Shivalik Pal & Mahak Khirwal, *Central Bank Digital Currencies & Cross-Border Payments: India's Digital Rupee Experiment in a Fragmented Global Financial Order,* 12 (1) SCHOLASTICUS 1 (2025)

CENTRAL BANK DIGITAL CURRENCIES & CROSS-BORDER PAYMENTS: INDIA'S DIGITAL RUPEE EXPERIMENT IN A FRAGMENTED GLOBAL FINANCIAL ORDER

Shivalik Pal[*] & Mahak Khirwal[†]

ABSTRACT

The proliferation of private digital currencies and stablecoin has compelled central banks worldwide to reassert monetary sovereignty through Central Bank Digital Currency (CBDC) initiatives. This paper examines India's Digital Rupee (e₹) within the broader context of global CBDC developments and cross-border payment infrastructure. Through doctrinal analysis and comparative methodology, we investigate India's hybrid CBDC architecture, its legal foundations under the RBI Act (1934) and related statutes and its positioning within emerging multilateral frameworks like mBridge.

India has processed over 2.73 crore retail CBDC transactions, demonstrating early adoption momentum. However, significant challenges persist like reconciling technological innovation with monetary sovereignty, ensuring cross-border legal certainty, and balancing financial surveillance with privacy rights. We analyse these tensions through comparative study of China's e-CNY, the Digital Euro, and BIS interoperability frameworks. Our findings suggest that India's tiered anonymity model and integration with digital public infrastructure ("DPI") offer a cautiously inclusive approach. Yet, without harmonized international legal standards, cross-border CBDC adoption risks deepening financial fragmentation rather than resolving it. The paper concludes with policy recommendations for statutory reform, data governance, and India's potential leadership in shaping Global South CBDC cooperation networks.

Keywords: Central Bank Digital Currency, Digital Rupee, Cross-border Payments, Monetary Sovereignty, Financial Technology, RBI, Payment Systems.

[*] Shivalik Pal is a fourth year law student at National University of Study and Research in Law, Ranchi, and can be contacted at shivalik[dot]pal[at]nusrlranchi[dot]ac[dot]in

[†] Mahak Khirwal is a fourth year law student at National University of Study and Research in Law, Ranchi, and can be contacted at mahak[dot]khirwal[at]nusrlranchi[dot]ac[dot]in

I. INTRODUCTION: THE DIGITAL CURRENCY MOMENT

A. Post 2020 Trend in Digital Money

The global financial landscape has undergone profound transformation since 2020. The COVID-19 pandemic accelerated digitalization across payment systems, while simultaneously exposing vulnerabilities in traditional correspondent banking networks[1]. Private stablecoins, notably Tether (USDT), USD Coin (USDC), and Facebook's aborted Libra/Diem project[2] emerged as significant actors in cross-border value transfer, processing billions in daily transactions outside conventional regulatory perimeters. Decentralized cryptocurrencies like Bitcoin and Ethereum demonstrated persistent volatility[3], yet attracted institutional interest as alternative stores of value.

This proliferation of over 5,000 privately issued digital currencies since Bitcoin's 2009 launch[4] has prompted an unprecedented response from central banks. Over 130 countries representing 98% of global GDP[5] are actively researching or piloting CBDCs[6], with 44 already in advanced pilot phases[7]. The urgency stems not merely from technological competition but from fundamental concerns about monetary sovereignty, financial stability, and the state's role in money creation.

B. India's Digital Public Infrastructure and the Digital Rupee Initiative

India's CBDC initiative is deeply embedded within its broader digital public infrastructure (DPI) strategy. The successful deployment of Aadhaar (a biometric identity system covering 1.3 billion residents), Unified Payments Interface (UPI, processing over 10 billion transactions monthly), and the India Stack framework has created a unique foundation for digital currency implementation[8]. The Reserve Bank of India's (RBI) launch of the Digital Rupee builds systematically on this infrastructure[9], aiming to address persistent gaps in financial inclusion while countering risks posed by unregulated cryptocurrencies. Its rollout is not merely technological but rooted in a layered statutory mandate that provides both authority and constraints. The RBI Act, 1934, particularly

---

[1] Vučinić, Milena and Radoica Luburić, *Fintech, Risk-Based Thinking and Cyber Risk*, 11 J. Cent. Banking Theory & Prac. 27 (2022).

[2] Ahmed Mahrous, et al*, Stablecoins: Fundamentals, Emerging Issues, and Open Challenges*, arXiv (2025), https://arxiv.org/abs/2507.13883.

[3] Cyrus Cole, *Institutional Adoption of Bitcoin and Ethereum ETFs: Reshaping Volatility and Unlocking Long-Term Value*, AInvest (Aug. 25, 2025), https://www.ainvest.com/news/institutional-adoption-bitcoin-ethereum-etfs-reshaping-volatility-unlocking-long-term-2508.

[4] List of Cryptocurrencies, *Wikipedia*, https://en.wikipedia.org/wiki/List_of_cryptocurrencies (last visited Oct. 19, 2025).

[5] Neha K. Chawla, *Implications of Central Bank Digital Currency in India: A Critical Analysis*, DME JOURNAL OF LAW (2023).

[6] Jianguo Xu, *Developments and Implications of Central Bank Digital Currency: The Case of China e-CNY*, Asian Economic Policy Review (2022).

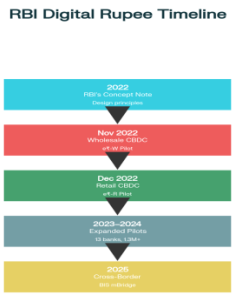
[7] Atlantic Council, *Central Bank Digital Currency Tracker*, https://www.atlanticcouncil.org/cbdctracker (last updated July 2025).

[8] Ministry of Electronics and Information Technology, *India Stack Global – Digital India*, https://www.digitalindia.gov.in/initiative/india-stack-global (last visited Oct. 19, 2025).

[9] Reserve Bank of India, *Annual Report on Currency and Finance – Chapter I: India's Digital Revolution: Opportunities and Challenges*, RBI Publications (July 29, 2024), https://www.rbi.org.in/scripts/PublicationsView.aspx?Id=22457.

