, Programmable money, Article 21, Digital money, Constitution, Homomorphic encryption.

Introduction

The digital currency of India launched by RBI also known as E-Rupi, it functions as legal tender equivalent to physical cash but in digital form. While "e-RUPI" originally referred to a 2021 government digital voucher[1] system for targeted welfare delivery, the term is now commonly associated with the broader e-Rupi CBDC ecosystem, which builds on similar programmable concepts for direct benefit transfers.

[1] Prof. Abhijit N Netke, Prof. Pravin D Kharat, e-RUPI: A Purpose Specific Digital Voucher, Research Trends in Commerce & Management, Chapter 1, Volume 2, 10.25215/9395456299.

It is a legal tender money as per RBI and it has a clear legal foundation, The Finance Bill 2022 amended the Reserve Bank of India Act, 1934, expanding the definition of "bank note" under Section 2(aiv)[2] to include "digital form of currency." This makes e-Rupi legal tender under Section 26 of the RBI Act[3], exchangeable at par with physical rupees and accepted for all financial obligations. Unlike private cryptocurrencies (Highly taxed), e-Rupi's explicitly sovereign and backed by the RBI's balance sheet and is shown as liabilities in RBI's balance sheet.

A defining feature of E-Rupi is programmability, the ability to embed rules such as expiry dates, geo-location restrictions, merchant category limitations, or purpose-bound usage, particularly for government welfare schemes like Direct Benefit Transfers (DBT).

This paper examines the legal status of India's e-Rupee and the inherent conflict between its programmable function and the fundamental right to privacy under Article 21 of the Indian Constitution[4], as affirmed in *Justice K.S. Puttaswamy v. Union of India* (2017)[5].Even though E-Rupi prohibits sharing the data with third party applications the main research question is: To what extent does the programmability of the e-Rupee, which enables enhanced traceability and usage restrictions, conflict with constitutional privacy protections requiring proportionality, legitimate aim, and least intrusive means?
Objectives of the study are to:

(i) Analyse the legal and regulatory framework of the e-Rupee

(ii) Examine the concepts and implications of programmable money

(iii) Assess privacy risks arising from data generation, access, and use[6]

(iv) Propose governance safeguards aligned with constitutional principles.

[2] The Reserve Bank Of India Act, 1934, S 2(aiv).
[3] The Reserve Bank Of India Act, 1934, S 26.
[4] INDIA CONST. art. 21
[5] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
[6] Onyango, G., & Jamil, I. (Eds.). (2025). Routledge Handbook of Public Policy in the Global South (1st ed.). Routledge. https://doi.org/10.4324/9781003561910.

The significance lies in India's context as the world's largest democracy with a robust privacy network and legal framework and ongoing e-Rupee (over five million users as of recent reports). The study highlights risks to civil liberties while acknowledging potential benefits for financial inclusion and efficiency.

The primary objectives of this research is to analyze different models of verifications such as operational models and verification methods impact user privacy and to evaluate the "privacy-by-design" framework as a solution to data abuse and data breach. This paper studies and analyses the inherent conflict between meeting anti-money laundering (AML) requirements and offering cash-like anonymity. It also explores how democratic institutions will uphold the trust of the citizens in these digital financial ecosystems and the build of trust by the government by enabling higher security across digital financial platforms.

This study is significant because it addresses the "time-consistency problem," where initial digital safeguards could be removed by future governments to weaponize financial data against political dissent. The scope is limited to retail CBDCs, focusing on the retailers and everyday miscellaneous transactions, digital payments are made so that the transactions will be lot more easier and it will be similar to cash transactions. The structure follows a logical flow from theoretical governance models to technical mitigation strategies and specific policy recommendations for protecting the future of financial privacy.

Literature Review

Existing literature on CBDCs has largely focused on economic, technical, and monetary policy dimensions, everyday transactions with governance, programmability, strict policies, two step verification and privacy receiving comparatively less attention until recently.

Freiman provides a governance perspective distinct from others, distinguishing two concepts of programmability: *programmable payments* (automation of transfers based on predetermined conditions, similar to smart contracts and digital payments) and *programmable money* (restrictions on usage imposed by authorities, such as limiting spending to specific purposes or merchants and imposing restrictions on total amount).[7] He argues that while these features can

[7] Oroi Freiman, CBDC Governance: Programmability, Privacy and Policies.

support social policies, they raise questions of state influence, control, and abuse of power on the transactions of individuals. Privacy is the most important in the current market and in the era of technological advancements, as meeting AML/CFT requirements while offering cash-like anonymity appears incompatible because all the transactions made using digital rupee is under the government control with restrictions . Authorities access to transaction data risks state-level surveillance, threatening civil liberties. Freiman highlights a "time-consistency problem" even initial safeguards can be overridden later and recommends legislative protection for cash and prohibitions or strict limits on programmable money.

