Vol. 8, No. 2, April 2026

Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Post-Quantum Migration in the Financial Sector: A Systematic Review of Readiness, Risks, and Transition Frameworks

Hillary Muzenda[1], Belinda Ndlovu[2]

[1,2]Informatics Department, National University of Science and Technology, Bulawayo, Zimbabwe

Received:
December 30, 2025
Revised:
March 3, 2026
Accepted:
March 31, 2026
Published:
April 12, 2026

Corresponding Author:
Author Name*:
Belinda Ndlovu
Email*:
belinda.ndlovu@nust.ac.zw

DOI:
10.63158/journalisi.v8i2.1477

Abstract: Quantum computing threatens the classical cryptographic systems underpinning financial infrastructure, exposing payment platforms, interbank networks, and digital services to Harvest-Now-Decrypt-Later (HNDL) risks. This study systematically reviews quantum threats and post-quantum cryptographic readiness in the financial sector to assess preparedness, identify implementation challenges, and synthesize migration pathways aligned with emerging standards. A PRISMA-guided review of 17 peer-reviewed studies published between 2020 and 2025 was conducted, examining quantum threat models, post-quantum cryptographic schemes, quantum key distribution architectures, and sector-specific deployment barriers. The review finds that lattice-based schemes, especially CRYSTALS-Kyber and CRYSTALS-Dilithium, are the leading candidates for financial adoption, while hybrid cryptographic approaches offer the most feasible transition strategy. However, the current evidence base is predominantly simulation-driven, with limited real-world deployment and validation. The study provides a sector-specific synthesis of quantum threats, post-quantum readiness, and migration pathways in financial systems, and advances an integrated readiness and migration framework based on cross-study thematic analysis.

Keywords: Post-Quantum Cryptography; Hybrid Cryptography; Cryptographic Agility; Financial Systems Security; Cryptographic Migration

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

Quantum computing is advancing rapidly and is expected to significantly alter the computational landscape with important implications for cybersecurity [1]. By leveraging quantum mechanical principles such as superposition and entanglement, quantum computers can solve certain classes of problems more efficiently than classical systems, including those underpinning widely used cryptographic systems. [2]. These developments introduce both opportunities and risks. While quantum computing may enhance computational capabilities, it also poses a direct threat to current cryptographic infrastructures [3];[4]. Algorithms such as the Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), which underpin much of today's secure communications, are particularly vulnerable in the presence of sufficiently powerful computers. [5]. The implications of these vulnerabilities are particularly pronounced in sectors that rely heavily on long-term data protection and cryptographic assurances.

Financial systems represent a high-value cryptographic domain due to stringent requirements for long-term confidentiality, integrity, and non-repudiation. Long-term secrecy, integrity, and non-repudiation must be maintained by key financial infrastructures such as interbank settlement networks, payment gateways, SWIFT messaging systems, and digital identity [6]. The financial sector is a prime target for Harvest-Now-Decrypt-Later attacks [7]. Financial data encrypted today may become vulnerable in the long term as advances in quantum computing could undermine current cryptographic protections. Consequently, financial institutions are increasingly required to collaborate with cybersecurity specialists to strengthen system security and meet regulatory expectations [8].

The lack of practical quantum-resilient encryption systems means the financial sector may become increasingly susceptible to quantum adversaries in the near future, when quantum computing technology matures [9];[10]. This means that organizations and institutions, particularly financial institutions, need to urgently upgrade their cybersecurity practices to avoid the significant security risks of quantum-related threats [11]. They need to accelerate the transition to Post-Quantum Cryptography (PQC).

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Classical computers use cryptography to ensure that data confidentiality, integrity, and authenticity are observed, deterring adversaries from accessing sensitive encrypted data [12];[13]. The capabilities of classical cryptographic algorithms are of great concern, whether these systems can withstand quantum-related threats [14]. As quantum computers become more scalable, classical cryptographic systems become vulnerable, exposing financial systems to data breaches and fraudulent transactions [15].. This underscores the need for organizations and institutions to develop quantum-resilient frameworks.

Despite the growing body of research on post-quantum cryptography, existing review studies remain largely technology-centric, with limited attention to sector-specific deployment contexts [1]. In financial systems cryptographic transition is influenced not only by technical feasibility but also by regulatory requirements, legacy infrastructure, constraints, and long-term data sensitivity. This creates a gap in the literature regarding integrated assessments of post-quantum readiness within financial ecosystems.

This study addresses this gap by providing a sector-focused synthesis of quantum threats, post-quantum readiness, and migration considerations in financial systems. Based on cross-study thematic analysis, the study proposes an integrated readiness and migration framework to support structured transition planning in the financial sector. The review is guided by the following research questions:

1) What are the major quantum threats to cryptographic systems?
2) Which post-quantum cryptographic (PQC) and quantum key distribution (QKD) techniques demonstrate practical feasibility for financial sector deployment?
3) What technical, organizational, and regulatory challenges hinder the adoption of quantum-safe cryptographic solutions in the financial sector?
4) Which existing frameworks and standards provide structured guidance for achieving quantum-resilient transformation in financial services?
5) How are the post-quantum cryptographic solutions applied across different financial sector use cases?

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

2. METHODS

The study adopts the PRISMA (2020) reporting framework to guide the systematic identification, screening, and selection of relevant literature [16]. The review aims to pinpoint, screen, and synthesize relevant information on quantum threats and post-quantum cryptography. The systematic review followed a structured PRISMA-guided workflow consisting of five sequential stages to ensure transparency and reproducibility.

2.1. Search Strategy Execution

A systematic literature search was conducted in accordance with PRISMA guidelines to identify relevant studies on post-quantum cryptography and quantum-safe migration in the financial sector. The search was performed across five major academic databases: IEEE Xplore, SpringerLink, ACM Digital Library, PubMed, and ScienceDirect. These databases were selected due to their strong coverage of cybersecurity, cryptography, and interdisciplinary financial systems research. The search strategy was designed to capture three core dimensions of the study: (i) post-quantum cryptographic concepts, (ii) financial sector applications, and (iii) migration and adoption processes. Boolean operators were used to combine search terms as follows:

("post-quantum cryptography" OR "quantum-safe cryptography" OR "PQC") AND ("financial systems" OR "banking" OR "payment systems" OR "financial security") AND ("migration" OR "adoption" OR "readiness" OR "implementation")

The search was limited to peer-reviewed journal articles and conference proceedings published in English between 2020 and 2025 to ensure inclusion of recent, high-quality contributions in a rapidly evolving field. The search yielded a total of n = 432 records across all databases, including IEEE Xplore (n = 191), SpringerLink (n = 92), ACM Digital Library (n = 67), PubMed (n = 42), and ScienceDirect (n = 40). These records were then exported to a reference management system for duplicate identification and subsequent screening.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

2.2. Inclusion and Exclusion Criteria

Studies were included if they (i) investigated post-quantum cryptographic algorithms, quantum-safe security architectures, or quantum key distribution; (ii) examined financial-sector data environments such as payment systems, interbank settlement platforms, digital identity infrastructures, Blockchain-based financial services, or financial cloud platforms; (iii) analyzed security, performance, scalability, or migration aspects of cryptographic deployment; and (iv) were published between 2020 and 2025 in peer-reviewed journals or conference proceedings. Studies were excluded if they focused solely on theoretical quantum computing without cryptographic applications, addressed non-financial domains without transferable implications for financial systems, lacked a technical evaluation of cryptographic performance, or were non-English publications. Studies with indirect financial relevance were included only where their findings could be reasonably extended to financial security contexts. While most studies demonstrate direct alignment, a small number provide indirect contributions by informing the broader quantum threat and cryptographic context relevant to financial systems.

2.3. Screening and Eligibility

Following the identification stage, all retrieved records (n = 432) were exported to Mendeley reference management software for duplicate detection and removal. A total of 35 duplicate records were identified and removed, resulting in n = 397 unique records for further assessment. In line with PRISMA 2009 guidelines, a two-step selection process comprising screening and eligibility assessment was applied. In the first step, title and abstract screening were conducted to evaluate the relevance of studies to post-quantum cryptography, quantum-safe security approaches, and financial sector applications. Studies were excluded if they (i) did not address cryptographic security, (ii) focused solely on theoretical quantum computing without cybersecurity implications, or (iii) were unrelated to financial systems or lacked transferable relevance to financial infrastructures. This process resulted in the exclusion of n = 319 records, leaving n = 78 studies for full-text evaluation.

2.4. Included

In the third step, a full-text eligibility assessment was conducted using the predefined inclusion and exclusion criteria. Studies were included if they explicitly examined post-

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

quantum cryptographic techniques, quantum-safe architectures, or migration strategies within financial systems or contexts with clear applicability to financial infrastructures. Studies were excluded if they lacked a technical evaluation of cryptographic performance, did not address migration or implementation aspects, or were not relevant to the financial sector. Following this assessment, 61 studies were excluded, leaving a final sample of 17 included in the qualitative synthesis. While the final sample size (n = 17) may appear modest, it reflects the emerging and specialized nature of research on post-quantum migration within financial systems. The strict inclusion criteria ensured that only studies directly relevant to the financial sector's cryptographic transition were retained, prioritizing depth and contextual relevance over volume. To ensure transparency and reduce selection bias, the screening and eligibility assessment were conducted independently by H.M and B.N, with disagreements resolved through discussion and consensus.

2.5. Quality Assessment

Two independent reviewers assessed each of the 17 articles that were included in the final review. This process involved the use of a structured scoring framework adapted from standard SLR appraisal checklists, most notably the Critical Appraisal Skills Program (CASP) and PRISMA [17]. This strategy sought to reduce prejudice while preserving dependability and consistency. The following modified CASP standards were used to assess each of the 17 articles mentioned.

1) Clarity of research aim
2) Clarity of research design
3) Appropriateness of methodology
4) Relevance and applicability to the financial sector

We excluded some standards as they were not consistently applicable to cryptographic and standards-based studies. A three-point rating system was used to assign scores. High - 3, Moderate - 2, Weak – 1. Studies scoring between 7 and 9 were classified as high quality, scores between 4 and 6 as moderate quality, and scores below 4 as low quality. All included studies were assessed using a predefined quality criterion, and the results are presented in Table 1. Most studies achieved high-quality scores, with all included studies meeting the threshold for inclusion in the final synthesis. No studies were

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

excluded at the quality appraisal stage. The thematic synthesis followed an inductive coding approach, where concepts were first extracted at the study level and subsequently grouped into higher-order themes through iterative comparison. Initial open coding generated first-order concepts, which were then used clustered into broader categories, including quantum threats, cryptographic feasibility, migration barriers, and governance readiness.

