



# A Review: India's Leading Role in the Evolution of Financial Cryptography and Consequent Data Security in the Digital Era

Dr Girish Vekaria, Dr K P Patel  
Sir P. T. Science College, Modasa (India)

## Abstract

*India has emerged as a distinctive global laboratory for financial cryptography and data security, demonstrating that a developing nation can leapfrog legacy systems to establish world-leading digital financial infrastructure. This article traces India's evolution from a cash-dominated economy to a global benchmark for digital payments, examining how the nation's unique approach—combining sovereign digital infrastructure, biometric identity systems, progressive cryptography, and comprehensive data protection legislation—has created a model of financial inclusion that balances innovation with security. The journey reveals India's transformation from a technology adopter to a standard-setter, with the Unified Payments Interface (UPI), Aadhaar, and the Digital Personal Data Protection Act, 2023 representing foundational contributions to global financial cryptography practice. As the nation confronts emerging challenges including quantum computing threats and decentralized finance regulation, its experience offers valuable lessons for economies navigating the digital transformation of financial systems.*

## 1. Introduction:

### India's Distinctive Path in Financial Cryptography

The evolution of financial cryptography has typically been narrated through the lens of Western innovations—David Chaum's blind signatures, the development of SSL/TLS, Bitcoin's blockchain breakthrough. However, this narrative overlooks one of the most significant and distinctive laboratories for financial cryptography and data security in the twenty-first century: India.

What makes India's journey remarkable is not merely the scale of its digital financial transformation—though the numbers are staggering—but the distinctive institutional and technological path it has forged. Unlike the market-led evolution of financial cryptography in Western economies, India's approach has been characterised by deliberate state-led infrastructure building, the integration of biometric identity systems with cryptographic protocols, and a regulatory philosophy that balances innovation with systemic stability and individual privacy.

This article argues that India has moved from being a technology adopter to a global standard-setter in financial cryptography and data security. The Unified Payments Interface (UPI), now processing billions of transactions monthly, represents a distinctive contribution to payment cryptography that prioritises interoperability and inclusion. The Aadhaar ecosystem demonstrates large-scale biometric authentication integrated with cryptographic protections. The Digital Personal Data Protection Act, 2023 establishes a comprehensive framework for data security that balances individual rights with innovation. And India's evolving approach to cryptocurrency regulation offers a model of calibrated engagement rather than outright prohibition or uncritical embrace.

As the nation confronts emerging challenges—quantum computing threats to existing cryptography, the integration of artificial intelligence in fraud detection, the regulatory treatment of decentralised finance—its experience offers valuable lessons for economies worldwide navigating the digital transformation of financial systems.

## **2. The Foundational Era: Building the Cryptographic Infrastructure for Digital India**

### **2.1 The Pre-Digital Landscape and the Cash Economy**

To appreciate India's achievements in financial cryptography, one must first understand the baseline from which the nation departed. Historically, India was a profoundly cash-dominated economy, not primarily due to cultural preference but because of structural gaps in financial infrastructure. As late as 2015, with a population exceeding 1.2 billion, India's banking system suffered from severe supply-side constraints: credit card issuance stood at merely 20 million, debit cards at 300 million, with active users numbering in the tens of millions rather than hundreds of millions.

This created what analysts term a "value vacuum"—a vast population of unbanked and underbanked individuals whom traditional financial institutions had failed to reach. For financial cryptography, this represented both a challenge and an opportunity: the absence of legacy infrastructure meant that new cryptographic systems could be designed for scale and inclusion from the ground up, without the constraints of backward compatibility with twentieth-century banking systems.

## **2.2 Early Regulatory Foundations: PKI and Two-Factor Authentication**

India's deliberate construction of financial cryptographic infrastructure began well before the digital payment's revolution captured global attention. In September 2013, the Reserve Bank of India (RBI) constituted a committee comprising representatives from banks, government agencies, and research organisations to examine security in electronic payments.