Section 22, establishes the central bank's exclusive power to issue currency, which has now been extended into the digital domain through Section 22A inserted by the Finance Act, 2022, giving explicit recognition to digital legal tender. Complementing this, the Payment and Settlement Systems Act, 2007 ensures that the Digital Rupee functions within India's regulated financial rails, while the Banking Regulation Act, 1949, defines how intermediary banks participate in the CBDC ecosystem. However, as India moves towards cross-border CBDC experimentation through platforms like BIS mBridge, the Foreign Exchange Management Act (FEMA), 1999, becomes central to determining the legal permissibility of holding and transferring Digital Rupee outside national borders. Simultaneously, the Digital Personal Data Protection Act (DPDP), 2023, introduces obligations of privacy, proportional data processing, and state accountability, making the design of Digital Rupee wallets a site of constitutional scrutiny.

Despite this robust statutory architecture, several legal and policy frictions remain unresolved. A primary tension lies between maintaining monetary sovereignty and enabling cross-border interoperability, especially as multilateral CBDC networks may require shared governance protocols. Equally significant is the challenge of balancing traceability requirements for anti-money laundering compliance with the right to privacy recognized under Indian constitutional jurisprudence. FEMA's current framework, built around conventional fiat and securities, lacks clarity on the legal status of CBDC once it leaves domestic jurisdiction or is held by non-residents. Moreover, as multiple countries pursue their own CBDC projects, the risk of fragmented bilateral arrangements looms large, raising the question of whether initiatives like mBridge will lead to true interoperability or simply a new layer of controlled financial blocs. Against this backdrop, the objective of this research is to critically examine the legal architecture of India's Digital Rupee within a comparative CBDC landscape, assess its cross-border, and data governance implications, and propose legal adjustments and multilateral coordination mechanisms necessary for a coherent and sovereignty-consistent CBDC framework.[10]



[10] K. M., Mahesh et al, *Impact of Centralized Blockchain Digital Currency (CBDC): For Financial Inclusion and Sustainability*, International Journal of Management, Technology, and Social Sciences (2024).

II. UNDERSTANDING THE CBDC FRAMEWORK: CONCEPTS AND CLASSIFICATIONS

Central Bank Digital Currencies represent a sovereign digital form of money issued by central banks, distinct from both physical cash and commercial bank deposits. The Bank for International Settlements (BIS) classifies forms of money based on four dimensions: the issuer (central bank versus private entities), the form (digital or physical), the accessibility (restricted wholesale access or open retail access) and the technology underpinning it (either identity-linked account-based models or cryptographic token-based systems). The BIS "money flower" further refines this classification by examining whether the digital currency constitutes a direct claim on the central bank or an indirect claim via intermediaries, the level of anonymity permitted and the extent of peer-to-peer, offline transactional capability it enables[11]. These conceptual distinctions are critical for understanding different CBDC design choices adopted by jurisdictions.

CBDC architectures around the world vary significantly. Under a Direct CBDC model, the central bank maintains all customer accounts and processes all retail transactions, resulting in full monetary control but imposing heavy operational burdens and potential disintermediation of commercial banks[12]. In contrast, Hybrid CBDC models distribute operational responsibilities between the central bank and regulated financial intermediaries, allowing the central bank to retain control over the monetary base while delegating KYC, wallet management, and transaction processing to banks and payment service providers[13]. There also exists an Intermediated CBDC model where retail users hold claims through intermediaries rather than directly against the central bank, raising questions about legal enforceability and insolvency risk. A more experimental form, the Synthetic CBDC ("sCBDC"), allows private stablecoin issuers to offer digital tokens fully backed by central bank reserves. While this model promotes private innovation, it blurs the boundary between public and private money creation. India has clearly signalled preference for a Hybrid model[14], balancing innovation with regulatory oversight[15].

On the technological front, CBDC infrastructure can operate on permissioned distributed ledger systems or traditional centralized databases. Distributed ledger technology (DLT) offers auditability, verifiability, and cryptographic assurance while permitting controlled validator access.

---

[11] Bank for International Settlements, *Central Bank Digital Currencies*, CPMI & Markets Committee Rep. No. 174, at 4–6 (Mar. 2018), https://www.bis.org/cpmi/publ/d174.pdf.

[12] Milena Vučinić & Radoica Luburić, *Fintech, Risk-Based Thinking and Cyber Risk*, 11 CENTRAL BANKING THEORY AND PRACTICE J. (2022) at 27.

[13] Bank for International Settlements, *A Prototype for Two-Tier Central Bank Digital Currency (CBDC): Project Aurum*, BIS Other Publications No. 57, at 6–7 (Oct. 2022), https://www.bis.org/publ/othp57.pdf.

[14] Dr. Pragya Nayyar & Dr. Jasdeep Kaur, *Origin of CBDC in India: Prospects and Challenges of Issuance & Management*, 7 INT'L J. ADV. RES. COM. MGMT. & SOC. SCI. at 222, 224–26 (2024).

[15] Mahrous, *supra* note 2.

Systems like Hyperledger Fabric and R3 Corda are actively explored in pilot environments, especially for wholesale interbank settlements. Conversely, centralized database infrastructure, with higher throughput and easier integration into existing core banking systems, is currently preferred for retail CBDC pilots due to efficiency and lower energy consumption[16]. India follows a pragmatic, technology-neutral stance, allowing infrastructure to vary depending on use-case requirements, including hybrid architectures combining centralized core systems with DLT features where needed.

Access mechanisms further shape CBDC design. Account-based CBDCs rely on identity authentication for every transaction, ensuring strong KYC and AML compliance but increasing surveillance risks.[17] Token-based systems, on the other hand, validate ownership through cryptographic keys rather than identity, enabling cash-like peer-to-peer offline transfers and greater privacy but complicating regulatory oversight[18]. India has adopted a tiered hybrid access model[19][20] that calibrates user anonymity and KYC stringency based on transaction value and risk category, allowing limited pseudonymity for low-value transactions while enforcing full transparency for high-value transfers.

The legal classification of CBDCs remains a developing area. Some jurisdictions define CBDCs explicitly as fiat currency backed by sovereign guarantee,[21] while others classify them as legal tender with mandatory acceptance for debt settlement[22]. A key legal distinction is whether CBDC constitutes a direct liability of the central bank, which ensures depositor protection even if intermediaries fail. While some scholars argue CBDCs could be regulated as financial instruments[23], India has taken a clear position by treating the Digital Rupee as currency under the RBI Act framework rather than a security or payment instrument under financial market

---

[16] Harsh Khandelwal et al., A Survey on Central Bank Digital Currency (CBDC) Implementation Using Hyperledger Fabric: Architecture, Challenges, and Future Prospects, 11 INT'L J. INNOVATIVE RES. TECH. (2024).

