



**Chintan
Research
Foundation**

POLICY BRIEF NO. 07/2027



GPS .lll 5G

PAYMENT

Credit Card Number*

Cardholder Name*

Expiry Date CCV
 MM/YY

Confirm

INDIA'S DIGITAL ECONOMY

A Policy Review and an
Assessment of Prospects Ahead



SEPTEMBER 2026

ABOUT CRF

Chintan Research Foundation is an independent think tank committed to shaping policy through rigorous research and thought leadership. With a strong focus on fostering collaboration between policymakers and industry, CRF aims to incorporate practical insights into its research and advocacy efforts. It conducts comprehensive research to support informed decision-making and engages with stakeholders through discussions, events, and workshops. By publishing research papers, articles, and op-eds, CRF seeks to address key challenges in India and the Global South, fostering diverse perspectives and contributing to impactful policy advocacy.

For more details: www.crfindia.org

INDIA'S DIGITAL ECONOMY

A Policy Review and an
Assessment of Prospects Ahead

The author would like to thank Mr Sanjeev Ahluwalia, Distinguished Fellow, Chintan Research Foundation (CRF); Mr Abhijit Mukhopadhyay, Senior Research Consultant, Centre for Economy and Trade (CET), CRF; Ms Rutuja Pol, Partner, Ikigai Law; Dr Bidisha Bhattacharya, Associate Fellow, CET, CRF, and Ms Ishita Sharma, Research Intern, CRF, for their valuable contributions to brainstorming and reviewing this report.

This paper draws heavily on the proceedings of a day-long conference titled 'India's Digital Economy: Potential and Prospects', held in New Delhi on 7 July 2026, by the Chintan Research Foundation (CRF) in partnership with Ikigai Law and Koan Advisory Group. Convening economists, regulators, bankers, technologists, and industry leaders, the forum examined India's digital financial rails, cross-border digital payments, digital risk, and cybersecurity, and offered valuable insights into the direction of future policy.

CONTENTS

India's Digital Economy: Past, Present and the Future	1
UPI: From Interoperability to Sustainable Monetisation.....	4
The Future of Digital Currency: CBDC and Stablecoins	8
Cross-Border Payments	12
Digital Fraud – Feeding Off Rapid Digitalisation	
Without Security Safeguards.	14
AI Optimism in India.	18
Conclusion: From Digitalisation to Digital Economic Maturity	19
Policy Recommendations	20

Abstract

India's digital economy has evolved by 'feeling its way across the stones whilst crossing the river', even as it has pursued clear medium-term policy perspectives. This paper charts that trajectory. India first laid a set of foundational digital rails, ranging from identity and bank accounts to connectivity, largely through domestic innovation rather than imported technology. It then demonstrated what those rails could deliver at national scale through the Unified Payments Interface (UPI), which transformed both the economics of banking and everyday financial behaviour. Having revolutionised how money moves, India is now asking a more fundamental question: can the nature of money itself be redesigned, through Central Bank Digital Currency (CBDC) on the one hand, and privately issued Virtual Digital Assets (VDAs)¹ and stablecoins, on the other? There is, however, no official recognition yet of either VDAs or stablecoins as payment instruments.

As digital finance extends across borders, early efficiency gains run into the harder constraints imposed by jurisdiction, regulation, and geopolitical divides. The growing digital economy also faces two primary fault lines: the exclusion of citizens who have not shared equally in its gains, and the vulnerability of those included to fraud, identity theft, and cyberattacks. The next digital frontier, artificial intelligence (AI), sits atop all of this, carrying with it both the potential for India's future economic leadership and an even higher risk of concentration of economic power and exclusion.

The central argument of this paper is that India's digital economy is transitioning from a phase of digitalisation (building access, infrastructure, and scale) to a phase of digital economic maturity. The core issue is no longer whether India can digitalise, but whether it can do so productively and securely, while ensuring that its benefits are broadly and inclusively shared.

Keywords: India's digital economy; digital public infrastructure; UPI; CBDC; Virtual Digital Assets (VDAs); stablecoins; digital financial inclusion; digital regulation

¹ VDA refers to any digital code, number, token, or cryptographic asset that can be stored, transferred, or traded electronically. Cryptocurrencies (e.g. Bitcoin), non-fungible tokens (NFTs), and utility tokens are prime examples of VDAs.

I. India's Digital Economy: Past, Present and the Future

India's digital transformation has moved from building the foundations of access to confronting the harder question of what those foundations can deliver. The journey began with connectivity, identity, bank accounts and institutional capability, but the next phase must be judged by whether digitalisation translates into deeper inclusion, higher productivity and greater economic opportunity.

No One Planned India's Digital Economy

India's digital economy is not the product of a single master plan. Instead, it emerged from the convergence of several favourable developments: the growth of the Information Technology (IT) services sector initially built on wage differentials favouring service exports, sustained investment in engineering education, the Y2K opportunity that gave Indian IT firms an early global foothold, and the expansion of mobile connectivity amid intense telecom competition, which drove data prices down. This was a story of serendipity as much as strategy; a set of forces that happened to align, rather than a blueprint executed in sequence.

What followed, however, was a deliberate build-out. Digitalisation behaves like a non-tradable good: unlike manufacturing capability, which spreads through global value chains and lifts entire regions together, digital transformation does not converge naturally across economies. It must be built domestically, drawing on domestic institutions and capabilities. This explains the wide disparities in digitalisation levels even among close neighbours – the United States (US) is far more digitalised than Mexico; France ranks well above Italy; Singapore leads the Association of Southeast Asian Nations (ASEAN), while Laos, Cambodia, and the Philippines trail behind; and India significantly outperforms its South Asian neighbours, despite shared geography and comparable starting points.

Successful digital transformation rests on strong

'analogue foundations' rather than on imported technology alone: skilled human capital, trusted and accountable institutions, and a supportive investment climate. Weak foundations dampen technology transfer, and thus, the most productive investment for developing digital economies is to build the ecosystem of government, academia, civil society, and business within which digital technology can take root.

Building Roads Rather Than Widening Them

India's Digital Public Infrastructure (DPI) is best understood as an economic institution, not merely a technology stack.² The distinction matters. In developed economies, digital technologies mainly widened roads that already existed: they enhanced the capacity of institutions that were already functioning, extending services to citizens who already had some form of access to financialisation. India's task is different: it is building the roads digitally, and creating entirely new opportunities for millions of citizens who were previously excluded from the formal economy altogether.

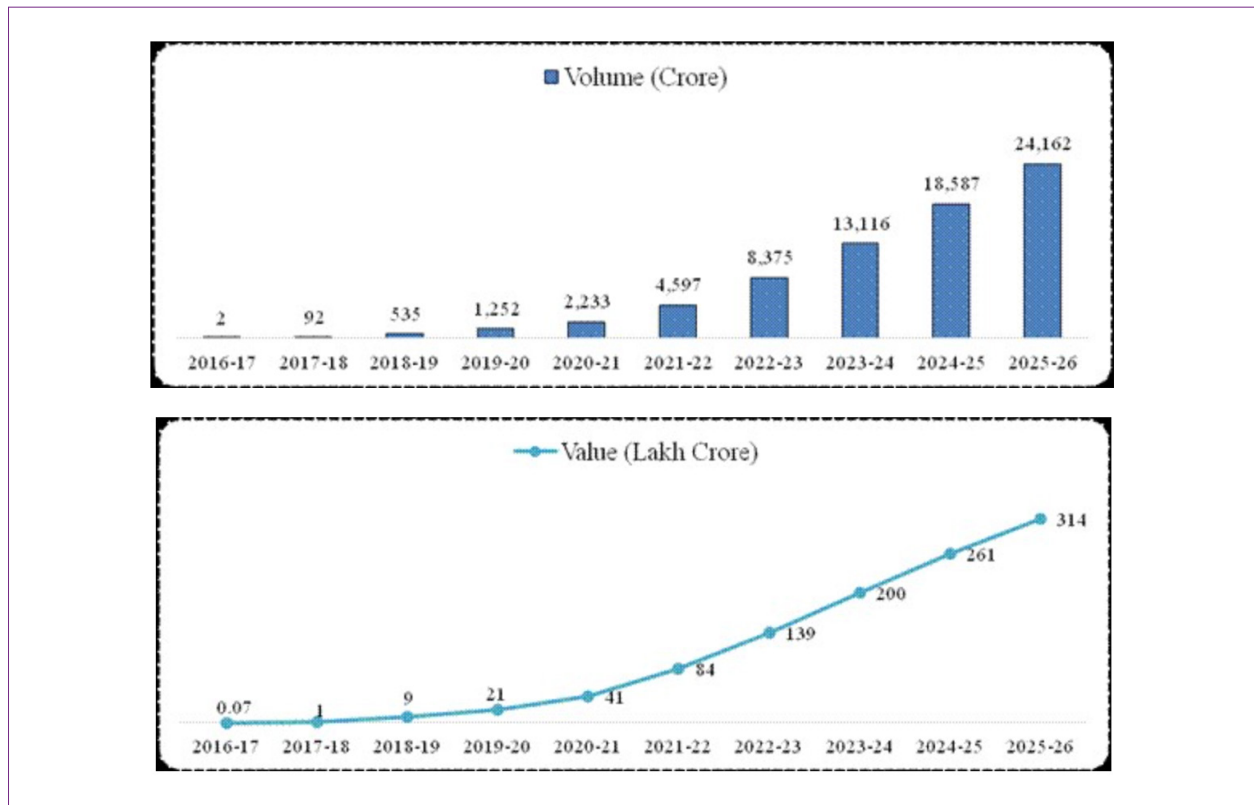
Digital infrastructure in the form of Jan Dhan bank accounts, Aadhaar digital identity, and the rapid expansion of mobile phone penetration coupled with falling data prices has reduced transaction costs, expanded market participation, improved economic efficiency, and materially increased financial inclusion (Figure 1).