The committee's final report, released in April 2014, recommended the systematic adoption of Public Key Infrastructure (PKI) technology for online banking transactions. PKI, which enables secure transactions over unsecure networks through cryptographic key pairs and digital certificates, was then accounting for only 25.1 percent of electronic transaction value in India during 2012-2013. The committee's three-stage implementation strategy—first for corporate internet banking login, then for transaction authorisation, and finally for personal banking users—established a roadmap for cryptographic adoption that would underpin subsequent innovations.

Critically, the RBI mandated two-factor authentication for online transactions, requiring "something the user knows" combined with "something the user has". This principle, which would later evolve into more sophisticated risk-based authentication, established a cryptographic baseline for Indian digital finance that prioritised security alongside functionality.

## **2.3 The Puttaswamy Watershed: Privacy as a Fundamental Right**

The constitutional foundation for India's data security framework was established by the Supreme Court's landmark 2017 judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India. This decision recognised privacy as a fundamental right under Article 21 of the Constitution, providing constitutional grounding for comprehensive

data protection legislation and establishing the proportionality test for any restrictions on privacy rights.

The Puttaswamy judgment transformed the legal landscape for financial cryptography in India. It established that cryptographic protections were not merely technical matters but constitutional imperatives—mechanisms for giving effect to fundamental rights in the digital age. The judgment also set in motion the legislative process that would culminate in the Digital Personal Data Protection Act, 2023, creating what the National Informatics Centre describes as "a citizen-centric legal framework that balances individual privacy rights with the legitimate need for lawful data processing".

### **3. The India Stack Revolution: Cryptographic Infrastructure at Population Scale**

#### **3.1 Aadhaar: Biometric Identity with Cryptographic Protection**

The foundation of India's digital financial transformation is the Aadhaar system, which provides a biometric-based digital identity to over 1.3 billion residents. From a cryptographic perspective, Aadhaar represents a distinctive approach to identity management: it uses biometric identifiers (fingerprints and iris scans) not as cryptographic keys themselves but as factors that unlock cryptographic authentication mechanisms.

The system's architecture incorporates multiple layers of cryptographic protection. Biometric data is stored in encrypted form, with strict access controls limiting which entities can verify identities. Authentication requests are transmitted over encrypted channels, and the system supports multiple authentication factors including One-Time Passwords (OTPs) generated through cryptographic algorithms. The Unique Identification Authority of India (UIDAI) has progressively enhanced these cryptographic protections in response to emerging threats and vulnerabilities.

#### **3.2 Unified Payments Interface: Redefining Payment Cryptography**

The Unified Payments Interface (UPI), launched in 2016, represents India's most significant contribution to global financial cryptography. Unlike traditional payment systems that route transactions through card networks or proprietary rails, UPI creates an interoperable layer that enables immediate fund transfers between bank accounts using virtual payment addresses.

The cryptographic architecture of UPI is distinctive in several respects. First, it separates identification from authentication: users transact using virtual addresses that reveal no bank account details, with the underlying payment infrastructure handling cryptographic verification of credentials. Second, it incorporates multi-factor authentication while maintaining user convenience—typically requiring a combination of device binding, PIN entry, and biometric verification depending on transaction risk. Third, it enables interoperability across hundreds of participating banks without requiring each institution to maintain separate cryptographic relationships with every other.

UPI's success has been staggering. By 2025, the system was processing over 10 billion transactions monthly, making India by volume the world's largest digital payments market. This scale has required continuous evolution of the underlying cryptographic infrastructure, with the National Payments Corporation of India (NPCI) implementing capacity enhancements and security upgrades to maintain system integrity.

### **3.3 Digi Locker and Consent-Based Data Sharing**

The Digi Locker platform extends cryptographic protections beyond payments to document storage and sharing. Citizens can store digitally signed versions of official documents—driver's licences, educational certificates, tax records—in encrypted cloud storage, then share them with requesting parties through consent-based mechanisms. From a data security perspective, Digi Locker implements several important cryptographic principles. Documents are stored in encrypted form, with access controlled through authentication mechanisms tied to Aadhaar. When citizens share documents with third parties, the sharing occurs through cryptographic protocols that verify the recipient's identity and authorisation while maintaining audit trails of all access attempts. This creates what the National Informatics Centre terms "a privacy-first approach" to data sharing, where citizens retain control over their information while enabling legitimate uses.