[17] Albina Gaisina & Matthias Finger, *Central Bank Digital Currencies (CBDCs): A Countermeasure to Anti-Money Laundering (AML) Challenges Posed by Cryptocurrencies?,* 7 Digital Finance 201, 230–32 (2025), https://link.springer.com/article/10.1007/s42521-025-00132-9.

[18] Marianne Bechara et al., *Private Law Aspects of Token-Based Central Bank Digital Currencies*, IMF Fintech Note No. 2025/003, at 3–6 (Mar. 2025), https://www.imf.org/-/media/Files/Publications/FTN063/2025/English/FTNEA2025003.ash.

[19] Xu, *supra* note 6.

[20] Raphael A. Auer & Rainer Böhme, *The Technology of Retail Central Bank Digital Currency*, Monetary Economics: Central Banks - Policies & Impacts eJournal (2020).

[21] Bank for International Settlements, *Legal Aspects of Retail CBDCs*, BIS Other Publications No. 88, at 3–5 (Oct. 2023), https://www.bis.org/publ/othp88_legal.pdf.

[22] IndusLaw, *Central Bank Digital Currencies – A Primer on the RBI's Concept Paper*, at 2–4 (Jan. 2022), https://induslaw.com/publications/pdf/alerts-2023/Induslaw-Infolex-Central-Bank-Digital-Currencies.pdf.

[23] Jus Corpus, *Legal Implications of RBI's Digital Rupee: A New Era in Indian Monetary Law*, Jus Corpus Blog (July 6, 2025), https://www.juscorpus.com/legal-implications-of-rbis-digital-rupee-a-new-era-in-indian-monetary-law.

regulations[24]. This places it within the domain of monetary law rather than securities law, aligning it with sovereign currency rather than regulated financial assets.

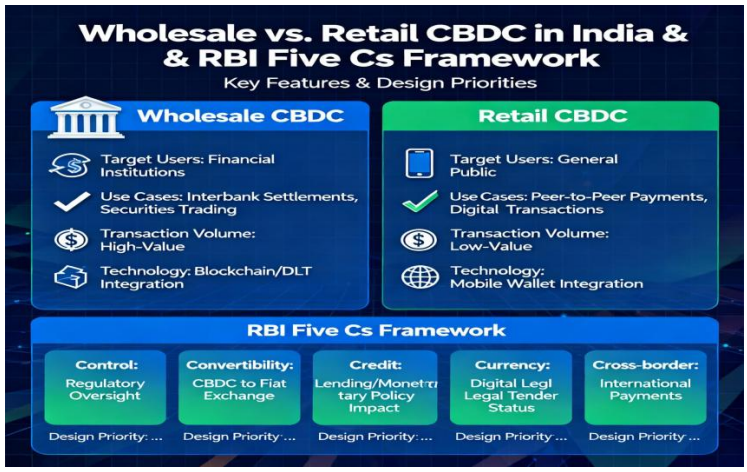


Image: Distinction between wholesale CBDC[25] & Retail CBDC[26] and Five C's[27]

III. INDIA'S DIGITAL RUPEE: REGULATORY DESIGN AND IMPLEMENTATION

The statutory authority of the Digital Rupee is grounded primarily in Section 22 of the RBI Act[28], 1934, which grants the central bank the exclusive right to issue banknotes. Earlier, the applicability of this provision to digital currency was debated, as the term "banknote" traditionally referred only to physical notes payable to bearer on demand. This ambiguity was explicitly addressed by the Finance Act, 2022[29], which inserted Section 22A[30], empowering the RBI to issue currency "including in digital form", thereby placing the Digital Rupee on the same legal footing as sovereign fiat currency. Consequently, the RBI retains a complete monopoly over CBDC issuance, and commercial banks are restricted to distribution and wallet management functions without any monetary creation authority. The Indian Penal Code provisions on counterfeiting (Sections 489A–489E[31]) have also been interpreted to extend to digital representations of currency, ensuring criminal liability for unauthorized duplication or manipulation of CBDC tokens. Under the Bharatiya Nyay Sanhita, 2023 (BNS), these offenses are now encapsulated under Sections *178 to*

[24] Reserve Bank of India, *Digital Rupee (e₹) – FAQs*, RBI (Jan. 9, 2025), https://www.rbi.org.in/commonperson/english/Scripts/FAQs.aspx?Id=3686.
[25] Chawla, *supra* note 5.
[26] Edwin Ayisi Opare & Kwangjo Kim, *A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures*, 8 IEEE Access 110810 (2020).
[27] Mahesh, *supra* note 10.
[28] Reserve Bank of India Act, 1934, No. 2 of 1934, § 22.
[29] Finance Act, 2022, No. 6 of 2022, § 22A.
[30] Reserve Bank of India Act, 1934, No. 2 of 1934, § 22A.
[31] Indian Penal Code, No. 45 of 1860, §§ 489A–489E.

181[32], which criminalize the making, using, circulating, possessing, or facilitating instruments or software intended for counterfeiting "currency or currency in digital form," explicitly recognizing CBDC within the statutory definition of currency. The Payment and Settlement Systems Act, 2007[33], further extends RBI's regulatory control to the entire CBDC infrastructure. Its provisions on authorization, oversight of payment intermediaries, and penalty mechanisms apply directly to entities participating in CBDC distribution and transaction processing. As India moves towards cross-border CBDC trials under BIS mBridge, the Foreign Exchange Management Act, 1999[34], becomes central in determining how Digital Rupee can legally flow across jurisdictions[35]. FEMA[36]'s existing Current and Capital Account rules would govern remittances, speculative CBDC holdings abroad, and the role of authorized dealers in settlement. Parallelly, the Digital Personal Data Protection Act, 2023[37], designates the RBI and participating banks as data fiduciaries, imposing obligations of consent-based processing, data localization of transaction history, and enforceable user rights over access and correction of personal financial data.[38]

Operationally, the Digital Rupee has been deployed through a carefully phased pilot structure. The Wholesale CBDC (e₹-W) was launched on November 1, 2022, initially involving nine major commercial banks[39]. It is currently used for government securities settlement, interbank transactions in the call money market, and is being explored for cross-border wholesale corridors. This wholesale CBDC is integrated into the Clearing Corporation of India Ltd. (CCIL) framework, and as of Q2 2024, over 1,329 wholesale transactions have been executed. The Retail CBDC (e₹-R) pilot began on December 1, 2022, targeting direct public use through wallet-based interfaces managed by 13 authorized banks[40]. With more than 1.3 million users and over 300,000 merchants, the retail pilot supports P2P and P2M payments via QR code infrastructure aligned with UPI standards[41]. A tiered wallet system governs user access, with minimal-KYC basic wallets allowing limited-value pseudonymous transactions, full-KYC standard wallets enabling unrestricted merchant payments, and premium wallets offering offline capability and higher value thresholds.