The IMF Fintech Note offers a framework for addressing the trade-off between CBDC data use and privacy protection. It details how CBDC design generates rich data categories: payer/payee identity, Fake identifiers, transaction data, and additional metadata along with two step verification. Unlike cash (full anonymity and the secrecy is maintained), CBDC can create a "digital trail" linking identities to behaviours. The note emphasises privacy-by-design, privacy-enhancing technologies (PETs) such as zero-knowledge proofs, homomorphic encryption, and differential privacy, and tiered approaches such as: high anonymity for small-value transactions resembling cash, while larger transactions align with existing digital payment privacy levels. Central banks are seen as well-positioned to manage this trade-off through institutional arrangements, transparency, and data-sharing mechanisms and the commercial banks follow the guidelines and rules by creating their own applications of E-Rupi backed by RBI guidelines.

Homomorphic encryption is an advanced cryptographic technique that enables computations such as mathematical operations or data processing or data analysis or transaction data to be performed directly on encrypted data without the need to decrypt it first. The result of these computations remains encrypted, and when eventually decrypted,[8] (encrypted data remains secured and protects the individuals) it yields the same outcome as if the operations had been carried out on the original, unencrypted data. This preserves the confidentiality of the underlying information throughout the process. This technology addresses a key challenge in

[8] Gandhi, V., Kak, R. (2026). India's DPI Experiment and Digital Finance Revolution. In: Hoven, IG., In, S.Y., Puschmann, T. (eds) Sustainable Digital Finance. Financial Innovation and Technology. Springer, Cham. https://doi.org/10.1007/978-3-032-02983-6_27.

data security: how to analyze or manipulate sensitive information without exposing it to potential risks, such as breaches or unauthorized access during processing[9].

India's Central Bank Digital Currency (CBDC),[10] known as the Digital Rupee or e-Rupee uses homomorphic encryption, homomorphic encryption is highlighted as a promising privacy enhancing technology (PET) to mitigate the inherent privacy risks and data protection associated with programmable money or transaction traceability or Security. As discussed in the research paper, the e-Rupee's design generates rich data trails including payer/payee identities, transaction data, and behavioral patterns which could enable surveillance if not properly safeguarded. Homomorphic encryption helps balance the need for data utility (e.g., for anti-money laundering/combating the financing of terrorism [AML/CFT] compliance, monetary policy analysis, or welfare targeting) with strong privacy protections under India's constitutional framework (Article 21 and the Puttaswamy proportionality test).

Bhunia and Mondal[11] provide an India-specific case study of the Digital Rupee. They trace the evolution from barter to digital payments and contrast traditional online transactions (involving multiple intermediaries and banks that includes third party applications user interface) with CBDC's direct, intermediary-light model. The e-Rupee enables efficient record-keeping and finality without interbank settlement and it provides privacy by disabling the third party applications by rendering own user interface application for digital rupee, offering advantages in welfare delivery through purpose bound tokens. However, the authors identify core privacy risks: transaction tracking, data profiling, and potential government surveillance. Complete anonymity is impossible due to the auditable ledger maintained by the RBI. They stress that users will resist systems posing confidentiality risks, particularly in a context of increasing privacy awareness and cyber frauds.

Research gaps addressed by this paper include the limited integration of India's constitutional privacy framework (Article 21 and Puttaswamy case) with CBDC programmability analysis. While global literature discusses governance and data trade-offs, and the Indian case study highlights risks, few works collaborate the legal status of the e-Rupee with the specific tension

[9] Akash Bhunia, Diptiman Mondal, Privacy Concerns in CBDC: A Case Study into Digital Rupee, https://doi.org/10.69953/nurs.v10iSpecial%20Issue.584.
[10] Shallu Sehgal, Mohd Yasir, Sukhleen Kour, E-Rupee: Unlocking India's Digital Economy, Challenges, and Opportunities, South Asian Journal of Social Studies and Economics Volume 21, Issue 8 https://doi.org/10.9734/sajsse/2024/v21i8860.
[11] Akash Bhunia, Diptiman Mondal, Privacy Concerns in CBDC: A Case Study into Digital Rupee, https://doi.org/10.69953/nurs.v10iSpecial%20Issue.584.

between programmable restrictions and individual autonomy. The amendment definitely changed the usage of blockchain technology and digital currency in India however, the anonymity of transactions is still considered as a privacy issue in the framework.

