International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Quantum-Safe Cryptography and Financial Infrastructure Resilience

Shruti Nikhil Zende

College of Management & Computer Application

MIT Art, Design and Technology University

Shubham Badrinath Jadhav

College of Management & Computer Application

MIT Art, Design and Technology University

Abstract

Quantum computing has moved from a theoretical physics curiosity to a board-level financial risk. Because financial infrastructure runs almost entirely on public-key cryptography — RSA and elliptic-curve algorithms that secure SWIFT messaging, core banking systems, trading platforms, and custody records — a cryptographically relevant quantum computer (CRQC) would not merely disrupt IT operations; it would undermine the confidentiality and integrity guarantees that global finance is built on. This paper examines quantum-safe cryptography through the lens of an MBA FinTech and business-strategy candidate rather than a cryptography researcher. It frames the "Harvest Now, Decrypt Later" (HNDL) threat as an immediate balance-sheet and reputational liability, not a distant technical problem; evaluates the cost and return-on-investment trade-offs of migrating legacy core banking systems to Post-Quantum Cryptography (PQC); and situates the discussion within the regulatory directives now shaping bank behaviour, including NIST's FIPS 203/204/205 standards, the Bank for International Settlements' (BIS) Project Leap, and the G7 Cyber Expert Group's 2026 migration roadmap. Drawing on real-world pilots at HSBC and JPMorgan Chase, the paper proposes a four-phase strategic migration roadmap — discovery, prioritisation, hybrid deployment, and governance — and argues that quantum-safe resilience is fast becoming a source of competitive advantage rather than a compliance cost. The central takeaway for financial leaders is that the migration decision is no longer whether to act, but how quickly and in what sequence, given multi-year implementation timelines and a market that is already rewarding early movers with trust and access.

1. Introduction & The Business Problem

1.1 Background: The Q-Day Horizon

Modern financial infrastructure is secured by asymmetric, or "public-key," cryptography — mathematical schemes such as RSA and Elliptic Curve Cryptography (ECC) that function, in business terms, as the digital equivalent of a notarised signature and a sealed envelope for a wire transfer. Every SWIFT message, every TLS-encrypted session between a customer's banking app and a core system, and every digital certificate that authenticates a trading counterparty depends on the assumption that certain mathematical problems — factoring large numbers, solving discrete logarithms — are practically unsolvable with classical computers. A sufficiently powerful quantum computer, applying Shor's algorithm, would solve those problems efficiently, unravelling the assumption on which decades of financial security architecture rests.

The arrival date of such a machine — colloquially "Q-Day" — remains genuinely uncertain. Expert surveys cluster around the early-to-mid 2030s: the Global Risk Institute's expert panel places the probability of a cryptographically relevant quantum computer at roughly one-in-three by 2034, up sharply from earlier assessments, while national security agencies such as the U.S. NSA plan on the assumption that high-value systems should be quantum-safe by 2035. Point estimates vary — some analysts argue RSA-2048 could fall as early as 2030, others place the threshold closer to 2040

— but the strategic implication for financial leaders is the same regardless of which forecast proves correct: multi-year migration timelines mean the planning clock has already started, irrespective of exactly when the quantum clock runs out.

1.2 The "Harvest Now, Decrypt Later" Threat

The most financially consequential aspect of the quantum threat is not futuristic — it is happening today. In an HNDL attack, adversaries (nation-states, organised cybercrime, or competitors) intercept and store encrypted financial data now, with no ability to read it, banking on the certainty that a future quantum computer will let them decrypt it retroactively. For a retail purchase confirmation, this is a non-event; the data is worthless in five years. But for a financial institution, an enormous share of the data it transmits and stores has a confidentiality shelf-life measured in decades: mortgage and loan documentation, wealth-management portfolios, merger and acquisition communications, sovereign debt issuances, know-your-customer (KYC) records, and long-dated derivative contracts. Data intercepted today that will still be commercially or personally sensitive in 2035 is, in effect, already compromised — the institution simply does not yet know it.

Framed this way, HNDL converts quantum risk from a future IT migration project into a present-day data-classification and liability problem: which data flowing across the network today will still matter in ten to fifteen years, and is it protected against an attacker who is patient rather than fast?

1.3 Quantifying the Threat: Expert Timeline Estimates

Because no single forecasting method commands consensus, the most defensible approach for a strategy document is to triangulate across several independent expert-survey and modelling efforts rather than anchor on one number. Table 2 summarises the range.

Source / Method	Estimate	Interpretation
Global Risk Institute expert panel (2024 survey)	≈34% probability of a CRQC by 2034	Roughly double the 17% probability the same panel assigned to 2034 in its 2022 survey — a marked acceleration
Survey of quantum-computing experts (RSA-2048 focus)	≈23% likely/highly likely by 2030; ≈50% likely/highly likely by 2035	Early-2030s break considered a minority view; mid-2030s treated as a coin-flip by the expert community
RAND Corporation expert consensus (2023)	CRQC unlikely before the 2030s	A more conservative reference point, still consistent with a 2030s-decade horizon
U.S. NSA planning assumption (CNSA 2.0)	Systems quantum-safe by ~2035	A defensive planning posture rather than a probability forecast — plan for the earlier end of plausible outcomes
Applied cryptanalysis / hardware-resource estimates	RSA-2048 feasibly broken 2030 (±2 years) under some analyses	Reflects recent reductions in estimated physical-qubit requirements (from ~20 million in 2019 estimates to under 1 million in more recent analyses)

Table 2: Expert Q-Day timeline estimates by source. Figures are illustrative syntheses of publicly reported expert-survey and modelling literature and should not be read as point predictions.

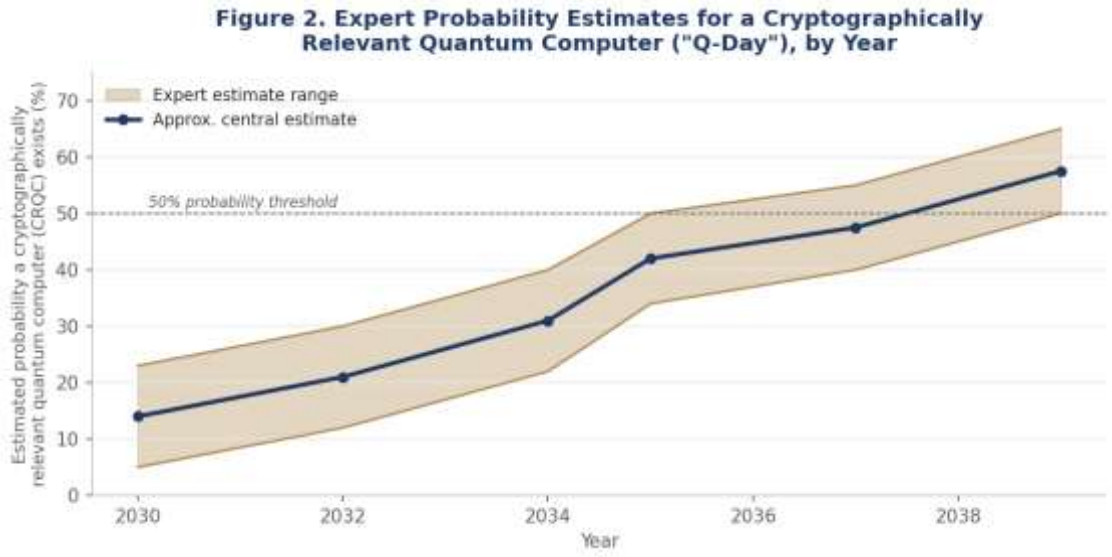


Figure 2: Estimated probability of a cryptographically relevant quantum computer existing, by year, synthesising the expert-survey ranges in Table 2.