---

[32] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 178–181.
[33] Payment and Settlement Systems Act, 2007, No. 51 of 2007.
[34] Foreign Exchange Management Act, 1999, No. 42 of 1999.
[35] Xu, *supra* note 6.
[36] *Id.*
[37] Digital Personal Data Protection Act, No. 22 of 2023.
[38] Chawla, *supra* note 5.
[39] Anulekha Ray, *Digital Rupee: RBI Plans to Expand CBDC Pilot to Include More Banks and Locations*, The Economic Times (May 30, 2023), https://economictimes.indiatimes.com/wealth/personal-finance-news/digital-rupee-rbi-to-expand-e-rupee-pilot-to-include-more-banks-and-locations/articleshow/100614794.cms.
[40] Press Information Bureau, *CBDC Pilot Launched by RBI in Retail Segment*, PIB Release (Dec. 12, 2022), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883.
[41] *India's Digital Rupee Pilot Onboards 1.3 Million Users, 300,000 Merchants*, AInvest (May 22, 2025), https://www.ainvest.com/news/india-digital-rupee-pilot-onboards-1-3-million-users-300-000-merchants-2505.

The integration of CBDC with India's Digital Public Infrastructure (DPI) adds a unique governance dimension to its deployment. The interoperability with UPI ensures that merchant acceptance networks remain unified rather than fragmented, although RBI continues to calibrate measures to prevent CBDC adoption from cannibalizing UPI transaction volumes. Aadhaar-linked eKYC enables instant onboarding, while biometric verification is reserved for high-value transfers in compliance with Supreme Court proportionality tests. The Account Aggregator framework further positions CBDC transaction data as a new layer for credit scoring and financial inclusion, especially for MSME and rural lending ecosystems. Complementary DPI layers like GSTN, Co-WIN, and ONDC present potential integration points for programmable CBDC payments, automated tax compliance, and public benefit transfers[42].

To support innovation, the RBI Innovation Hub operates as a regulatory sandbox for testing programmable transactions, offline settlement designs, and cross-border CBDC interoperability. The Public Tech Platform for Frictionless Credit explores how CBDC transaction trails can aid in real-time credit assessment, especially for agriculture finance through Kisan Credit Card digitization. BBPS integration allows recurring bill payments using Digital Rupee, advancing RBI's objective of reducing cash friction in semi-urban and rural economies[43]. Financial inclusion remains a core mandate, with targeted initiatives such as training Business Correspondents, deploying regional language CBDC apps[44], and subsidizing smartphone access for Jan Dhan households to achieve a projected 500 million CBDC-ready citizens by 2027[45].

Despite its strong statutory backing and phased rollout, the CBDC ecosystem faces regulatory challenges that demand precise legal responsiveness. The risk of double-spending and cyber fraud is directly tied to the digital nature of CBDC and is mitigated through cryptographic validation and unique serial identification of tokens. Offline transaction capability introduces an additional risk layer, as real-time reconciliation is not always possible; hence RBI has adopted a hybrid settlement protocol with capped offline limits. CBDC must also align with FATF and PMLA guidelines on KYC/AML enforcement without excluding low-income or undocumented populations from financial access, which is being addressed through tiered KYC frameworks[46]. Under the DPDP Act[47], transaction history becomes protected personal data, raising new compliance questions around purpose limitation and data minimization, especially when CBDC data is considered for

[42] Mahrous, *supra* note 2.
[43] Public Tech Platform for Frictionless Credit, PTPFC, https://ptpfc.org.
[44] K. M. Mahesh et al., *Impact of Centralized Blockchain Digital Currency (CBDC): For Financial Inclusion and Sustainability*, International Journal of Management, Technology, and Social Sciences (2024).
[45] Reserve Bank of India, *RBI to Launch Pilot Project for Public Tech Platform for Frictionless Credit*, Press Release (Aug. 14, 2023), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=56200 .
[46] Auer, *supra* note 20.
[47] Digital Personal Data Protection Act, No. 22 of 2023.

credit analytics or behavioral profiling[48]. There are also concerns about potential bank disintermediation, where large-scale migration of deposits to CBDC wallets could deprive commercial banks of lending capital. RBI currently mitigates this risk by maintaining non-interest-bearing CBDC design, exploring balance caps, and retaining parallel infrastructure for bank deposits and physical cash. Finally, legal certainty is required on claim enforceability in cases where a payment service provider managing a CBDC wallet becomes insolvent. Ensuring segregation of user balances and portability of wallets across intermediaries may necessitate new statutory provisions similar to deposit insurance frameworks, bringing CBDC regulation closer to the robustness of traditional banking law.

IV. COMPARATIVE ANALYSIS: GLOBAL CBDC MODELS

While China's e-CNY enforcement framework relies heavily on administrative mandates and real-time cybersecurity supervision to deter unauthorized manipulation of digital tokens, India has opted for a more formal statutory route through the *Bharatiya Nyay Sanhita (BNS), 2023*, which replaces the Indian Penal Code. The former IPC provisions on currency counterfeiting (Sections 489A–489E[49]) have been systematically recast into Sections 178–181 of the BNS[50], with a significant doctrinal expansion the definition of "currency" now explicitly includes "currency in digital form", bringing CBDC-related offenses squarely within the ambit of criminal prosecution. Under Section 179 of the BNS[51], not only the physical circulation of counterfeit notes but also the transfer of fake CBDC tokens such as QR-based payments using manipulated e₹ units, constitutes a punishable offense. Likewise, Section 181[52] extends the offence of possessing instruments for counterfeiting to include software scripts, malicious code, and unauthorized cryptographic tools designed to duplicate or simulate CBDC wallet balances[53]. This represents a marked departure from frameworks like the EU, which place greater emphasis on regulatory compliance and data governance rather than punitive criminal enforcement.