Significant existing research has focused on the economic and technological aspects of CBDC, such as its effect on financial stability, credit markets, and bank disintermediation. Scholars like Francesca Carapella and Jean Flemming[12] have analyzed CBDC's impact on commercial banks, while others have explored motivations like crime prevention and competition in digital payments. However, multiple researchers acknowledge that literature on the legal and societal facets of CBDCs has been scarce, with primary research themes often ignoring governance or social implications.

A critical gap identified in the literature is the "digital trail" created by CBDC, which contrastingly generates a wealth of personal data, including transaction histories and behavioral patterns. In India, the RBI's concept note and subsequent pilot projects have initiated a conversation on how e-Rupi can revolutionize the financial landscape. Yet, experts like Mervyn King[13] have questioned the fundamental "raison d'être" of CBDC, suggesting that private sector solutions may already solve payment-related problems more effectively.

The literature on BigTech payments offers a cautionary tale for CBDC design, illustrating how data-driven business models can lead to data monopolies or "walled gardens".[14] If a single non-bank Payment Service Provider (PSP) is allowed to retain CBDC data, it could lead to anticompetitive behavior and a loss of consumer privacy similar to that seen in dominant tech platforms. This underscores the need for central banks to avoid data silos and encourage competitive, safe data-sharing arrangements.[15]

[12] Ori Freiman, CBDC Governance: Programmability, Privacy and Policies, https://www.cigionline.org/static/documents/DPH-paper-Freiman.pdf.

[13] Cash, Justin. 2022. "Ex-BoE governor Mervyn King calls Britcoin a 'solution without a problem'." Financial News, January 18. www.fnlondon.com/articles/ex-boe-governor-mervyn-kingcalls-britcoin-a-solution-without-a-problem-20220118.

[14] Privacy regulations may facilitate the prevalence of "walled gardens" on the Internet, because consumers have a difficult time understanding privacy notices in the absence of standardized language (Kelley and others 2010), thus giving large firms an advantage over small firms.

[15] Central Bank Digital Currency Data Use and Privacy Protection, IMF, https://www.imf.org/-/media/files/publications/ftn063/2024/english/ftnea2024004.pdf.

Existing studies on privacy also highlight the "privacy paradox,"[16] where individuals express deep concerns about their data but continue to use systems that exploit it. However, empirical studies in digital payments suggest this paradox may not be as strong in financial contexts, as users prioritize privacy protection as a top characteristic for any digital currency. This gap in the research reconciling user demands for privacy with the state's demand for data for AML/CFT purposes is a central theme addressed in this paper.[17]

Methodology

This study adopts a doctrinal legal research approach, supplemented by a qualitative case-study of India's e-Rupee. The doctrinal method involves systematic analysis of primary legal sources: statutes (Reserve Bank of India Act, 1934 as amended), policy documents (RBI Concept Note on CBDC, 2022), and constitutional jurisprudence (*Puttaswamy*, 2017). Secondary sources from the attached papers Freiman (2023), Murphy et al. (2024), and Bhunia & Mondal (2024) provide conceptual frameworks on programmability, data generation/use, and India-specific risks.

The case-study method examines the e-Rupee pilot's design features (token-based architecture, programmability for DBT, tiered privacy explorations) against constitutional standards. Data collection draws from official RBI documents, concept notes, and the detailed analyses in the attached papers. No primary empirical data (surveys or interviews) were collected, as the focus is on normative and design implications at the pilot stage.

Analytical tools include the **proportionality test** from *Puttaswamy* (legitimate aim, rational nexus, necessity, and balancing) and comparative evaluation of CBDC design choices (direct/indirect models, token vs. account-based verification, PET integration) drawn from Freiman and the IMF note. The approach is qualitative and interpretive, identifying themes of efficiency versus liberty, surveillance potential, and governance safeguards. Limitations include the early stage of the e-Rupee rollout, restricting predictive empirical insights.

[16] The term "privacy paradox" was first coined and documented by Athey, Catalini, and Tucker (2017), although empirical studies focusing on digital payments since have found a significant role of privacy suggesting no paradox for digital payments specifically (for example, European Central Bank 2022).
[17] Central Bank Digital Currency Data Use and Privacy Protection, IMF, https://www.imf.org/-/media/files/publications/ftn063/2024/english/ftnea2024004.pdf.