Table 1: Quality appraisal of the included studies (n=17)

Study Ref	Clarity of Research Aim & Design	Appropriateness of Methodology	Alignment with Cybersecurity Applications	Total Score	Quality Rating
[18]	3	3	1	7	High
[19]	3	3	3	9	High
[20]	3	3	3	9	High
[21]	3	3	3	9	High
[22]	3	3	3	9	High
[23]	3	2	2	7	High
[24]	3	3	2	8	High
[25]	3	3	3	9	High
[26]	3	3	3	9	High
[27]	2	3	3	8	High
[28]	3	3	3	9	High
[29]	3	3	3	9	High
[30]	3	3	3	9	High
[31]	3	3	2	8	High
[32]	3	3	3	9	High
[33]	3	3	2	8	High

2.6. Data Extraction and Synthesis

A structured data extraction process was applied to capture key attributes from each included study, including study context, methodology, identified quantum threats, cryptographic techniques, financial sector applications, and reported challenges. The extracted data were analyzed using a thematic synthesis approach. This involved coding

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

recurring concepts across studies and grouping them into higher-level themes such as quantum threat categories, cryptographic feasibility, migration barriers, and organizational readiness. These themes were then used to support cross-study comparison and to inform the development of a structured understanding of post-quantum migration in the financial sector.

Building on this thematic synthesis, the identified themes were further used to inform the development of the proposed readiness and migration frameworks. First-order codes derived from the included studies were iteratively grouped into higher-order themes, which were then mapped to conceptual components representing risk exposure, technical transition requirements, operational constraints, and governance readiness. This mapping process enabled the translation of thematic findings into structured framework elements, which are presented in the Results section. The visual summary of the PRISMA flow diagram in Figure 1 clarifies how the initial pool of retrieved articles was systematically narrowed to those eligible for synthesis.

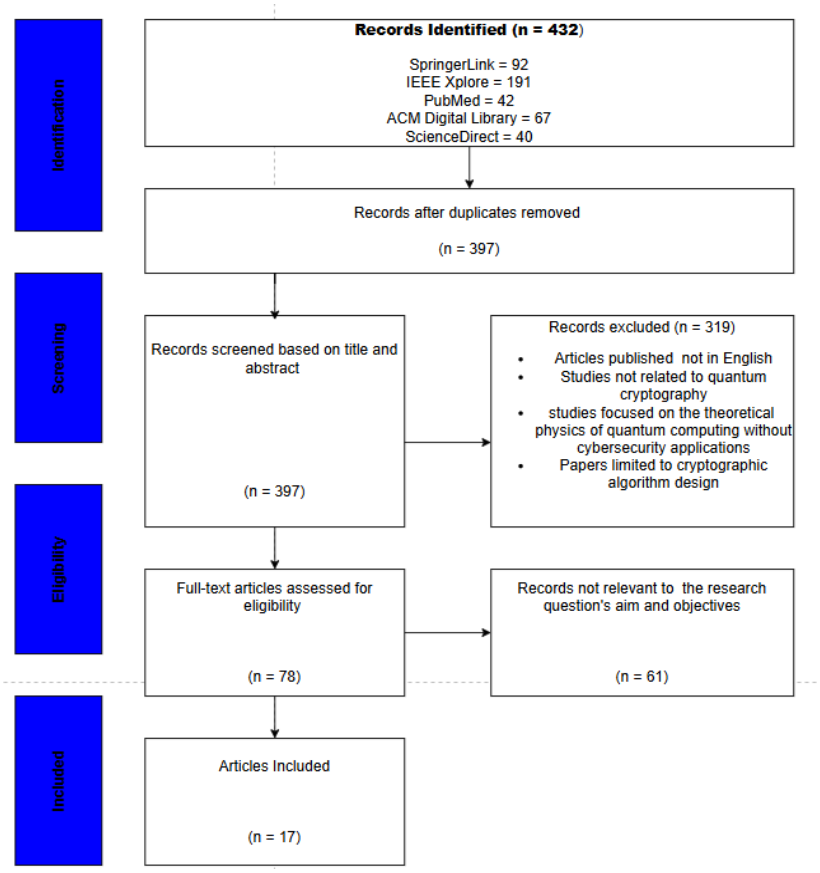

Figure 1. PRISMA Flow Diagram

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

3. RESULTS AND DISCUSSION

The Data Extraction as shown in Table 2 presents the detailed characteristics of the studies that met the inclusion criteria.

Table 2: Studies that met inclusion criteria

Ref	Country	Method	Quantum Threat	Cryptographic Technique	Financial Sector Application	Challenges
[18]	Netherlands	Design Science	Shor's Algorithm rendering RSA/ECC Obsolete Harvest Now, Decrypt Later (HNDL) attacks	PQC (ML-KEM-1024, ML-DSA-65) QKD (COW protocol) Classical RSA, ECC	payment processing corporate vpns	low secret key rate (SKR) vs Distance performance overhead of QKD
[19]	Australia	Mixed-methods	Shor's Algorithm Grover's Algorithm HNDL	lattice-based and Hash-based Hybrid Cryptosystems (PQC+RSA)	General Enterprise Security	longer keys high computational storage demand lack of expertise lack of final standardization
[25]	Spain	Experimental	Shor's algorithm	PQC (ML-KEM, ML-DSA) Hybrid TLS configurations	Secure communication protocols (TLS) Secure internet-based services	Pre-migration Cryptographic breaches Increased key sizes Implementation complexity performance overhead
[26]	Switzerland; Canada; France	Mixed-methods (roadmap + pilot)	Shor's (RSA/ECC) Grover's (AES), HNDL, TLS 1.2	RSA, ECC, AES-256 PQC (Kyber, Dilithium, Falcon, SPHINCS+ QKD	Financial system migration planning Interbank systems	Performance trade-offs legacy TLS Governance gaps QKD infrastructure limits
[20]	Indonesia	Simulation/Modelling	Quantum algorithms	QKD Protocols (E91) Classical RSA, ECC	QKD (E91); RSA, ECC	lower key production rate technological difficulties

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Ref	Country	Method	Quantum Threat	Cryptographic Technique	Financial Sector Application	Challenges
						environmental noise
[21]	Italy	Simulation/Modelling + Case Study	Shor's (RSA/ECC), Grover's (AES) IoT/blockchain signature threats	Dilithium-5 PQClean ESP32 hardware	Blockchain-based financial systems; secure transactions	IoT resource limits Side-channel/fault attacks Integration complexy
[34]	USA	Conceptual/ Analytical	Shor's breaking RSA/ECC Grovers algorithm	hash-based	securing digital signatures	latency constraints compliance interoperability performance overhead
[22]	Korea	Simulation/Modelling (QKD simulators, TLS integration)	Shor's and Grover's breaking RSA/ECC	QKD PQC (Dilithium, NTRU) TLS v1.3 hybrid	Secure communication infrastructure	Infrastructure cost of QKD limited distance interoperability issues latency issues
[28]	India;Malaysia	Qualitative	Shor's breaking RSA/ECC	Lattice (Kyber, Dilithium, Falcon) Code-Based (McEliece, BIKE) Hash-based (SPHINCS+, PICNIC) Multivariate (Rainbow) Isogeny (SIKE)	Cryptographic infrastructure for financial systems	Large key sizes Slow operation Interoperability lack of standards
[29]	India	Quantitative	Quantum threat	Digital signatures	Organizational readiness in financial cybersecurity	Privacy security governance lack of skills complexity
[30]	Netherlands	Qualitative (expert interviews)	Shor's algorithm HNDL risk	PQC types: Lattice based, Hash-based	Secure information sharing/ critical infrastructure	Organizational readiness, policy gaps, coordination complexity
[31]	USA	Experimental setup	Shor's algorithm breaking RSA, ECDH, ECDSA in TLS	ML-KEM, ML-DSA, Post-Quantum TLS 1.3	Secure web communications including e-banking	performance overhead storage requirements

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Ref	Country	Method	Quantum Threat	Cryptographic Technique	Financial Sector Application	Challenges
					Online financial services Data transfer systems	interoperability issues larger key sizes high computational time
[23]	UK	Mixed method case studies Comparative jurisdictional review	Shor's algorithm Grover's Algorithm	PQC: Lattice-based and Hash based algorithms	Portfolio optimization Open banking APIs DLTsDigital Currencies	Regulatory challenges Shortages in skilled quantum personnel
[24]	India	Simulation/Modelling (quantum computing patterns, experiments)	Shor's algorithm (RSA Break) Grover's (search speedup) Decoherence issues	RSA, ECC Shor's Grover's QKD PQC	Cryptographic systems for financial security	Noise / decoherence Error correction Scalability Mistrust protocols
[32]	UK	Qualitative	Shor's algorithm breaking RSA/ECC Grover's algorithm weakening AES/SHA	Quantum Key Distribution (QKD); post-quantum cryptography; AI-enhanced cryptography; neural network-based cryptographic optimisation; public key cryptography; digital signatures	Financial data protection systems, Fraud-resistant systems	Large key sizes Scalability limits Infrastructure costs performance overhead need for hybrid adoption strategies
[27]	USA, Switzerland, Ireland	Conceptual	Quantum threat Shor's algorithm Harvest Now, Decrypt Later attacks	PQC Approaches:	Simulation of financial systems	Uncertain timeline Migration complexity lead time needed
[33]	Czechia/Bosnia	Simulation/Modelling	QKD limits adoption	QKD (BB84) QKDNetSim StrongSwan IPsec VPN	Secure network communication	Cost of QKD Integration issues Interoperability issues

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

The findings of this systematic review show that Quantum cryptography and post-Quantum cryptography (PQC) converge as twin pillars of future-proof security, yet adoption levels are very low. The findings regarding the financial sector suggest that the technological feasibility of QKD and the standardization of PQC algorithms are not solely matters of technology but also of organizational awareness, infrastructural investment, and regulatory alignment.

3.1. Country and Regional Distribution of Research

Figure 2 shows the country and regional distribution of research and it can be pinpointed that research on quantum cryptography and post-quantum security is heavily concentrated in developed regions. Europe and North America dominate the research landscape in quantum cryptography and post-quantum security, collectively accounting for approximately 65% of the included studies. This concentration reflects not only differences in research funding and technological infrastructure, but also the early institutional prioritization of cryptographic transition in these regions. In particular, the presence of formal standardisation initiatives—such as those led by the National Institute of Standards and Technology in the United States and the European Telecommunications Standards Institute in Europe—has accelerated both research activity and practical engagement with post-quantum migration.