## **4. The Data Protection Framework: The Digital Personal Data Protection Act, 2023**

### **4.1 Legislative Evolution and Constitutional Foundation**

India's journey toward comprehensive data protection legislation reflects the nation's maturation in digital governance. The Information

Technology Act, 2000 provided an initial framework but offered limited privacy protection, with only Sections 43A and 72A addressing sensitive personal data security. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 strengthened these provisions but remained sectoral in scope.

The constitutional turning point arrived with the Puttaswamy judgment in 2017. Following this affirmation of privacy as a fundamental right, the Government appointed the Justice B.N. Srikrishna Committee, which recommended a rights-based framework emphasising responsibility, consent, and data protection. The subsequent legislative process involved multiple iterations—the Personal Data Protection Bill, 2019, which faced parliamentary scrutiny and was withdrawn in 2022, followed by the Digital Personal Data Protection Bill, 2022, which adopted a more balanced approach.

The Digital Personal Data Protection Act, 2023 was finally enacted on 11 August 2023, establishing India's modern data protection regime. The subsequent notification of the Digital Personal Data Protection Rules, 2025 on 14 November 2025 marked the transition from legislative intent to operational reality.

#### **4.2 Foundational Principles of the DPDP Act**

The DPDP Act rests on seven core principles that govern all data processing activities in India:

##### **Principle Requirement**

Consent and Transparency Data processing requires affirmative, informed consent; purposes must be transparent

Purpose Limitation Personal data shall be used only for specified purposes for which consent was obtained

Data Minimisation Only necessary personal data shall be collected and processed

Accuracy Data fiduciaries must ensure data accuracy, particularly where processing affects individuals

Storage Limitation Personal data shall be retained only for the period necessary to serve its purpose

Security Safeguards Reasonable technical and organisational security measures must be implemented

Accountability Data fiduciaries bear demonstrable responsibility for compliance

The Act deliberately adopts what it terms the "SARAL" approach: Simple, Accessible, Rational, and Actionable. This reflects recognition that data protection cannot succeed if its requirements are intelligible only to lawyers and technologists; ordinary citizens and small businesses must understand their rights and obligations.

#### **4.3 Key Stakeholders and Their Cryptographic Responsibilities**

The DPDP Act establishes a sophisticated stakeholder framework that assigns cryptographic responsibilities across the data ecosystem:

Data Principals are individuals to whom personal data relates. They possess rights to consent, access, correction, erasure, nomination, and grievance redressal. For minors or persons with disabilities, lawful guardians act as Data Principals.

Data Fiduciaries are entities that decide why and how personal data is processed. They bear primary responsibility for implementing security safeguards, including encryption of personal data at rest and in transit.

Data Processors process personal data on behalf of Data Fiduciaries under contract. While they handle data operationally, Data Fiduciaries remain fully responsible for their compliance.

Significant Data Fiduciaries (SDFs) face heightened obligations including mandatory Data Protection Officers, independent data auditors, and annual Data Protection Impact Assessments. SDF designation is triggered by criteria including processing data of 10 million or more individuals, large-scale processing of financial or biometric data, or systemic societal impact.

Consent Managers represent a novel institutional innovation—regulated intermediaries that provide transparent, interoperable platforms through which individuals can give, manage, review, and withdraw consent across multiple Data Fiduciaries from a unified interface. Consent Managers must be Indian companies with minimum net worth of ₹2 crore and must register with the Data Protection Board.

The Data Protection Board of India serves as the central enforcement and adjudicatory mechanism, operating through digital-first infrastructure that enables online complaint filing and case tracking.