Data collection was conducted by reviewing working papers from the Digital Policy Hub, Fintech Notes from the International Monetary Fund (IMF), and the Reserve Bank of India's concept notes. The research also incorporates findings from public consultations in Canada and the European Union to gauge societal preferences. Legal documents, such as India's Digital Personal Data Protection Act (DPDPA) of 2023[18], were analyzed to assess current regulatory safeguards.

The study focuses on a sample of jurisdictions representing different stages of CBDC exploration: India's active pilot project (e-Rupi), Canada's theoretical democratic framework, and the European Union's regulatory-heavy "digital euro" proposal.[19] This sampling strategy allows for a comparison between authoritarian contexts, where digital money could become a tool for control, and democratic contexts where institutions uphold individual rights.

The analytical tools used include the "privacy-by-design" philosophy, which mandates that privacy be embedded into the system's architecture from the outset. The paper also utilizes a "tiered transaction" framework to analyze how different levels of data intensity can be applied based on transaction value. Finally, specific Privacy-Enhancing Technologies (PETs) like Zero-Knowledge Proofs and Homomorphic Encryption are evaluated for their effectiveness in masking identities while allowing for regulatory compliance.[20]

Results/Findings

Legal Status of the E-Rupee: The e-Rupee is statutorily recognised as legal tender. The Finance Bill 2022 amended the RBI Act, 1934,[21] explicitly including digital currency within the definition of "bank note." It is exchangeable at par with physical rupees and backed by the RBI's balance sheet, distinguishing it from private cryptocurrencies.

Programmability Features: The e-Rupee supports both programmable payments[22] (automated conditional transfers) and programmable money (usage restrictions). In welfare

[18] Digital Personal Data Protection Act (DPDPA), 2023.
[19] European Central Bank. 2020. Report on a digital euro. October. www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.
[20] Central Bank Digital Currency Data Use and Privacy Protection, IMF, https://www.imf.org/-/media/files/publications/ftn063/2024/english/ftnea2024004.pdf.
[21] The Reserve Bank Of India Act, 1934.
[22] Nyffenegger, R. A proposal for a layer-2 CBDC on a rollup. *Digit Finance* **6**, 543–571 (2024). https://doi.org/10.1007/s42521-024-00115-2.

applications, tokens can be purpose-bound (e.g., restricted to specific merchants, categories) (groceries, fuel), or with expiry enabling precise DBT delivery and leakage reduction. This creates a "sweet spot" between cash (anonymous but poor record-keeping) and traditional digital payments (traceable but intermediary-heavy).

Privacy and Data Implications: CBDC design inherently generates rich data trails (payer/payee identity, transaction metadata, behavioural patterns). In India's model, the RBI maintains records, granting authorities direct or indirect access. This enables transaction tracking and profiling, contrasting sharply with cash's full anonymity. Risks include state surveillance, data breaches, and chilled economic autonomy. Programmability amplifies control: a future authority could restrict spending or monitor compliance in real time.

Mitigations Identified: The design explores tiered privacy (higher anonymity for low-value transactions) and PETs (zero-knowledge proofs for balance validation without revelation, homomorphic encryption). India has considered a "right to be deleted" for transactions to maintain anonymity. The IMF framework suggests embedding privacy-by-design, with central banks coordinating policies for data access, sharing, and accountability.

The research finds that the operational model of a CBDC[23] is the most critical factor in determining data generation: a "direct" model makes the central bank the primary repository of all identity and transaction data, whereas a "two-tier" model distributes this data among intermediaries. Furthermore, verification methods significantly impact privacy; account-based CBDC[24] requires the verification of user identity, while token-based CBDC resembles physical cash and requires only the verification of the token's authenticity.

Regarding programmability, the findings distinguish between "programmable payments, "which automate transactions like rent, and "programmable money," which imposes built-in rules restricting where and how money is spent. Programmable money can support social policies, such as ensuring welfare is spent on food, but it also provides an unprecedented ability for authorities to influence behavior and exclude citizens from the financial system.

[23] Syeda Rukhsana Khalid, From Barter to Blockchain: Tracing the Evolution of Trade and Payments in India, Sanskriti and Science: Perspectives on the Indian Knowledge System. Deep Science Publishing. https://doi.org/10.70593/978-93-7185-138-1.