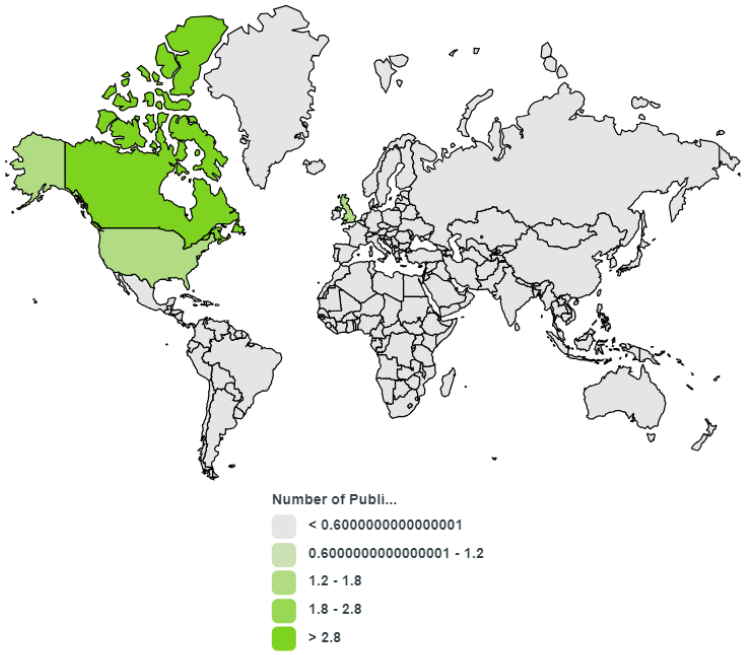

Figure 2. Country and Continent Representation

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

These regions also host highly digitized financial systems with strong regulatory oversight, where long-term data protection and compliance requirements create immediate pressure to address quantum-related risks. As a result, research is more closely aligned with implementation pathways rather than remaining purely theoretical. Asia accounts for approximately 25%, indicating growing engagement, particularly in technologically advanced economies. In contrast, Oceania and Africa each account for only 5% of the publications, reflecting more limited institutional investment, fewer standardization initiatives, and slower integration of post-quantum considerations into financial-sector policy and infrastructure.This uneven distribution suggests that global quantum-readiness is likely to evolve asymmetrically, potentially widening the security gap between developed and developing financial systems and increasing the latter's exposure to long-term cryptographic risk.

3.2. Quantum Threat Landscape

Figure 3 illustrates the quantum threat landscape that has been identified in the study. The reviewed literature indicates that quantum threats in the financial sector cluster around three primary vectors: algorithmic compromise, accelerated brute-force capability, and long-term confidentiality risks. Shor's algorithm emerges as the dominant threat, appearing in 76% of the included studies, reflecting its capacity to fundamentally break widely deployed public-key cryptosystems such as RSA and elliptic curve cryptography (ECC). This dominance is not incidental but stems from the structural reliance of financial systems on public-key infrastructures for authentication, digital signatures, and secure communication. In contrast, Grover's algorithm is identified in 47% of studies. It primarily reduces the effective security margin of symmetric cryptography rather than rendering it obsolete, as its impact can be mitigated by increasing key lengths. This distinction highlights an asymmetric threat landscape in which public-key systems require urgent cryptographic replacement.

In contrast, symmetrical systems can be incrementally adapted. Additionally, limited attention is given to hardware-level constraints, such as quantum decoherence, which affect the practical realization of large-scale quantum attacks. Although there is currently a technical limitation, decoherence underscores the uncertainty surrounding

the timeline of quantum threat materialization, reinforcing the need for proactive yet staged migration strategies in financial environments.

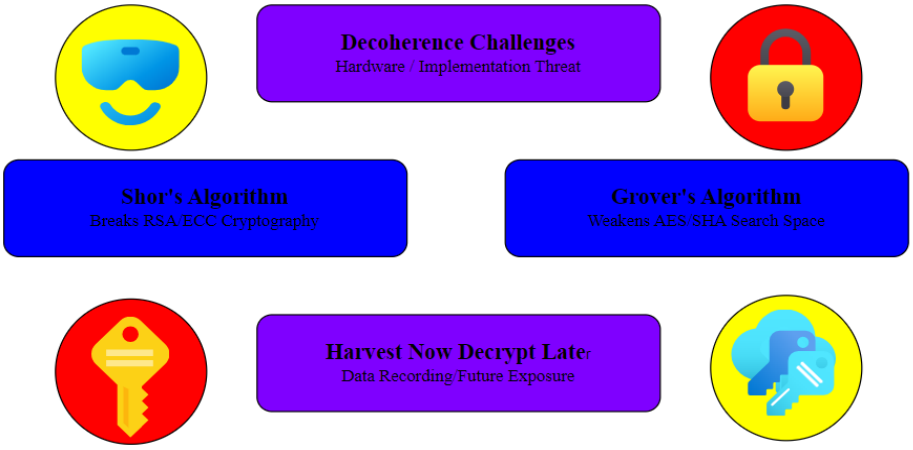

Figure 3. Quantum Threat Landscape

3.3. Cryptographic Techniques: Feasibility and Performance

Figure 4 illustrates the comparative feasibility and performance of selected cryptographic techniques in relation to quantum threats. The reviewed studies consistently indicate that post-quantum cryptographic (PQC) approaches—particularly lattice-based and hash-based schemes—offer the most viable migration pathways for financial institutions. This aligns with NIST's standardization outcomes, which prioritize lattice-based algorithms for their favourable balance of security, efficiency, and implementation feasibility. In contrast, code-based and hash-based approaches, although theoretically robust, receive comparatively less emphasis due to practical deployment constraints, including large key sizes, higher computational overhead, and integration challenges within existing financial infrastructures.

Among the evaluated techniques, CRYSTALS-Kyber and CRYSTALS-Dilithium are most frequently identified as offering an optimal trade-off between security and performance. However, their reliance on larger key sizes—often significantly exceeding those of traditional RSA systems—introduces non-trivial performance implications in high-throughput financial environments, where latency and bandwidth efficiency are critical. Similarly, hash-based signature schemes such as SPHINCS+ provide strong security guarantees. However, they are slower to sign and verify, limiting their suitability for time-

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

sensitive applications. Code-based systems, particularly McEliece variants, remain highly secure but are constrained by extremely large public keys, which pose challenges for compatibility with legacy banking systems and for deployment in constrained environments.

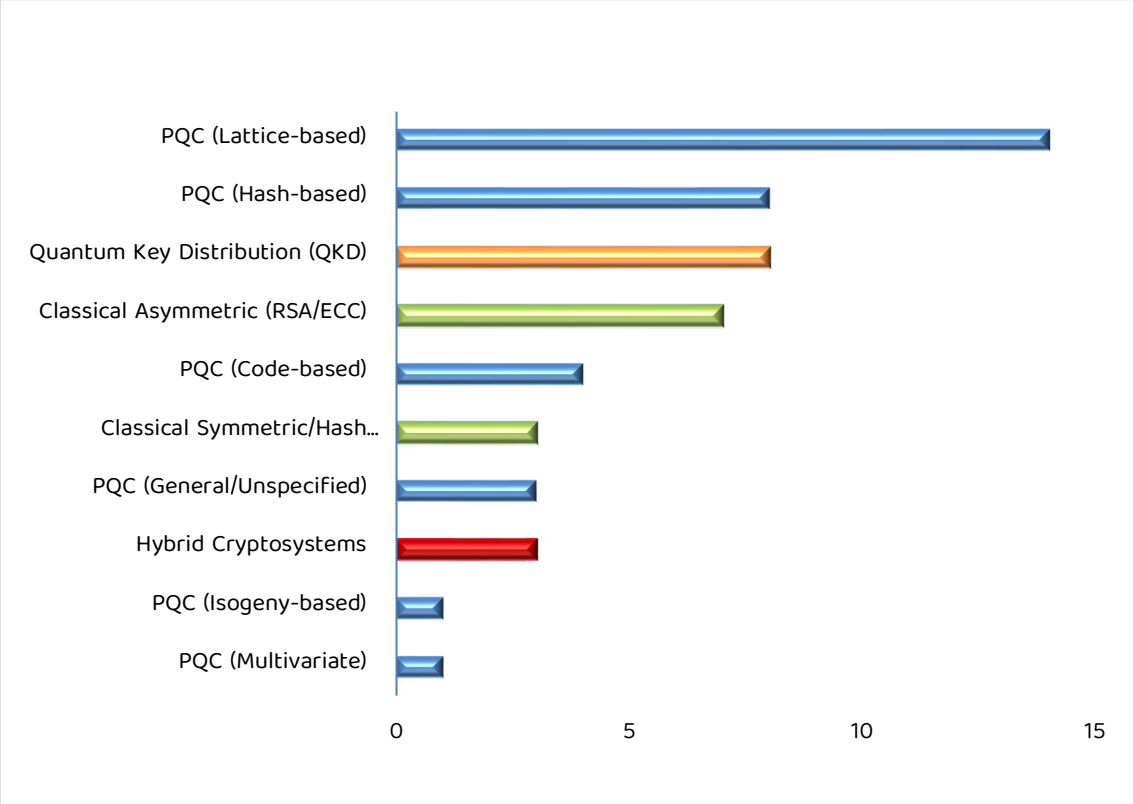

Figure 4. Cryptographic Techniques Feasibility and Performance

The observed preference for lattice-based cryptography reflects a broader convergence between theoretical robustness and practical deployability. However, this comes at the cost of increased computational and communication overhead, creating a fundamental trade-off between security strength and operational efficiency. This tension explains the prominence of hybrid cryptographic strategies in the literature, where classical and post-quantum algorithms are deployed in parallel to balance immediate performance requirements with long-term security objectives. Such phased coexistence models are increasingly positioned as pragmatic transition pathways for financial institutions navigating the complexities of post-quantum migration.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

3.4. Thematic Classification of Financial Sector Applications

This section presents the explicit financial sector applications reported in the included studies. Table 3 presents studies with explicit applications to financial-sector contexts, illustrating how post-quantum and cryptographic security approaches are operationalized in real-world financial systems. The evidence shows that earlier work predominantly focuses on securing core financial operations, including payment processing systems, interbank communication, and enterprise network infrastructure, where the protection of sensitive transactional data is critical. Several studies also address the growing risk of financial fraud by strengthening transaction security through protocols such as Transport Layer Security (TLS) and established standards, including SWIFT secure signature mechanisms and EMV-based payment systems [34]. These applications highlight the central role of cryptography in maintaining trust, integrity, and confidentiality across financial ecosystems. Studies without direct applications to the financial sector were excluded unless their findings demonstrated clear transferability to financial system security, ensuring that the synthesis remained contextually relevant. Collectively, the results indicate that while foundational cryptographic protections are well established in financial systems, the transition to quantum-safe alternatives remains largely conceptual, with limited evidence of large-scale, real-world deployment.