#### **4.4 Phased Implementation and Current Status**

The DPDP Rules introduce a carefully structured 18-month phased compliance period, reflecting recognition that organisations require time to redesign systems and implement cryptographic controls:

Stage 1 (13 November 2025): Data Protection Board established and operational; digital complaint portal launched; institutional framework activated

Stage 2 (13 November 2026): Consent Manager registration commences; obligations for Consent Managers become operative

Stage 3 (13 May 2027): Full operational compliance obligations in force, including 72-hour breach notification requirements, data principal rights enforcement, and penalties for violations

As of early 2026, India stands at the inception of Stage 1, with organisations in the critical planning and preparation phase.

### **5. Evolution of Payment Authentication: From OTP to Risk-Based Cryptography**

#### **5.1 The Limitations of OTP-Based Authentication**

For years, Indian digital payments relied heavily on SMS-based One-Time Passwords (OTPs) as the primary authentication mechanism. While OTPs represented an improvement over static passwords, their limitations became increasingly apparent with the growth of digital transactions. RBI data revealed 13,516 internet and card fraud cases worth nearly ₹520 crore in FY 2024-25, with total banking frauds reaching ₹36,014 crore driven largely by digital and loan frauds.

Security experts identified several cryptographic weaknesses in OTP-based authentication. OTPs are vulnerable to SIM-swapping attacks, where fraudsters transfer a victim's mobile number to a SIM card they control. They can be intercepted through malware on smartphones or through SS7 protocol vulnerabilities in telecommunications infrastructure. Moreover, OTPs provide only single-factor authentication—possession of the mobile device—without verifying the user's identity.

#### **5.2 The RBI's New Authentication Framework**

In September 2025, the Reserve Bank of India issued a comprehensive framework on authentication mechanisms for digital payment transactions, to take effect from 1 April 2026. This framework represents a fundamental evolution in India's approach to

payment cryptography, replacing the OTP-dominant model with risk-based, multi-factor authentication.

The new framework requires all digital payment transactions to be authenticated using at least two distinct factors from three categories:

Something the user knows: PINs, passwords, passphrases

Something the user has: SMS-based OTPs, hardware tokens, app-based tokens, device binding

Something the user is: Biometrics such as fingerprints or facial recognition, Aadhaar-based verification

Critically, at least one factor must be dynamic unique to each transaction ensuring that proof of possession cannot be reused or intercepted. This cryptographic requirement addresses the vulnerability of static authentication factors to replay attacks.

### **5.3 Risk-Based Authentication: The New Paradigm**

The framework introduces risk-based authentication mechanisms that enable issuers to assess transactions based on contextual parameters:

- Transaction location and behavioural patterns
- Device attributes and history
- Historical transaction patterns and anomalies
- Time of transaction and velocity checks

When transactions appear suspicious—initiated from new devices, at odd hours, or involving unusual amounts—additional verification layers may be triggered. Conversely, routine transactions such as bill payments or small purchases remain seamless. This approach represents what PwC India's cyber leader describes as "India's payment ecosystem maturing into a zero-trust architecture" where "checks take place in silence and only come into focus when something seems suspicious".

### **5.4 Cross-Boarder Implications and Global Standards**

For cross-border card-not-present transactions, issuers must implement risk-based mechanisms by 1 October 2026, including validating non-recurring transactions initiated by overseas merchants and registering their Bank Identification Numbers with card networks. This extends India's cryptographic standards beyond domestic transactions, effectively requiring foreign merchants to comply with Indian authentication protocols when serving Indian customers.

Industry experts view this framework as potentially establishing global benchmarks. As Deloitte India's Anand Venkatraman notes,

"Risk-based authentication uses signals like device compromise, behaviour, location, and transaction history to detect anomalies. This reduces false rejections and helps detect fraud early". The framework balances security enhancement with consumer convenience, recognising that overly burdensome authentication drives users toward less secure alternatives.

## **6. India's Approach to Cryptocurrency and De-centralized Finance**

### **6.1 The Regulatory Journey: From Caution to Calibrated Engagement**

India's relationship with crypto currency has evolved through several distinct phases, reflecting a regulatory philosophy that balances innovation with systemic stability. The journey began in 2013, when the RBI issued its first advisory warning users about potential security risks associated with virtual currencies.