[24] N. A. Abu *et al*., "Digital Ringgit: A New Digital Currency with Traditional Attributes," *2023 11th International Conference on Cyber and IT Service Management (CITSM)*, Makassar, Indonesia, 2023, pp. 1-6, DOI: 10.1109/CITSM60085.2023.10455426.

In the case of India's Digital Rupee, the retail pilot has reached over five million users across 16 banks. The findings indicate that while the RBI proposes cash-like anonymity for small transactions, the centralized ledger inherently creates an auditable record that could be used for data profiling and targeted surveillance. There is also a significant finding regarding the DPDPA 2023: the Union Government has the power to exempt state agencies (like the RBI) from certain privacy protections, potentially diminishing the sanctity of user data stored at the central bank.

Finally, the study identifies several successful Privacy-Enhancing Technologies (PETs) being explored in pilots, such as Switzerland's "Project Tourbillon," which aims for anonymity in transactions while ensuring security and scalability. The data shows that "managed anonymity"—as seen in China and Nigeria—requires no personal identifiable information for the lowest tier of transactions, though this is often balanced against strict limits on transaction volume.

Discussion

The findings reveal a direct tension with constitutional privacy rights. Under *Puttaswamy*, any intrusion on privacy must satisfy proportionality. While legitimate aims (AML/CFT compliance, welfare efficiency, monetary sovereignty) exist, programmable money's usage restrictions and traceability may fail the "least intrusive means" and balancing stages. Unlike cash, which preserves individual autonomy, the e-Rupee risks transforming money into a tool of behavioural control, potentially leading to self-censorship or targeting of dissenters[25].

Freiman's analysis of the time-consistency problem is particularly relevant: democratic safeguards today do not guarantee protection against future abuse. The combination of programmability and surveillance capability could limit freedoms, echoing concerns about financial instruments used against protests.

The IMF's trade-off framework suggests central banks can improve outcomes through transparency, PETs, and tiered designs—e.g., cash-like privacy for small transactions. However, in India's context, integration with Aadhaar-linked systems and potential DPDP Act

[25] Dhamija, D., Dhamija, A., Ranjan, R., Jha, S.S., Renu (2023). E-Rupi Recent Advancement in Digital Payment System. In: Gupta, D., Khanna, A., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 471. Springer, Singapore. https://doi.org/10.1007/978-981-19-2535-1_16.

exemptions heightens risks. Bhunia and Mondal correctly note that users will reject systems perceived as compromising confidentiality, threatening adoption.

Implications: For policy, a dedicated CBDC law is essential, incorporating privacy-by-design, independent oversight, and explicit limits on programmable restrictions. Legislative protection for cash as a parallel anonymous option is advisable. For practice, robust institutional mechanisms (auditable "proofs of correct execution," data minimisation) are needed to build trust.

Limitations: The study relies on pilot-stage documents and doctrinal analysis; full-rollout impacts remain speculative. Empirical user perception studies would strengthen future work.

The interpretation of these findings suggests that CBDC is a "game changer" that could either enhance financial inclusion or lead to systemic oppression depending on its governance.[26] The fundamental tension lies in the fact that full anonymity is often ruled out to meet AML/CFT requirements, meaning "identification at some level" is central to design. This creates a "privacy-security" landscape where every transaction leaves a digital footprint, unlike the "full anonymity" score of physical cash.

There are profound implications for civil liberties if a future government weaponizes this data to profile social activism or political dissent. The "time-consistency problem" is a primary concern: a government might promise privacy today but override those software safeguards tomorrow in the name of national security or economic crisis. Furthermore, programmable money could lead to "social engineering," where a state restricts purchases based on geographic location, merchant type, or even the time of day.

The discussion also highlights the importance of maintaining physical cash as a safeguard against excessive surveillance. Cash serves as a "backup payment method" in case of digital system failures, such as the outages experienced by the Eastern Caribbean CBDC. Without legislative protection requiring merchants to accept cash, vulnerable groups who rely on it for their daily livelihoods could be excluded from the economy.

[26] Jagadeesha R. Bhat, Salman A. AlQahtani, Maziar Necole, FinTech enablers, use cases, and role of future internet of things, Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 1,2023,https://doi.org/10.1016/j.jksuci.2022.08.033.