Digital outreach seeking to export India's successful DPI model must distinguish between exporting the DPI stack, which is tuned to India's institutional arrangements, and exporting the principles on which each country can create its own supportive institutions and accompanying software. What made India's model work was chiefly trust, transparency, credibility, and legitimacy, and these outcomes would need to be replicated in exported clones working in different institutional environments. India's digital success comes with caveats: the risk of 'digital determinism' or 'digital solutionism' – the belief that technology

² DPI comprises an identity layer, a trust layer, a storage layer, and a transaction layer.

can resolve any policy challenge without institutional support – is naïve. Failures in critical layers such as identity verification, biometric authentication, consent systems, or basic connectivity can just as easily exclude citizens from essential services as include them.

Figure 1: Unified Payments Interface (UPI) Transactions Growth Trend



Source: Ministry of Finance (2026b)

The Inclusion Paradox

DPI, built without sufficient customisation to ensure inclusion, can become an instrument of unintended exclusion via a failed authentication, an unregistered device, or a consent flow nobody explained.

India has achieved remarkable scale in digital adoption. The harder challenge is deepening its reach. Research shows that while most households own a mobile phone, only a small proportion have access to computers, laptops, or tablets; over one quarter of households remain entirely offline, and around one in five households still require assistance to access the internet at all (Press Trust of India 2026).

Persistent gender gaps in independent access to and use of digital technologies further cloud this picture.

Women from more patriarchal social settings may be less confident in using digital technologies, which limits their ability and willingness to adapt to rapidly evolving digital systems. Survey evidence suggests that cash usage among women has actually risen in some rural areas even as digital payments continue to expand nationally, offering a striking counterpoint to narratives of uniform digital progress (Smile Foundation 2025). Trust and concerns around fraud continue to influence payment choices, particularly among rural women, highlighting dimensions of digital exclusion that aggregate adoption and transaction statistics alone cannot capture. Similarly, older adults show particularly low levels of independent internet use despite widespread smartphone ownership. Device penetration statistics conceal this gap between functional digital capabilities and device access.

'Functional Digital Inclusion' extends well beyond internet availability to ensure equitable access across gender and age groups, access to multiple devices rather than phones alone, and the digital literacy and confidence to move to digital transactions. It will not happen automatically without investment in high-quality education, digital skills, and reliable broadband connectivity. During the COVID-19 pandemic, unequal access to connectivity and digital infrastructure measurably widened learning gaps: nearly 826 million students – roughly half of all learners worldwide – were kept out of the classroom for want of access to a household computer or internet connection (UNESCO 2020).

A critical evidence gap deserves attention. India has extensive data on the *growth* of Unified Payments Interface (UPI) transactions, but comparatively little evidence on their *social impact*. Whether digital payments have genuinely improved inclusion among women and the aged, whether previously unbanked populations are meaningfully using digital payments, which regions have benefited most, and many more such nuanced questions remain conjectures rather than statistically supported conclusions. The government's own data machinery only partly closes this gap. Census 2027 will, for the first time, ask households how many bank accounts they hold. However, that measures possession, not participation, and says nothing about whether that account is actively used (MGMMTeam 2026). A Department of Financial Services (DFS) study released in February 2026 came closer, finding UPI preferred over cash among surveyed users, with adoption skewed young; but it was a one-off, scheme-specific evaluation, not a recurring, disaggregated instrument (Ministry of Finance 2026a). So while the evidence gap is being narrowed at the edges, it is not yet fully closed.

At the macro level, digitalisation lowers transaction costs for most citizens. At the micro level, however, those excluded from digital systems often face significantly *higher* costs in accessing government services. Closing this gap requires not only expanding access but also ensuring that citizens have effective recourse when digital systems fail them. Public

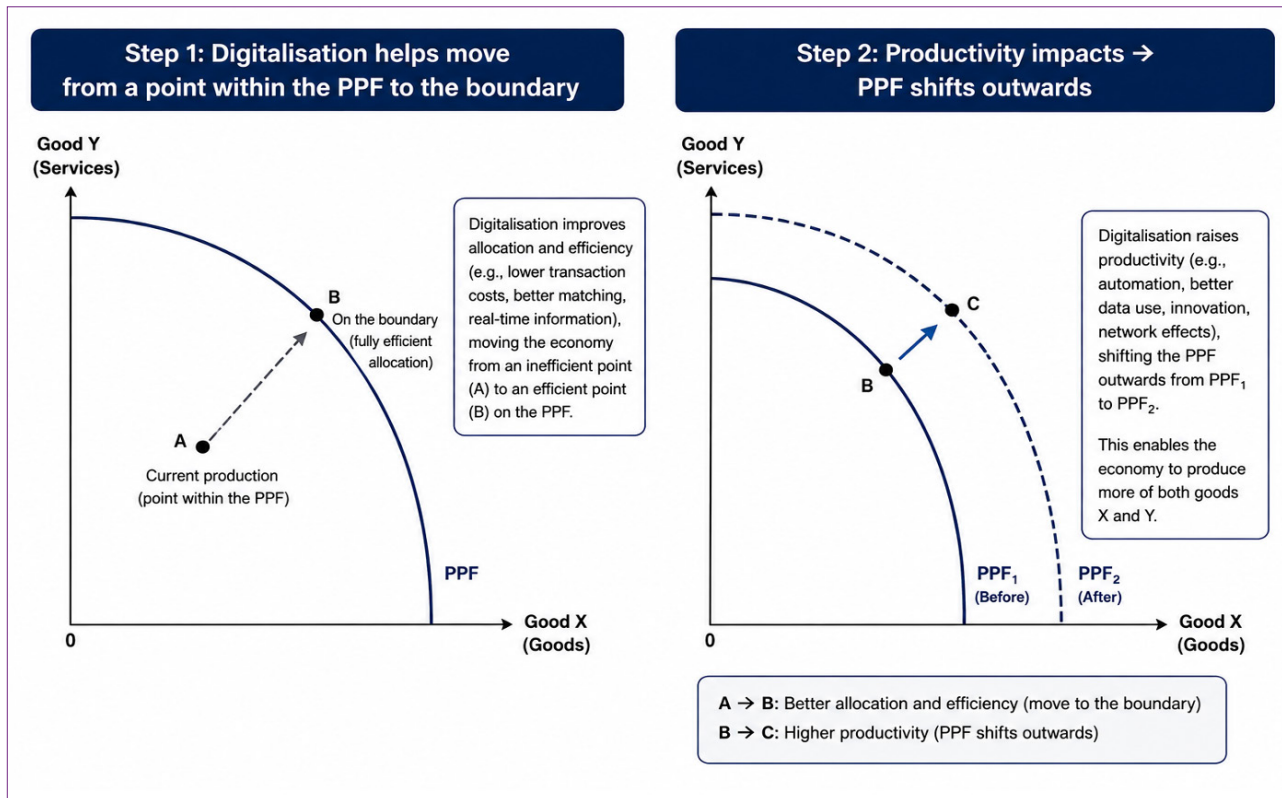
investments in strengthening grievance redressal systems and expanding access to proactive, efficient, accessible mechanisms are critical. To be fair, considerable progress has been made. Government ministries and regulators now monitor complaints more closely through digital grievance platforms, and regular performance reviews are fostering healthy interdepartmental competition. Resolution has thus become faster, more transparent, and more accountable than in the past, even as further improvement remains necessary.

From Efficiency to Productivity

India has already banked substantial efficiency gains from digitalisation; reduced transaction costs and faster service delivery are visible and measurable. But have these efficiency gains translated into productivity gains? This is the more difficult frontier, and the more consequential one: efficiency accumulates, but the accumulation of inputs (i.e. labour, capital, and infrastructure) is subject to diminishing returns. Productivity growth requires shifting the frontier itself, achievable only through investment in research and development (R&D), compute capacity, and innovation ecosystems.

This reframes the task ahead. The best market benchmark of productivity enhancement is export competitiveness. India must move beyond being primarily a consumer of digital technologies and become a producer and exporter of sophisticated digital products and services. The digital dividends India has already captured through leapfrogging, by skipping older generations of technology entirely, were unusually large precisely because they came from a low base. By their nature, these gains are subject to diminishing returns to scale. The next phase of growth cannot rely on leapfrogging alone. It requires complementary investments in R&D, data infrastructure, and skilled talent.

Figure 2: The Two-Stage Impact of Digitalisation on Economic Productivity



Source: Author's compilation; image generated using AI

Digital technologies, in the end, are only ever as effective as the foundations supporting them. This is the frame that carries directly into the rest of this paper: having built broad-based digital access, India's task now is to extract maximum value from that access. And the clearest demonstration of what is possible sits in the story of UPI.

II. UPI: From Interoperability to Sustainable Monetisation

If India's broader digital transformation built the roads, UPI demonstrated what could happen when those roads were made interoperable and used at national scale. Its first decade has been defined by rapid adoption, low-cost transactions and a fundamental change in how Indians interact with money. The challenge now is to ensure that this scale translates into a payment ecosystem that is competitive, resilient and commercially sustainable.

A Decade of Interoperability and Scale

UPI has now completed nearly a decade of scaled-

up operation and stands as one of India's most consequential digital innovations alongside Aadhaar, itself among the country's most successful global technology products. Its first decade was defined by two achievements: interoperability, allowing any bank account to transact with any other through a common rail, and massive scale, now reaching virtually every corner of India's retail economy.

The efficiency case is grounded in measurable outcomes. India's banking system today operates at a cost-to-income ratio of roughly 47–48.5 per cent, better than the global average of 52–55 per cent, and more efficient than banks in the US and much of Europe, though China and parts of the Middle East perform better still. UPI's expanding footprint also helps explain the slowdown in legacy bank branch networks and a decline in ATM numbers, as digital payments replace physical banking infrastructure. On the customer-service side, public grievance platforms facilitate easier resolution.