The practical reading of Figure 2 for a financial institution is not the specific year at which the curve crosses 50% — reasonable experts disagree on that by a decade or more — but the shape of the curve: probability estimates have been revised upward at every successive survey, and the gap between "comfortably safe" and "actively at risk" has been narrowing rather than widening. A capital-planning process that waits for certainty before allocating budget will, by construction, always be several years late.

1.4 Problem Statement

The financial industry's cryptographic backbone was engineered for durability and interoperability, not for rapid replacement. Core banking platforms, payment rails, and messaging standards were built on RSA and ECC with the reasonable expectation that these algorithms would remain secure for the operational life of the systems. That assumption no longer holds. The economic cost of inaction compounds over time: every certificate issued, every API secured, and every long-lived dataset encrypted under classical cryptography between now and full migration adds to a growing inventory of retroactive exposure. Yet because the threat has no fixed, universally agreed trigger date, many institutions are systematically under-investing relative to the risk — a classic case of a low-probability, high-severity event competing poorly for budget against quarter-to-quarter operational priorities.

2. Financial Implications & Risk Assessment (The MBA Perspective)

2.1 Systemic Financial Risk

Quantum risk is systemic because financial infrastructure is a network, not a set of isolated institutions. SWIFT alone connects more than 11,000 member institutions across roughly 200 countries; a cryptographic weakness anywhere in that mesh can undermine confidence in the whole. Central clearing houses, real-time gross settlement systems, and card networks share the same characteristic: they are only as strong as their least-prepared participant. Industry surveys of SWIFT readiness illustrate the concern concretely — as of 2025, a large majority of Tier 1 banks had begun PQC evaluation, but only a small fraction of Tier 3 institutions had started planning, creating exactly the kind of weakest-link vulnerability that concerns systemic-risk regulators. For a CFO or CISO, the implication is that an institution's own migration timeline is necessary but not sufficient; counterparty and vendor readiness must be assessed as part of enterprise risk management.

2.2 Valuation & Balance-Sheet Risk

Cryptographic vulnerability is increasingly a factor institutional investors, rating agencies, and regulators will price into their assessments of a bank, much as cybersecurity posture already is. A credible, board-owned PQC migration roadmap signals operational risk maturity; the absence of one is a governance gap that can affect operational risk-capital requirements under frameworks such as Basel's operational risk provisions, and may eventually feature in credit-rating methodology and cyber-insurance underwriting, in the same way unpatched legacy IT already does.

2.3 Cost of Migration versus Cost of Breach

The core capital-allocation question facing every financial institution is a classic cost-of-prevention-versus-cost-of-failure trade-off, complicated by radical uncertainty about timing. Independent cost estimates vary by scope and methodology, but converge on the order of magnitude below.

Cost Category	Illustrative Estimate	Basis / Source Context
U.S. federal agency PQC migration (excl. national security systems), 2025–2035	≈ US$7.1 billion	Government cost assessment cited in academic literature on global PQC roadmaps
Annual IT budget allocation for PQC transition (per institution, 3–5 years)	≈ 0.5% – 1.2% of IT budget	World Economic Forum estimate referenced in coordination-economics research
Global coordinated PQC migration cost (all sectors)	≈ US$280 – 420 billion	Policy-brief estimate modelling financial system as a coordination network
Cost of a delayed / disorderly cryptographic break (global)	up to ≈ US$3.5 trillion	Same source — probabilistic, back-loaded cost of inaction
Indirect losses from a quantum-enabled disruption to one major bank's Fedwire access	≈ US$2 – 3.3 trillion (10–17% of a benchmark measure)	Estimate originating with the Hudson Institute, cited in subsequent Federal Reserve and industry analysis
Telecom-scale enterprise PQC program (illustrative proxy for a large bank's network layer)	≈ US$50 – 300+ million over program life	Industry program-management cost modelling

Table 1: Illustrative cost estimates for PQC migration versus inaction. Figures vary widely by methodology and scope and should be treated as directional, not predictive.

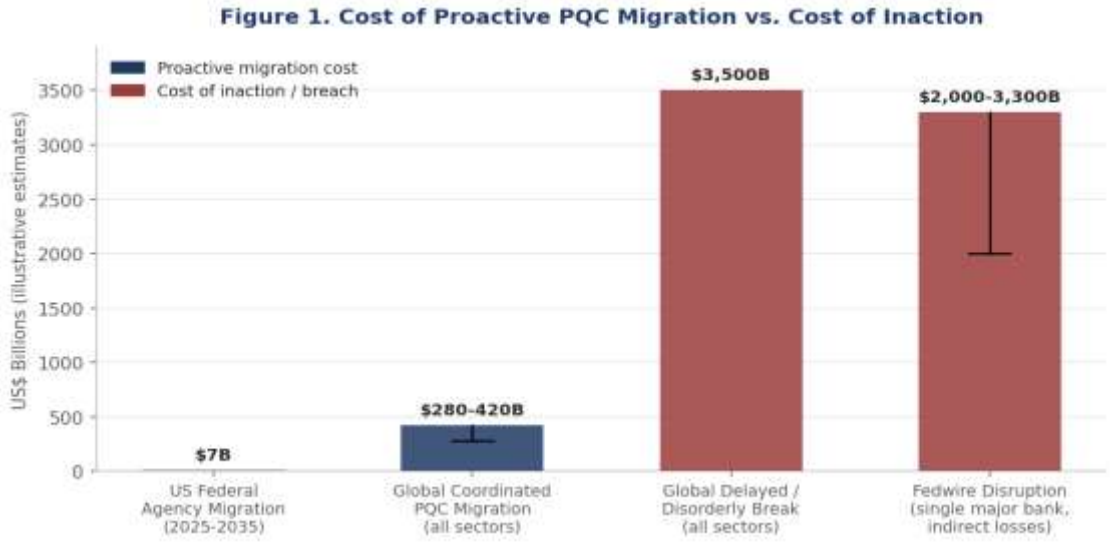


Figure 1: Cost of proactive PQC migration compared with the cost of inaction, plotted from the estimates in Table 1. Note the order-of-magnitude gap between the two categories.

Two features of this cost asymmetry matter for capital budgeting. First, migration costs are front-loaded and comparatively knowable — an institution can scope a discovery-and-inventory exercise, staff a program office, and budget accordingly. Second, breach costs are probabilistic and back-loaded, and standard corporate discount rates of 8–12% mechanically shrink the present value of a loss that might materialise five to fifteen years out. This is precisely the bias that makes proactive migration a hard sell inside conventional capital-budgeting frameworks, even when the expected value of early action is clearly positive — a dynamic MBA finance training recognises as a classic real-options mispricing problem: the option to migrate early has value that a naive discounted-cash-flow comparison understates.