As crypto currency adoption grew, with exchanges like Zebpay, Unocoin, and Coinsecure emerging, regulatory concern intensified. In 2017, the RBI and 财政部 issued further warnings clarifying that virtual currencies were not legal tender. The most dramatic intervention came in April 2018, when the RBI directed banks, non-banking financial companies, and payment system providers not to facilitate virtual currency transactions—effectively cutting off the banking system from cryptocurrency exchanges. This circular caused trading volumes to collapse by approximately 99 percent.

### **6.2 The #IndiaWantsCrypto Movement and Public Engagement**

The banking ban sparked organised resistance from the cryptocurrency community. In November 2018, WazirX founder Nischal Shetty launched the #IndiaWantsCrypto movement on Twitter, advocating for positive regulation rather than prohibition. The movement gained traction, attracting support from industry figures, investors, and eventually policymakers. By July 2021, #IndiaWantsCrypto had completed 1,000 consecutive days of advocacy, demonstrating sustained public engagement with cryptocurrency policy.

This public pressure, combined with international developments and judicial intervention, led to the Supreme Court in March 2020 striking down the RBI's banking ban as disproportionate. The Court's judgment recognised that while cryptocurrency regulation was

legitimate, complete exclusion from the banking system without statutory authority violated constitutional protections.

### **6.3 The PMLA Framework: Bringing VASPs Under Anti-Money Laundering Oversight**

The transformative moment in India's cryptocurrency regulation arrived on 7 March 2023, when the Ministry of Finance issued the PMLA VASP Notification, classifying entities providing services related to virtual digital assets as "reporting entities" under the Prevention of Money Laundering Act, 2002. This notification marked a fundamental shift from regulatory ambiguity to active oversight.

The notification defined five specific activities as subject to regulatory purview:

1. Exchange between virtual digital assets and fiat currencies
2. Exchange between different forms of virtual digital assets
3. Transfer of virtual digital assets
4. Safekeeping or administration of virtual digital assets or instruments enabling control over such assets
5. Participation in financial services related to an issuer's offer and sale of virtual digital assets

Each activity, when conducted "for or on behalf of another person in the course of business," now triggers comprehensive compliance obligations including Know Your Customer (KYC) requirements, transaction monitoring, and reporting to the Financial Intelligence Unit-India (FIU-IND).

### **6.4 Enforcement and International Reach**

The PMLA framework has been accompanied by active enforcement. In December 2023, FIU-IND issued show-cause notices to several major international cryptocurrency exchanges—including Binance, KuCoin, Kraken, and others—for non-compliance with PMLA provisions. Non-compliant platforms faced URL blocking, effectively cutting off Indian users' easy access.

Enforcement intensified in June 2024, when FIU-IND passed a detailed order against Binance imposing penalties for operating without registration and failing to meet KYC/AML obligations. In January 2025, Bybit Fintech Limited was fined ₹9.27 crore for similar violations. Additionally, in August 2024, India's Directorate General of GST Intelligence issued a show-cause notice to Binance alleging

₹722.43 crore (approximately \$85 million) in unpaid goods and services tax on transaction fees collected from Indian users.

These actions underscore several critical principles in India's approach:

- The decentralised or offshore nature of a platform does not automatically exempt it from Indian regulatory oversight
- Enforcement is substantive, not merely symbolic, with authorities imposing significant penalties
- The approach is activity-based, focusing on services provided rather than technical structure or self-identification

### **6.5 The DeFi Challenge: Regulating Decentralised Systems**

The application of traditional financial regulation to decentralised finance presents distinctive challenges. The PMLA framework defines Virtual Asset Service Providers through activities rather than corporate structure, but the phrase "for or on behalf of another person in the course of business" requires interpretation in decentralised contexts.

Internationally, Financial Action Task Force guidance recognises that decentralised platforms are not automatically VASPs unless a person or entity exercises sufficient control over them. In the Indian context, this distinction remains to be clearly articulated, creating uncertainty for DeFi developers.