UPI is a standard bearer for India's frugal

innovation. The National Payments Corporation of India's (NPCI's) operating cost is roughly 10 paise per transaction, of which around 5 paise is spent on marketing and processing, across well over 20 billion transactions annually. By comparison, the US FedNow system reportedly required more than USD 500 million to implement. The natural next step is to globalise this innovation, which will likely reduce the cost of cross-border payments and integrate UPI clones into international banking systems.

Exporting Infrastructure, Not Just an Application

Exporting digital payments is not about exporting a product; it is more about adapting the product to customer needs. Developed markets operate with different customer behaviour and pre-existing infrastructure. Hence, QR code-based payments might not naturally displace contactless card systems already embedded in consumer habits. A more useful target is to export a custom-made UPI, compatible with the institutions, regulations, and payment ecosystems of the importing jurisdiction. What is genuinely exportable is not the product but the underlying concept: interoperability, resilience, and the broader DPI construct. In other words, it is the technical know-how and institutional design principles that benefit an entire economy, not merely the application layer sitting on top of them.

This distinction becomes clearer when UPI is compared with Aadhaar. The Government of India has signed Memoranda of Understanding (MoUs) with 23 countries for sharing or cooperation on India Stack / DPI, primarily for replication and adoption of India's digital governance platforms. A technology such as Aadhaar is relatively easier to export because digital identity systems are typically government-led, whereas payment ecosystems are deeply intertwined with existing commercial infrastructure, consumer behaviour, and market participants. The adoption of common global standards is a necessary precondition for global adoption. 'Identity Passportisation' is the potential for a digital identity verified in one country to be

trusted and recognised across borders. Realising such possibilities requires agreement on shared platforms and standards through which information can be securely transferred, authenticated, and validated across jurisdictions.

UPI-like systems may find greater traction in developing economies than in mature markets with embedded and functional legacy systems. India's UPI and Brazil's Pix are cases in point of developing country innovation. Yet even here, replication is not simply a matter of adopting the same technology. UPI's own success was enabled by a particular configuration of complementary capabilities – Aadhaar, widespread mobile penetration, government support, and the Direct Benefit Transfer (DBT) architecture. Countries seeking to develop comparable systems will need to build or adapt these enabling conditions to their own institutional and economic contexts.

The opportunity for India, therefore, extends beyond exporting a payment application. The NPCI's work in areas such as fraud management, cybersecurity, and payment resilience is already shaping the development of capabilities and standards with relevance beyond India's borders. This reputational and institutional export may ultimately prove as important as the technology itself. India can contribute not by offering a one-size-fits-all solution, but by demonstrating how interoperable infrastructure and institutional design can work together to build digital payment systems at scale.

The Risks Created by Scale

India's payment ecosystem is dominated by NPCI and UPI. This can be read as a concentration risk. NPCI represents a concentration risk within the payment ecosystem, while UPI represents the largest concentration risk within NPCI. Just two third-party applications process more than 80 per cent of all UPI transaction volume.³ China also has only two apps that dominate payments, but both are Chinese. Neither Google Pay nor PhonePe is substantively

³ PhonePe and Google Pay process roughly 78 per cent to 82 per cent of all UPI transaction volume in India.

⁴ The initial deadline of 31 December 2022 was first extended to 31 December 2024.



owned by Indian investors. Operational failure, geopolitical disruption, or the failure of a single dominant application are not abstract risks; they are structural vulnerabilities sitting directly beneath India's most important payment rail.

Introduced to curb market dominance by any single player and to ensure a competitive and equitable UPI ecosystem, the NPCI's proposal to cap any single third-party application's UPI market share at 30 per cent remains, notably, unimplemented and has been extended to 31 December 2026.⁴ It is unclear whether a top-down directed market cap is the best way to promote competition. Other options include increasing the profitability of such businesses, thereby incentivising more Indian apps to compete.

Between 2004 and 2016, India rolled out several new payment systems.⁵ Since UPI's 2016 launch, however, innovation has largely been confined to newer versions of UPI itself rather than newer payment instruments. The New Umbrella Entity (NUE) proposal of 2017, which was never intended to create a new payment product, but rather to license two or three additional operators implementing common standards to reduce concentration risk, has not fructified (Moneycontrol n.d.).⁶

A workable alternative remains available:

- multiple licensed payment operators,
- common messaging and communication standards,
- mandatory bank connectivity to all payment networks (e.g. for banks above a certain customer threshold),
- commercial freedom for banks to choose transaction routing, and
- automatic failover to alternative networks during outages.

This redundancy, rather than any single new product, is what would meaningfully strengthen resilience.

None of the above is possible without the payments business becoming viable through mechanisms other than data access or the development of adjacent markets like credit or trade benefits. A pain point in the digital ecosystem is the Merchant Discount Rate (MDR). Zero MDR remains publicly popular, yet commercially unresolved. UPI was designed primarily as public digital infrastructure meant to deliver societal benefit, rather than direct profit- a version of *compassionate capitalism*, where social benefit is a primary objective rather than a byproduct. The government reimburses banks for UPI transaction costs – in effect, an annual subsidy. Fintech companies operating on UPI were aware

⁶ NUE is a framework proposed by the RBI to set up private, pan-India retail payment systems that compete with the NPCI.

from the outset that MDR is zero and were expected to build revenue through adjacent services such as lending and credit products, merchant hardware such as soundbox devices, and other value-added offerings built on top of the rail rather than through the payment itself.

A payment system requiring near-perfect uptime cannot be solely dependent on subsidy without market-based revenue to sustain world-class resilience. A system, especially one that demands continuous evolution, cannot simultaneously remain entirely free for everyone and maintain that resilience without adequate commercial incentive somewhere in the chain. To this end, the government has amended the Payments and Settlement Systems Act 2007, allowing for the levy of MDR on transactions other than P2P and only on transactions above Rs 2000 in value. The government further gives its assurance that the levy will be nominal (Ministry of Finance 2026c).

From scale to resilience and fraud prevention: UPI handles roughly 90 per cent of India's digital payment transactions, a clear demonstration that it has already achieved scale. Uninterrupted availability is now a matter of systemic importance rather than just customer convenience. Outages demonstrate the need for stronger backup systems and automatic failover capability. The rise of what might be called 'Fraud-as-a-Service', that is, organised, commoditised fraud infrastructure available to bad actors at scale, could make AI-driven, proactive fraud detection one of the central priorities for the system's next phase (a theme this paper returns to in Sections V and VI).

Remittances and the Wider Payments Landscape

India's remittance economy adds further weight to the case for reforming cross-border payments. V. Anantha Nageswaran, Chief Economic Advisor,

Government of India, projected in early 2023 that the economy would reach USD 7–7.5 trillion within seven years, a trajectory the Ministry of Finance's own economic review has since reiterated (Press Trust of India 2023; Department of Economic Affairs 2024). Formal remittance inflows, meanwhile, are on a similarly steep trajectory: India received a record USD 137 billion in remittances in 2024, the highest of any country in the world, and that figure is expected to keep climbing well beyond current levels. Whatever the eventual scale, the speed, efficiency, and cost of international money transfers will meaningfully shape economic activity. Delays in crediting remittances impose real costs on recipients and the wider economy, whereas faster and cheaper settlement allows more funds to enter legitimate and productive use, including funds that might otherwise move through informal channels such as hawala, whose true scale is inherently difficult to measure precisely but has, on some estimates, rivalled formal remittance flows.⁷

Recent initiatives demonstrate that legacy payments and transfer systems are fighting back and raising the efficiency bar for digital transactions. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) streamlined purpose codes for remittance payments between India and Australia, reducing the time required for a transaction from 24 hours to just 37 seconds (Standard Chartered 2026).

As cross-border payments grow in scale and diversity, the inclusivity of the institutional architecture supporting them will also need to be enhanced. International payment-messaging infrastructure typically operates through bank-owned cooperative structures. Greater representation of emerging economies in their governance can accelerate harmonisation of standards and procedures. India's growing participation in these institutions signals a broader shift from being primarily a user of global

⁷ Estimates of hawala's scale vary widely given its undocumented, informal nature. Older Interpol estimates have placed it as high as 40 per cent of India's GDP, though such figures are dated and disputed rather than independently verified. What is measurable is that formal channels captured a record USD 137 billion in remittances in 2024 (World Bank data) – and that narrowing the cost and speed gap with formal settlement is one of the more direct levers available for pulling flows away from informal channels.

payment standards towards playing a more active role in shaping them.

The cross-border payments ecosystem is also becoming more diverse, with platforms such as Razorpay, Payoneer, PayPal, and Stripe facilitating international transactions alongside traditional banking channels. As settlement times continue to compress, the policy challenge will be to ensure that regulatory frameworks, payment infrastructure, and institutional coordination evolve at a comparable pace.

Once a digital system becomes as systemically important as UPI, the central question shifts from adoption alone to sustainability, competition, and resilience. That shift in turn raises the next question this paper addresses: if the payment system is digital, can money itself be redesigned? The answer brings Central Bank Digital Currencies (CBDCs) and privately issued digital money, particularly stablecoins, into focus.

III. The Future of Digital Currency: CBDC and Stablecoins

UPI changed the way existing money moves; the next frontier asks whether money itself can be redesigned. Central Bank Digital Currencies and privately issued digital assets, particularly stablecoins, represent two fundamentally different responses to this question. For India, the challenge is not simply technological adoption, but determining where new forms of digital money add genuine value alongside an already highly effective payments infrastructure.

CBDC's Current Value Proposition

In India, the CBDC's value proposition is put in the shade by UPI's ubiquity, including among small merchants at around 94 per cent. Consumers receive the benefits they need through UPI while continuing to earn interest on bank deposits. CBDC, as currently constituted, offers little additional value for everyday users.

India positions CBDC as a sovereign-backed digital

currency. This is in deliberate contrast with the US, where private instruments such as PayPal balances and dollar-backed stablecoins occupy much of this space. CBDC in India is intended to complement UPI rather than replace it, with a larger prospective role reserved for more specialised applications such as cross-border payments and wholesale financial transactions. The availability of UPI in India allows a more deliberative introduction of CBDC than might otherwise have happened.