Further, digital impersonation via fake CBDC wallets, Aadhaar-spoofed KYC, or UPI-linked identity fraud is now categorized as "cheating by personation using electronic means" under Section 316 of the BNS[54], replacing the IPC 419 + IT Act 66C regime. The Bharatiya Sakshya Adhiniyam, 2023[55] modernizes evidentiary standards by recognizing CBDC ledger entries, UPI

[48] Vučinić, *supra* note 12.
[49] Xu, *supra* note 6.
[50] *Id.*
[51] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[52] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 181.
[53] Vučinić, *supra* note 12.
[54] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 31.
[55] Bharatiya Sakshya Adhiniyam, No. 47 of 2023.

transaction logs, and RBI wallet metadata as primary electronic evidence, eliminating the procedural hurdles previously associated with Section 65B certification under the Evidence Act[56]. The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023[57] further consolidates the enforcement ecosystem by classifying unauthorized access to CBDC systems or manipulation of wallet infrastructure as cognizable offenses, enabling law enforcement to arrest without warrant in high-value digital currency fraud cases. This gives India a centralized, statute-backed enforcement model, in contrast to the United States, where CBDC does not yet exist and enforcement would be fragmented across multiple federal and state authorities[58].

Overall, India's legal posture positions it uniquely within the CBDC landscape, combining a sovereign-issued digital currency with a purpose-built criminal law framework that directly targets duplication, manipulation, and unauthorized circulation of digital legal tender. This creates a jurisprudentially robust foundation that aligns with emerging multilateral platforms like BIS Project mBridge[59], where effective cross-border CBDC settlement requires clear domestic criminal liability regimes.

While India has codified a CBDC-specific criminal liability regime, China does not create a separate penal category for e-CNY misuse. Instead, it subsumes all illicit digital currency activity under existing RMB counterfeiting provisions in the *Penal Law (Articles 170–174[60])*, bolstered by expansive administrative enforcement powers under the *PBOC Law[61]* and Cybersecurity Law[62]. Enforcement is technologically embedded, allowing pre-trial wallet freezing and device blocking by Public Security Bureaus without resort to judicial process, under the doctrine of "controllable anonymity."[6364]

In contrast, the European Union adopts a data rights and procedural fairness model. Misuse of the digital euro would not automatically be treated as currency counterfeiting; instead, it would fall under Directive (EU) 2019/713[65] on fraud involving non-cash means of payment, interpreted alongside GDPR and eIDAS. Here, CBDC violations are framed as payment system abuse and

[56] Indian Evidence Act, 1872, No. 1 of 1872, § 65B.
[57] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023.
[58] Opare, *supra* note 26.
[59] Chawla, *supra* note 5.
[60] Criminal Law of the People's Republic of China, arts. 170–174, Order No. 83, Mar. 14, 1997, amended Dec. 26, 2020, Standing Comm. Nat'l People's Cong. (P.R.C.), https://en.spp.gov.cn.
[61] Law of the People's Republic of China on the People's Bank of China, Order No. 46, Mar. 18, 1995, amended Dec. 27, 2003, Standing Comm. Nat'l People's Cong. (P.R.C.), http://www.pbc.gov.cn..
[62] Cybersecurity Law of the People's Republic of China, Order No. 53, Nov. 7, 2016, effective June 1, 2017, Standing Comm. Nat'l People's Cong. (P.R.C.), Stanford Digi China Translation.
[63] Xu, *supra* note 6.
[64] Mahesh, *supra* note 44.
[65] Directive (EU) 2019/713, of the European Parliament and of the Council, Apr. 17, 2019, on combating fraud and counterfeiting of non-cash means of payment, 2019 O.J. (L 123) 18 (EU), https://eur-lex.europa.eu/eli/dir/2019/713/oj.

data integrity breaches, placing privacy and proportionality above sovereign enforcement imperatives.

The United States, lacking a CBDC, operates on a projected enforcement logic. Any future digital dollar misuse would likely be prosecuted under existing financial crime statutes, 18 U.S.C. §§471–474[66] (counterfeiting), §1028A[67] (identity theft), §1343[68] (wire fraud), and the Computer Fraud and Abuse Act[69] (CFAA), with enforcement divided between the FBI and Secret Service. However, widespread political resistance to a CBDC on grounds of "financial surveillance" suggests that any attempt to classify CBDC token tampering as a sovereign currency offence would face robust Fourth Amendment scrutiny.

V. CROSS-BORDER PAYMENT IMPLICATIONS AND JURISDICTIONAL CHALLENGES

The current architecture of cross-border payments, dominated by the correspondent banking model, suffers from inherent inefficiencies that disproportionately impact high-remittance economies like India. Traditional remittance channels impose a multi-layered cost structure; global World Bank data for 2023 places the average remittance cost at 6.2% per transaction, compounded by intermediary correspondent bank fees ranging between 1–3% and foreign exchange spreads of 2–5%.[70] For India, which receives over $100 billion in annual inward remittances, this translates into an economic leakage exceeding $6 billion in transaction costs alone[71]. These financial burdens are exacerbated by systemic time delays, with settlement cycles ranging from 3–5 working days and extending beyond a week for transactions routed through less liquid currency corridors. Cut-off times, weekend closures, and sequential compliance checks across multiple jurisdictions further slow down processing.

Beyond cost and speed, opacity remains a defining flaw of the SWIFT-based correspondent model. Transaction routing across multiple intermediary banks introduces duplicative Know-Your-Customer (KYC) and Anti-Money Laundering (AML) checks, fragmented sanctions screening, and limited visibility for end-users tracking payments in real time. Such friction is compounded by the trend of global "de-risking," wherein major correspondent banks withdraw from jurisdictions perceived as high-risk, reducing available corridors and increasing reliance on limited channels with

[66] 18 U.S.C. §§ 471–474 (2023).
[67] 18 U.S.C. § 1028A (2023).
[68] 18 U.S.C. § 1343 (2023).
[69] 18 U.S.C. § 1030 (2023).
[70] World Bank, *Remittance Prices Worldwide – Issue 47*, at 3 (Sept. 2023), https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q423_final.pdf.
[71] Press Information Bureau, *Annual Remittances to India Reach $125 Billion*, PIB Release (Dec. 19, 2023), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2023/dec/doc20231219290501.pdf.

higher cost structures. For India, this introduces vulnerability, particularly with respect to the Gulf region, its single-largest remittance source, where banking de-risking could jeopardize financial inclusion for overseas workers.

In this context, Central Bank Digital Currencies (CBDCs) emerge as a structural alternative to legacy correspondent banking. Wholesale CBDC models introduce three plausible architectures for cross-border settlements. The first is a bilateral CBDC bridge model, wherein two central banks establish a direct digital settlement corridor with atomic cross-ledger swaps, preserving monetary sovereignty while enabling near-instant settlements. A potential RBI-Monetary Authority of Singapore (MAS) INR-SGD[72] wholesale corridor exemplifies this approach. The second, more advanced design is the multi-CBDC shared ledger model, represented by the BIS-led mBridge initiative[73], where multiple central banks issue and transact their CBDCs over a common technical infrastructure using smart contracts for automated conversion and settlement. This model offers superior interoperability and network effects but raises complex questions around shared governance and jurisdictional authority. The third model relies on interlinking domestic CBDCs through FX platforms, integrating private intermediaries like CLS to facilitate currency conversion without merging sovereign infrastructures, thereby maximizing autonomy but reintroducing intermediary risk elements.