Critical factors in determining regulatory treatment include:

- Admin keys and multisig controls: The presence of mechanisms enabling parties to alter or override protocol behaviour
- Upgrade or pause authority: The ability to intervene in otherwise autonomous systems
- Economic parameter control: The capacity to set interest rates, collateral requirements, or other parameters
- Custodial elements: Smart contract escrows, liquidity pools, staking services, or bridges that temporarily hold user assets

As Global Legal Insights notes, "self-identifying as 'DeFi' is not sufficient to remain outside the scope of Indian regulation. Regulators will test the degree of decentralisation in fact, and hybrid or semi-decentralised protocols remain particularly exposed due to identifiable points of control"

### **6.6 The Taxation Framework**

India has also established a taxation framework for virtual digital assets. Income from VDA transfers is taxed at 30 percent, with no

deduction for expenses except the cost of acquisition. Additionally, a 1 percent tax deducted at source applies to VDA transfers above specified thresholds. This taxation framework operates independently of the legal status of cryptocurrencies, ensuring that even if regulatory classification remains uncertain, tax obligations are clear.

## **7. The Quantum Challenge and Future-Proofing Indian Cryptography**

### **7.1 Recognising the Quantum Threat**

As India's digital financial infrastructure scales to serve over a billion users, the cryptographic systems protecting these transactions face an emerging threat: quantum computing. Shor's algorithm, running on sufficiently powerful quantum computers, can efficiently solve the integer factorisation and discrete logarithm problems underlying RSA and elliptic curve cryptography—the mathematical foundations of current digital signatures and key exchange.

RBI officials and industry experts have recognised this vulnerability. As Parimal Kumar Shivendu, Group Head at Easebuzz and former RBI AGM, noted in response to the RBI's new authentication framework, "OTPs, though widely adopted, are not quantum-safe and leave gaps in security". This acknowledgment reflects growing awareness that India's cryptographic infrastructure must evolve to address quantum threats.

### **7.2 The "Harvest Now, Decrypt Later" Risk**

Even before large-scale quantum computers exist, Indian financial institutions face operational threats through "harvest now, decrypt later" attacks. Adversaries—particularly nation-states with long time horizons—can intercept and store encrypted financial communications and data, waiting for quantum capabilities that will enable retrospective decryption.

For data requiring long-term confidentiality—including healthcare records, financial histories, and personally identifiable information—this creates immediate urgency. Data encrypted today with classical algorithms may be decryptable in five, ten, or fifteen years when quantum computers mature. India's data protection framework must therefore consider not only current threats but also future capabilities.

### **7.3 Post-Quantum Cryptography Preparedness**

India's response to quantum threats is developing across multiple fronts. The RBI's authentication framework, while not explicitly

mandating post-quantum cryptography, establishes principles of crypto-agility—the capacity to replace cryptographic algorithms without disrupting systems. By moving away from single-factor OTPs toward layered authentication mechanisms, the framework creates flexibility for future algorithm transitions.

The National Informatics Centre and other government bodies are increasingly engaged with international developments in post-quantum cryptography. The August 2024 finalisation of NIST's first post-quantum cryptography standards, including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, provides a foundation for Indian institutions to begin migration planning.

However, as analysts note, the transition presents significant challenges. Unlike previous algorithm updates, which could occur gradually as systems were refreshed, post-quantum migration must occur before the threat materialises, across interconnected systems that cannot be upgraded in isolation. With migration timelines measured in years or decades, Indian financial institutions face a narrowing window for action.

#### **7.4 India's Potential Leadership in Quantum-Ready Finance**

India's experience in building digital public infrastructure at scale positions it potentially for leadership in quantum-ready financial cryptography. The country has demonstrated ability to coordinate complex technological transitions across hundreds of institutions—as evidenced by UPI's rollout, Aadhaar's integration, and GST implementation.