Use Cases Worth Taking Seriously

The case for CBDC in everyday retail payments, albeit limited, does not imply an absence of meaningful use cases. More than 26 countries are currently piloting CBDCs, including India. CBDCs are being actively developed for wholesale settlement, programmable money, and participation in a globally interoperable financial network. Programmable CBDCs are specifically being explored for delivering welfare schemes and direct benefit payments. This remains an exclusive application area where privately issued stablecoins currently have no equivalent role and are unlikely to develop one, given the public-purpose nature of welfare disbursement.

Trust and consumer protection are meaningful differentiators for CBDC. The digital rupee carries greater public trust because it is issued by the central bank and offers the strongest consumer protection. The trade-off is that this stronger protection than even a bank fixed deposit (beyond ₹5 lakhs) – CBDC being a Reserve Bank of India (RBI) liability – must be weighed against the interest lost because CBDC wallets do not pay interest. For transactional needs, UPI is unmatched at zero cost. This is a key reason for limited domestic uptake, even as the RBI continues to actively experiment with pilots.

Why CBDCs Have Not Scaled

Two distinct causes explain the limited scaling of CBDCs in India, and they are worth separating clearly because they call for different responses. The first is a lack of a compelling domestic use case: India's existing digital payment infrastructure, especially UPI, already meets most retail payment needs, so CBDC currently addresses a problem that

has largely already been solved by other means. The second is the **institutional symmetry required for cross-border adoption** based on cooperation from multiple countries.

The Reserve Bank of Australia and the Bank of Canada have both slowed or reconsidered retail CBDC initiatives; the US Federal Reserve has publicly questioned the need for a retail CBDC altogether, with the US instead emphasising stablecoins as part of its broader financial and geopolitical strategy. For India, a successful cross-border CBDC would require participation from other major trading partners. The challenge is geopolitical rather than technical.

The deeper point, applicable to both CBDC and cross-border payment infrastructure more broadly, is that the **real challenge is rarely the technology of creating digital tokens. It is network effects**, which enhance the value of a product or service for each user as the number of users increases. Cross-border networks additionally require alignment across jurisdictions, shared standards, and interoperability between otherwise disparate financial systems. Distribution and network-building, not token engineering, are the binding constraints.

VDA and Stablecoins: A Necessary Distinction

UPI transformed how existing money moves. CBDCs change the nature and functionality of money. This is where the digital-money universe diverges for the State and for users.

- (1) The state's response to this is CBDCs, which retain State/RBI centrality.
- (2) The private sector response is VDAs and stablecoins, which lie outside the traditional sovereign monetary framework.⁸

VDAs and stablecoins are conceptually and practically different, even though they are frequently used interchangeably. Stablecoins are a subset of VDAs. From a financial-regulatory standpoint, the central

concern is the money-laundering and terrorist-financing risk associated with these technologies. From this regulatory perspective, both should be regulated using two complementary principles: **technology neutrality and risk-based assessment**. If a VDA and a stablecoin have similar risk profiles, they should be regulated similarly; where their risk profiles diverge, so should the regulations.

A further distinction is necessary between VDAs such as digital art and collectibles, unbacked crypto assets such as Bitcoin, and stablecoins or other asset-backed tokens. Unlike stablecoins and asset-backed tokens, Bitcoin is not linked to any currency and does not carry issuer redemption risk. It has a fixed maximum supply of 21 million coins, giving rise to valuation dynamics that differ fundamentally from conventional sovereign money.

The Monetary Impact of 'New Privately Issued Money Like Digital Assets'

A vexed issue related to the use of stablecoins or crypto assets like Bitcoin is that they bypass the monetary authority of the central bank. If privately issued and non-INR-backed stablecoins were to achieve widespread adoption for cross-border payments, they would directly affect the Balance of Payments, which would in turn bear on domestic monetary conditions and central banks' ability to influence the supply and circulation of money. It would also weaken the ability of banks to fund their assets via the fractional reserve system they presently use to 'create money out of thin air' on the assumption that not all depositors will ask for their deposits to be encashed simultaneously or, if they do, the central bank will provide them liquidity.

This concern helps explain the cautious regulatory approach adopted by governments around the world. Rather than formally recognising cryptocurrencies as currency or banning the underlying technology outright, regulators have largely sought to 'ring-fence' the ecosystem, containing its financial and

⁸ The RBI does not recognise VDAs or stablecoins as payment instruments. Nor are they regulated by any other regulatory authority in India.

illicit-finance risks while allowing the technology and associated markets to continue developing. The resulting regulatory ambiguity is therefore not necessarily a sign of indecision; it reflects uncertainty about the eventual role that privately issued digital assets may play within the monetary and financial system.

Coexistence, Not Replacement

Emerging use cases already point towards complementarity rather than exclusivity. Programmable CBDCs have potential applications in welfare and direct-benefit delivery. Dollar-backed stablecoins, by contrast, currently show a stronger practical proposition in cross-border payments, particularly where they can reduce settlement frictions and facilitate transfers across jurisdictions.

The question of whether CBDCs and stablecoins *can* coexist, however, is distinct from the normative question of whether they *should*. Coexistence raises questions around monetary sovereignty, financial stability, competition, consumer protection, and regulatory oversight that cannot be resolved simply through technological interoperability. The appropriate policy framework will therefore need to distinguish between the technical possibility of multiple forms of digital money operating alongside one another and the broader question of what role privately and publicly issued digital money should ultimately play within the monetary system.

The Architecture Behind Stablecoins

Stablecoins are best understood as tokenised assets backed by real underlying reserves (cash or cash equivalents), a fundamentally different structure from most other digital assets, which typically lack any such backing. Stablecoins combine the benefits of blockchain technology with traditional financial compliance frameworks: they retain the ability to freeze wallet balances, implement regulatory controls, support transaction traceability, and maintain a meaningful degree of anonymity, all while operating on global, neutral blockchain networks (e.g. Ethereum) that are not controlled by any single country. This combination of global interoperability and regulatory compliance is the central reason for

stablecoins' rapid global adoption, and financial regulation built up over decades to address risk and close loopholes is, in effect, being absorbed into this new architecture rather than discarded by it.

Perhaps the most useful conceptual frame for understanding stablecoins' current trajectory is the comparison to a digital-era equivalent of the Eurodollar system. Most major stablecoins are USD-backed, functioning as a modern instrument of dollar-denominated liquidity operating outside the direct control of the US banking system; much as Eurodollars historically operated outside US jurisdiction while still denominated in dollars. Stablecoins have evolved well beyond their original role as a store of value and an on-ramp into VDAs; they are now independent payment and settlement infrastructure, functional payment rails, no longer simply a bridge to speculative crypto assets.

Although technically stablecoins are a subset of crypto assets, they (especially Bitcoin) are practically different due to the fact that stablecoins (at least the well-known ones) have a dollar value. As a result, stablecoins and cryptocurrency assets have distinct uses and markets, and therefore, distinct regulatory frameworks are also necessary for these.

Stablecoins emerged specifically to address the lack of trust and high volatility associated with cryptocurrencies, functioning as a bridge between crypto and fiat currency. The overwhelming majority remain pegged to the US dollar, underscoring the continued global dominance of the dollar despite challengers on the horizon. That stablecoins have gained currency so quickly illustrates the demand for global certainty. Modern financial systems favour market-determined exchange rates, yet stablecoins rely on fixed-value pegs, typically mostly to the dollar, which itself has a special status as a reserve currency, because of the dollar's unmatched global acceptance and liquidity linked to the depth and transparency of its financial markets. Europe's parallel effort to develop euro-backed stablecoins is less endowed with comparable network effects.

This produces a useful summary contrast:

Table 1: CBDCs, Stablecoins, and Crypto Assets – Key Differences

	CBDC	Stablecoin	Crypto Asset (e.g. Bitcoin)
Issuer	Sovereign (central bank)	Private entity	No single issuer (i.e. decentralised, protocol-based)
Structure	Centralised, public	Technology-enabled, potentially global	Decentralised, no backing entity
Current	Wholesale settlement, DBT, welfare payment	Largely absent domestically; strongest use case is cross-border	Primarily speculation and investment; not used for payments given regulatory ambiguity and tax treatment
Trust basis	Central-bank backing	Reserve backing + compliance architecture	Protocol design and market confidence, with no reserve or sovereign backing

Is There a Domestic Use Case for Stablecoins?

The INR is not freely tradable, which inhibits its status independent of RBI management. Given how effectively UPI already serves retail person-to-person and person-to-merchant payments, the use case for a private digital domestic currency has not yet been made. Cross-border payments might represent a more plausible application, given India's position as the world's largest inbound remittance market, where it would compete with legacy systems and UPI, if it is globalised.

Regulatory Coordination on VDAs and VASPs: A Future Need

As privately issued digital assets become increasingly integrated with the broader financial system, the challenge is not simply to determine their permissible uses, but to ensure that the entities facilitating their issuance, exchange, custody, and transfer operate within a coherent regulatory framework. This makes coordination across jurisdictions and between regulators particularly important, bringing the focus to the regulation of Virtual Asset Service Providers (VASPs).

India's Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) framework already applies substantially to this ecosystem. VDAs and VASPs are regulated by the Financial

Intelligence Unit-India (FIU-IND), and a growing number of domestic and foreign VASPs have already registered. Because VASP registration under the Prevention of Money Laundering Act (PMLA) is based on activities performed rather than physical location, India's legal framework is, in principle, well suited to regulating offshore VASPs, even though practical enforcement (discussed in the next section) remains a challenge.

VDAs must also be declared for tax purposes, and while some users currently believe they can avoid detection if tax deducted at source (TDS) is not captured on a given transaction, this apparent arbitrage is illusory: undeclared VDA holdings surface eventually, even years later, once a taxable transaction occurs, at which point the earlier non-disclosure becomes visible and actionable.