Retail CBDC cross-border use cases introduce further possibilities.[74] Under a tourist and remittance wallet model, foreign users may temporarily hold limited-purpose e₹ balances after simplified onboarding through passport-based KYC, similar to China's e-CNY deployment during the 2022 Winter Olympics[75]. Alternatively, a wallet interoperability model could allow domestic apps to host foreign CBDCs with real-time FX conversion, contingent on deep technical and legal harmonization between participating central banks. For high-volume corridors like India-UAE, a CBDC remittance corridor architecture could facilitate instant, low-cost transfers with shared AML/CFT compliance responsibilities between the RBI and the Central Bank of the UAE, positioning CBDCs as a direct policy instrument for remittance cost reduction[76].

---

[72] The Hindu, *RBI Explores Cross-Border CBDC Pilots as e₹ Circulation Surges* (May 29, 2025), https://www.thehindu.com/business/e-rupee-in-circulation-grows-to-1016-crore-rbi-explores-cross-border-cbdc-pilots/article69632789.ece.

[73] Forbes, *Cross-Border CBDC Focused Project mBridge Moves Forward* (June 23, 2024), https://www.forbes.com/sites/digital-assets/2024/06/23/cross-border-cbdc-focused-project-mbridge-moves-forward.

[74] Auer, *supra* note 20.

[75] Xu, *supra* note 6.

[76] Mahesh, *supra* note 44.

However, these innovations trigger complex jurisdictional and legal challenges. Under Indian FEMA regulations[77] fundamental ambiguities arise regarding whether a domestic resident holding e₹ abroad constitutes a current or capital account transaction and whether FEMA's currency holding caps extend to CBDC wallets. Similarly, when a foreign national holds Digital Rupee, the legal tender status becomes territorially ambiguous, raising questions on enforceability and tax obligations. In a multi-CBDC environment like mBridge, determining the applicable legal system for dispute resolution, particularly when smart contracts autonomously execute cross-currency swaps presents an unresolved conflict-of-laws dilemma. These issues necessitate statutory clarification, particularly through amendments to FEMA[78] defining CBDCs as a distinct legal category separate from conventional foreign exchange assets.

Furthermore, AML compliance under FATF's "travel rule" requires reconciling the pseudonymity of token-based CBDC systems with mandatory identity disclosures in cross-border transactions[79]. Indian legal obligations under the Prevention of Money Laundering Act (PMLA), such as Section 12 (record keeping) and Section 12A[80] (client due diligence), need calibrated integration into CBDC protocols[81] through tiered anonymity models, where domestic low-value transactions remain private, while cross-border transfers trigger identity-linked reporting mechanisms and real-time suspicious transaction alerts via bilateral FIU integration.

Taxation and transfer pricing concerns further complicate CBDC deployment in international settlements. Under Section 195 of the Income Tax Act[82], withholding tax obligations apply to payments made to non-residents, but CBDC-based pseudonymous transactions may obscure payer identity unless explicit compliance triggers are embedded at protocol level. GST applicability on digital services paid via e₹ would depend on "place of supply" rules, demanding CBDC-specific interpretive guidance. For multinational corporations using CBDCs for intra-group settlements, transfer pricing compliance would necessitate transparent CBDC transaction documentation and potentially new Advance Pricing Agreement (APA) frameworks adapted to CBDC corridors[83].

At the macroeconomic level, India faces a monetary sovereignty trilemma. Full sovereignty over e₹ issuance, seamless cross-border CBDC interoperability, and absolute financial stability cannot

[77] Foreign Exchange Management (Overseas Investment) Regulations, No. FEMA 400/2022-RB, Gazette of India, Aug. 22, 2022.
[78] Chawla, *supra* note 5.
[79] Financial Action Task Force, *FATF Updates Standards on Recommendation 16 on Payment Transparency*, FATF (June 18, 2025), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html.
[80] Prevention of Money Laundering Act, No. 15 of 2003, §§ 12–12A (India), amended by Act No. 2 of 2013.
[81] Bank for International Settlements, *Project mBridge: Building a Multi-CBDC Platform for International Payments*, Sept. 2022, https://www.bis.org/publ/bppdf/bispap125.pdf.
[82] Income-tax Act, No. 43 of 1961, § 195.
[83] Mahrous, *supra* note 2.

be simultaneously achieved. India's current strategy prioritizes sovereignty through controlled issuance and restrictive FEMA-led capital controls, while cautiously experimenting with selective bilateral corridors, reflecting a phased interoperability approach[84]. Fragmentation risks persist, however, as divergent CBDC standards could lead to regional digital currency blocs unless harmonized under BIS, IMF, or G20-led governance frameworks[85].

Strategically, India views the Digital Rupee as a geopolitical instrument for rupee internationalization, enabling CBDC-based trade invoicing for energy imports and BRICS-led de-dollarization initiatives. In the remittance domain, integrating e₹ corridors with key jurisdictions like UAE and Singapore offers the potential to reduce transaction costs by up to 90%. Multilaterally, platforms like BRICS Pay and ASEAN's Project Nexus[86] offer fertile ground for Digital Rupee integration, building on existing UPI-PayNow linkages and expanding them into a CBDC settlement layer.[87]

Stablecoins have demonstrated utility in cross-border payments, remittances, and trade finance. However, they also expose jurisdictional vulnerabilities, AML/CFT compliance, taxation, and exchange control. The Digital Rupee's cross-border phase must contend with FEMA restrictions[88] and international standards such as ISO 20022.[89]

The survey paper identifies regulatory arbitrage and extraterritoriality as key risks. Without harmonized legal frameworks, CBDCs may replicate the fragmentation seen in stablecoin markets. India's leadership in BRICS Pay and ASEAN linkages offers a strategic opportunity to shape South-South CBDC cooperation.[90]

VI. DATA, PRIVACY, AND SOVEREIGNTY IN THE CBDC REGIME

The introduction of CBDCs globally has reignited the classical tension between monetary surveillance and individual financial privacy. CBDCs, by design, create a digital trace for every unit of currency, unlike physical cash which leaves no transactional footprint. This produces what may be termed the surveillance, anonymity dilemma, within which jurisdictions are experimenting with varied privacy models along a spectrum ranging from full anonymity to complete traceability. A cash-like anonymity model, involving zero identity disclosure and unrestricted peer-to-peer