A major limitation identified is that technology alone cannot build trust; it requires rigorous legal requirements and institutional safeguards. The "privacy paradox" suggests that while technology can mask data, the public must be convinced through transparency and accountability that the technology will not be misused. Ultimately, trust in a CBDC depends on the democratic institutions that maintain the delicate balance of power between authorities

Case Study 1: Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (PMJAY) for Healthcare Benefits

Background and Implementation: Under the Ayushman Bharat scheme, e-RUPI vouchers were deployed to provide drugs, diagnostics, and treatments for low-income families to enable the use of digital rupee and promote digital rupee among low-income families. Eligible beneficiaries received purpose bound vouchers for specific medical services, redeemable at enlisted hospitals. The system integrated with NPCI's UPI platform, allowing seamless issuance by government bodies without needing beneficiaries to have bank accounts and providing services to the families directly[27].

Challenges Addressed: Leakages in subsidy delivery and corruption in healthcare reimbursements were mitigated by restricting voucher use to approved providers and services, ensuring direct benefit transfers (DBT) reached intended users. The direct benefit transfer ensured that the money was used only up to the limits set by the government in the voucher and to prevent corruption.[28]

Outcomes and Impact: This application improved access to healthcare for millions, particularly in rural areas in low-income families, by enabling leak-proof delivery and avoiding corruption. It supported TB eradication programs and nutritional support, with potential to cover over 500 million beneficiaries under PMJAY. Early feedback highlighted reduced out-of-pocket expenses and better scheme governance, fostering greater trust in public health initiatives[29].

[27] Press bureau information, Ministry of Finance, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1616022&reg=3&lang=2.
[28] Kadambi, Pooja and Joseph, Peter T and Ajitsaria, Divya, Ayushman Bharat Digital Mission, From Infrastructure to Impact: A Tri-lens assessment of India's Digital Health System (December 25, 2025). http://dx.doi.org/10.2139/ssrn.5988514.
[29] Prasad Khanzod, Deepesh Kumar Zamad, e-Rupi: Efficient and Transparent Solution for DBT To Masses.

Case Study 2: Fertilizer Subsidies in Agriculture

Background and Implementation: e-RUPI was adapted for agricultural subsidies, where farmers received vouchers for fertilizers redeemable at state-specified counters or dealers. The government issued these via partnering banks[30], targeting smallholder farmers to ensure subsidies were used only for approved inputs like urea or other fertilizers, this ensures that the prescribed fertilisers to be used by the farmers from the government and a record of digital entry provides transparency.

Challenges Addressed: Conventional subsidy systems suffered from diversion, black marketing, and inefficiencies. e-RUPI's person- and purpose-specific design plugged these gaps, allowing real-time tracking and reducing intermediary involvement. The reduction in intermediary involvement is addressed through programmable money and direct benefit transfers (DBT).

Outcomes and Impact: This led to more equitable distribution, benefiting unbanked rural farmers and enhancing agricultural productivity[31]. In initial phases, it minimized leakages, promoted bio degradable fertilisers, potentially saving significant public funds while promoting sustainable farming practices by using the bio degradable fertilisers provided by the government. The model's scalability could extend to other inputs like seeds or irrigation equipment and machinery input[32].

Case Study 3: Mother and Child Welfare Schemes

Background and Implementation: For schemes like the Pradhan Mantri Matru Vandana Yojana, e-RUPI vouchers[33] provided nutritional support and maternity benefits. Pregnant women and mothers received vouchers for drugs, supplements, and check-ups, redeemable at authorized health centers without cash transactions this enables direct benefits to the need

[30] Ministry of Electronics and Information Technology, Government of India. e-RUPI initiative New Delhi: Digital India; 2025.
[31] Reserve Bank of India. RBI expands scope of e-RUPI digital voucher issuance Business Today; 2023.
[32] S Ashok Kumar, P Ganga Devi and V Himaja, e-RUPI: A secure and purpose-driven digital payment mechanism for welfare distribution in India,
DOI: https://www.doi.org/10.22271/27084515.2026.v7.i2f.1077.
[33] N. Prakash , Y. Indiradevan P. Subhasri A Study on Fintech Revolution in India: A Review, Vol.17,Iss. 2, DOI:10.26634/jmgt.17.2.19158.

without intermediaries and the digital transactions ensures that the benefits were provided to the families and promotes transparency.

Challenges Addressed: Delays in benefit transfers and misuse were common in traditional methods. e-RUPI ensured targeted, timely delivery, focusing on vulnerable groups in unrecognised regions. These vouchers provided timely benefits to the unrecognised groups.