The comparison financial institutions have lived through before is instructive. The industry's shift from magnetic-stripe cards to EMV chips took roughly two decades and cost the sector billions; SWIFT's move to the ISO 20022 messaging standard alone took about seven years. The PQC transition touches a comparable footprint — every certificate authority, hardware security module (HSM), API, and long-lived dataset — but with a harder, less negotiable deadline, since NIST guidance points toward deprecating RSA-2048 and ECC-256 by 2030 and disallowing them after 2035.

2.4 Risk Matrix by Business Line

Because HNDL exposure depends heavily on how long data must remain confidential, and systemic exposure depends on how tightly a function is coupled to the wider network, the quantum risk profile differs materially across a bank's business lines. Table 3 offers an illustrative first-pass risk matrix that a CISO or CRO could use as a starting template for the discovery phase discussed in Section 6.

Business Line / Function	Typical Data Confidentiality Horizon	Network / Systemic Coupling	Illustrative Priority
Wire transfers & correspondent banking (SWIFT)	Short (transaction detail); long (audit trail)	Very high — multi-institution network	Critical
Custody & wealth management records	Very long (decades)	Moderate	Critical
Trade finance & letters of credit	Long (contract life plus dispute window)	High — counterparty banks	High
FX & derivatives trading platforms	Short-to-moderate	High — market infrastructure	High
Retail digital banking (app authentication)	Short-to-moderate	Moderate	Medium
Mortgage & long-dated loan documentation	Very long (loan life, 15-30 years)	Low-to-moderate	High
KYC / AML customer records	Very long (regulatory retention)	Low	High
Internal collaboration & low-sensitivity IT	Short	Low	Low

Table 3: Illustrative risk matrix by business line, combining data-longevity (HNDL exposure) with network coupling (systemic exposure). Actual prioritisation should be based on an institution-specific cryptographic inventory (Section 6, Phase 1).

A useful heuristic emerges from Table 3: the business lines that feel least urgent day-to-day — custody records, KYC files, long-dated mortgages — are often the most urgent from a quantum-risk standpoint, precisely because their data outlives most institutions' current planning horizons. This is a case where risk prioritisation driven by cyber-incident frequency (which would favour retail banking, the most-attacked surface) diverges from risk prioritisation driven by HNDL exposure (which favours long-lived, low-attack-frequency archives) — a distinction the discovery and prioritisation phases of the roadmap in Section 6 are explicitly designed to surface.

3. Technology Overview (Simplified for Business Executives)

For a finance executive, the two families of quantum-safe technology can be understood through a simple analogy: one changes the lock, the other changes how the key is delivered.

3.1 Post-Quantum Cryptography (PQC): Changing the Lock

PQC is a software-based solution — new mathematical algorithms that run on ordinary computers and are believed to resist attack from both classical and quantum machines. In August 2024, after an eight-year public evaluation process, NIST finalised the first three PQC standards: FIPS 203 (ML-KEM, for establishing a shared secret key — the digital equivalent of two parties agreeing on a combination for a shared vault, even while a third party is listening to every word of the negotiation); FIPS 204 (ML-DSA, for digital signatures — the electronic notarisation on a wire transfer or a trade confirmation); and FIPS 205 (SLH-DSA, a more conservative, hash-based signature scheme kept in reserve as a structurally different fallback in case weaknesses are later found in the lattice-based mathematics underlying the other two). Because PQC is software, it can, in principle, be integrated into existing banking applications, TLS connections, and messaging platforms through updates — the practical challenge is less "can we install it" than "can we find every place classical cryptography is quietly embedded across a decades-old technology estate".

Table 4 summarises the three finalised NIST standards in terms a non-cryptographer can use directly, and Figure 4 visualises how much larger PQC keys and signatures are than their classical predecessors — a practical engineering consideration, since larger keys and signatures consume more bandwidth and storage across millions of daily transactions.

Standard	Common Name	Function	Business Analogy	Relative Size vs. Classical
FIPS 203	ML-KEM (from CRYSTALS-Kyber)	Key encapsulation — establishing a shared secret	Two parties agreeing a vault combination while someone listens to the whole conversation	Public key ≈5x larger than RSA-2048
FIPS 204	ML-DSA (from CRYSTALS-Dilithium)	Digital signatures — primary replacement for ECDSA/RSA signing	Electronic notarisation on a wire transfer or trade confirmation	Signature ≈13x larger than RSA-2048
FIPS 205	SLH-DSA (from SPHINCS+)	Hash-based digital signatures — conservative fallback	A second, structurally independent notary stamp kept in reserve	Signature ≈31x larger than RSA-2048; markedly slower to compute

Table 4: NIST-standardised PQC algorithms at a glance.

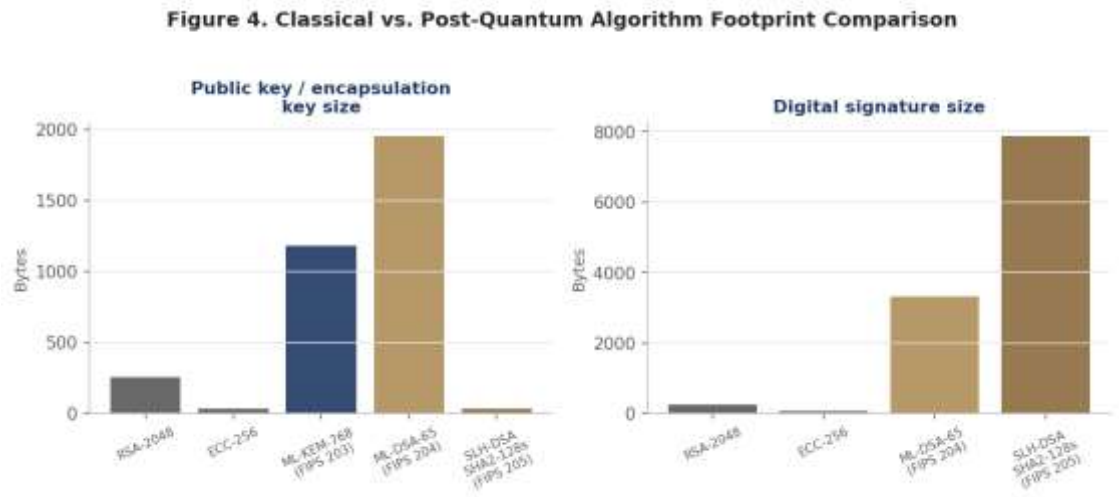


Figure 4: Public key and digital signature sizes for classical (RSA-2048, ECC-256) versus post-quantum (ML-KEM-768, ML-DSA-65, SLH-DSA SHA2-128s) algorithms. Larger footprints translate into real infrastructure costs — more bandwidth per transaction, larger certificate stores, and in some cases hardware upgrades to payment terminals and HSMs.