Table 3: Financial Sector Applications Identified in Studies Included

Application Category	Description	Supporting Studies
Secure Communication Systems (TLS, VPN, APIs)	Protection of financial data-in-transit through quantum-resistant communication protocols, including PQC-enabled TLS, VPNs, and secure APIs used in interbank communication, e-banking platforms, and enterprise networks	[18];[25];[22];[20];[31];[33]
Financial Data Protection & Confidentiality	Safeguarding sensitive financial records and stored data against quantum-enabled threats such as Harvest-Now-Decrypt-Later (HNDL), ensuring long-term	[18];[30];[32]

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Application Category	Description	Supporting Studies
	confidentiality of transactions and customer information	
Cryptographic Infrastructure & Enterprise Security	Integration of post-quantum cryptographic algorithms into existing enterprise security architectures, including hybrid cryptosystems and organizational cybersecurity frameworks for financial institutions	[19];[29];[30]
Blockchain & Digital Financial Systems	Application of quantum-resistant cryptographic techniques in blockchain platforms, digital currencies, and distributed ledger technologies to ensure secure transaction validation and integrity	[21];[23]
Migration Strategy & Readiness Planning	Development of structured migration roadmaps, governance frameworks, and institutional readiness strategies for transitioning financial systems to quantum-safe cryptographic environments	[26];[27];[30]
Digital Signatures & Authentication Systems	Deployment of PQC-based digital signature schemes and authentication mechanisms to secure financial identity verification, transaction authorization, and access control systems	[28];[34]
Quantum Key Distribution (QKD)-based Security Systems	Utilization of QKD protocols for ultra-secure key exchange in high-security financial environments, including interbank networks and critical infrastructure requiring information-theoretic security	[18];[20];[22];[33]

3.5. QKD Implementation Positives and Challenges

Figure 5 presents the key advantages and challenges of implementing Quantum Key Distribution (QKD) in cybersecurity. The reviewed studies indicate that QKD receives moderate attention, appearing in 41% of the included literature, and is primarily valued for its ability to provide a theoretically secure key exchange based on quantum-mechanical principles. Unlike classical cryptographic approaches, QKD is resistant to both Shor's algorithm and long-term "harvest-now, decrypt-later" attacks, positioning it as a strong candidate for protecting highly sensitive financial communications. However, despite these advantages, its practical adoption remains constrained. The most frequently cited challenges reported in 29% of studies relate to interoperability and integration difficulties, limited secret key generation rates, and distance restrictions, which collectively hinder scalability across distributed financial networks. A further 24% of studies highlight high infrastructure and deployment costs, as well as performance limitations arising from environmental noise, latency, and system complexity. Governance and policy gaps, identified in 12% of studies, further underscore institutional and regulatory barriers to implementation.

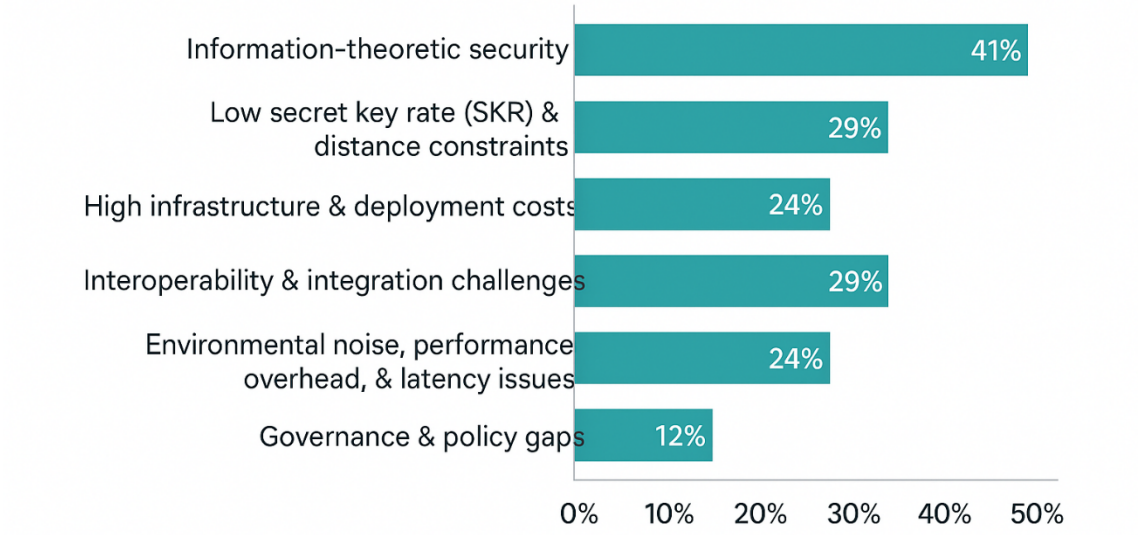

Figure 5. QKD Adoption Potential and Limitations

The limited uptake of QKD, therefore, reflects a convergence of technical, economic, and organizational constraints. This limited uptake largely reflects a mismatch between QKD's dependence on specialized hardware and point-to-point links, and the financial sector's need for scalable, software-based solutions that can be integrated into existing systems.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

While QKD offers strong theoretical security guarantees, its reliance on specialized hardware and limited transmission distances limits its feasibility for large-scale financial deployment. Consequently, the literature consistently positions QKD as a complementary solution, best suited for high-security, point-to-point communication channels rather than as a primary, system-wide cryptographic replacement. Across the included studies, a consistent pattern emerges whereby QKD adoption is constrained by scalability and infrastructure limitations. However, variations are observed depending on network architecture, deployment environment, and security requirements.

3.6. Hybrid Approach to Quantum-Safe Cryptography

Figure 6 shows a Hybrid Cryptography Architecture visualizing how QKD is best deployed alongside PQC. Figure 6 illustrates the evolutionary transition of cryptographic architectures in response to quantum computing threats. Public-key and symmetric algorithms under classical cryptography form the foundation of current secure communication. From classical cryptography, the first pathway leads to post-quantum cryptography (PQC), where quantum-resistant algorithms replace or augment vulnerable classical public-key schemes. The second pathway highlights quantum key distribution (QKD) as an alternative approach to secure key exchange based on quantum principles. The diagram emphasizes hybrid cryptographic systems that augment classical cryptography with PQC and, where appropriate, QKD protocols. It reflects the most practical and advocated transition strategy to quantum-safe mechanisms.

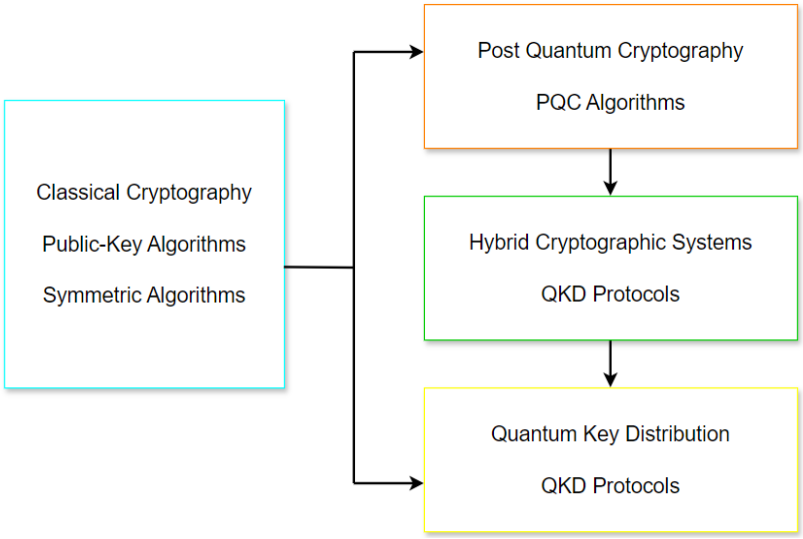

Figure 6. Hybrid Cryptography Architecture (Classical + PQC + QKD)

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

3.7. Migration Barriers and Organizational Readiness Gaps

Figure 7 shows that barriers were categorized into technical, organizational, regulatory and compliance, and economic/cost barriers. The findings show that technical barriers dominate, appearing in 49% of the reviewed studies, and include challenges related to performance overhead, large key sizes, and infrastructure limitations. Organizational barriers follow at 21%, including shortages of specialized expertise, resistance to change, and slow system upgrade cycles. Economic constraints account for 16% of the studies, reflecting the high costs of transitioning to post-quantum infrastructure. In comparison, regulatory and compliance barriers (14%) highlight uncertainties around standards, policy alignment, and governance frameworks.

Importantly, the evidence indicates that quantum-safe migration is constrained not only by technical feasibility but also by institutional coordination challenges and policy ambiguity. The prominence of technical barriers underscores the engineering complexity of transitioning to quantum-resistant systems; however, the concurrent presence of organizational and regulatory constraints reveals that technological readiness alone is insufficient. Rather, successful migration depends on aligning technical capability with organizational capacity, governance structures, and regulatory clarity. This reinforces the characterization of the post-quantum transition as a socio-technical transformation that requires coordinated adaptation across technological, institutional, and policy dimensions.

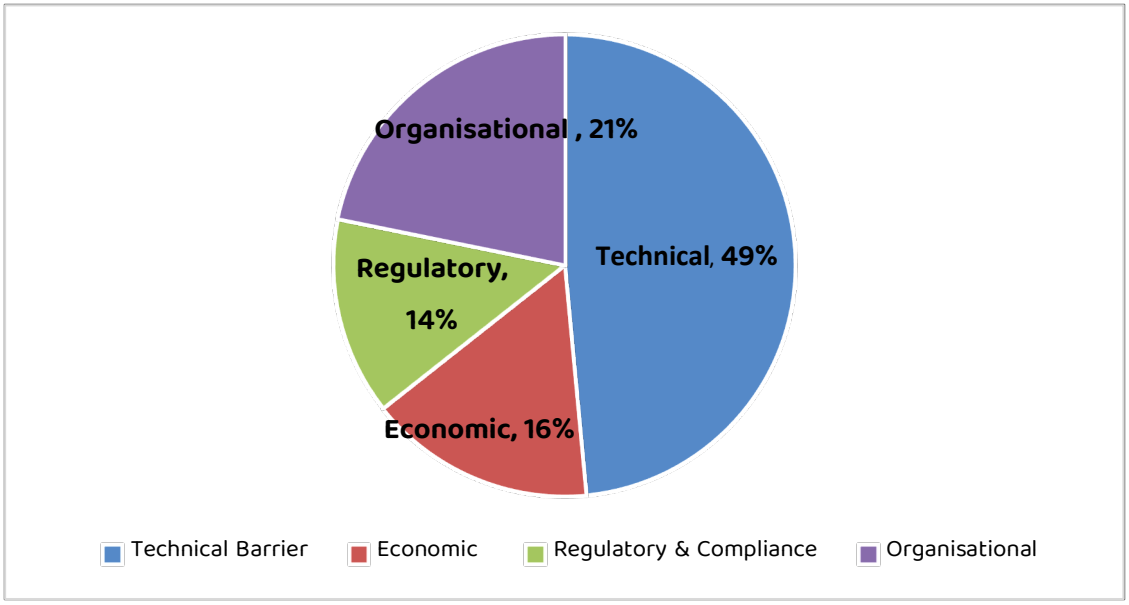

Figure 7. Migration Barriers

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

3.8. Opportunities for Quantum-Safe Migration in the Financial Sector

This section presents five key opportunities for quantum-safe migration from the reviewed literature, including their descriptions, significance, and supporting evidence.