Outcomes and Impact: The initiative boosted maternal and child health outcomes by facilitating access to essential services. It reduced corruption, with vouchers ensuring funds were spent on nutrition and care, potentially lowering infant mortality rates. Corporate extensions for employee welfare further expanded its reach, demonstrating versatility beyond government programs. Children with nutrition deficiency received the benefits and promoted child welfare through a transparent system.[34]

Conclusion

This research demonstrates that India's e-Rupee possesses clear legal status as sovereign legal tender but introduces programmable features that create a fundamental conflict with constitutional privacy rights. Programmability offers significant efficiency and targeting benefits for public policy, yet it risks eroding the anonymity and autonomy traditionally provided by cash, potentially enabling pervasive surveillance and state control over economic choices.

The attached studies collectively underscore that privacy is not merely a technical challenge but a governance imperative. Without deliberate safeguards—such as prohibiting unrestricted programmable money, embedding PETs architecturally, establishing a statutory "right to be deleted," protecting cash legally, and ensuring democratic oversight—the e-Rupee may undermine public trust and constitutional values.

Recommendations include: (1) enactment of comprehensive CBDC legislation balancing innovation with rights;

[34] Saurav Mangalmurti, PWC , e-RUPI: Revolutionising prepaid payments, 2023, https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/point-of-view/pov-downloads/e-rupi.pdf

(2) adoption of tiered privacy models with high anonymity for low-value use;

(3) independent audits and transparency mechanisms; and

(4) public participation in design choices. Further research should monitor pilot outcomes and user adoption in light of privacy perceptions.

Ultimately, democratic institutions and legal protections must uphold trust in any new form of money. The e-Rupee can strengthen India's digital economy only if it respects the foundational right to privacy that defines its constitutional democracy.

The research concludes that while CBDCs offer opportunities for a "more innovative economy," their implementation poses significant threats to individual autonomy if not strictly governed. The core finding is that trust is the foundation of any monetary system, and for a CBDC to succeed, it must command public confidence through verified privacy protection rather than mere promises. The decision to issue such a transformative technology should not rest solely with central banks but must involve meaningful engagement with the legislative branch and civil society.

The implications for policy are clear: governments must maximize privacy by design and minimize data collection to the absolute necessary minimum. Any "programmable money" features that restrict the usage of currency should be prohibited by law to prevent systemic oppression and preserve the "soul of money" as an instrument of freedom. Furthermore, the transition to digital currency must not result in the elimination of physical cash, which remains the best guarantor of financial inclusion and privacy.

Recommendations based on this study include a "tiered transaction" system where small-value everyday purchases remain completely anonymous through the use of Zero-Knowledge Proofs or similar PETs. For larger transactions, data should be stored with distributed intermediaries rather than a centralized government ledger to reduce the risk of a single point of failure or surveillance. Public oversight of the CBDC governance structure is essential to ensure that established privacy principles are actually followed and that violators are held accountable.

Ultimately, the goal is to reach a "win-win" situation where privacy and data utility coexist. By adopting a "privacy-by-design" philosophy and fostering continuous dialogue between technologists and human rights advocates, societies can harness the efficiency of digital

payments without sacrificing the fundamental right to be left alone. CBDCs must be designed as a complement to, not a replacement for, the democratic values that underpin the global financial system.

BIBLIOGRAPHY

1. Prof. Abhijit N Netke, Prof. Pravin D Kharat, e-RUPI: A Purpose Specific Digital Voucher, Research Trends in Commerce & Management, Chapter 1, Volume 2, DOI: 10.25215/9395456299.
2. The Reserve Bank Of India Act, 1934, S 2(aiv).
3. The Reserve Bank Of India Act, 1934, S 26.
4. INDIA CONST. art. 21.
5. K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
6. Central Bank Digital Currency Data Use and Privacy Protection, IMF, https://www.imf.org//media/files/publications/ftn063/2024/english/ftnea2024004.pdf.
7. Shallu Sehgal, Mohd Yasir, Sukhleen Kour, E-Rupee: Unlocking India's Digital Economy, Challenges, and Opportunities, South Asian Journal of Social Studies and Economics Volume 21, Issue 8, DOI: https://doi.org/10.9734/sajsse/2024/v21i8860.
8. Gandhi, V., Kak, R. (2026). India's DPI Experiment and Digital Finance Revolution. In: Hoven, IG., In, S.Y., Puschmann, T. (eds) Sustainable Digital Finance. Financial Innovation and Technology. Springer, Cham, DOI: https://doi.org/10.1007/978-3-032-02983-6_27.
9. Akash Bhunia, Diptiman Mondal, Privacy Concerns In CBDC: A Case Study Into Digital Rupee, DOI: https://doi.org/10.69953/nurs.v10iSpecial%20Issue.584.
10. Ori Freiman, CBDC Governance: Programmability, Privacy and Policies, https://www.cigionline.org/static/documents/DPH-paper-Freiman.pdf
11. Cash, Justin. 2022. "Ex-BoE governor Mervyn King calls Britcoin a 'solution without a problem'." Financial News, January 18. www.fnlondon.com/articles/ex-boe-governor-mervyn-kingcalls-britcoin-a-solution-without-a-problem-20220118.
12. Privacy regulations may facilitate the prevalence of "walled gardens" on the Internet, because consumers have a difficult time understanding privacy notices in the absence of standardized language (Kelley and others 2010), thus giving large firms an advantage over small firms.
13. The term "privacy paradox" was first coined and documented by Athey, Catalini, and Tucker (2017), although empirical studies focusing on digital payments since have found a significant role of privacy suggesting no paradox for digital payments specifically (for example, European Central Bank 2022).