The practical business implication of Figure 4 is that PQC migration is not simply "swap algorithm A for algorithm B" inside existing infrastructure sized for classical cryptography. Systems built around the assumption of small, fixed-size keys and signatures — smart cards, legacy point-of-sale terminals, some embedded ATM controllers — may need hardware, not just software, upgrades, which is precisely why payments-industry analysts have flagged device-replacement volumes in the tens of billions as a multi-year capital-expenditure programme in its own right.

3.2 Quantum Key Distribution (QKD) & Quantum Random Number Generators (QRNG): Changing the Delivery

QKD is a physics-based hardware solution: rather than relying on a mathematical problem being hard to solve, it uses the properties of quantum mechanics so that any attempt to intercept a cryptographic key physically disturbs it, alerting both parties. This makes QKD attractive for the highest-value, highest-bandwidth links between fixed points — for example, connections between a bank's own data centres, or between two exchanges — but it requires dedicated fibre-optic or satellite infrastructure and remains costly relative to a software update, which is why it is being piloted for specific, high-value corridors rather than deployed institution-wide. QRNG, a related technology, generates truly unpredictable random numbers from quantum physical processes, strengthening the key-generation step that underpins both classical and post-quantum cryptography.

3.3 Cryptographic Agility: The Strategic Prerequisite

Perhaps the most important concept for a business audience is cryptographic agility — the ability of a system to swap out an encryption algorithm without rebuilding the surrounding application. Many legacy core-banking and payment systems today hard-code a specific algorithm (RSA, or a specific elliptic curve) directly into contracts, firmware, or application logic, meaning that changing it requires a full engineering project rather than a configuration change. Building agility is, in effect, an insurance policy against the next cryptographic transition, whichever algorithm eventually needs replacing — a lesson reinforced by BIS Project Leap, which found that a successful cryptographic proof-of-concept is not the same as a production-ready, agile service, and that realistic testing must include peak transaction volumes, certificate rotation, and failover, not just a laboratory demonstration.

4. Regulatory, Compliance, and Governance Landscape

4.1 Global Regulatory Expectations

Regulatory attention has moved quickly from academic interest to formal coordination. NIST's FIPS 203, 204, and 205 (effective August 2024) give the financial sector standardised algorithms to build against, with the U.S. National Security Agency's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) setting 2030 as a mandatory migration deadline for national security systems, and NIST guidance signalling deprecation of RSA-2048/ECC-256 by 2030 and prohibition after 2035.

At the international level, the Bank for International Settlements published a landmark roadmap, "Quantum-readiness for the financial system," in July 2025, urging central banks and supervisors to treat quantum risk as a proactive, coordinated cybersecurity priority rather than a distant research topic. Its BIS Innovation Hub initiative, Project Leap, has run in two phases: Phase 1 demonstrated hybrid (classical-plus-PQC) encryption of payment messages between two central banks; Phase 2, run with the Bank of Italy, Bank of France, Deutsche Bundesbank, Nexi-Colt, and Swift, went further and replaced traditional digital signatures with post-quantum cryptography inside an operational payment system — the Eurosystem's TARGET2 liquidity-transfer messages — demonstrating that PQC can function inside live, mission-critical settlement infrastructure, not just in a laboratory.

In January 2026, the G7 Cyber Expert Group — co-chaired by the U.S. Department of the Treasury and the Bank of England, and which advises G7 finance ministers and central bank governors — released a coordinated roadmap for the sector's transition to post-quantum cryptography. Notably, the G7 CEG statement explicitly does not set binding guidance or regulatory expectations; it is intended to inform planning and encourage a harmonised transition, leaving national supervisors such as Singapore's Monetary Authority (MAS) and Switzerland's FINMA to translate the roadmap into jurisdiction-specific supervisory expectations. For a multinational institution, this means quantum-readiness will likely arrive unevenly by jurisdiction, and coordination through cross-border bodies like the G7 CEG and BIS is precisely what is meant to reduce that fragmentation risk.

Figure 6. Timeline of Key Regulatory and Standardisation Milestones



Figure 6: Timeline of key regulatory and standardisation milestones, 2016–2035. The pace of formal coordination has accelerated markedly since NIST's 2024 standardisation.

Jurisdiction / Body	Instrument	Character	Indicative Timeline
United States — NIST / NSA	FIPS 203/204/205; CNSA 2.0	Binding federal standard; mandatory for national security systems	Effective 2024; NSS deadline 2030–2033; RSA-2048/ECC-256 disallowed after 2035
Global — Bank for International Settlements	"Quantum-readiness for the financial system" roadmap; Project Leap	Advisory framework and technical pilots for central banks and supervisors	Published July 2025; phased awareness (2025-26), planning (2026-28), migration (late 2020s)
G7 — Cyber Expert Group (US Treasury / Bank of England co-chairs)	Coordinated transition roadmap	Explicitly non-binding — informs planning, does not set regulatory expectations	Released January 2026
Singapore — Monetary Authority (MAS)	Supervisory guidance (jurisdiction-specific)	National supervisory expectations, informed by international roadmaps	Evolving; institutions should track MAS circulars directly
Switzerland — FINMA	Supervisory guidance (jurisdiction-specific)	National supervisory expectations	Evolving; institutions should track FINMA circulars directly
European Union	EU quantum-safe roadmap referenced in industry commentary	Policy direction for critical financial infrastructure	Industry commentary points to PQC on critical financial infrastructure by 2030

Table 5: Regulatory and supervisory landscape by jurisdiction. This table is illustrative and non-exhaustive; institutions operating across borders should confirm current requirements directly with each supervisor, since guidance in this area is evolving quickly.

4.2 Vendor Risk & Supply-Chain Bottlenecks

Very few financial institutions build their own core banking software, hardware security modules, cloud infrastructure, or ATM networks — they rely on a concentrated set of third-party vendors, which means an institution's quantum-safety is only as strong as its slowest supplier. Effective governance therefore requires extending PQC requirements into vendor contracts and due-diligence questionnaires: does the core-banking provider have a published PQC roadmap; can the HSM vendor support hybrid classical/PQC keys today; does the cloud platform offer PQC-enabled TLS. The payments industry illustrates the scale of this bottleneck starkly — industry estimates cited in payments-sector analysis put the eventual replacement need for quantum-vulnerable payment cards and terminals in the tens of billions of devices globally, a supply-chain and capital-expenditure undertaking with few historical parallels outside the EMV chip transition.

5. Strategic Migration Roadmap for Financial Institutions

Translating the regulatory direction above into an executable program is best organised as a four-phase roadmap, consistent with the approach BIS, NIST, and the G7 CEG each independently recommend.

Phase	Objective	Key Activities
Phase 1 — Cryptographic Discovery & Inventory	Know what you have	Map every RSA/ECC asset, API endpoint, certificate, HSM, and long-lived dataset across the technology estate; classify data by confidentiality shelf-life to prioritise HNDL exposure
Phase 2 — Prioritisation & Risk Matrix	Know what matters most	Rank assets by business criticality and data longevity — wire-transfer authentication and custody records rank above low-sensitivity internal tools; align with vendor and counterparty readiness
Phase 3 — Hybrid Deployment & Testing	De-risk the transition	Deploy hybrid classical-plus-PQC schemes (as tested in BIS Project Leap) so an attacker must break both algorithms; test under realistic transaction volumes, peak load, certificate rotation, and failover conditions
Phase 4 — Full PQC Governance & Agility	Make it permanent	Retire classical algorithms once PQC is proven at scale; institutionalise cryptographic agility so future transitions are configuration changes, not rebuilds; establish continuous board-level oversight and reporting

Table 6: Four-phase strategic migration roadmap.