Table 4: Quantum-Safe Migration Opportunities

Identified Opportunity	Description of the Opportunity	Significance of the Opportunity	Evidence from Reviewed Literature
Adoption of Hybrid Cryptographic Architectures	• Combines classical cryptography (RSA, ECC, AES) with PQC algorithms, and a selective integration of QKD	• Enables gradual, low-risk migration • Maintains backward compatibility • Mitigates uncertainty in quantum timelines • Aligns with NIST and ETSI	• Frequently tested via pilots, simulations, and experimental deployments • Proposed in TLS hybrids, payment systems, VPNs, SWIFT signatures, and enterprise security across various studies [19];[26];[30];[22];[35].
Cryptographic Inventories and Crypto-Agility Enablement	• Systematic identification and management of cryptographic assets • Combined with the ability to replace algorithms without redesign	• Reduces hidden RSA/ECC exposure • Enables phased migration • Supports governance, audits, and compliance	• Indirectly highlighted through limitations such as governance gaps, migration complexity, and interoperability issues in the following studies [26];[36];[30].
Performance-optimized PQC for Financial Workloads	• Optimization of PQC implementations to meet latency, throughput, and storage requirements	• Addresses adoption barriers caused by large keys, high computational costs, and latency constraints	• Explored via experimental setups, simulations, embedded systems, and PQC libraries in studies [18];[19];[21];[36];[22];[35]
Organizational Readiness and Human-	• Integration of skills, governance, leadership, and	• Addresses non-technical barriers such as skills	• Explicitly modelled only once using the TOE framework in study.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Identified Opportunity	Description of the Opportunity	Significance of the Opportunity	Evidence from Reviewed Literature
Centric Migration Models	institutional capacity into migration planning	shortages, resistance to change, and governance gaps.	• Implicitly recognized as a gap in studies [19];[26];[23]
Targeted Deployment of QKD for High-Sensitivity Links	• Selective use of QKD for critical financial communication links	• Balances theoretical security benefits with cost and infrastructure constraints	• Evaluated mainly through simulations and pilots in studies [18];[26];[20];[22];[35];[33] typically as a complement to PQC.

Hybrid Cryptographic Architectures in Table 4 emerge as the most dominant opportunity in the reviewed literature because they are widely recognized and practically viable. Most of the examined studies identified it as the most viable option, signifying robust and comprehensive Intellectual unanimity about its importance. Studies have noted that Hybrid Cryptographic Architectures can be applied across different sections of financial systems. These include payment systems, banking platforms, enterprise security environments, TLS, VPNs, and SWIFT. The other advantage of going the hybrid way is that it can be implemented and run within current live systems without the need to completely overhaul existing classical cryptographic infrastructures. Hybrid Cryptographic Architecture aligns itself closely with established international standards and is supported by major standardization bodies such as NIST and ETSI.

3.9. Research Questions

This session answers the research questions posed in the study.

1) RQ1: What are the major quantum computing threats to financial sector cryptographic systems?

The review demonstrates that the most immediate and structurally disruptive quantum threat to financial cryptographic systems arises from Shor's algorithm, which fundamentally challenges the security assumptions underpinning widely deployed public-key infrastructures. By enabling polynomial-time factorization of large integers and

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

efficient computation of discrete logarithms, Shor's algorithm renders established schemes such as RSA and elliptic curve cryptography (ECC) vulnerable [44];[6];[45];[37]. This vulnerability is not merely technical but systemic, given the deep integration of public-key cryptography into financial operations, including digital payment protocols, authentication mechanisms, and digital signatures. The predominance of this threat across 76% of the reviewed studies reflects the structural dependence of financial ecosystems on cryptographic primitives that are intrinsically incompatible with quantum adversaries. Beyond key compromise, the implications extend to the erosion of trust mechanisms, in which adversaries could impersonate financial institutions, forge transaction approvals, and undermine non-repudiation guarantees essential to regulatory compliance and dispute resolution.

In contrast, Grover's algorithm represents a secondary but still significant threat, operating through a quadratic speed-up in brute-force search that effectively reduces the security margin of symmetric cryptographic schemes [38];[39]. Unlike Shor's algorithm, however, its impact does not necessitate complete algorithmic replacement but rather parameter adaptation. The continued viability of symmetric encryption schemes such as AES and hashing standards like SHA-2, therefore, depends on proactive adjustments, including increased key sizes and strengthened configurations [5];[9]. This creates a differentiated risk profile in which symmetric cryptography remains resilient but is conditional on timely upgrades. Delayed adaptation, particularly within legacy financial systems, introduces exploitable vulnerabilities and extends exposure to quantum-enabled attacks [40].

A further layer of risk is introduced by "harvest-now, decrypt-later" (HNDL) attack strategies, in which adversaries capture encrypted financial data in the present with the intention of decrypting it once sufficiently powerful quantum capabilities become available [7]. This threat is particularly acute in the financial sector, where data such as customer identities, transaction histories, and contractual records are long-term sensitive, with confidentiality requirements that extend well beyond current cryptographic lifecycles. HNDL attacks, therefore, shift the threat landscape from immediate compromise to deferred exposure, reinforcing the urgency of early migration even in the absence of fully mature quantum computers.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

At the same time, the review highlights an important counterpoint: quantum decoherence, which currently constrains the practical realization of large-scale quantum attacks. Decoherence, resulting from environmental noise and instability in quantum states-limits the reliability and scalability of quantum systems [41];[42]. While this introduces uncertainty into the timeline of quantum threat materialization, it should not be interpreted as a mitigating factor but rather as a temporary technological barrier. The coexistence of severe theoretical vulnerability and delayed practical realization creates a paradoxical risk environment, where financial institutions must act pre-emptively despite the absence of immediate large-scale quantum attacks.

Taken together, these findings reveal a fundamentally asymmetric threat landscape. Public-key cryptography faces existential risk under quantum conditions, symmetric cryptography remains conditionally secure, and long-term data confidentiality is increasingly exposed through deferred attack models. This convergence of immediate, incremental, and latent threats underscores that quantum risk in financial systems is not a singular event but a multi-dimensional transformation, requiring coordinated, forward-looking migration strategies that extend beyond purely technical mitigation to encompass governance, policy, and institutional readiness.

2) RQ2. Which Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) approaches have been reported as feasible for adoption in financial sector systems?

The review indicates that the feasibility of adopting post-quantum cryptography in financial systems is shaped not only by theoretical security guarantees but also by deployability in performance-sensitive, high-throughput environments. Among the evaluated approaches, lattice-based cryptography emerges as the most operationally viable pathway for near-term migration. Its dominance is driven by a convergence of factors, including advanced standardization under the NIST Post-Quantum Cryptography programme, mature security analysis, and relatively efficient performance on conventional hardware [43]. Algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium are consistently identified as offering a favourable balance between security and efficiency, making them leading candidates to replace vulnerable public-key systems such as RSA and ECC [44]. This reflects a broader trend in which feasibility is determined less

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

by cryptographic strength alone and more by compatibility with existing financial infrastructures and system constraints.

In contrast, hash-based signature schemes, while offering strong quantum-resistant guarantees grounded in well-established cryptographic primitives [45];[46], present notable limitations in practical deployment. Their large signature sizes and comparatively high computational costs introduce latency and bandwidth challenges, particularly in real-time financial applications where speed and scalability are critical [47]. As a result, the literature consistently positions these schemes as suitable for specialized use cases—such as firmware or software integrity verification-rather than as comprehensive replacements for existing digital signature mechanisms. This illustrates a key tension between security robustness and operational efficiency, where theoretically strong solutions may be constrained by system-level performance requirements.

Similarly, code-based cryptographic schemes, particularly those derived from the McEliece framework, demonstrate strong resistance to both classical and quantum attacks [48], [49]. However, their extremely large public key sizes pose a significant barrier to integration into financial systems characterized by constrained communication protocols and legacy infrastructure. Despite their cryptographic soundness, these limitations reduce their immediate attractiveness compared to more implementation-friendly alternatives, reinforcing the importance of practical deployability in determining feasibility.

Beyond PQC approaches, Quantum Key Distribution (QKD) is also explored as a potential quantum-safe solution, offering a theoretically secure key exchange based on quantum-mechanical principles. However, its adoption remains limited due to infrastructure complexity, high deployment costs, and scalability constraints, particularly in geographically distributed financial networks. Consequently, QKD is more commonly positioned as a complementary solution for high-security communication channels rather than a primary cryptographic replacement.

Taken together, these findings suggest that no single approach fully satisfies the security, performance, and integration requirements of financial systems. Instead, the literature

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

converges on hybrid cryptographic strategies that combine classical and post-quantum techniques as a transitional pathway. Such approaches enable financial institutions to maintain operational continuity while incrementally introducing quantum-resistant capabilities, reflecting a pragmatic balance between immediate feasibility and long-term security objectives.

3) RQ3: What barriers hinder timely quantum-safe migration in the financial sector?

The review reveals that barriers to quantum-safe migration are multi-dimensional, spanning technical, organizational, economic, and regulatory domains, and collectively constraining the pace and effectiveness of transition efforts within financial systems. Among these, technical barriers are the most prominent, reflecting the inherent complexity of deploying post-quantum cryptography (PQC) and quantum key distribution (QKD) in performance-sensitive, highly interconnected financial infrastructures. Key challenges include increased computational overhead, larger key sizes, latency implications, and interoperability issues between classical and post-quantum cryptographic components [50],[51],[52]. These constraints are amplified by the persistence of legacy systems, which remain tightly coupled to RSA and ECC-based architectures, making rapid replacement both technically risky and operationally disruptive [53]. The requirement for hybrid coexistence during transition further complicates system integration, as financial ecosystems rely on seamless interoperability across APIs, payment platforms, and interbank networks [54]. Consequently, technical feasibility is not solely a function of algorithm design but of system-wide compatibility and integration readiness.

However, the dominance of technical constraints does not imply that migration is purely an engineering challenge. Organizational barriers introduce a critical human and institutional dimension, where shortages of specialized expertise, incomplete cryptographic inventories, and resistance to large-scale transformation impede progress [19] , [55]. Financial institutions, by design, prioritize stability and risk minimization, which can slow the adoption of disruptive security innovations [56]. This inertia is further reinforced by the limited availability of PQC-skilled professionals and the absence of sustained training and capacity-building initiatives [56];[57]. Effective migration, therefore, depends not only on technical solutions but also on leadership commitment,

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

change management strategies, and organizational alignment that support enterprise-wide transformation [58].

Economic constraints further complicate adoption by introducing cost-benefit uncertainties that discourage early investment. Migration to PQC entails a significant total cost of ownership (TCO), encompassing implementation, integration, maintenance, training, and potential operational disruption. In highly competitive financial environments, where budgets are constrained and prioritized toward initiatives with immediate returns, quantum-safe migration competes with other strategic investments such as digital transformation and regulatory compliance. Moreover, the return on investment (ROI) for PQC adoption is inherently indirect and long-term, as it is driven by the mitigation of future probabilistic threats rather than immediate performance gains [59]. This temporal disconnect between cost and benefit reduces institutional incentives for proactive migration.

Regulatory and compliance barriers further reinforce this hesitation, as existing cybersecurity frameworks are largely designed around classical threat models and provide limited guidance on quantum-related risks [23]. The absence of clear regulatory mandates or enforcement mechanisms creates uncertainty, leading institutions to adopt a wait-and-see approach. At the same time, ongoing standardization efforts by bodies such as NIST and ETSI, while critical for long-term alignment, introduce transitional ambiguity due to evolving specifications and incomplete standards [50]. This regulatory uncertainty delays decision-making and limits coordinated action across the financial sector.

Taken together, these findings indicate that an interplay of technical complexity, organizational readiness, economic feasibility, and regulatory clarity constrains quantum-safe migration. The convergence of these barriers underscores that migration cannot be treated as a purely technological upgrade but must be approached as a coordinated socio-technical transformation. Addressing these constraints, therefore, requires integrated strategies that align technological innovation with institutional capacity, economic justification, and policy direction, ensuring that financial systems can transition effectively in the face of emerging quantum risks.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

4) RQ4: What frameworks, roadmaps, or standards are there to support quantum-resilient transition in the financial sector?