Key advantages include the centralised coordination capabilities of the RBI and NPCI, the existence of national cryptographic standards through bodies like the Bureau of Indian Standards, and the demonstrated capacity for public-private collaboration in infrastructure development. These institutional factors may enable India to implement post-quantum transitions more rapidly than jurisdictions where cryptographic standards are fragmented across private institutions with limited coordination.

### **8. Convergence: Privacy, Security, and Trust in India's Digital Future**

#### **8.1 The DPDP Act and Payment Authentication: Complementary Frameworks**

The convergence of India's data protection framework and payment authentication requirements illustrates the maturation of financial cryptography as a multidisciplinary practice. The RBI's authentication framework and the DPDP Act are not separate regulatory regimes but complementary layers of a unified approach to digital trust.

As Smrithi Nair, partner at Juris Corp, observes, "The use of contextual and behavioural data to determine transaction risk will fall under the scope of the Digital Data Protection Act". This means that authentication mechanisms must comply not only with RBI security requirements but also with DPDP privacy obligations—including consent requirements for data collection, purpose limitations, and data minimisation principles.

### **8.2 Inclusion as a Cryptographic Design Principle**

India's approach to financial cryptography has consistently prioritised inclusion alongside security. The recognition that "trust and safety are the real enablers of inclusion, especially for first-time and underserved users" has shaped cryptographic design choices.

This is evident in UPI's support for feature-phone users through UPI 123, enabling those without smartphones or hesitant to use conventional digital interfaces to access digital finance. It is evident in the RBI's authentication framework, which preserves OTP options for users with restricted smartphone access while enabling more sophisticated mechanisms for those with capable devices. And it is evident in the DPDP Act's phased implementation, which recognises that smaller entities require transition time to implement cryptographic controls.

Savita Vashist, Co-founder of NPST, emphasises that "achieving the Reserve Bank of India's target of one billion digital payments users by 2029 will rely on such inclusive solutions". This vision recognises that cryptographic security that excludes substantial populations is not truly secure—it merely drives excluded users toward less protected alternatives.

### **8.3 Global Interoperability and India's Standard-Setting Role**

India's digital payment infrastructure is increasingly global in ambition. The internationalisation of UPI through bilateral agreements with countries including Singapore, UAE, Nepal, Bhutan, and France creates a foundation for faster, more efficient cross-border

payments. This expansion positions India as a competitive player in the global payments landscape.

The RBI's authentication framework similarly contemplates global interoperability, requiring mechanisms for cross-border card-not-present transactions and expecting foreign merchants to comply with Indian protocols. As Sundareshwar Krishnamurthy of PwC India notes, the framework "signals that India's payment ecosystem is maturing" and may establish global benchmarks.

#### **8.4 The Trust Fabric: Building Continuous Assurance**

The evolution traced in this article—from isolated cryptographic mechanisms to integrated, layered security—points toward what might be termed a "trust fabric": continuous layers of assurance extending from identity through authentication to data protection.

In this model, Aadhaar provides foundational identity verification with biometric cryptographic protection. UPI enables secure payment transmission with risk-based multi-factor authentication. The DPDP Act ensures that personal data collected during transactions receives comprehensive protection with rights-based controls. And the PMLA framework extends anti-money laundering oversight to virtual asset service providers, closing potential regulatory gaps.

Each layer reinforces the others, creating what the National Informatics Centre describes as "systems where personal data protection is not an afterthought, but a design principle". This integrated approach distinguishes India's model from jurisdictions where financial cryptography has evolved more fragmentedly.

#### **9. Conclusion**

India's Contribution to Global Financial Cryptography The evolution of financial cryptography and data security in India offers lessons that extend far beyond the nation's borders. India has demonstrated that a developing economy can leapfrog legacy financial infrastructure to establish world-leading digital payment systems. It has shown that state-led infrastructure development, when properly designed, can foster private innovation rather than crowd it out. It has proven that biometric identity systems can be deployed at population scale while maintaining cryptographic protections. And it has illustrated that comprehensive data protection legislation can balance individual privacy with legitimate data processing needs.

Three distinctive features of India's approach warrant particular attention from the global financial cryptography community.