Figure 3: Illustrative timeline for the four-phase migration roadmap, overlaid against the NIST/CNSA 2.0 2030 deprecation marker. Phases overlap deliberately — prioritisation can begin before discovery is complete for the highest-risk systems, and hybrid testing can begin on early-discovered assets while lower-priority systems are still being inventoried.

This phasing mirrors the BIS roadmap's own suggested cadence — awareness and inventory work concentrated in 2025–26, planning through 2026–28, and major migrations toward the end of the decade — and reflects the hard-won lesson from Project Leap Phase 2 that a working pilot and a production-ready, resilient service are two different engineering problems.

5.1 Governance: Who Owns the Programme

A migration of this scope cuts across technology, risk, compliance, treasury, and the executive committee, and experience from comparable enterprise-wide transitions (EMV, ISO 20022) suggests that unclear ownership is one of the most common causes of schedule slippage. Table 7 sketches an illustrative RACI (Responsible, Accountable, Consulted, Informed) structure for a large institution's programme.

Activity	CISO / Security	CTO / Engineering	CFO / Treasury	Board Risk Committee	Business Line Owners
Cryptographic discovery & inventory	A	R	I	I	C
Risk prioritisation matrix	R	C	C	A	C
Budget allocation & capital planning	C	C	R	A	I
Hybrid deployment & testing	C	R	I	I	C
Vendor / third-party PQC due diligence	R	C	C	I	A
Regulatory reporting & board oversight	C	I	C	A	I

Table 7: Illustrative governance RACI for a PQC migration programme (R = Responsible, A = Accountable, C = Consulted, I = Informed). Structures should be adapted to each institution's existing risk-governance model.

6. Case Studies & Real-World FinTech Applications

6.1 HSBC: Tokenised Assets and FX Trading

HSBC has run the financial sector's most publicly documented set of quantum-safe pilots. In 2024, working with Quantinuum, the bank trialled PQC and Quantinuum's Quantum Origin randomness technology to protect the transfer of tokens representing physical gold on its Orion digital-asset platform — explicitly framed as protection against "store now, decrypt later" attacks on tokenised assets, and including interoperability testing that converted HSBC gold tokens into ERC-20 fungible tokens across distributed ledgers. Separately, HSBC partnered with BT and Toshiba to join London's Quantum Secure Metro network and, in a further first, used QKD alongside PQC to protect a simulated €30 million foreign-exchange trade on a live AI-driven trading terminal — the first time a bank had trialled quantum-safe protection of an active trading system. HSBC has been notably open about sharing these results, framing industry collaboration ("we all need to move forward together") as essential given the network nature of the risk described in Section 3.1.

6.2 JPMorgan Chase: Quantum-Secured Infrastructure

JPMorgan Chase has pursued a parallel, infrastructure-first strategy, deploying a Quantum-secured Crypto-Agile Network (Q-CAN) linking two data centres over roughly 29 miles of fibre in Singapore, combining QKD-secured infrastructure operating at 100 Gbps with a PQC-enabled key exchange. In March 2025, the bank also published a certified quantum-randomness milestone with Quantinuum, reflecting a dual strategy of investing in both PQC software and QKD hardware rather than treating the two as substitutes.

6.3 Payment-Network Readiness: SWIFT

At the network-infrastructure layer, industry analysis expects SWIFT to make its SwiftNet 8.0 messaging platform PQC-enabled around 2027, with an approximate 15-month migration window for participating institutions — underscoring the earlier point that an individual bank's readiness is necessarily bounded by the readiness of the shared network it depends on.

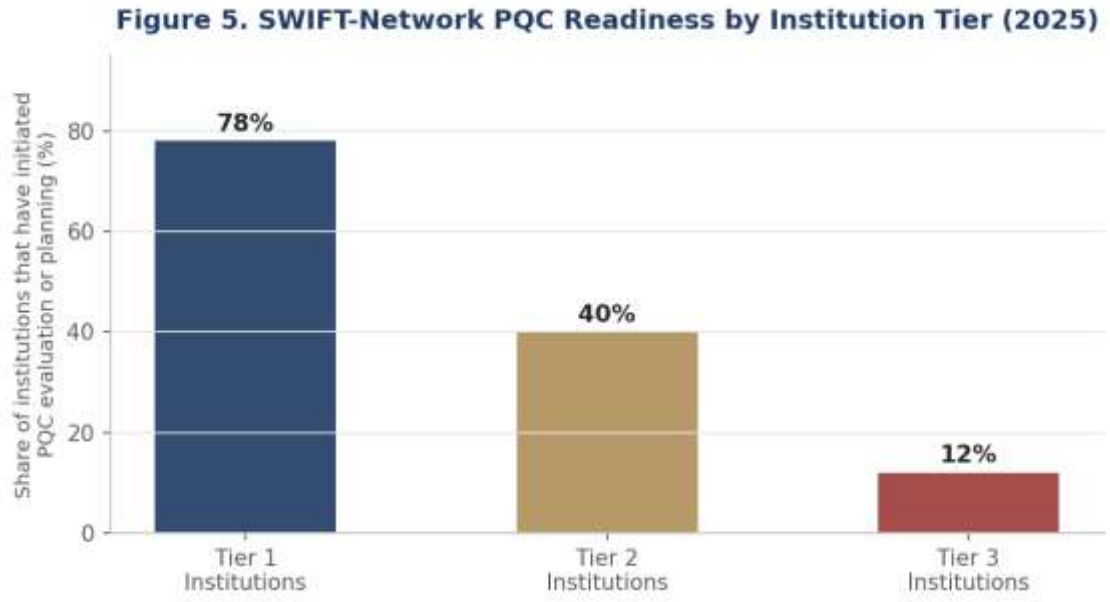


Figure 5: Share of SWIFT-network institutions that had initiated PQC evaluation or planning by institution tier, 2025. The steep drop-off from Tier 1 to Tier 3 illustrates the weakest-link dynamic described in Section 3.1.

Dimension	HSBC	JPMorgan Chase	SWIFT (network layer)
Primary technology focus	PQC + QKD (dual strategy)	QKD-secured infrastructure + PQC key exchange	PQC-enabled messaging standard
Flagship initiative	Tokenised gold PQC pilot; QKD-protected €30m FX trade	Quantum-secured Crypto-Agile Network (Q-CAN), Singapore	SwiftNet 8.0 PQC enablement
Key partners	Quantinuum, BT, Toshiba, AWS	Quantinuum (quantum randomness milestone)	Central banks and member institutions via BIS Project Leap
Primary use case protected	Digital asset tokenisation; live FX trading terminal	Inter-data-centre confidentiality (100 Gbps over ~29 miles of fibre)	Interbank messaging across ~11,000 member institutions
Indicative timeline	Pilots completed 2024-2025	Operational network; randomness milestone March 2025	PQC enablement expected ~2027; ~15-month member migration window

Table 8: Case study comparison — HSBC, JPMorgan Chase, and SWIFT. HSBC and JPMorgan illustrate institution-level pilots; SWIFT illustrates the shared network layer both institutions (and ~11,000 others) ultimately depend on.

