

The Architecture of Trust: Moving Beyond Payments into Intelligence and Programmability

(Keynote Address to be delivered by Shri Ajay Kumar Choudhary, Non-Executive Chairman and Independent Director, National Payments Corporation of India – Sept 10, 2026, Global Fintech Fest 2026, Jio World Convention Centre in Mumbai, India)

Good afternoon, colleagues, distinguished policymakers, regulators, leaders from financial institutions, members of the FinTech ecosystem, technology innovators, members of academia, and esteemed guests. It is a privilege to be with you at the Global FinTech Fest 2026, a forum that has consistently brought together ideas, institutions, and innovation to shape the future of finance.

This year's theme, *"Potential to Impact: Agentic AI, Tokenisation and Quantum,"* is both timely and ambitious. It asks us to look beyond individual technologies and consider the transformation taking shape across finance. Systems are becoming more intelligent, assets and transactions more programmable, and the foundations of digital trust are entering a new phase.

These technological advancements are set to transform the structure of financial services. The question is no longer whether new technologies will affect finance, but how effectively we navigate this transition, and capture the opportunities without losing control of the risks. The challenge, therefore, is not simply to adopt more technology, but to do so in a way that makes the financial system more efficient, secure, resilient and trusted.

India enters this conversation with considerable experience. We have demonstrated that interoperable digital infrastructure can move money safely, instantly, and at population scale. In August 2026, UPI processed

more than 24.5 billion transactions (Total Value- Rs 29.8 lakh crore) through 752 participating banks. This scale reflects more than technology; it represents trust built through common standards, institutional collaboration, and shared participation across banks, FinTechs, merchants, and public institutions alike.

This year also marks ten years of UPI. In one decade, it has moved from a new payment interface to infrastructure embedded in the everyday life of India. Its growth has been accompanied by something equally important: the trust of consumers, merchants, banks, and the wider ecosystem. Over the decade, UPI has also grown in influence, demonstrating how interoperable digital public infrastructure can combine scale, innovation, and inclusion. Its journey has been shaped by the collective efforts of regulators, banks, FinTechs, technology partners, and millions of users and merchants. Equally important has been the consistent national leadership that placed digital payments at the heart of India's development journey. Our Hon'ble Prime Minister, Shri Narendra Modi Ji, has repeatedly taken India's UPI story to the world, making it one of the most visible expressions of India's technological capability and confidence.

As UPI enters its second decade, the question is what more these trusted rails can enable. Can they support authorised intent, coordinate multiple actions, connect assets with conditions, and execute transactions across increasingly complex digital environments?

This is not a movement away from payments, but a progression built upon the infrastructure already created. The next financial architecture must add

intelligence and programmability while preserving trust, accountability, and resilience.

It is through this lens that I would like to reflect on the next financial infrastructure.

Intelligence: From Instructions to Intent

Traditional payment systems execute an instruction. A user selects the beneficiary, enters the amount, authenticates, and pays. Agentic AI may change where technology enters this journey. An intelligent agent may understand an objective, divide it into tasks, compare options across providers, and act within an authorised mandate. Households may use agents for recurring payments, while financial institutions may deploy them for liquidity, compliance, and fraud monitoring.

These remain emerging possibilities, and adoption will depend on accuracy, regulation, and safeguards. The central tension is that AI is adaptive and its output is probabilistic, while payment infrastructure must remain deterministic, auditable, and final. An agent may interpret intent, but authorisation must verify identity, mandate, limits, and consent. A sound architecture must, therefore, separate intent, authorisation, and settlement, with settlement remaining rules-based, secure, and legally final.

NPCI is also examining the protocols that may be required to identify and authorise digital agents within the UPI ecosystem, while preserving interoperability, auditability, and settlement finality. The objective, therefore, is not unlimited machine autonomy. It is to be bounded and accountable.

Programmability: From Moving Money to Coordinating Value

Programmability uses self-executing code, defined by humans, to establish rules that follow strict 'if-then' conditions. It, therefore, executes predetermined instructions, making its behaviour deterministic and its output predictable.

The immediate benefit of programmability is that it can turn passive assets and data into active, self-executing systems. As an illustration, financial transactions today often rely on separate systems for information, reconciliation, asset transfer, and settlement, adding time, cost, and complexity. Programmability can bring these functions closer together, enabling simultaneous payment and delivery, automatic collateral adjustment when conditions are met, and asset movement with less reconciliation across ledgers. It, therefore, goes beyond simply transferring money by linking the movement of money or assets to agreed conditions.