[84] Vučinić, *supra* note 12.
[85] Chawla, *supra* note 5.
[86] Reserve Bank of India, *RBI and ASEAN Countries to Create a Platform to Facilitate Instantaneous Cross-Border Retail Payments,* Press Release, Jul. 1, 2024, https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=58197.
[87] Opare, *supra* note 26.
[88] Foreign Exchange Management (Overseas Investment) Regulations, 2022, No. FEMA 400/2022-RB, Gazette of India, Aug. 22, 2022.
[89] Committee on Payments and Market Infrastructures, *Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments*, Bank for Int'l Settlements, Oct. 17, 2023, https://www.bis.org/cpmi/publ/d218.htm.
[90] Mahrous, *supra* note 2.

transfers beyond the view of intermediaries or the state, has been conceptually discussed but rejected by all major central banks due to its potential to facilitate illicit finance, tax evasion, and sanctions circumvention[91]. In contrast, the pseudonymous tiered model, which India has adopted, allows limited identity disclosure for low-value CBDC wallets while mandating full KYC compliance and transaction traceability for higher-value transfers, thus retaining investigatory visibility for law enforcement under due process. At the other end of the spectrum lies the full traceability model, exemplified by China's e-CNY, where every transaction is identity-linked and centrally monitored in real time under the doctrine of "controllable anonymity."

In India's constitutional context, such levels of surveillance necessarily invite scrutiny under the fundamental right to privacy articulated in *Justice K.S. Puttaswamy v. Union of India,*[92] which held that informational privacy, including financial data, falls within the protection of Article 21[93]. Any intrusion by the state into personal transaction data must therefore satisfy the tripartite test of legality, legitimate state aim, and proportionality. While combating money laundering, ensuring tax compliance, and preserving monetary stability are arguably legitimate aims, a question arises as to whether a fully traceable CBDC architecture would be a proportionate restriction or whether a tiered privacy approach, like the one currently adopted by the RBI, better aligns with constitutional standards. Litigation may emerge if CBDC regulations were to mandate identity linkage for all categories of users or impose excessive data disclosure obligations without strong procedural safeguards.

This debate directly intersects with India's evolving data protection regime under the Digital Personal Data Protection Act (DPDP), 2023[94], which treats the RBI and participating banks as Data Fiduciaries responsible for lawful processing and protection of CBDC transaction data, while payment intermediaries function as Data Processors operating under delegated compliance.[95] The DPDP Act[96] imposes principles of purpose limitation, data minimization, storage limitation, and security safeguards, meaning that CBDC-related data collection must be strictly limited to what is necessary for payment settlement, AML obligations, or monetary policy functions. However, potential conflicts arise between the data minimization mandate and reporting requirements under

[91] ICAIE, *Central Bank Digital Currencies: Risks and Rewards – Global Finance and the Fight Against Money Laundering*, ICAIE Report (Jan. 7, 2025), https://icaie.com/2025/01/icaie-releases-new-report-on-central-bank-digital-currencies-risks-and-rewards-global-finance-and-the-fight-against-money-laundering.
[92] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[93] India Consti. Art. 21.
[94] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[95] Vučinić, *supra* note 12.
[96] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.

PMLA[97] and FATF standards[98], which require exhaustive transaction monitoring. The DPDP Act[99] provides an exemption for legal obligations, but ambiguity persists regarding whether economic analysis, behavioral profiling, or credit-scoring based on CBDC data falls within the RBI's statutory mandate or constitutes excessive data use requiring explicit user consent.[100]

A comparative glance at global CBDC models reveals three distinct privacy governance orientations. China's e-CNY adopts a state-surveillance-first approach, allowing only minimal pseudonymity while ensuring full visibility for the central bank, with transactional metadata such as device ID, IP address, and location logs retained indefinitely. Such a system aligns with China's broader cybersecurity and data localization regime, where state access eclipses individual data rights[101]. In contrast, the European Union's Digital Euro project adopts a privacy-by-design architecture, mandating GDPR-compliant data minimization, anonymized offline transactions, and the use of cryptographic techniques like zero-knowledge proofs to verify compliance without revealing user identity or spending patterns[102]. India occupies an intermediate position, adopting a tiered compromise model under which basic low-value wallets retain some pseudonymity to support inclusion and microtransactions, while higher-value usage triggers stricter KYC thresholds and deeper supervisory visibility.

As India enters cross-border CBDC experiments such as Project mBridge, the issue of data sovereignty becomes even more pressing. The RBI's 2018 data localization mandate[103] requires all payment-related data to be stored exclusively on Indian servers, with only limited, regulated data mirroring permitted abroad. However, cross-border CBDC platforms operate on shared ledgers distributed across multiple jurisdictions, raising the risk that Indian CBDC transaction data could be stored on foreign nodes and subjected to foreign data access laws such as the US CLOUD Act or China's National Intelligence Law, both of which compel companies to disclose data to national authorities regardless of where it is stored. To prevent extraterritorial surveillance, India would need to enforce technical safeguards like domestic-only data residency, encryption with sovereign key control, and legal clauses within bilateral CBDC arrangements prohibiting foreign data claims. Additionally, any interoperation with European CBDC systems will trigger GDPR adequacy requirements, for which India's DPDP framework currently falls short due to the absence of an

[97] Prevention of Money Laundering Act, No. 15 of 2003.
[98] Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (updated June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.
[99] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[100] Opare, *supra* note 26.
[101] Xu, *supra* note 6.
[102] Mahrous, *supra* note 2.
[103] Reserve Bank of India, *Storage of Payment System Data*, Circular No. DPSS.CO.OD.No 2785/06.08.005/2017-18, Apr. 6, 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

independent data protection authority with strong enforcement powers. Strengthening domestic data governance institutions will therefore be a prerequisite for India to assert true data sovereignty in cross-border CBDC use[104].