6.4 Lessons for FinTech Startups versus Incumbent Tier-1 Banks

The contrast between HSBC and JPMorgan's pilots and the broader industry survey data in Section 3.1 (strong Tier 1 engagement, weak Tier 3 engagement) points to two different strategic postures:

- FinTech startups and challengers carry less legacy cryptographic debt and can plausibly build cryptographic agility in from day one — turning quantum-readiness into a genuine differentiator when competing for institutional partnerships or banking-as-a-service mandates, where counterparties increasingly ask about PQC roadiness in due diligence.
- Incumbent Tier-1 banks carry decades of hard-coded cryptography across core banking, card networks, and messaging systems, but also have the balance sheet and influence to run the kind of large, cross-institutional pilots — HSBC and JPMorgan among them — that shape industry standards and vendor roadmaps.
- Tier 2 and Tier 3 institutions face the least favourable combination — meaningful legacy debt without the scale to run independent pilots — and are best served by closely tracking vendor and network-level readiness (core banking providers, SWIFT, card schemes) rather than attempting to lead.

7. Conclusion & Strategic Recommendations

7.1 SWOT Analysis of Quantum-Safe Resilience as a Strategic Initiative

Before setting out final recommendations, it is useful to step back and frame quantum-safe migration the way an MBA strategy course would frame any major capital initiative — as a position with internal strengths and weaknesses, and external opportunities and threats.

Strengths	Weaknesses
Standards are finalised and stable (FIPS 203/204/205); vendors and cloud providers are actively shipping PQC-enabled products; hybrid deployment allows risk-managed rollout without a single cutover event.	Legacy core-banking systems often hard-code cryptography, raising migration cost and duration; larger PQC key/signature sizes strain constrained hardware (cards, terminals, embedded HSMs); PQC expertise is scarce and unevenly distributed across the industry.
Opportunities	**Threats**
Early movers (HSBC, JPMorgan) are building reputational and regulatory goodwill and shaping vendor/standards roadmaps; quantum-readiness is emerging as a differentiator in institutional due diligence and correspondent-banking relationships; cryptographic agility built now reduces the cost of the next (inevitable) cryptographic transition.	Network dependency means a single unprepared counterparty, vendor, or Tier 3 institution can undermine an otherwise well-migrated institution's protection; HNDL means today's inaction is retroactively punished once a CRQC exists; regulatory fragmentation across jurisdictions raises coordination cost for multinational institutions.

Table 9: SWOT analysis of quantum-safe resilience as a strategic initiative.

7.2 Concluding Assessment

Quantum-safe cryptography sits at an unusual intersection for financial leaders: the underlying technology risk is genuinely uncertain in timing, yet the required response is not. NIST's finalised standards mean the primary constraint on migration is no longer algorithmic — it is organisational discovery, vendor coordination, and capital sequencing. The "Harvest Now, Decrypt Later" threat converts a future risk into a present one for any institution holding long-lived sensitive data, which describes nearly every bank, insurer, and asset manager. And the regulatory signal, from NIST through BIS to the G7 Cyber Expert Group, has moved decisively from research-stage interest to coordinated, phased expectation over the 2025–2035 window.

Three strategic recommendations follow directly from the analysis in this paper:

1. Treat discovery as the first and most urgent budget line. An institution cannot prioritise, hybridise, or govern cryptographic assets it has not inventoried; the discovery phase is comparatively inexpensive and de-risks every subsequent phase of the roadmap in Section 6.

2. Extend quantum-readiness into vendor and counterparty risk management now, not after core systems are migrated, since network effects mean an institution's own migration delivers only partial protection until its critical counterparties — card networks, correspondent banks, cloud and HSM vendors — migrate as well.

3. Build cryptographic agility as the durable capability, treating the current PQC transition as the first of what will likely be several future cryptographic transitions, rather than a one-time project to be completed and forgotten.

For CFOs and CISOs, the business case increasingly resembles other infrastructure resilience investments made in advance of a known but unpredictably timed shock: the expected cost of early, orderly migration is a known and bounded number, while the expected cost of a late, disorderly one is unbounded and reputationally severe. Institutions that treat quantum-safe resilience as a genuine strategic capability — visible to regulators, counterparties, and increasingly to institutional clients conducting cryptographic due diligence — are positioning quantum readiness not merely as a defensive necessity but as a differentiator in a financial system where trust in the integrity of a transaction is, ultimately, the product being sold.

8. References

Bank for International Settlements. (2025). Quantum-readiness for the financial system: A roadmap. BIS Innovation Hub. https://www.bis.org

Bank for International Settlements Innovation Hub. (2025). Project Leap: Quantum-proofing payment systems (Phase 2 report). https://www.bis.org/publ/othp107.pdf

G7 Cyber Expert Group. (2026). Advancing a coordinated roadmap for the transition to post-quantum cryptography in the financial sector [Statement]. U.S. Department of the Treasury and Bank of England. https://home.treasury.gov

National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. U.S. Department of Commerce. https://csrc.nist.gov

National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. U.S. Department of Commerce. https://csrc.nist.gov

National Institute of Standards and Technology. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. U.S. Department of Commerce. https://csrc.nist.gov

National Institute of Standards and Technology. (2024, August). NIST releases first 3 finalized post-quantum encryption standards [Press release]. https://www.nist.gov

HSBC Holdings plc. (2024). HSBC pilots quantum-safe technology for tokenised gold [Media release]. https://www.hsbc.com

HSBC Holdings plc. (2025). HSBC and quantum [Corporate disclosure]. https://www.hsbc.com/who-we-are/hsbc-and-digital/hsbc-and-quantum

ISACA Journal. (2025). Building resilient security in the age of quantum computing. ISACA Journal, 2025(6). https://www.isaca.org

The Quantum Insider. (2026). Post-quantum cryptography timelines: When will organizations migrate? https://thequantuminsider.com

Global Risk Institute. (2024). Quantum threat timeline report (expert survey). Referenced in: Securing cryptography in the age of quantum computing and AI. arXiv:2603.06969.

Postquantum.com. (2026). Global roadmaps for post-quantum era in finance: Policies, timelines, and a pragmatic playbook for migration. MDPI FinTech, and related industry analyses on payments and PQC migration economics.

Mishra, D., & Phansalkar, S. (2025). Blockchain security in focus: A comprehensive investigation into threats, smart contract security, cross-chain bridges, vulnerabilities detection tools & techniques. IEEE Access.

Sahoo, D. R., & Sahoo, V. D. (2026). Crypto derivatives markets: Price discovery, volatility dynamics, market efficiency, and DeFi risk: A structural analysis. Journal of Engineering and Technology Management, 80(April–June), 774–799.