The review indicates that quantum-resilient transition in the financial sector is currently guided more by evolving standards and strategic roadmaps than by fully mature, sector-specific frameworks. Leading this effort are standardization bodies such as the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI), which provide foundational guidance on post-quantum cryptographic selection, validation, and implementation [60]. These initiatives establish a critical baseline for algorithm standardization and interoperability; however, they remain largely technology-centric and do not fully address the operational complexities of financial-sector migration.

Building on these standards, several studies propose structured migration roadmaps that emphasize staged, risk-managed transition processes. Common elements across these roadmaps include the development of comprehensive cryptographic inventories, capacity building through technical and governance upskilling, and the execution of controlled pilot deployments to test post-quantum solutions in real-world environments [61];[62]. This reflects a growing consensus that quantum-safe migration cannot be approached as a one-time replacement but must be embedded in existing system life cycles, enabling incremental adaptation and validation.

However, a key insight emerging from the synthesis is the absence of fully integrated, sector-specific frameworks that simultaneously address technical implementation, organizational readiness, and regulatory alignment. Existing approaches tend to prioritize either cryptographic standardization or high-level strategic guidance, with limited integration across socio-technical dimensions. This fragmentation highlights a critical gap between standardization efforts and practical deployment requirements within financial systems, where interoperability, governance, and compliance considerations are tightly coupled.

Consequently, the literature suggests that effective quantum-resilient transition requires a shift from isolated standards and roadmap-driven approaches toward integrated frameworks that align technical, organizational, and policy dimensions. Such frameworks

must support not only cryptographic migration but also institutional preparedness, risk governance, and regulatory coordination. This gap directly motivates the development of a unified, sector-oriented migration framework, positioning the present study's contribution within the evolving landscape of quantum-safe transition strategies.

5) RQ5. How are the post-quantum cryptographic solutions applied across different financial sector use cases?

The review indicates that the adoption of post-quantum cryptography (PQC) solutions in the financial sector is increasingly framed as a proactive risk mitigation strategy to safeguard systems against current and future quantum-enabled threats. This shift reflects the recognition that widely deployed cryptographic mechanisms, particularly those underpinning authentication and key exchange, are vulnerable to quantum algorithms such as Shor's and Grover's, thereby exposing critical financial processes to long-term compromise. As a result, PQC adoption is not confined to isolated systems but is progressively embedded across core financial functions.

In authentication and digital identity management, PQC is used to enhance the resilience of high-value targets, such as digital wallets, electronic Know Your Customer (e-KYC) platforms, and identity verification systems [63]. These environments require strong guarantees of integrity and non-repudiation, making them particularly sensitive to quantum threats. The literature highlights the use of modular and hybrid cryptographic architectures, which enable incremental integration of PQC into multi-factor authentication and onboarding processes without disrupting existing services [64]. This reflects a broader strategy to maintain operational continuity while transitioning to quantum-resistant mechanisms.

In payment systems and financial transactions, PQC solutions are increasingly considered for integration into payment gateways and transaction routing infrastructures to ensure confidentiality and integrity under future threat models [65]. Given the real-time, high-throughput nature of financial transactions, the feasibility of such integration depends on maintaining performance while enhancing security. In high-value or interbank contexts, Quantum Key Distribution (QKD) is explored as a complementary mechanism for secure key exchange, particularly where the sensitivity of transmitted data justifies

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

the associated infrastructure costs. This demonstrates a differentiated application strategy, in which more resource-intensive solutions are reserved for critical communication channels.

The role of PQC is particularly pronounced in long-term data protection, where the risk of "harvest-now, decrypt-later" attacks necessitate forward-looking security measures. Financial institutions increasingly apply PQC to protect customer records, transaction histories, and contractual data, ensuring confidentiality over extended time horizons [66]. This extends beyond active systems to include archival and internal storage environments, reflecting a lifecycle-oriented approach to data security.

Similarly, interbank communication and financial market infrastructure require secure, quantum-resistant communication channels to preserve system integrity and operational resilience. The alignment of such applications with evolving standards from NIST and ETSI further reinforces the importance of maintaining secure communication protocols across interconnected financial ecosystems [66]. These developments highlight the growing interdependence between technical implementation and regulatory guidance. Finally, in digital contracts, signatures, and blockchain-based systems, PQC is applied to ensure the long-term validity and integrity of digital signatures, which are foundational to financial record-keeping and legal enforceability [65]. The threat of quantum-enabled forgery introduces significant risks to blockchain systems and distributed ledgers, necessitating the adoption of quantum-resistant signature schemes to preserve immutability and trust [67].

Collectively, these findings demonstrate that PQC adoption in the financial sector is not uniform but context-dependent, varying according to the sensitivity, performance requirements, and lifecycle of specific use cases. This results in a layered application model in which different cryptographic approaches are selectively deployed across authentication, transactions, data protection, and infrastructure systems. Such an approach reinforces the need for flexible, hybrid, and use-case-driven migration strategies that balance security, performance, and operational continuity in the transition toward quantum-resilient financial systems.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

3.10. Discussion of Gaps and Implications

The synthesis of findings reveals that current research on quantum-safe cryptography in the financial sector remains fragmented, predominantly technology-driven, and insufficiently aligned with the socio-technical realities of large-scale cryptographic transition. While significant progress has been made in identifying quantum threats, evaluating post-quantum cryptographic (PQC) techniques, and outlining migration challenges, the literature lacks an integrated perspective that connects these dimensions into a coherent transition logic.

A key gap emerges in the limited theoretical grounding of existing studies. As observed in the reviewed evidence, only a single study explicitly applied an established theoretical framework-specifically, the Technology–Organization-Environment (TOE) model-to assess post-quantum readiness, while most studies rely on technical simulations, algorithmic evaluations, or conceptual discussions. This over-reliance on technical perspectives results in an incomplete understanding of quantum-safe migration, which, in practice, is shaped not only by cryptographic feasibility but also by organizational capacity, governance structures, and regulatory environments. Consequently, existing approaches risk oversimplifying migration as a purely technical upgrade rather than a complex socio-technical transformation.

Beyond theoretical limitations, the findings highlight a lack of integration across critical dimensions of quantum-safe transition. The results demonstrate that research tends to examine quantum threats, cryptographic solutions, migration barriers, and organizational readiness in isolation, without sufficiently explaining how these elements interact in real-world financial systems. For example, while lattice-based cryptography is identified as the most feasible technical solution, its adoption is constrained by performance overheads, legacy infrastructure, and interoperability challenges. Similarly, migration barriers extend beyond technical issues to include organizational resistance, regulatory uncertainty, and cost constraints, yet these factors are rarely synthesized into a unified adoption pathway. This fragmentation limits the practical applicability of existing studies, as financial institutions require coordinated strategies that address technical, organizational, and regulatory dependencies simultaneously.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

A further gap lies in the absence of lifecycle-oriented migration models grounded in empirical synthesis. Although several studies propose high-level roadmaps or recommend phased adoption, they do not provide structured, end-to-end transition frameworks that guide institutions from initial readiness assessment to full-scale deployment and continuous monitoring. As a result, there is limited clarity on how financial institutions should operationalize quantum-safe migration in practice, particularly in environments characterized by legacy systems, high transaction volumes, and stringent regulatory requirements.

The review also identifies a disconnect between cryptographic innovation and institutional readiness. While advancements in PQC and QKD demonstrate strong theoretical security, their real-world deployment remains constrained by skills shortages, governance gaps, and limited regulatory direction. This imbalance highlights a critical gap between technological development and operational adoption, suggesting that existing research does not adequately address the institutional conditions required for successful migration.

Collectively, these gaps indicate that current literature does not provide a sufficiently integrated, theory-informed, and implementation-oriented approach to quantum-safe transition in the financial sector. Studies with weaker alignment were primarily used to contextualize broader trends rather than to inform sector-specific migration conclusions. In response, this study proposes a two-stage conceptual contribution. First, a Post-Quantum Cryptography Readiness Migration Model is developed to address challenges in early-stage assessment and preparedness. Second, a broader Quantum-Safe Migration Framework is introduced to extend this into a full lifecycle transition process, integrating strategy, implementation, validation, and continuous monitoring. These complementary models provide a unified pathway that bridges the gap between technical feasibility and organizational deployment, thereby addressing the limitations identified in existing research.

3.11. Post-Quantum Cryptography Readiness Migration Model

The gaps identified in the previous section highlight the lack of structured approaches for assessing organizational preparedness before the quantum-safe transition. In

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

response, this study proposes a Post-Quantum Cryptography (PQC) Readiness Migration Model (Figure 8), which focuses on the pre-migration phase of quantum-safe transformation. The model addresses the critical need for institutions to understand their current cryptographic exposure, operational constraints, and institutional capacity before undertaking large-scale migration. The proposed framework should be interpreted as a synthesis-driven conceptual model rather than a prescriptive standard. Given the evolving nature of post-quantum technologies and the limited availability of large-scale empirical deployments, the framework provides a structured foundation for guiding transition efforts but requires validation through future empirical and industry-based implementations.

Table 5. Alignment of Codes, Themes, and Framework Components

Code Example	Theme	Framework Component
RSA/ECC vulnerability, HNDL risk	Quantum Threats	Risk
PQC performance, algorithm selection	Cryptographic feasibility	Technical
Legacy systems, interoperability issues	Migration Barriers	Operational
Regulation, policy, skills readiness	Governance Readiness	Governance

Figure 8 and 9 present the resulting frameworks derived from this transformation process, illustrating how the identified themes are operationalized into structured readiness and migration components.

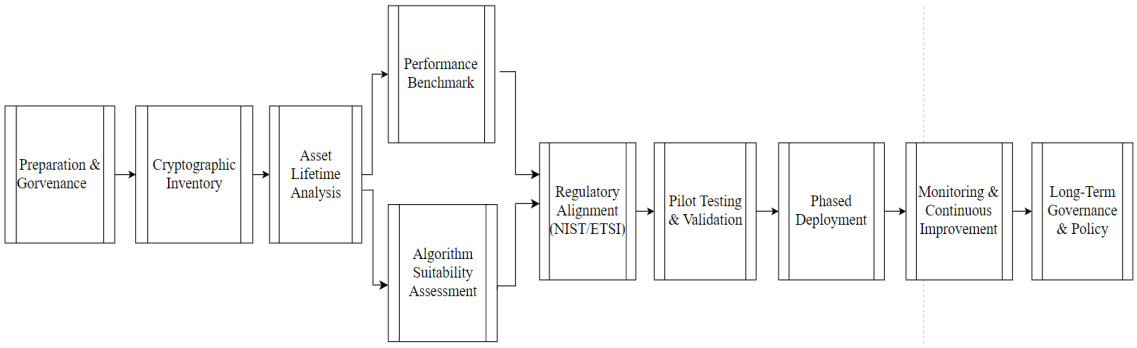

Figure 8. PQC Readiness Migration Model

Unlike existing approaches that prematurely emphasize implementation, the proposed readiness model recognizes that financial institutions operate in complex environments characterized by legacy infrastructure, regulatory obligations, and performance-sensitive

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

systems. As such, migration cannot begin without a comprehensive assessment of cryptographic dependencies and system vulnerabilities.