A significant share of the ecosystem is presently regulated in ways not always visible to the holder of such assets. VASPs must already comply with AML/CFT obligations, Know Your Customer (KYC) requirements, customer due diligence, Suspicious Transaction Reporting (STR), and beneficial-ownership verification, and the Income Tax Department has already established a taxation framework for VDAs. Regulation here is not an obstacle to be minimised. It is central to protect

holders of VDAs and strengthen trust.

The need for comprehensive and collaborative international enforcement is what carries the discussion into this paper's next theme: once digital money, whether public or private, crosses a border, regulation, jurisdiction, and geopolitics cross with it.

IV. Cross-Border Payments

The transformation of digital finance does not end at the national border. As payments become faster and digital forms of money become more sophisticated, the next challenge is to carry the efficiency of India's domestic digital infrastructure into international transactions. Here, however, technology is only part of the problem: interoperability, regulation, liquidity, jurisdiction and geopolitical interests determine how quickly borders can become less relevant to the movement of money.

The Search for Efficiency

Remittances in India account for USD 155 billion, or about 14 per cent of receipts in the current account and 4 per cent of GDP (FY2026). A single day's reduction in transfer time delivers benefits of USD 30 million at 7 per cent interest per annum to the sender and the receiver – a benefit that is presently shared by intermediary banks in the supply chain. Remittances through legacy systems take between two and four days from the US to India.

The obstacles to faster cross-border payments are trust, policy, and interoperability convergence between countries, and the self-interest of banks in legacy systems. Digital technology already exists, but institutional change invites political economy barriers – vested interests and resistance to change. Reducing a day-long settlement window to well under a minute, as India's own recent bilateral experience has shown, is achievable if processes and standards between two systems are aligned.

Within-country operational reform is urgently required. Indian banks wait until end-of-day batch reconciliation before notifying customers of incoming remittances. Many developed countries

match payment messages in real time, informing customers immediately when funds arrive. Reform is kicking in. India is expected to move to real-time processing in October 2026 (UNESCO 2020). A complementary '*positive pay*' facility for cross-border remittances would allow exporters to pre-register expected incoming payments, so that banks already have the required information and can credit funds instantly rather than processing them through a delayed batch cycle.

On capital-control reform, several processes, including issuing Foreign Inward Remittance Certificates (FIRCs), remain incongruously manual given India's existing strength in DPI. Automating these procedures is a natural next step.

G20 cross-border payment research indicates that liquidity remains one of the largest contributors to transaction costs in international payments, and that reducing liquidity requirements could significantly lower the overall cost of cross-border transfers. Where payment providers can anticipate recurring flows in advance, they can maintain liquid reserves ahead of time rather than sourcing liquidity reactively, materially reducing costs. Proactive regulation and competition from digital payment options are the best drivers to nudge banks to improve treasury management and pass on the benefits to consumers.

As payment flows become faster and more integrated, the infrastructure, standards, legal frameworks, and jurisdictional arrangements governing them must evolve in parallel. Successfully globalising financial transaction systems therefore rests on four essential pillars:

- (1) Building integrated financial infrastructure
- (2) Harmonising procedures and technical standards across countries rather than relying solely on bilateral arrangements
- (3) Ensuring congruence in legal frameworks, where countries' laws align in intent even where they are not identical
- (4) Establishing clear, unambiguous jurisdictional frameworks to govern cross-border financial transactions

Governments and regulators prioritise sovereign concerns within this architecture. Preventing money laundering, combating terrorist financing, and building effective grievance-redressal and transaction-reversal mechanisms, particularly for cross-border payments where jurisdictional complexity makes redress harder to obtain. Technological models for seamless payments already exist. The harder work, therefore, lies in addressing the regulatory and security concerns layered on top of them. Much as toll systems evolved from manual collection to automated payment without losing the ability to selectively screen vehicles, cross-border payment systems face the more complex challenge of enabling fast transactions while remaining capable of detecting prohibited activity and enforcing regulatory safeguards, without compromising the efficiency the entire reform effort is meant to deliver.

Rupee Internationalisation

The internationalisation of the rupee is an essential part of India's broader internationalisation agenda. Rupee internationalisation will depend on the stability, growth, and global integration of the Indian economy, rather than on financial infrastructure alone. The central question is the global demand for the rupee – **demand, not infrastructure, will ultimately determine international acceptance and value.**

The RBI's own vision for rupee internationalisation rests on three pillars:

- (1) Expanding international trade,
- (2) Promoting digital integration, and
- (3) Developing and expanding financial markets

All three are valid and necessary, even as technological infrastructure, already largely in place, still requires efficiency improvements at the margin.

Regulatory review is a natural starting point, with the Foreign Exchange Management Act (FEMA) worth examining specifically to ensure it supports smoother financial flows. Any system built to facilitate cross-border financial transactions must allow **two-way, reciprocal flows**, not merely one-directional movement of funds. Making remittances

faster and more efficient so funds reach and benefit the Indian economy more quickly is a legitimate and worthwhile goal; it also implies accepting reciprocal arrangements. In short, is India ready for liberalising cross-border capital controls?

VASPs, Financial Action Task Force, and the Limits of Enforcement

Cross-border regulatory cooperation remains the weakest link in this entire chain. FIU-IND is actively working to bring offshore VASPs into AML/CFT compliance, and this effort has already produced results: out of the 49 registered VASPs, exactly 45 onshore and 4 offshore VASPs have already complied with India's regulatory requirements (Pandey 2026). Yet supervision of offshore VASPs serving Indian customers remains a genuinely difficult regulatory challenge. Even with an appropriate legal framework in place, VASP registration under the PMLA is based on activity performed rather than physical location, making India's legal architecture well aligned in principle to regulating offshore providers. Law enforcement agencies struggle to obtain information from foreign jurisdictions and to investigate cross-border transfers. Financial Action Task Force (FATF) Recommendation 15 requires member countries to identify VASP-related risks, strengthen international cooperation between regulators and FIUs, implement the Travel Rule for virtual asset transfers, and establish effective registration, licensing, and supervision. FATF does maintain a formal review mechanism for this: member countries undergo periodic Mutual Evaluations and report back at the Plenary's three annual meetings, with follow-up assessments tracking progress against identified gaps over time. Even so, these cycles are widely spaced, a single assessment takes over a year to complete, and full follow-up can stretch across several more, and FATF's authority rests on peer pressure and public reporting rather than direct enforcement power over any member state.

Domestically, inter-agency cooperation functions considerably better. FIU-IND, the Ministry of Finance, and the Ministry of Home Affairs work closely on crypto-related regulation and enforcement; the Indian Cyber Crime Coordination Centre (I4C)

monitors emerging cybercrime trends and VDA misuse; and 'FIU 2.0' enables real-time dissemination of intelligence, alongside regular FIU-IND outreach to law enforcement agencies and financial institutions. This domestic coordination has directly contributed to a growing number of successful investigations involving virtual digital assets. Making it compulsory for offshore VASPs to establish a local presence or local incorporation in India, with assured reciprocal requirements for Indian VASPs, is one step to materially improve regulatory oversight and enforcement.

Domestic VASPs already comply with TDS obligations, company registration requirements, information-sharing requirements, and consumer protection obligations that offshore providers largely avoid even while meeting FIU-IND's AML/CFT requirements. This regulatory imbalance remains one of the industry's central unresolved challenges, and one that a level playing field, achieved through comparable standards for domestic and offshore providers alike, would meaningfully address. Encouragingly, this gap appears to be narrowing gradually as global compliance standards converge and regulators across jurisdictions adopt increasingly similar approaches to supervising virtual assets.

The blockchain and cybersecurity ecosystem underpinning this activity continues to mature in parallel. Cybersecurity evolves alongside blockchain technology in a continuous cycle: every major technological innovation creates new risk even as it generates lessons that improve security. As the pace of innovation in decentralised finance (DeFi), wallets, stablecoins, smart contracts, and NFTs has slowed somewhat compared to earlier years, the industry has focused on strengthening security across each of these areas. Traditional financial institutions are increasingly entering the blockchain ecosystem and contributing expertise in governance, risk management, operational controls, security frameworks, and compliance. The convergence of blockchain innovation and mature financial-sector governance is, on balance, making the industry stronger.

The narrative arc of *efficiency*, then *complexity*, and then *regulatory challenge* sets up the deliberate

pivot this paper takes next: away from technological optimism altogether, and towards the harder question of 'who is actually benefiting from all of this, and who is being left exposed'.

V. Digital Fraud – Feeding Off Rapid Digitalisation Without Security Safeguards

Success in expanding the digital economy breeds its own **vulnerabilities**. As more users transact digitally, dependence on digital infrastructure increases, and so does the potential impact of fraud, system failures, and other forms of digital harm. Inclusion and security must therefore be treated as complementary objectives. Expanding participation without strengthening the safeguards around digital systems can leave newly connected users disproportionately vulnerable.

Digital fraud has evolved from relatively simple scams into sophisticated social engineering attacks. Frauds such as spoofed calls, phishing links, and manipulation that span multiple layers of the digital ecosystem make it very difficult for a single institution to plausibly solve the problem alone. While stronger banking systems, faster response mechanisms, and stricter regulation all matter, the human element remains the single biggest vulnerability, which makes improved digital literacy the most durable long-term solution, alongside safeguards designed to reduce the chances of users unintentionally harming themselves during this ongoing transition.

In this sense, consumer education is the single most important lever for reducing fraud. Alongside strengthening internal cybersecurity practices, large-scale awareness campaigns on phishing, fake websites, and impersonation matter considerably. Three coordinated gaps require joint action across the ecosystem: **digital literacy, interoperability between systems, and jurisdictional coordination across agencies**. Within this, individuals, industry, and government all carry meaningful responsibility for closing them.