Programmable platforms may reduce friction in cross-border payments by way of instant settlement by hard coding the compliance checks into the transfer logic, and support delivery-versus-payment and more efficient collateral management in securities markets. But programmability must preserve finance's foundations. A token must represent a legally recognised claim, every instruction must remain traceable to an accountable entity, the singleness of money must be protected, and settlement must remain certain and final. This is also where common and interoperable infrastructure becomes important. NPCI's open-source enterprise blockchain platform, Drunix, is designed to support tokenisation platforms, digital asset ecosystems, and multi-organisation networks, helping institutions experiment and scale without creating disconnected financial systems.

The real risk is not tokenisation itself, but fragmentation across incompatible platforms. Innovation should flourish at the edges, while common standards at the infrastructure level should prevent fragmentation and preserve connectivity at the core.

Trust: From Present Security to Future Resilience

Agustín Carstens, former General Manager of the Bank for International Settlements and previously Governor of the Bank of Mexico, has observed, ***“Trust requires sound institutions that can stand the test of time.”***

Technology can change how value is represented and how quickly transactions are completed. It can, however, not substitute for credible institutions. Trust means confidence that money will retain its value, transactions will complete as intended, data will be protected, and responsibility will remain identifiable when something goes wrong.

Quantum computing adds a new horizon to this question. Systems capable of compromising some forms of today’s public-key cryptography may still be a few years away, but financial infrastructure cannot wait for the risk to materialise. Arthur Yuen, Deputy Chief Executive of the Hong Kong Monetary Authority, has similarly emphasised the need for banks to become post-quantum cryptography ready before the first attacks emerge, and to begin preparing now. Cryptographic transitions are slow and system-wide. Post-quantum cryptography has already been tested within an operational European payment environment, demonstrating its feasibility while also revealing challenges in performance and interoperability. The lesson for us is readiness: knowing where cryptography resides, planning how it can be replaced without disrupting critical services, and coordinating migration

across the ecosystem. Quantum readiness is, therefore, not a standalone technology project, but a long-term resilience programme involving boards, regulators, infrastructure providers, banks, FinTechs, and cybersecurity specialists. A payment network, after all, is only as secure as its weakest critical connection.

The Convergence of the Three Layers

The real transformation will emerge when intelligence, programmability, and trust operate together. When an AI agent is integrated with smart contracts, it can provide the context to determine when or why to act.

Consider a small business replenishing inventory. An authorised agent compares verified suppliers and financing options within limits the owner has set. A programmable arrangement links the purchase order, delivery confirmation, and payment obligation. Regulated payment infrastructure executes settlement only after the required conditions and authorisations are satisfied.

In such an emerging architecture, no single technology would complete the journey. Agentic AI could coordinate actions, tokenisation could enable programmable execution, while payment systems would continue to provide trusted and final settlement. Their convergence can reduce friction, but it also links risks. Model risk can become payment or conduct risk, dependence on a single cloud provider may create both operational vulnerability and sovereignty concerns, and an error in a programmable condition may become a settlement problem. Risk management must, therefore, follow the activity across the entire chain, not each technology in isolation.

The Institutional Transition Ahead

As financial infrastructure evolves, institutional roles must evolve with it. Customers may move from initiating each transaction to defining mandates within which authorised agents can act. Financial institutions must continue to own customer relationships, risk decisions, and regulatory accountability, even as execution becomes more distributed. Infrastructure providers, in turn, will need to verify not only payment instructions, but also the authority, mandates, and conditions attached to them.

This transition will require deliberate change management. New technologies will reshape operating models, decision rights, workflows, and employee responsibilities. Adoption should, therefore, be phased, supported by controlled experimentation, continuous feedback, and close coordination across business, technology, risk, and operations. Employees must understand when automated systems can be relied upon, when escalation is necessary, and where human judgment must prevail. Change management must begin with the design of the new architecture, not after its deployment.