The model is structured around five interrelated readiness components. First, cryptographic inventory and asset discovery establish visibility into existing cryptographic assets, including RSA and ECC dependencies embedded within financial systems. This stage directly responds to findings on hidden exposure risks and the prevalence of legacy systems. Second, risk and asset lifetime analysis evaluates the sensitivity and longevity of protected data, particularly in the context of "harvest-now, decrypt-later" threats, thereby ensuring the prioritization of high-risk assets. Third, algorithm suitability and performance benchmarking assess the feasibility of PQC alternatives under real-world constraints such as latency, throughput, and storage overhead, reflecting the trade-offs identified in results. Fourth, regulatory alignment and governance readiness ensure that migration planning is consistent with emerging standards such as NIST and ETSI, while also addressing institutional governance capacity. Finally, pilot testing and validation enable controlled experimentation of PQC solutions within operational environments before full-scale deployment. Importantly, the readiness model does not prescribe migration itself but rather establishes the conditions under which migration becomes feasible and sustainable. This distinction is critical, as it separates assessment from execution, thereby reducing the risk of premature or poorly coordinated transitions. In doing so, Figure 8 provides a structured foundation that prepares financial institutions for the subsequent migration process.

The development of the PQC Readiness Migration Model was not prescriptive but inductively derived from the synthesis of evidence across the included studies, particularly those addressing cryptographic exposure, migration constraints, and organizational preparedness. The model consolidates recurring elements identified in results, including asset visibility, risk prioritization, performance feasibility, and governance alignment, into a structured pre-migration assessment logic. However, it is important to emphasize that readiness is inherently context dependent. Financial institutions vary significantly in terms of infrastructure maturity, regulatory obligations, and operational scale. As such, the model should be interpreted as a guiding structure

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

rather than a one-size-fits-all solution, requiring adaptation to institutional and jurisdictional contexts.

3.12. Integrated Quantum-Safe Migration Framework

While the readiness model addresses pre-migration preparedness, it does not capture the full lifecycle of quantum-safe transition. To bridge this gap, this study advances a Quantum-Safe Migration Framework (Figure 9), which extends the readiness model into a comprehensive, end-to-end transition process. The proposed Quantum-Safe Migration Framework was systematically constructed through cross-sectional synthesis of the review findings, integrating four key evidence domains: (i) quantum threat characterization, (ii) cryptographic feasibility and performance trade-offs, (iii) migration barriers and organizational readiness constraints, and (iv) emerging standards and migration roadmaps. Rather than introducing new constructs, the framework reorganizes empirically observed patterns into a coherent lifecycle structure, thereby addressing the fragmentation identified in existing literature.

The relationship between Figure 8 and Figure 9 is therefore sequential and complementary. Importantly, the readiness model is diagnostic in nature, focusing on assessing cryptographic exposure, institutional capacity, and preparedness conditions prior to transition. The migration framework is execution-oriented, guiding the lifecycle process of strategy formulation, implementation, and continuous governance. The readiness model provides the diagnostic foundation, while the migration framework operationalizes it into a structured implementation pathway. Together, they form a unified transition architecture that moves from assessment to execution and continuous governance. The framework is organized into four iterative stages. The first stage, threat and readiness assessment, builds directly on the outputs of the readiness model, incorporating cryptographic inventories, risk prioritization, and institutional preparedness into a consolidated decision base. This ensures that migration decisions are evidence-driven rather than reactive.

The second stage, strategy formulation and planning, defines migration pathways based on organizational context. This includes selecting PQC algorithms, identifying hybrid cryptographic strategies, and aligning with regulatory and operational requirements. The

emphasis on hybrid approaches reflects the consistent finding that full replacement is neither feasible nor desirable in the short term, particularly in high-throughput financial systems.

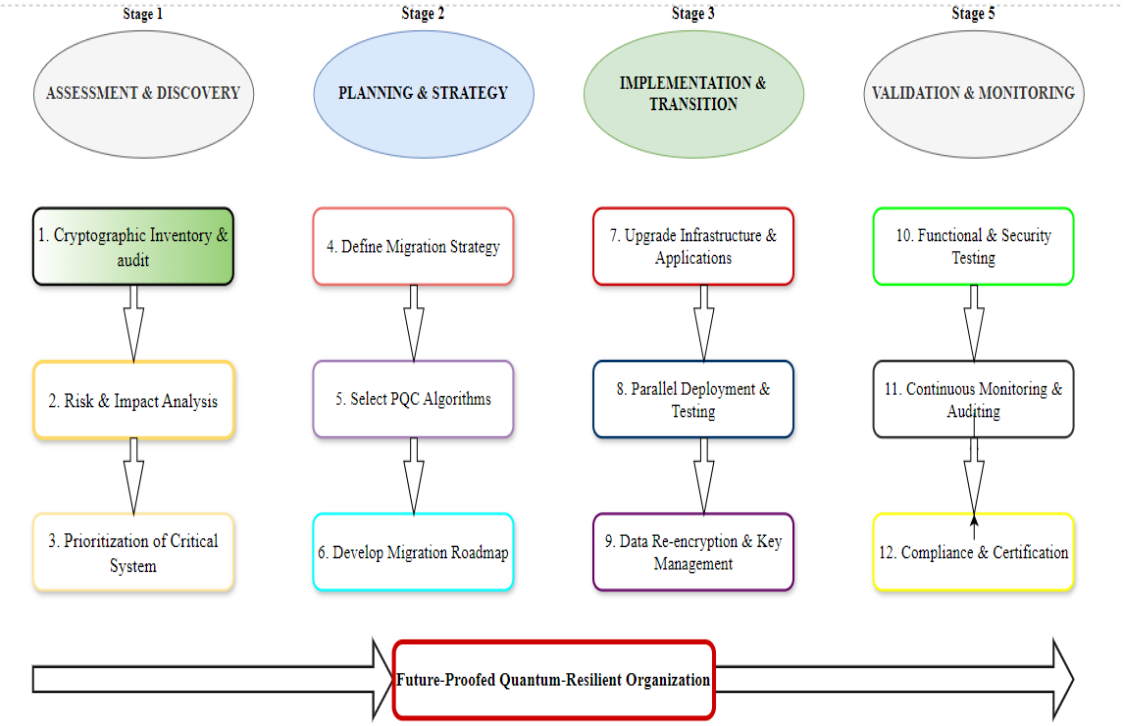

Figure 9. Quantum-Safe Migration Framework

The third stage, implementation and transition, focuses on the gradual deployment of quantum-safe solutions. This includes infrastructure upgrades, system integration, and coexistence of classical and post-quantum cryptographic mechanisms. The phased nature of this stage directly addresses technical, organizational, and economic barriers identified in Section 3.5, ensuring minimal disruption to critical financial operations. The final stage, validation, monitoring, and continuous governance, ensures that deployed solutions remain effective over time. This includes performance testing, security validation, compliance auditing, and continuous monitoring of emerging quantum threats. Given the evolving nature of both quantum computing and cryptographic standards, this stage reinforces the need for adaptive governance rather than static implementation.

A key contribution of the framework lies in its integration of technical and organizational dimensions into a single transition logic. Unlike prior models that focus primarily on

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

algorithmic replacement, the proposed framework explicitly incorporates governance structures, regulatory alignment, and institutional capacity as core components of migration. This reflects the broader finding that quantum-safe transition is inherently socio-technical and cannot be achieved solely through technological change. Furthermore, the framework adopts a nonlinear, iterative perspective, recognizing that financial institutions may revisit earlier stages as new threats, standards, or operational constraints emerge. This adaptability is essential in environments characterized by uncertainty in quantum timelines and evolving standardization processes.

Taken together, Figure 9 operationalizes the insights from this review into a coherent, lifecycle-oriented framework that guides financial institutions from readiness assessment to sustained quantum-safe operation. When combined with the readiness model in Figure 8, the proposed approach resolves the fragmentation identified in existing literature by providing a clear, structured, and empirically grounded pathway for quantum-safe migration in the financial sector.

While the framework provides a structured pathway for quantum-safe migration, its application must be approached with caution. The findings of this review reflect an evolving research landscape characterized by ongoing standardization efforts, limited large-scale implementations, and uncertainty about quantum computing timelines. Consequently, the framework should not be interpreted as a fixed implementation blueprint but rather as an adaptive governance and migration guide. In practice, financial institutions will need to tailor the framework based on their risk appetite, regulatory environment, and technological capabilities. Furthermore, as post-quantum standards mature and new empirical evidence emerges, elements of the framework may require refinement. This reinforces the need for iterative adoption, continuous validation, and governance-driven adaptation, rather than static implementation.

3.13. Implications for Theory, Practice, and Policy

The findings of this study have important implications that extend beyond descriptive synthesis, particularly in advancing how quantum-safe migration is conceptualized, operationalized, and governed within financial sector environments. From a theoretical perspective, this study contributes by reframing quantum-safe migration as a socio-

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

technical transformation rather than a purely cryptographic problem. The existing literature predominantly emphasizes algorithmic resilience and performance evaluation, often overlooking the organizational and governance dimensions that shape real-world adoption. By integrating insights across quantum threats, cryptographic feasibility, migration barriers, and governance readiness, this study advances a more holistic perspective that aligns with socio-technical and technology adoption theories. In particular, the limited application of formal theoretical models such as the Technology–Organization–Environment (TOE) framework-highlights a critical gap in current research, which this study begins to address by embedding organizational and environmental considerations into the proposed models. This positions quantum-safe migration within a broader theoretical discourse on digital transformation, risk governance, and infrastructure resilience.

From a practical perspective, the study provides actionable guidance for financial institutions navigating the transition toward quantum-safe systems. The findings demonstrate that migration cannot be approached as a direct replacement of cryptographic algorithms, but rather requires phased, risk-informed, and hybrid strategies. The dominance of lattice-based cryptography reflects its practical feasibility; however, performance trade-offs, interoperability constraints, and legacy system dependencies necessitate incremental adoption. The proposed readiness model (Figure 8) enables institutions to assess cryptographic exposure, prioritize high-risk assets, and evaluate institutional preparedness prior to implementation. Building on this, the migration framework (Figure 9) offers a structured pathway for executing transition strategies while maintaining operational continuity. Importantly, identifying organizational and economic barriers underscores the need to invest in cryptographic expertise, system modernization, and change management processes rather than relying solely on technological upgrades.

From a policy and regulatory perspective, the study highlights the critical role of governance and standardization in shaping quantum-safe adoption. The reliance on emerging standards from organizations such as NIST and ETSI underscores the importance of coordinated regulatory direction; however, the findings indicate that uncertainty around standardization timelines and limited regulatory guidance continue

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

to delay institutional commitment. This suggests that policymakers must move beyond high-level recommendations toward clear, sector-specific guidance on migration timelines, compliance expectations, and risk management practices. Furthermore, the uneven global distribution of research and preparedness raises concerns about disparities in quantum readiness, particularly for developing financial systems that may lack the resources to implement advanced cryptographic solutions. Addressing this imbalance will require collaborative efforts among regulators, industry bodies, and international standardization organizations to ensure inclusive, globally aligned quantum-safe strategies.