Moreover, two structural bottlenecks confront state-level investigation of cross-border digital fraud specifically:

- (1) **Jurisdictional Fragmentation:** Fraud funds move rapidly across states and international borders, while police jurisdiction remains largely state-based, slowing both investigation and inter-agency coordination.
- (2) **Sound Legal Provisions Not Matched by Investigative Capacity:** The IT Act (drafted, notably, with an orientation towards liberalising the IT sector rather than enabling enforcement) requires only officers of Inspector rank and above to investigate cybercrimes. Such officers are very limited relative to the caseload. Law enforcement agencies select cases to pursue, leaving substantial cybercrime undetected. In Uttarakhand, roughly 1,500 reported cases of cybercrime resulted in only around 500 being converted into formal First Information Reports (FIRs), purely because of investigative capacity constraints. This underscores that the binding constraint is the number of trained investigating officers available, not the willingness of victims to report.

Offshore, unregulated platforms compound this enforcement gap. The VDA sector is structured so that offshore platforms can legally serve Indian users only if registered with the FIU. In practice, a significant share of Indian crypto trading (roughly three out of every four trades involving Indian users) still occurs on unregistered offshore platforms outside Indian law and taxation. A few operational indicators that reliably signal active targeting of Indian users by such platforms are: **easy availability** through Indian app stores, **marketing and advertising** directed specifically at Indian consumers, and **INR on-ramp and off-ramp facilities** enabling deposits and withdrawals. Addressing only one of these channels is insufficient. Regulators must tackle all three simultaneously.

The European Union's MiCA framework, which limits the 'reverse solicitation' defence (preventing offshore platforms from claiming that customers approached them voluntarily and therefore fall outside local jurisdiction), offers a workable model that India could adapt directly.

The consequences of enforcement action against offshore platforms are also worth noting honestly: reports of India's blocking a set of offshore exchanges resulted in activity surging on the remaining, still-accessible offshore exchanges. Usage climbed by about 77 per cent over a nine-month window in 2024 even as tariffs on the blocked exchanges reportedly rose sharply. This illustrates that enforcement against individual platforms alone, without offering legal alternatives for the underlying demand, tends to *displace rather than eliminate* the underlying illegal activity.

Mule accounts illustrate a similar dynamic of systemic rather than individual failure. Fraudsters have long relied on multiple intermediary accounts to move stolen funds, and such accounts are often willingly rented out by economically vulnerable individuals in exchange for small payments, frequently without full awareness of how they are being exploited. Simply banning mule accounts is unlikely to solve the underlying problem. New account holders will continue to replace those removed. The more durable approach is to trace ultimate beneficiaries by 'following the money' rather than pursuing individual account holders who are themselves often more victim than perpetrator. Financial inclusion is an important public-policy objective. So, clamping down on opening bank accounts is not a desirable response. The RBI, as the regulator, should ensure that commercial banks instead bear greater responsibility for improved customer profiling, stronger monitoring systems, and better identification of suspicious activity patterns.

On the exchange side, FIU-registered platforms rely on transaction-monitoring systems that identify suspicious behavioural patterns rather than isolated transactions. For instance, newly opened accounts conduct unusually large transactions, customers are unwilling to disclose the source of funds, and transactions at times involve accounts already flagged elsewhere in the system. Registered exchanges maintain reasonably strong monitoring mechanisms, but the greater share of problematic activity occurs outside the regulated ecosystem altogether, reinforcing the case for stronger government-industry collaboration alongside

continued consumer education encouraging users towards regulated exchanges and away from private wallets and unregulated platforms. The competitive challenge facing Indian exchanges here is better framed as one of consumer protection and a level playing field than as one of market competition in the conventional sense. Platforms complying with Indian regulation incur significant obligations around KYC, reporting, taxation, and regulatory oversight that many offshore operators simply avoid.

Regulation must also extend meaningfully beyond exchanges to cover adjacent sectors where cryptocurrency functions as a payment mechanism, such as gambling websites, prediction markets, and gaming platforms among them, all of which contribute significantly to fraud risk while typically escaping VDA-specific oversight altogether. Enforcement against individual platforms in isolation is insufficient on its own, since new platforms quickly replace those shut down; stronger oversight of these adjacent sectors, combined with closer government-industry collaboration, is essential to closing this gap durably.

Prevention, Institutions, and the Road Ahead

Prevention deserves considerably greater policy priority than post-fraud investigation currently receives. India must invest more heavily in preventive systems and risk mitigation rather than relying primarily on enforcement after funds have already moved beyond recovery. A cyber fraud insurance scheme, with costs shared between financial institutions and consumers, would help formalise this shared responsibility rather than leaving it undefined. While I4C has meaningfully improved information collection and sharing, enforcement itself remains fragmented across states and agencies, underscoring the case for a dedicated federal cybercrime investigation agency with nationwide jurisdiction, capable of improving coordination across states and international borders in a way that state-based police jurisdiction structurally cannot.

A proposed virtual asset forensics lab, situated appropriately and adequately resourced, could extend the real-time, nationally coordinated model

already functioning reasonably well in banking-sector cybercrime response (through I4C) into the virtual-asset space specifically, offering deeper blockchain forensic capability than currently exists anywhere in the system. Improved information-sharing mechanisms, drawing lessons from CKYC in traditional finance, and enabling lawful information-sharing among regulated private-sector participants while remaining consistent with evolving data-protection law such as the DPDP framework, would strengthen consumer confidence and reduce fraud without necessarily requiring an entirely new layer of sector-specific regulation.

Looking forward, future digital fraud will very likely combine AI, regulatory, and institutional-coordination challenges simultaneously, rather than resolving into any single dominant problem. AI will make fraud considerably more sophisticated by enabling convincing, adaptive social engineering at scale, requiring detection and enforcement capability to evolve in close parallel rather than reactively. Blockchain-based traceability is a genuinely promising countervailing tool here, capable of improving accountability by making fraudulent transactions traceable even years after they occur. This can prove to be a meaningful asymmetry in the defender's favour, if built out properly.

Whether India's proposed Digital Payment Intelligence Platform can do for fraud prevention what UPI did for payments will depend on collaborative intelligence-sharing platforms connecting banks, private institutions, and regulators, with the VDA ecosystem integrated into these initiatives rather than treated as a separate silo. Furthermore, fraud statistics should increasingly be evaluated relative to *transaction volumes* rather than absolute numbers, given that digital transactions will continue to grow regardless. On India-based scam call centres targeting victims globally, it is worth stating plainly that cybercriminals can operate from anywhere while targeting victims across jurisdictions, reinforcing the need for stronger domestic and international cooperation among regulators, law enforcement, financial institutions, and technology platforms alike. In this journey, increased consumer awareness,

vigilance, and compliance remain, in the end, one of the strongest and most durable defences available against digital fraud of every kind.

Cybersecurity, Enforcement, and Regulation

The broader cybersecurity conversation has shifted meaningfully over roughly the last fifteen years, from checklist-based compliance towards real-time security analysis, a change that has accelerated considerably over the last five years specifically. India's cybersecurity posture is increasingly framed around resilience, both in cyberspace specifically and as a matter of national-threat preparedness more broadly. The relevant question is no longer only whether something can go wrong, but *how quickly a system can bounce back and limit damage once it does*. This calls for a more coordinated approach across a genuinely diverse set of stakeholders, a more multidimensional approach across the many distinct facets of cyber risk, and greater automation to reduce response-time lag, since threats today are increasingly multi-dimensional and leave no meaningful time for manual intervention. This shift is now visibly reflected in bilateral and multilateral regulatory frameworks worldwide.

The acute vulnerability of small and mid-sized players in the financial ecosystem deserves particular attention. If it rains, everyone gets wet. This implies that attackers naturally go for the low-hanging fruit, and small and medium enterprises are frequently that fruit. Cybersecurity has, in a sense, entered the compliance conversation as a mandated obligation, but has not yet fully earned its place in the boardroom as a genuine strategic priority. Resilience carries real cost, and SMEs are often simply unable to absorb that cost financially.

Individual cyber incidents should never be treated as isolated cases divorced from broader national risk. A 2024 data leak involving police-department data, for instance, demonstrates that no single breach can be dismissed as a purely local or 'micro' concern. Each incident represents a genuine national-security-relevant threat, particularly as AI capability continues to expand the attack capabilities of bad actors. Ground-level enforcement

remains a necessary complement to any macro-level cyber-defence strategy, since micro-level threats, left unaddressed, are exploitable for larger systemic exposure.

The industry is moving from managing third-party risk to managing systemic risk. Regulators must move beyond checklist compliance towards anticipating what could plausibly go wrong rather than simply auditing against fixed, backward-looking criteria. This does not mean abandoning supply-chain risk management. It rather means managing that risk without making compliance so stringent and complex that innovators, researchers, and start-ups struggle to operate within it.

A mechanism for mapping a 'critical dependency registry' can identify how organisations, sectors, or the economy are structurally dependent on specific vendors, platforms, or infrastructure and can lay bare the risk for entire value chains.

Making cybersecurity affordable: CERT-In-style advisory bodies could play a stronger enabling role for medium and smaller enterprises through public-private partnerships, regional expert teams, proactive training, and standardised incident-response playbooks. Such an ecosystem-based approach would strengthen baseline cybersecurity across the economy while ensuring that compliance requirements remain proportionate to the capacity and risk profile of different organisations.

For AI-driven threats specifically, organisations need to move decisively beyond traditional cybersecurity playbooks. Replace periodic security audits with continuous security monitoring, automating patch and vulnerability management to reduce response time, run regular crisis simulations that involve senior management and board members directly rather than technical teams alone (since these are the people who make critical decisions during live incidents), and shift institutional culture decisively from 'audit-ready' to 'attack-ready'.

The effectiveness of international cooperation for threat neutralisation depends on the formal

and informal linkages with the key intelligence agencies. Countries are generally willing to share high-level threat information but are less willing to share operational capabilities, and national-security concerns routinely override broadly agreed international frameworks. Within India's financial sector, reducing the regulatory overlap for incident-reporting requirements is a must for dealing with AI-accelerated attacks, which require quicker responses.