For NPCI, the task is not to determine what choice an agent should make for a user, but to ensure that any authorised instruction reaching the payment system carries a valid mandate, enforceable controls, secure execution, and clear accountability. Regulators and supervisors will also need visibility across interconnected activities, common standards for auditability, and mechanisms to identify concentration and operational risks before they become systemic. As technology assumes a larger role, institutional boundaries must become clearer, not weaker.

Building the Architecture of Trust & Criticality of Managing Sovereignty Risk

A few principles for building the architecture of trust could be:

- i. Human authority must remain the source of every mandate, supported by consent that is specific, limited, understandable, and revocable.
- ii. Identity must extend to digital agents to establish on whose behalf they act, what authority they carry, and where liability rests.
- iii. Decision-making and execution must remain separate: AI may recommend, but authentication and final settlement must follow deterministic, auditable rules.
- iv. Interoperability must remain non-negotiable, allowing agents and tokenised platforms to work across institutions without creating new walled gardens.
- v. The same principle must guide AI infrastructure. AI sovereignty is an important requirement; however, it should not mean isolation or building every component domestically but retaining control and meaningful choice over the critical elements of the architecture.

For financial institutions, this requires clarity on the models used, the decisions they influence, where sensitive data is processed, how outputs are tested, and whether operations can continue if a provider becomes unavailable or changes its terms.

On the issue of sovereignty, it comes from a combination of control, capability, choice, and preparedness. In this context, it may be noted that integrated AI stacks comprising compute, cloud, models, and applications can accelerate adoption. Recent U.S. policy promoting an integrated American AI technology stack makes this question particularly relevant. Such access can accelerate capability, but dependence on a single national or commercial stack may, over time, reduce sovereign choice. Applications should therefore be designed, wherever practicable, to operate across multiple models and infrastructure providers. Data, business logic, and workflows must remain portable, allowing institutions to change providers as performance, cost, risk, or regulatory requirements evolve.

Open-source and open-weight models can also strengthen sovereignty by widening choice and enabling deployment in controlled environments. But their availability at this point of time is insufficient. Institutions also need computing capacity, technical skills, cybersecurity, governance, and operational capability.

This must be complemented by multidisciplinary expertise to evaluate performance, manage third-party dependencies, validate outcomes, and translate technological possibilities into safe and scalable financial services.

Professor Amartya Sen, Nobel laureate economist and philosopher, has written ***“Development can be seen as a process of expanding the real freedoms that people enjoy.”***

That is an important test for the architecture of trust. Intelligence and programmability should strengthen people’s ability to understand, choose, and act, without transferring control or technological risk away from them.

Inclusion must remain our measure of progress. These systems should reduce complexity, and should work across languages, devices, and levels of financial literacy, and preserve comprehension, choice, and control.

Conclusion: Technology Guided by Purpose

One should always keep in mind that no organisation is likely to thrive if it adopts technology mainly as a way to take cost out. Efficiency of course matters. But the bigger gain is better decisions, better services and better risk management. Also, tomorrow's professional will need to work fluently across two interfaces: with other people, and with intelligent systems. For any organisation making more use of advanced technologies, the key to success is to ensure that humans and machines complement each other and bring out the best in one another. To achieve this, reskilling and upskilling of the workforce will be a critical part of the equation.

Against this backdrop, we are navigating three transitions: from instructions to intent, from digital records to programmable value, and from present-day cybersecurity to long-term cryptographic resilience. These shifts can improve efficiency, inclusion, and resilience, but may also create fragmentation through closed ecosystems and weakening interoperability, concentration, and new operational risks. The outcome will depend on the architecture and governance we choose.

Alan Turing, the British mathematician and pioneer of computer science and machine intelligence, concluded his seminal work on machine intelligence with the words, ***“We can only see a short distance ahead, but we can see plenty there that needs to be done.”***

That may be the right perspective for this moment. We cannot predict how intelligent agents, tokenised assets, or quantum technologies will evolve, nor should financial infrastructure be built upon predictions alone. But our responsibilities are clear: define how authority is delegated, preserve the distinction between intelligent coordination and valid authorisation, build interoperability before fragmentation and dependence take hold, and prepare post quantum cryptographic systems well before quantum risk becomes immediate.

The next financial infrastructure must be intelligent enough to understand intent, programmable enough to coordinate value, resilient enough to withstand future threats, and inclusive enough to serve every citizen. The architecture must remain accountable in governance, deterministic in settlement, and human in purpose.