VII. LEGAL REFORM AND POLICY RECOMMENDATIONS

A coherent CBDC ecosystem cannot rest solely on pilot experimentation and regulatory circulars; it requires statutory precision and legislative architecture that clearly defines the legal status, enforceability, liability regime, and cross-border operability of digital currency. To that end, amendments to India's financial legal framework must be both targeted and future-proof, calibrated to preserve monetary sovereignty while enabling technologically adaptive governance. The insertion of a new Section 22A into the RBI Act, 1934[105], explicitly recognizing the RBI's authority to issue digital currency with full legal tender status, would eliminate interpretive ambiguity around whether e₹ constitutes "currency" or merely a regulated payment instrument. Supplementary amendments to Sections 31 and 58 would not only mandate 100% reserve backing for intermediaries managing CBDC wallets, preventing fractionalization of sovereign digital currency but also criminalize unauthorized issuance or counterfeiting, aligning digital monetary protection with the severity traditionally accorded to physical currency integrity.[106]

Complementing the RBI Act[107], the Payment and Settlement Systems Act, 2007, requires definitional expansion to incorporate CBDC as a distinct payment category, accompanied by a new Section 4A establishing authorization, interoperability and dispute resolution standards specific to CBDC infrastructure. Parallel to this, amendments to FEMA, 1999, through a dedicated Section 3A on cross-border CBDC flows, are essential to govern the holding, transfer and conversion of foreign digital currencies within India's capital control regime, ensuring that digitization does not create a regulatory backdoor for uncontrolled foreign currency circulation. Critically, the Digital Personal Data Protection Act, 2023, must be refined to embed CBDC transaction data within a regulated exception framework, permitting controlled processing for monetary stability and AML purposes while prohibiting commercial exploitation or non-regulatory profiling. A new Section 18A under DPDP[108] would institutionalize user rights to access, rectification and transparency in CBDC data handling, anchoring financial privacy as a statutory entitlement rather than a discretionary administrative assurance.[109]

---

[104] Auer, *supra* note 20.
[105] Cole, *supra* note 3.
[106] Chawla, *supra* note 5.
[107] Cole, *supra* note 3.
[108] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 179.
[109] Mahesh, *supra* note 44.

Beyond legislative text, regulatory refinement through a dedicated RBI Master Direction on CBDC would operationalize supervisory expectations across technological standards, intermediary licensing, consumer redressal and cross-border compliance.[110] Such a framework must articulate offline transaction protocols, wallet portability rights, zero-liability norms for unauthorized digital rupee transactions and tiered KYC systems aligned with FATF guidelines. Interoperability sits at the core of CBDC functionality; therefore, the adoption of ISO 20022 messaging formats, UPI-compatible QR logic, open APIs and offline connectivity frameworks (NFC/Bluetooth mesh protocols) becomes essential to prevent CBDC from becoming a parallel, isolated payment system rather than an integrated layer of India's digital financial infrastructure[111]. Legal interoperability, too, demands attention, standardized choice-of-law clauses, CBDC arbitration templates and mutual recognition agreements must accompany technical integration to ensure cross-border legal enforceability.

To give CBDC geopolitical and trade relevance, India must transition from pilot-stage diplomacy to treaty-grade monetary coordination, beginning with bilateral digital currency agreements with high-volume corridors such as the UAE, Singapore, UK and Saudi Arabia. These agreements should not merely provide transactional permissions but establish a comprehensive governance framework, specifying settlement architecture, recognition of KYC identities, AML data-sharing protocols, dispute resolution through BIS-linked arbitration, and explicit exit clauses to protect user holdings in scenarios of diplomatic breakdown or technical severance. India's evolving participation in Project mBridge offers a strategic foothold to embed the rupee in multilateral CBDC clearing pathways. By upgrading from observer to full participant with node infrastructure hosted in Mumbai, India can influence governance rules, technical standards and onboarding criteria for future participant economies, ensuring that global CBDC frameworks do not default to yuan or dollar dominance.

In parallel, BRICS-level CBDC cooperation presents an opportunity to design a South-led digital financial bloc, with the Digital Rupee positioned as one of multiple interoperable CBDCs within a non-dollar settlement ecosystem. This vision would be further amplified by embedding CBDC transaction support within New Development Bank financing and BRICS Pay architectures, reducing dependence on Western-controlled correspondent banking channels[112]. Leveraging its demonstrable success with digital public infrastructure and its normative advantage as a democratic technology state, India is uniquely positioned to lead a Global South CBDC Knowledge and Legal Harmonization Network. Such an initiative, featuring an open-source CBDC stack modelled on

[110] Vučinić, *supra* note 12.
[111] Mahesh, *supra* note 44.
[112] Mahrous, *supra* note 2.

India Stack, model legislation for developing central banks and technical training programs would not only institutionalize India's leadership but also construct an alternative to Western regulatory dominance in digital currency governance.

VIII. CONCLUSION

India's Digital Rupee represents a cautiously ambitious experiment at the intersection of monetary policy, financial technology and legal innovation. Anchored in statutory legitimacy and layered upon a decade of digital public infrastructure, the e₹ stands out as a pragmatic model for emerging economies seeking to reconcile innovation with regulatory prudence, financial inclusion with compliance imperatives, and domestic sovereignty with the realities of global economic interdependence. By selecting a hybrid architecture, centralized issuance by the RBI with intermediated distribution through commercial banks, India has avoided both extremes: neither the state-monopoly design of China's e-CNY, nor the multi-sovereign coordination difficulties faced by the European Union. This architectural pragmatism enhances scalability while preserving the RBI's monetary authority and leveraging existing banking networks for consumer interface and risk management.

Yet, the legal foundations, while grounded in the RBI Act, PSSA, and FEMA remain incomplete. Without a dedicated CBDC statute, questions persist on the enforceability of digital rupee contracts, cross-border settlements, consumer liability in failed transactions, and the legal status of programmability features. These structural ambiguities could generate friction as adoption scales and cross-border corridors emerge. Privacy emerges as a persistent site of constitutional negotiation: India's tiered anonymity model reflects an attempt to reconcile low-barrier financial inclusion, AML/CFT compliance, and the right to informational privacy under Article 21. The durability of this compromise will depend on strict implementation of the Digital Personal Data Protection Act, 2023, credible supervisory oversight, and judicial readiness to enforce the privacy-proportionality doctrine laid down in Puttaswamy.

Cross-border use of CBDCs offers both strategic promise and systemic risk. Through participation in mBridge and potential bilateral corridors with the UAE, Singapore and the UK, the Digital Rupee could reduce remittance frictions, enhance rupee settlement in trade flows and diversify India's financial linkages in a fragmenting global economy. However, data sovereignty, jurisdictional conflicts under FEMA, and the absence of harmonized global legal norms for CBDCs risk the creation of fragmented currency blocs rather than a coherent interoperable system. This reflects a broader shift toward "fragmented globalization," where CBDCs become instruments of geopolitical alignment as much as financial innovation.