Cyber attackers already collaborate globally through coordinated campaigns, while defenders remain comparatively fragmented across institutions, sectors, and borders. This asymmetry is worth correcting deliberately. Small and medium businesses comprise about 31 per cent of GDP but often lack the resources for robust cybersecurity. They become an easy entry point for sabotaging large segments of the economy. Incentivising proactive adoption of secure practices by MSMEs can prevent a systemic collapse.

India's cybersecurity strategy must evolve from a compliance-focused approach to one centred on preparedness, resilience, collaboration, and continuous adaptation. This shift mirrors the broader argument running through this entire paper.

VI. AI Optimism in India

Having traced India's digital journey from foundational infrastructure, through payments, digital money, cross-border finance, inclusion gaps, and digital risk, it is worth closing with a forward-looking question: *what is the next phase of India's digital transformation?* The answer is AI. The rationale behind addressing it last in this paper is that the interplay between AI and the economy is still evolving.

Where India Stands

According to the State of India's Digital Economy (SIDE) Report 2026, released by the Indian Council for Research on International Economic Relations (ICRIER), India is the fifth most intensively digitised economy globally and ranks fourth in AI. The SIDE Report measures a country's digital ecosystem through the Connect, Harness, Innovate, Protect, and

Sustain (CHIPS) framework. This framework differs deliberately from indices produced by the World Bank, International Monetary Fund (IMF), World Economic Forum (WEF), or United Nations (UN), in that it explicitly separates the scale of digitalisation from its intensity.

Combining scale and intensity places India among the top five globally for digitisation (alongside the US, China, Singapore, and the United Kingdom) and among the top four for AI (alongside the US, China, and Singapore). India's strongest scores come from scale, with over a billion connected citizens generating a genuinely massive network effect. Large-scale diffusion, attributable to DPI, could not have resulted in this by itself. Trust within the ecosystem plays a major role. Despite real and ongoing cyber-fraud concerns, Indians remain considerably more trusting of the internet and digital economy than citizens of many other countries, and this trust score carries through directly into AI as well. India has a very large AI-user workforce concentration, is the world's second-largest user base for AI after China, and records the highest measured trust in AI among the countries studied.

India's digital transformation story is therefore more than just a story of connectivity and scale. Its strong performance on *Harness* and *Innovate*, alongside its growing adoption of AI, points towards the next stage of the digital economy: translating India's existing digital capabilities into productivity gains and new economic opportunities through emerging technologies. AI is likely to be central to this transition. Yet the impact of AI on employment, particularly in India's large IT and services sector, is a genuine cause for concern. Such concerns are not unique to India and need closer examination.

AI Pessimism and Optimism: Are these partial views of Producers and Workers?

India was late to both the IT and the internet transformations, and on each occasion the obituary for Indian industry was written prematurely. Extensive automation is coming. But this is neither a reason for panic nor for complacency. Informed analysis grounded in evidence and good

data, such as the SIDE report, suggests a more granular perspective.

India has the world's second-largest number of AI users, but this fact is not evidence that India will remain only an AI *consumer*. Three reasons support a more balanced viewpoint:

- First, AI is a productivity tool, not merely a consumer product. Widespread adoption within enterprises should raise productivity across businesses and individuals, not only within the technology sector narrowly defined.
- Second, today's AI users are tomorrow's innovators. Research consistently shows that exposure to new technology increases future innovation. India's large and growing AI-user base constitutes a genuine foundation for future AI developers and entrepreneurs rather than merely a captive consumer market to be monetised by others.
- Third, and perhaps most concretely, India has succeeded at exactly this before. Despite not inventing the internet or fibre optics, India became one of the largest beneficiaries of the ICT transformation by building a globally competitive IT-services industry from a standing start. The same trajectory can plausibly be repeated with AI. India already exports more ICT services than all developing countries combined (except China), illustrating that India can be both a major technology user and a major technology producer simultaneously, rather than one at the expense of the other.

India is genuinely well positioned to pursue this path, in terms of **foundational digital infrastructure, skills, and scale**. The only major binding constraint that now remains is R&D investment, which continues to be comparatively insufficient. Accumulation of inputs alone is subject to diminishing returns. It is only investment that would shift the productive frontier itself (in R&D, data centres, and the complementary investments discussed in Section I) and convert India's current position of scale into a durable position of **Digital Thought Leadership**.

Learning from the Past Whilst Building AI Capability

AI is presently anticipated to unleash never-before-seen productivity gains. Sustained AI-driven gains will require investment in R&D, data centres, advanced digital infrastructure, innovation ecosystems, intellectual property, and high-value digital services. It is unclear how partnerships will evolve and how the productivity gains will be shared. A useful strategy might be to say yes wherever the result is higher domestic competitiveness, and the fiscal burden is bearable.

Global collaboration and digital sovereignty sit uneasily together. The investments span cloud infrastructure, compute capacity, semiconductor manufacturing, access to refined critical minerals, and technical talent. Policies and regulations for infrastructure providers and platform operators would need to respond to global demand-supply balances. Digital sovereignty would mean diversifying technological dependencies rather than pursuing full self-sufficiency.

In summary, India's digital journey is moving from creating access and infrastructure, to building platforms and financial systems, and now towards developing deeper technological capability through AI. The defining challenge for this next phase is harnessing the technological opportunities but also targeting productivity enhancement in an inclusive, secure, and broadly distributed manner. This is the standard against which every theme discussed in this paper should be measured.

Conclusion: From Digitalisation to Digital Economic Maturity

Read end to end, this paper traverses a single, coherent arc. India built its digital foundations largely through domestic effort rather than imported infrastructure, building Digital Public Infrastructure as an economic institution rather than merely a technology stack.

UPI demonstrated what those foundations could produce at national scale, transforming banking economics and consumer behaviour alike. In the process, the lack of safeguards to promote

competition, ensure sustainability, and enhance resilience has generated unanticipated outcomes that call for design alteration.

CBDC and stablecoins now raise a more fundamental question than UPI ever did. The question is no longer limited to how money moves, but extends to whether the nature of money itself can change. The government's preference is for CBDC, but the trend overseas favours private-sector-promoted stablecoins. Both warrant distinct regulatory treatment rather than a single blended framework. Extending this activity across borders exposes the gap between what technology can achieve and what jurisdiction, regulation, and geopolitics will currently allow.

Running underneath are two connected dysfunctionality that any honest account of India's digital economy must confront: the exclusion of citizens who have not shared equally in digital gains, and the vulnerability of those who have, to fraud and cyberattacks that grow more sophisticated as the underlying systems grow more capable.

AI sits at the end of this arc deliberately, not incidentally. It represents both India's opportunity to move from being a technology consumer to a technology producer, and a test of whether the country has actually learned from the concentration and exclusion problems visible in its digital economy.

The central challenge for India, therefore, is no longer simply to digitalise. It is to ensure that its digital economy is productive, inclusive, resilient, and capable of generating deeper technological value, both for the citizens already inside the system and for the substantial number still waiting to benefit from it.

Policy Recommendations

These recommendations follow directly from the themes explored in this paper. They are organised by theme rather than by priority and are intended to start conversations rather than end arguments.

(1) On UPI Sustainability and Competition:

- a. Pursue a multi-operator model with common messaging standards, mandatory bank connectivity across networks, and automatic failover in case of operator outage.
- b. Implement the revised zero-MDR framework as announced by the government on August 8, 2026, for long-term commercial sustainability without compromising UPI's public-utility characteristics.
- c. Generate greater competition in digital payments with better representation of Indian corporates before resorting to regulatory fiat to determine maximum market shares for individual operators as a less preferred option – previously suggested by NPCI.

(2) On CBDCs:

- a. Prioritise wholesale settlement, programmable welfare/DBT applications, and cross-border use cases over retail adoption, given UPI's continued dominance in domestic retail payments
- b. Pursue cross-border CBDC arrangements with key trading partners as a means of strengthening geopolitical and technical cooperation.

(3) On VDAs and Stablecoins:

- a. Maintain and refine the risk-based, technology-neutral regulatory approach. Although currently followed in practice through the FATF Cell's alignment with FATF's Recommendation 15 guidance, this is not yet codified in a single Indian statute and remains a gap the Parliamentary Standing Committee on Finance has itself flagged.
- b. Evolve regulatory criteria and approaches suited to the variety of VDA use cases and potential risks, rather than following a single fixed template.
- c. First, explore the feasibility of INR-backed stablecoins, while recognising that India's rupee internationalisation ambition remains a long haul, at best. If feasible at all, then explore the possible sequencing of such an INR-backed stablecoin.
- d. Require local incorporation/presence for offshore VASPs serving Indian users to level the regulatory playing field.

(4) On Cross-border Payments:

- a. Accelerate real-time remittance processing and 'positive pay' mechanisms nationally.
- b. Extend RBI's existing EDPMS/e-FIRA digitisation (already covering most export remittances since 2016) to the remaining manual processes, such as physical Foreign Inward Remittance Certificates (FIRCs) still issued for FDI and FII inflows.
- c. Increase India's technical representation on ISO's payment-messaging standard-setting committees (such as those governing ISO 20022) and pursue a more active role in FATF's policy and working-group processes, moving India from a standards taker towards a standards shaper commensurate with its transaction volumes.

(5) On Inclusion:

- a. Commission and publish rigorous social-impact evidence on the impact of UPI on women's financial inclusion, unbanked populations, and the levelling of regional disparities.
- b. Invest in grievance-redressal infrastructure co-terminus with payment infrastructure.
- c. Treat digital sovereignty as a full-stack capability (compute, semiconductors, critical minerals, talent, and regulation), not merely a consumer application.

(6) On Fraud and Consumer Protection:

- a. Expand investigative capacity (these are good- and forward-looking jobs) as envisaged in the IT Act's minimum rank of Inspector for cybercrime-investigation provisions.
- b. Build dedicated capacity in a central nodal agency for cybercrime investigation with nationwide suo motu jurisdiction along with associated virtual-asset forensics lab capacity.
- c. Extend VDA-adjacent regulation to gaming, gambling, and prediction-market platforms.
- d. Introduce cyber-fraud insurance with shared institutional-consumer cost structures.
- e. Adopt EU MiCA-style restrictions on the 'reverse solicitation' defence for offshore platforms targeting Indian users.