Sahoo, V. D., & Sahoo, D. R. (n.d.). Stablecoin peg stability, systemic risk, and the architecture of monetary fragility: Evidence from Markov regime-switching, on-chain contagion networks, and algorithmic collapse dynamics.

Mishra, U. M., & Dash, A. S. (n.d.). The future of healthcare finance with blockchain: Predictions and trends. In Decentralized Healing (pp. 367–392).

Dr. Gupta M, Dr. M. U. (2014). Financial regulatory framework.

Sahoo, D. R., & Deepak, S. V. (2024). Exploring the nexus of sustainable finance: ESG ethical framework practices. In Ethical Quandaries in Business Practices (pp. 253–280). IGI Global.

Deepa U. Mishra, P. W., Shwetambari A. Chiwhane, Kajal Adsul, Gauri Sawant, Swati Shende. (2016). Augmented Reality based multipurpose application for 3D interface. *International Engineering Research Journal*, *2*(6), 2211–2213.

Anand Mohan, Dr. U. M., M. Sundararajan. (2022). GREEN COMPUTING: IMPROVISED SUSTAINABILITY WITH LONG TERM VIABILITY. *Journal of Emerging Technologies and Innovative Research (JETIR) Www.Jetir.Org*, *9*(9), 6.

Chaurasiya, S., Shekhar, S., Shariq, S., Chavan, S., & Mishra, D. (n.d.). *ONLINE MARKET SYSTEM BASED ON BIDDING MECHANISM USING AN AI AUCTIONEER*.

Chiwhane, S., Deepa, M., & Shweta, K. (2017). IOT Based Fuel Monitoring for Future Vehicles. *International Journal of Advanced Research in Computer and Communication Engineering*, *6*, 295–297.

Dash, A. S., & Mishra, U. (2024a). Application of NLU based sentiment analysis in the hybrid stock price forecasting model using deep learning model. *2024 IEEE Pune Section International Conference (PuneCon)*, 1–6.

Dash, A. S., & Mishra, U. (2024b). Stock market trend prediction model using deep learning based sentiment analysis of financial data. *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, 1–7.

Deepa Mishra, T. Y. (2017). Secure IOT Based HealthCare System with BSN. *International Engineering Research Journal*, *2*(9), 3208–3011.

Deepak Ranjan Sahoo, P. D. K. (2017). Emotional Intelligence: Managing Stress and Anxiety at work Place. *International Journal Of Multifaceted And Multilingual Studies*, *4*(10), 88–93.

Deepak Ranjan Sahoo, V. D. S. (2019a). A Study of Economic Literacy and sustainable development with context to India. *COSMOS Bi- Annual Referred Journal*, *10*(1), 47–53.

Deepak Ranjan Sahoo, V. D. S. (2019b). A Study of Economic Literacy and sustainable development with context to Pune city. *Scholarly Research Journal for Interdisciplinary Studies*, *7*(41), 382–389.

Deepak Ranjan Sahoo, V. K. J. (2017). DERIVATIVES: A device for Risk Management. *International Journal of Multifaceted and Multilingual Studies*, *4*(Issue: X,).

Dr. Gupta M, Dr. M. U. (2014). *Financial Regulatory Framework*.

Dr. Harshal Raje, Mr. S. P., Dr. Ujjwal Mishra. (2020). Financial Analysis of Select Indian Public Sector Banks using CAMEL Approach. *Tathapi*, *19*(38), 193–212.

Dr. Lalkar P, Dr. M. U., Dr. Tejwani N, Dr. Rayate B. (2013). *Accounting for Business Decisions*.

Dr. Ujjwal M. Mishra, Mr. C. B. (2017). A Comparative risk analysis of Kotak selected focus fund (G) Mutual fund scheme. *Https://Www.Ijrar.Org/Papers/IJRAR19UP003.Pdf*, *3*(3), 4.

Dr. Ujjwal M. Mishra, Mr. N. C. (2018). Financial Performance of Selected Automobile Companies. *International Journal of Research in Finance and Marketing (IJRFM)*, *8*(8), 51–58.

Dr. Ujjwal M. Mishra, Ms. A. K. R. (2019). Risk Analysis of Selected Mutual Fund Scheme. *International Journal of Research and Analytical Reviews (IJRAR)*, *6*(1), 13–19.

Dr. Ujjwal Mishra, A. G. (2017). A Study on Impact of Accounts Receivable on Working Capital and Profitability at S. H. Kelkar Ltd Company, Mumbai. *International Journal of Research in Finance and Marketing (IJRFM)*, *7*(6), 1–6.

Dr. Ujjwal Mishra, C. S. (2014). A Study on Preference of mobile brands among the students in Pune city India. *The International Manager*, *1*(IV), 08.

Dr. Ujjwal Mishra, Dr. I. S. (2015). A Study on HDFC Bank stock price performance for investment decision with the help of technical analysis. *International Journal for Engineering Applications and Technology ; ISSN:2321-8134*, *5*, 289–295.

Dr. Ujjwal Mishra, M. P. N. (2016). A Study on credit risk management and apprisal process at punjab national bank, Nagpur. *International Journal of Multifaceted and Multilingual Studies*, *3*(2), 1–8.

Dr. Ujjwal Mishra, Mr. A. D. (2023). sentiment analysis Using Machine learning for Forecasting Indian Stock Trend: A Brief Survey. *FINANCE: THEORY AND PRACTICE, Vol. 27, No. 6'2023 F I N A N C E T P.F A.R u*, *27*(6), 136–147.

Dr. Ujjwal Mishra, Mr. A. K. (2017). A Study of various ways of tax avoidance and tax envasion in agricultural sector and their effect. *Journal for Research*, *3*(04), 4–8.

Dr. Ujjwal Mishra, Mr. V. P. (2016). Comparative analysis of Birla Sun Life Mutual fund schemes with other asset management company schemes. *International Journal of Engineering and Management*, *6*(1), 241–244.

Mishra, D. (2013). Knowledge Based Context Awareness Network Security For Wireless Networks. *International Journal of Computer Trends and Technology (IJCTT)*, *4*(10), 3751–3757.

Mishra, D., Deshpande, S., Anna, M. G., & Tiwari, A. (2024). Exploring the Ethical Dimensions and Societal Consequences of Affective Computing. *Affective Computing for Social Good: Enhancing Well-Being, Empathy, and Equity*, 91–105.

Mishra, D. U. (n.d.). Inflation and its Impact on India Economy. *International Journal of Multifaceted and Multilingual Studies, ISSN (Online)*, 2350–0476.

Mishra, D. U., & Kadale, N. K. (2017). Mining Association Rules using R Environment. *International Journal of Computer Applications*, *157*(4).

Mishra, Dr. U. (2013). The role of human resources and the challenges on globalization. *Anveshan IMR's Management Research Journal*, *3*(1), 34–37.

mishra, Dr. U. (2014). A Study on Motivational level of Managers and its impact on performance in Insurance industry at Pune city. *Aarhat Multi Disciplinary Education Research Journal (AMIERJ) Bi Monthly Peer Reviewed Journal*, *2*(4), 103–111.