First, India has prioritised interoperability as a cryptographic design principle. UPI's success rests on its ability to connect hundreds of banks through standardised protocols, enabling network effects that proprietary systems cannot match. This contrasts with approaches where cryptographic protections are optimised for individual institutions rather than systemic connectivity.

Second, India has embedded inclusion in cryptographic architecture. By designing systems that accommodate feature-phone users, preserve multiple authentication pathways, and phase implementation to allow adaptation, India has demonstrated that security and inclusion need not be traded off against each other.

Third, India has pursued regulatory coherence across domains. The alignment of payment authentication requirements with data protection obligations, the integration of cryptocurrency oversight with anti-money laundering frameworks, and the constitutional grounding of privacy rights all reflect recognition that financial cryptography cannot succeed in silos.

As India confronts the quantum challenge, its institutional capacity for coordinated technological transitions, its experience in building national-scale cryptographic infrastructure, and its demonstrated commitment to balancing innovation with security position it potentially for continued leadership. The institutions that succeed in the quantum era will be those that treat cryptographic migration as business continuity rather than technical compliance, that design for agility rather than stasis, and that recognise financial cryptography as the multidisciplinary practice it has always been.

For the global community, India's journey offers both inspiration and practical lessons. It demonstrates that with vision, coordination, and sustained commitment, nations can build digital financial infrastructure that is simultaneously secure, inclusive, and innovative. The padlock icon in the browser, the biometric authentication on the smartphone, the consent manager on the data platform—these manifestations of financial cryptography are increasingly shaped by Indian experience. Their continued evolution will owe much to the distinctive path India has forged.

## References

Binance Square. (2025). India's Cryptocurrency Journey. [online] Available at: <https://www.binance.me/zh-CN/square/post/22914252954226>

- BW Businessworld. (2025). RBI Sets New Digital Payments Authentication Rules, Ends OTP-only Era From April 2026. [online] Available at: <https://www.businessworld.in/article/rbi-sets-new-digital-payments-authentication-rules-ends-otp-only-era-from-april-2026-573192>
- Cointelegraph 中文. (2026). India's Crypto Asset Regulatory Policy Continues to Evolve, Legal Positioning Not Yet Clear. [online] Available at: <https://cn.cointelegraph.com/flash-news/18660713>
- FinTech Futures. (2014). India's Central Bank Pushes for Enhanced Security. [online] Available at: <https://www.fintechfutures.com/cybersecurity/india-s-central-bank-pushes-for-enhanced-security-april-24-2014->
- Global Legal Insights. (2025). Blockchain & Cryptocurrency Laws and Regulations 2026 – India. [online] Available at: <https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/india/>
- IBS Intelligence. (2025). India's Digital Payments Shift Toward Inclusion and Security. [online] Available at: <https://ibsintelligence.com/ibsi-news/indias-digital-payments-shift-toward-inclusion-and-security/>
- Legal500. (2026). The Digital Personal Data Protection Act, 2023: Comprehensive Framework, Latest Developments, and Compliance Roadmap. [online] Available at: <https://my.legal500.com/developments/thought-leadership/the-digital-personal-data-protection-act-2023-comprehensive-framework-latest-developments-and-compliance-roadmap-2/>
- National Informatics Centre. (2025). Building Trust by Design: DPDP Readiness for India's Digital Future. [online] Available at: <https://www.nic.gov.in/building-trust-by-design-dpdp-readiness-for-indias-digital-future/>
- The Economic Times. (2025). Experts Welcome RBI's Digital Payment Authentication Overhaul. [online] Available at: [https://m.economictimes.com/tech/technology/experts-welcome-rbis-digital-payment-authentication-overhaul/amp\\_articles/124321797.cms](https://m.economictimes.com/tech/technology/experts-welcome-rbis-digital-payment-authentication-overhaul/amp_articles/124321797.cms)
- 雷电财经. (2025). Comprehensive Interpretation of India's Crypto Payment Landscape. [online] Available at: <http://web3the.com/news/761055.html>