(7) On Cybersecurity:

- a. Harmonise overlapping regulatory reporting requirements across financial-sector regulators.
- b. Shift institutional posture from 'audit-ready' to 'attack-ready' through continuous monitoring and automated patching.
- c. Build community-pooled cybersecurity resources for SMEs, potentially anchored around a 'critical dependency registry'
- d. Expand CERT-In's advisory and community-building role, particularly for smaller enterprises.

(8) On AI:

- a. India's burgeoning AI-user base will provide a massive data pool. Using that data pool for innovating and creating indigenous AI products is the way to go. Otherwise, the country will remain a mere market for foreign AI products. India's AI innovation should be driven by targeted R&D, data infrastructure, and IP investment.
- b. AI's economics differ from a typical scale-driven platform business. Training frontier models involves enormous fixed costs, creating a high barrier to entry. However, the marginal cost of running each additional query does not fall neatly with scale the way it did for earlier digital platforms, since AI infrastructure already runs near full utilisation and costs like electricity, hardware and cooling can rise, not fall, as data centres expand. India's AI space is nonetheless at real risk of firm-level concentration because only well-capitalised players can absorb the upfront cost of competing at the frontier at all. Designing an appropriate AI infrastructure policy, with relevant safeguards, is an absolute necessity to ensure future innovation and a fair business environment for all. •

By Avni Goel

References

- Department of Economic Affairs. 2024. The Indian Economy – A Review. January 29, 2024. Ministry of Finance, Government of India. https://dea.gov.in/sites/default/files/The%20Indian%20Economy%20-%20A%20Review_Jan%202024.pdf. Accessed September 7, 2026.
- Kriti. 2026. “RBI Guidelines 2026: Faster Cross-Border Inward Payments & Timely Credit.” SCC Times, April 11, 2026. <https://www.sconline.com/blog/post/2026/04/11/rbi-guidelines-faster-cross-border-inward-payments-2026/>. Accessed September 7, 2026.
- MGMMTeam. 2026. “Centre Notifies Comprehensive Questionnaire for Census 2027 Population Enumeration.” Mahatma Gandhi’s Music and Musings, August 14, 2026. <https://www.shabariseva.com/post/centre-notifies-comprehensive-questionnaire-for-census-2027-population-enumeration>. Accessed September 7, 2026.
- Ministry of Finance. 2026a. “DFS, M/O Finance Releases Report Titled ‘Socio-Economic Impact Analysis of Incentive Scheme for Promotion of RuPay Debit Card and Low-Value BHIM-UPI Transactions (P2M)’ at Chintan Shivir 2026.” Press Information Bureau, Government of India, February 16, 2026. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228651&lang=1®=1>. Accessed September 7, 2026.
- Ministry of Finance. 2026b. “UPI Completes 10 Glorious Years, Emerges as World’s Largest Real-Time Payments Platform, Anchoring India’s Digital Economy.” Press Information Bureau, Government of India, April 30, 2026. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2257087@=3&lang=2>. Accessed September 7, 2026.
- Ministry of Finance. 2026c. “No Charges for UPI Users: Vast Majority of the Transactions to Remain Free of Charge for Merchants as Well.” Press Information Bureau, Government of India, August 8, 2026. <https://www.pib.gov.in/PressReleaseFramePage.aspx?PRID=2296594&lang=2®=48>. Accessed September 7, 2026.
- Moneycontrol. n.d. “What Is a New Umbrella Entity?” <https://www.moneycontrol.com/news/mcminis/what-is-a-new-umbrella-entity-10387061.html>. Accessed September 7, 2026.
- Pandey, Devesh K. 2026. “Report Highlights Steps Taken to Mitigate Risks Posed by Offshore Virtual Asset Service Providers.” The Hindu, March 29, 2026. <https://www.thehindu.com/news/national/report-highlights-steps-taken-to-mitigate-risks-posed-by-offshore-virtual-asset-service-providers/article70799962.ece>. Accessed September 7, 2026.
- Press Trust of India. 2023. “India Expected to Become \$7 Trillion Economy in Seven Years: CEA.” The Hindu, January 10, 2023. <https://www.thehindu.com/business/Economy/india-expected-to-become-dollar-7-trillion-economy-in-seven-years-cea/article66358446.ece>. Accessed September 7, 2026.
- Press Trust of India. 2026. “Over 27% of Indian Households Remain Offline Despite 95% Mobile Penetration: NCAER Report.” BusinessLine, June 5, 2026. <https://www.thehindubusinessline.com/info-tech/over-27-of-indian-households-remain-offline-despite-95-mobile-penetration-ncaer-report/article71068340.ece>. Accessed September 7, 2026.
- Smile Foundation. 2025. “How Can Rural Women Access Markets Digitally?” September 6, 2025. <https://www.smilefoundationindia.org/blog/digital-markets-for-indian-women/>. Accessed September 7, 2026.
- Standard Chartered. 2026. “Standard Chartered Processes Real Time Remittance Payments to India Within Seconds.” July 2, 2026. <https://www.sc.bank.in/scb-processes-real-time-remittance-payments-to-india-within-seconds/>. Accessed September 7, 2026.
- UNESCO. 2020. “Startling Digital Divides in Distance Learning Emerge.” April 21, 2020. <https://www.unesco.org/en/articles/startling-digital-divides-distance-learning-emerge>. Accessed September 7, 2026.

Acknowledgements

This paper would not have been possible without the insight and generosity of the speakers, moderators and partner organisations who shaped the conference that inspired it. The Chintan Research Foundation (CRF) is grateful to Ikigai Law and Koan Advisory Group for their partnership in convening the conference and for their expertise in digital policy.

The Foundation thanks Dr Deepak Mishra, Distinguished Visiting Professor, ICRIER; Dr Rajat Kathuria, Dean, School of Social Sciences, Shiv Nadar University; Mr Tamal Bandyopadhyay, Consulting Editor, Business Standard; and Ms Aparajita Bharti, Co-founder, The Quantum Hub, for their contributions to the session on *'India's Digital Economy, Evolution, Future and Inclusion'*, moderated by Mr Sanjeev Ahluwalia, Distinguished Fellow, CRF.

For the session on *'UPI as India's Flagship Digital Rail'*, the Foundation thanks Dr Balakrishnan Mahadevan, Former COO, NPCI; Ms Monica Jasuja, Payments & Product Leader; Mr Kiran Shetty, Managing Director, Swift India; and Mr Ashok Lavasa, former Finance Secretary and former Election Commissioner, with the session moderated jointly by Mr Sanjeev Ahluwalia, Distinguished Fellow, CRF, and Mr Vivan Sharan, Partner, Koan Advisory.

The session on *'New Payment Rails – the Digital Rupee, Stablecoins and Virtual Digital Assets'* benefited from the contributions of Ms Megha Sidhu, Officer on Special Duty (Joint Commissioner), FATF Cell, Department of Revenue, Government of India; Mr Manhar Garegrat, Senior Vice President, Country Head, India & Global Partnerships, Liminal Custody; Mr Mandar Kagade, Founder & Principal, Black Dot Public Policy Advisors; and Mr Abhijit Mukhopadhyay, Senior Research Consultant, Centre for Economy and Trade (CET), CRF, moderated by Mr Anirudh Rastogi, Founder, Ikigai Law.

The session on *'Digital Risks – Fraud, Phishing and Identity Theft'* was shaped by the contributions of Mr Abhinav Kumar, DGP, Uttarakhand, Government of India; Mr Sumanta Dey, Vice President, Public Policy, Delta Exchange; Mr Aashish Aryan, Senior Assistant Editor, Business Standard; and Mr Dilip Chenoy, Chairman, Bharat Web3 Association, moderated jointly by Ms Rutuja Pol, Partner, Ikigai Law, and Ms Avni Goel, Research Analyst, CET, CRF.

Finally, the session on *'Cybersecurity, Enforcement and Regulation'* drew on the expertise of Ms Meghna Pradhan, Research Analyst, MP-IDSA; Mr Inder Chaudhry, Head, Cyber Security & Cyber Resilience Practice, MitKat Advisory Services; and Mr Atul Kumar, Head, Government Affairs, DSCI, moderated by Mr Dhruv Garg, Partner, Indian Governance and Policy Project.

The views and analysis presented in this paper are those of the Chintan Research Foundation and do not necessarily represent the individual positions of the speakers, moderators, or partner organisations named above.

ABOUT THE AUTHOR



Ms. Avni Goel is a Research Analyst at the Centre for Economy and Trade at Chintan Research Foundation (CRF). She holds a Master of Arts (M.A.) in Economics from O.P. Jindal Global University. Her research focuses on digital money and payments architecture, financial regulation, and technology-driven development. At CRF, she has worked extensively on India's digital payments ecosystem, including UPI, CBDCs, digital public infrastructure, cross-border payments, crypto-assets, and stablecoins. Her broader interests encompass development economics, technological capability, financial inclusion, productivity, structural transformation, and evidence-based policy measurement, with a focus on generating actionable research to support India's inclusive and technology-led economic growth.

Designed by: **Sarika Batra, Graphic Designer**

Edited by: **Shraddha Ratori, Editorial Consultant**

Image Source: **Shutterstock**

Copyright ©2026 Chintan Research Foundation

Recommended Citation

Goel, A. (2026). India's Digital Economy: A Policy Review and an Assessment of Prospects Ahead, Chintan Research Foundation (CRF), New Delhi



ELEVATING IDEAS | EMPOWERING PEOPLE



1st Floor, Bharti Crescent Building, 1 Nelson Mandela Marg, Vasant Kunj Phase II, New Delhi - 110070



info@crfindia.org



+91 9311630957, +91 6358871398



www.crfindia.org