Mishra, Dr. U. (2015). A Study on Impact of Interest rates and the performance of stock market. *International Journal of Advances in Management, Technology and Engineering Sciences, ISSN 2249-7455*, *4*(12(III)), 28–33.

Mishra, Dr. U. (2016). A study of consumer buying behaviour in organized retail sector: Electronic Industry (Samsung Televisions). *International Journal of Engineering and Management Research*, *6*(2), 401–406.

Mishra, Dr. U. M. (2022). Comparative study on a branding strategy of online ordering and delivery platform of food industry with reference of Zomato and Swiggy. *Journal of Positive Psychology*, *6*(3), 09.

Mishra, U. (2012). Competition and its impact on life insurance corporation of India ltd. *Anveshan IMR's Management Research Journal, ISSN -0976-4186*, *3*(2), 80–82.

Mishra, U. (2013a). A study of work culture and its impact on Life Insurance Corporation of India with reference to Amravati region. *VIIT Research Journal Baramati*, *2*(1), 80–84.

Mishra, U. (2013b). Impact of performance of commodity market on Equity market. *National Conference on The Changing Trends in Indian Capital Market. Sponsored by Indian Council of Social Sciences and Research*, *1*(1), 311–317.

Mishra, U., & Dash, A. S. (2025). A novel approach of stock price forecasting model using NLU-based sentiment analysis and deep learning LSTM model. *Neural Computing and Applications*, 1–30.

Mishra, U. M., & Borole, M. C. (2017). A Comparative Risk Analysis of Kotak Select Focus Fund (G) Mutual Fund Scheme. *Imperial Journal of Interdisciplinary Research*, *3*(3), 4.

Mishra, U. M., & Dash, A. S. (n.d.). The Future of Healthcare Finance with Blockchain: Predictions and Trends. *Decentralized Healing*, 367–392.

Mishra, U. M., & Pawaskar, J. R. (2017). A study of non-performing assets and its impact on banking sector. *Journal for Research*, *3*(1).

Mishra, U. M., & Peerapur, V. (2016). Comparative Analysis of Birla Sun Life Mutual Fund Schemes with other Asset Management Company's Schemes. *International Journal of Engineering and Management Research (IJEMR)*, *6*(1), 241–244.

Mishra, U., & Raje, H. (2019). Fundamental Analysis of selected banks for Investment Decisions. *International Journal of Research in Social Sciences*, *9*(2).

Naik, D. T. (n.d.). *Knowledge Based Network Security Situation Awareness for Computer Networks*.

Phansalkar, S., Mishra, D., Chaube, N., & Sonkamble, R. (2023). Towards adoption of green blockchain with emphasis on blockchain type, consensus protocols, data sharding and smart contracts. *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 1–8.

Pol, A., Raje, H., & Mishra, U. (2021). Comparative performance analysis of selected mutual fund schemes in tax saver category. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(7), 2325–2337.

Prof. Deepa Mishra, N. K., Manvi Singh, Mudit Maheshwari. (2023). A Comparative Study of Face Recognition Models for Smart Attendance. *International Journal For Research in Applied Science and Engineering Technology*.

Raje, H., & Mishra, U. (n.d.). *COMPARATIVE PERFORMANCE ANALYSIS OF SELECT MUTUAL FUND SCHEMES IN TAX SAVER CATEGORY*.

Sahoo, D. D. R., and Dr Vaishali Deepak Sahoo. (2026a). *Personal Finance for Millennials & Gen Z: From Broke to Building Wealth.*

Sahoo, D. D. R., and Dr Vaishali Deepak Sahoo. (2026b). *Wealth Begins Within: The Psychology of Money, Meaning, and the Mind*.

Sahoo, D. D. R., and Dr Vaishali Deepak Sahoo. n. d. (2026). *DERIVATIVES AND EQUITY MARKETS: A Comprehensive Academic Book*.

Sahoo, D. R. (2017a). Creative Accounting: A Critical Study. *International Journal of Multifaceted and Multilingual Studies*, *4*(IX).

Sahoo, D. R. (2017b). Emotional Intelligence: Managing Stress and Anxiety at work place. *International Journal of Multifaceted and Multilingual Studies*, *4*(IX).

Sahoo, D. R. (2018). Corporate Governance: Need of the Hour (Companies Act 2013). *International Journal of Management Studies (IJMS)*, *4*(ii).

Sahoo, D. R., & Deepak, S. V. (2024a). Exploring the Ethical Perspectives of Sustainable Finance: A Research Study. In *Advances in Business Strategy and Competitive Advantage* (pp. 119–142). IGI Global.

Sahoo, D. R., & Deepak, S. V. (2024b). Exploring the Nexus of Sustainable Finance: ESG Ethical Framework Practices. In *Ethical Quandaries in Business Practices: Exploring Morality and Social Responsibility* (pp. 253–280). IGI Global.

Sahoo, D. R., & Jagatp, V. K. (2017). IND AS 109: Its impact on Financial Statements. *International Research Journal Of Multidisciplinary Studies*, *3*(12), 1–5.

Sahoo, D. R., & Sahoo, V. D. (2026). Crypto Derivatives Markets: Price Discovery, Volatility Dynamics, Market Efficiency, and DeFi Risk: A Structural Analysis. *Journal of Engineering and Technology Management*, *80*(April-June), 774–799.

Sahoo, V. D., & Sahoo, D. R. (n.d.). Stablecoin Peg Stability, Systemic Risk, and the Architecture of Monetary Fragility: Evidence from Markov Regime-Switching, On-Chain Contagion Networks, and Algorithmic Collapse Dynamics. *Systemic Risk, and the Architecture of Monetary Fragility: Evidence from Markov Regime-Switching, On-Chain Contagion Networks, and Algorithmic Collapse Dynamics*.

Sahoo, V. D., & Sahoo, D. R. (2025a). Promoting inclusivity: Corporate social responsibility in game-based learning and professional employment. In *Game-based education approaches to inclusive business management* (pp. 101–126). IGI Global Scientific Publishing.

Sahoo, V. D., & Sahoo, D. R. (2025b). Prospective of Blockchain in Derivative Markets: An Empirical Review. *Innovations in Blockchain-Powered Intelligence and Cognitive Internet of Things (CIoT)*, 229–252.

Shekhar, S., Chaurasiya, S., & Mishra, D. (n.d.). *Smart Reselling: Leveraging MERN Stack and AI for Intelligent Bidding in E-Commerce*.

Shende, M. A., & Sahoo, D. R. (2021). Talent Management critical implications and Strategic approach reference to employer and employees prospective. *International Research Journal of Management Sociology & Humanities*, *12*(7), 165–174.

Shrihari Chaurasiya, D. U. M., Swarnim Shekhar. (2025). Smart Reselling: Leveraging MERN Stack and AI for Intelligent Bidding in E-Commerce. *International Journal of Advanced Research in Science, Communication and Technology*, *5*, 402–410.

Siddiqui, Dr. U. M., & Irfan, D. (2015). Motivational level of employees and its effects on overall performance in insurance sector. *International Journal of Innovative Research and Preactices*, *3*(2), 43–49.

***