That is how potential will become impact, innovation will become trusted infrastructure and how we can shape the next chapter of finance with both ambition and foresight.

Before concluding, I would like to compliment and congratulate the entire ecosystem, the leadership and staff of NPCI and thank the Reserve Bank of India and the Government of India for the exemplary journey of UPI over the last ten years. I am very confident that NPCI will continue to provide leadership in the emerging, scalable and inclusive technologies, helping redefine the finance of tomorrow.

Thank you.

Jai Hind.

References:

1. See Global FinTech Fest, “**Theme of GFF 2026: Potential to Impact – Agentic AI, Tokenisation and Quantum**” (<https://www.globalfintechfest.com/theme>)
2. See National Payments Corporation of India, “**Unified Payments Interface Product Statistics**”, June 2026 (<https://www.npci.org.in/product/upi/product-statistics>)
3. See Sonja Davidovic and Hervé Tourpe, International Monetary Fund, “**How Agentic AI Will Reshape Payments,**” IMF Notes No. 2026/004, April 2026 (<https://www.imf.org/en/publications/imf-notes/issues/2026/04/22/how-agentic-ai-will-reshape-payments-575560>)
4. See Bank for International Settlements, “**The Next-Generation Monetary and Financial System,**” BIS Annual Economic Report 2025, Chapter III, June 2025 (<https://www.bis.org/publ/arpdf/ar2025e3.htm>)
5. See Bank for International Settlements, “**Anchoring Trust in Money: Innovation Beyond Stablecoins,**” BIS Annual Economic Report 2026, Chapter III, June 2026 (<https://www.bis.org/publ/arpdf/ar2026e3.htm>)
6. See National Payments Corporation of India, “**Drunix: Performant, Enterprise-Grade Blockchain Platform,**” NPCI GitHub Repository, 2026 (<https://github.com/npci/drunix>)
7. See Agustín Carstens, Bank for International Settlements, “**Digital Currencies and the Soul of Money,**” January 18, 2022 (<https://www.bis.org/speeches/sp220118.htm>)
8. See Raphael Auer, Donna Dodson, Angela Dupont, Maryam Haghighi, Nicolas Margaine, Danica Marsden, Sarah McCarthy and Andras Valko, Bank for International Settlements, “**Quantum-Readiness for the Financial System: A Roadmap,**” BIS Papers No. 158, July 2025 (<https://www.bis.org/publ/bppdf/bisap158.pdf>)
9. See BIS Innovation Hub, “**Project Leap Phase 2: Quantum-Proofing Payment Systems,**” December 2025 (<https://www.bis.org/publ/othp107.htm>)
10. See The White House, “**Promoting the Export of the American AI Technology Stack,**” Executive Order 14320, July 23, 2025 (<https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/>)

11. See Juan Carlos Crisanto, Shubhika Singh and Wenguang Wu, Financial Stability Institute, Bank for International Settlements, **“Regulating AI in the Financial Sector: Recent Developments and Main Challenges,”** FSI Insights No. 63, December 2024
(<https://www.bis.org/fsi/publ/insights63.pdf>)
12. See Organisation for Economic Co-operation and Development, **“Benefits of AI Openness,”** May 2026
(https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/05/benefits-of-ai-openness_40eaff39/746e8c9a-en.pdf)
13. See National Payments Corporation of India, **“NPCI Advances India’s Sovereign AI Infrastructure for Digital Payments with NVIDIA,”** February 18, 2026
(https://www.npci.org.in/uploads/NPCI_Advances_India_s_Sovereign_AI_Infrastructure_for_Digital_Payments_With_NVIDIA_7305ed3754.pdf)
14. See Amartya Sen, **“Development as Freedom,”** Oxford University Press, 1999
(<https://india.oup.com/product/development-as-freedom-9780195655261>)
15. See Alan M. Turing, **“Computing Machinery and Intelligence,”** Mind, Volume LIX, Issue 236, October 1950
(<https://academic.oup.com/mind/article/LIX/236/433/986238>)
16. See Arthur Yuen, Hong Kong Monetary Authority, **“Opening Remarks at the HKMA-HKAB Seminar on Quantum Computing and Quantum Resilience for the Banking Industry,”** July 2026. (<https://www.hkma.gov.hk/eng/news-and-media/speeches/2026/07/20260706-1/>)