14. Digital Personal Data Protection Act (DPDPA), 2023.
15. European Central Bank. 2020. Report on a digital euro. October. www.ecb.europa.eu/pub/pdf/ other/Report_on_a_digital_euro~4d7268b458.en.pdf.
16. Central Bank Digital Currency Data Use and Privacy Protection, IMF, https://www.imf.org/-/media/files/publications/ftn063/2024/english/ftnea2024004.pdf
17. The Reserve Bank Of India Act, 1934.
18. Syeda Rukhsana Khalid, From Barter to Blockchain: Tracing the Evolution of Trade and Payments in India, Sanskriti and Science: Perspectives on the Indian Knowledge System. Deep Science Publishing. DOI: https://doi.org/10.70593/978-93-7185-138-1.
19. N. A. Abu *et al*., "Digital Ringgit: A New Digital Currency with Traditional Attributes," *2023 11th International Conference on Cyber and IT Service Management (CITSM)*, Makassar, Indonesia, 2023, pp. 1-6, DOI: 10.1109/CITSM60085.2023.10455426.
20. Dhamija, D., Dhamija, A., Ranjan, R., Jha, S.S., Renu (2023). E-Rupi—Recent Advancement in Digital Payment System. In: Gupta, D., Khanna, A., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 471. Springer, Singapore, DOI: https://doi.org/10.1007/978-981-19-2535-1_16.
21. Press bureau information, Ministry of Finance, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1616022&reg=3&lang=2
22. Prasad Khanzod, Deepesh Kumar Zamad, e-Rupi: Efficient and Transparent Solution for DBT To Masses.
23. Ministry of Electronics and Information Technology, Government of India. e-RUPI initiative New Delhi: Digital India; 2025.
24. Reserve Bank of India. RBI expands scope of e-RUPI digital voucher issuance Business Today; 2023.
25. S Ashok Kumar, P Ganga Devi and V Himaja, e-RUPI: A secure and purpose-driven digital payment mechanism for welfare distribution in India, DOI: https://www.doi.org/10.22271/27084515.2026.v7.i2f.1077.
26. Saurav Mangalmurti, PWC , e-RUPI: Revolutionising prepaid payments, 2023, https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/point-of-view/pov-downloads/e-rupi.pdf.
27. Nyffenegger, R. A proposal for a layer-2 CBDC on a roll up. *Digit Finance* 6, 543–571 (2024), DOI: https://doi.org/10.1007/s42521-024-00115-2.

28. Onyango, G., & Jamil, I. (Eds.). (2025). Routledge Handbook of Public Policy in the Global South (1st ed.). Routledge, DOI: https://doi.org/10.4324/9781003561910.
29. N. Prakash , Y. Indiradevan P. Subhasri A Study on Fintech Revolution in India: A Review, Vol.17,Iss. 2, DOI:10.26634/jmgt.17.2.19158.
30. Jagadeesha R. Bhat, Salman A. AlQahtani, Maziar Necole, FinTech enablers, use cases, and role of future internet of things, Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 1,2023, DOI:https://doi.org/10.1016/j.jksuci.2022.08.033.
31. Kadambi, Pooja and Joseph, Peter T and Ajitsaria, Divya, Ayushman Bharat Digital Mission, From Infrastructure to Impact: A Tri-lens assessment of India's Digital Health System (December 25, 2025, DOI: http://dx.doi.org/10.2139/ssrn.5988514.