Finally, the study carries important implications for future research and methodological development. The identified gaps highlight the need for more empirically grounded studies that examine large-scale implementation of PQC and QKD in operational financial environments. Future work should also prioritize integrating theoretical frameworks, conducting longitudinal evaluations of migration strategies, and developing performance benchmarks that reflect real-world constraints in the financial system. In addition, the evolving nature of quantum threats and cryptographic standards calls for adaptive research approaches that continuously reassess the effectiveness of proposed solutions over time.

3.14. Limitations and Future research direction

This study is subject to several limitations that should be considered when interpreting the findings. First, although the review followed a PRISMA-guided approach, the analysis was limited to studies retrieved from selected databases, potentially excluding relevant work published in other sources or emerging industry reports. Given the rapidly evolving nature of quantum computing and post-quantum cryptography, some recent developments—particularly in standardization and real-world deployments—may not yet be fully captured in the academic literature.

Second, the study relies on secondary data from published research, which varies in methodological rigour, scope, and contextual focus. While quality assessment procedures were applied, the heterogeneity of included studies introduces variability in how findings can be interpreted and synthesized. In particular, the limited number of empirical, large-

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

scale implementation studies in the financial sector constrains the ability to draw definitive conclusions about operational performance and real-world feasibility of proposed solutions.

Third, the proposed readiness model and migration framework are conceptual and synthesis-driven, rather than empirically validated through case studies or experimental deployment. Although they are grounded in patterns identified across the reviewed literature, their applicability may vary across different institutional contexts, regulatory environments, and technological infrastructures. As such, they should be interpreted as adaptive guiding structures rather than fixed implementation models.

These limitations provide several avenues for future research. There is a clear need for empirical validation of quantum-safe migration strategies through case studies, pilot implementations, and longitudinal evaluations within financial institutions. Future studies should examine how PQC and QKD solutions perform under real-world constraints, including transaction throughput, latency, interoperability, and integration with legacy systems. In addition, further research should focus on developing and testing theoretically grounded models that incorporate organizational, technological, and environmental dimensions of quantum-safe adoption. The application of frameworks such as TOE, diffusion of innovation, and socio-technical systems theory can provide deeper insights into adoption dynamics beyond purely technical considerations.

Future work should also explore the economic and strategic dimensions of migration, including cost–benefit analyses, return on investment, and prioritization strategies for phased implementation. Given the long-term and uncertain nature of quantum threats, understanding how institutions justify and sequence investments in quantum-safe technologies remains a critical research gap. Finally, there is a need for further research on policy and regulatory alignment, particularly in developing regions where quantum readiness remains limited. Comparative studies examining regulatory approaches, standardization efforts, and institutional preparedness across different jurisdictions can contribute to more globally inclusive and coordinated quantum-safe strategies.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

4. CONCLUSION

This study provides a sector-focused synthesis of quantum threats, post-quantum cryptographic solutions, and migration challenges in financial systems, highlighting that the quantum-safe transition extends beyond algorithm replacement to a broader socio-technical transformation. The findings indicate that while lattice-based cryptography offers a practical near-term pathway, effective migration is constrained by legacy infrastructure, organizational readiness, and regulatory uncertainty. The study contributes a two-stage conceptual approach comprising a readiness assessment model and a lifecycle-oriented migration framework, which together support more structured transition planning. In practice, this suggests that financial institutions should prioritize early assessment of cryptographic exposure and adopt phased, hybrid migration strategies aligned with operational and regulatory conditions. A key limitation of this review is its reliance on existing literature with limited large-scale empirical validation in financial environments. Future research should focus on empirical evaluation of quantum-safe migration strategies in real-world financial systems to assess performance, scalability, and governance implications.

REFERENCES

[1] M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array*, vol. 15, no. August, p. 100242, 2022, doi: 10.1016/j.array.2022.100242.

[2] I. A. Vasilenko, "Quantum Cyber Threats and Their Impact on the Security of Critical Information Infrastructure," *Phys. At. Nucl.*, vol. 88, no. 12, pp. 2478–2483, 2025, doi: 10.1134/S106377882510045X.

[3] N. R. Mosteanu and A. Faccia, "Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation," *J. Open Innov. Technol. Mark. Complex.*, vol. 7, no. 1, pp. 1–19, 2021, doi: 10.3390/joitmc7010019.

[4] A. Tiwari, R. Chauhan, N. Joshi, S. Devliyal, S. Aluvala, and A. Kumar, "The Quantum Threat: Implications for Data Security and the Rise of Post-Quantum Cryptography," *2024 IEEE 9th Int. Conf. Converg. Technol. I2CT 2024*, pp. 1–7, 2024, doi: 10.1109/I2CT61223.2024.10543513.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[5] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, pp. 1–31, 2021, doi: 10.22331/Q-2021-04-15-433.

[6] A. Karakaya and A. Ulu, "A survey on post-quantum based approaches for edge computing security," *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 16, no. 1, 2024, doi: 10.1002/wics.1644.

[7] A. Titilola, S. Abayomi, A. Justina, and O. Cynthia, "Future-Proofing Data : Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate ' Harvest Now , Decrypt Later ' Attacks," *Arch. Curr. Res. Int.*, vol. 25, no. 3, pp. 60–80, 2025.

[8] D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham, and T. T. Hoang, "A survey of post-quantum cryptography: start of a new race," *Cryptography*, vol. 7, no. 3, pp. 1–18, 2023, doi: 10.3390/cryptography7030040.

[9] M. A. Mansur, "A quantum-safe, interoperable, and decentralized payment infrastructure for the post-classical era as a strategic framework for secure global transactions," 2025, *ESJ Social Sciences, United States*. doi: 10.19044/esj.2025.v21n19p17.

[10] S. Kumar, A. Klappenecker, G. Brown, and S. Saravanan, "Quantum apocalypse: fortifying critical infrastructure in the age of cyber warfare," *Eur. Conf. Inf. Warf. Secur. ECCWS*, pp. 293–301, 2025, doi: 10.34190/eccws.24.1.3757.

[11] L. Jančí Ćut, "Cybersecurity in the financial sector and the quantum-safe cryptography transition : in search of a precautionary approach in the EU Digital Operational," *Int. Cybersecurity Law Rev.*, pp. 145–154, 2025, doi: 10.1365/s43439-025-00135-7.

[12] S. Dixit, "The impact of quantum supremacy on cryptography: implications for secure financial transactions," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, pp. 611–637, 2020, doi: 10.32628/cseit2064141.

[13] S. Li *et al.*, "Post-Quantum Security: Opportunities and Challenges," *Sensors*, 2023, doi: 10.3390/s23218744.

[14] H. H. Shadan, "Quantum computing and cybersecurity in accounting and finance in the post-quantum world: challenges and opportunities for securing accounting and finance systems," pp. 1–41, 2025, doi: 10.3390/fintech4040052.

[15] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," *Proc. 2022 7th Int. Conf. Mob. Secur. Serv. MobiSecServ 2022*, pp. 1–8, 2022, doi: 10.1109/MobiSecServ50855.2022.9727214.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[16] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *BMJ*, vol. 339, no. 7716, pp. 332–336, 2009, doi: 10.1136/bmj.b2535.

[17] H. A. Long, D. P. French, and J. M. Brooks, "Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis," *Res. Methods Med. Heal. Sci.*, vol. 1, no. 1, pp. 31–42, 2020, doi: 10.1177/2632084320947559.

[18] C. R. Garcia, A. C. Aguilera, C. Stan, J. J. V. Olmos, S. Rommel, and I. T. Monroy, "Enhanced network security protocols for the quantum era: combining classical and post-quantum cryptography, and quantum key distribution," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 8, pp. 2765–2781, 2025, doi: 10.1109/JSAC.2025.3568011.

[19] K. F. Hasan *et al.*, "A framework for migrating to post-quantum cryptography: security dependency analysis and case studies," *IEEE Access*, vol. 12, no. January, pp. 23427–23450, 2024, doi: 10.1109/ACCESS.2024.3360412.

[20] M. F. Zulfa and K. Anwar, "Development of quantum key distribution (QKD) with E91 protocol for future secure quantum networks," *J. Phys. Conf. Ser.*, vol. 2980, no. 1, 2025, doi: 10.1088/1742-6596/2980/1/012038.

[21] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices," *IEEE Trans. Ind. Informatics*, vol. 21, no. 2, pp. 1674–1683, 2025, doi: 10.1109/TII.2024.3485796.

[22] K. S. Shim, B. Kim, and W. Lee, "Research on Quantum Key, Distribution Key and Post-quantum Cryptography Key Applied Protocols for Data Science and Web Security," *J. Web Eng.*, vol. 23, no. 6, pp. 813–830, 2024, doi: 10.13052/jwe1540-9589.2365.

[23] A. Zafar, "Quantum Computing in Finance: Regulatory Readiness, Legal Gaps, and the Future of Secure Tech Innovation," *Eur. J. Risk Regul.*, vol. 2, no. May, pp. 1–32, 2025, doi: 10.1017/err.2025.10050.

[24] S. Nagpal *et al.*, "Quantum Computing Integrated Patterns for Real-Time Cryptography in Assorted Domains," *IEEE*, vol. 12, no. September, pp. 132317–132331, 2024, doi: 10.1109/ACCESS.2024.3401162.

[25] J. A. Montenegro, R. Rios, and J. Lopez-Cerezo, "A performance evaluation framework for post-quantum TLS," *Futur. Gener. Comput. Syst.*, vol. 175, no. February 2025, p. 108062, 2026, doi: 10.1016/j.future.2025.108062.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[26] R. Auer, D. Dodson, A. Dupont, M. Haghighi, N. Margaine, and D. Marsden, "Quantum-readiness for the financial system : a roadmap, BIS Papers No. 158," 2025.

[27] D. J. Egger *et al.*, "Quantum Computing for Finance: State-of-the-Art and Future Prospects," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, doi: 10.1109/TQE.2020.3030314.

[28] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats," *Procedia Comput. Sci.*, vol. 215, pp. 834–845, 2022, doi: 10.1016/j.procs.2022.12.086.

[29] V. Laxman, N. Ramesh, S. K. Jaya Prakash, and R. Aluvala, "Emerging threats in digital payment and financial crime: A bibliometric review," *J. Digit. Econ.*, vol. 3, no. March, pp. 205–222, 2024, doi: 10.1016/j.jdec.2025.04.002.

[30] I. Kong, M. Janssen, and N. Bharosa, "Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions," *Gov. Inf. Q.*, vol. 41, no. 1, p. 101884, 2024, doi: 10.1016/j.giq.2023.101884.

[31] P. Kampanakis and W. Childs-klein, "The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections," in *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)*, 2024. doi: 10.14722/madweb.2024.23010.

[32] P. Radanliev, "Artificial intelligence and quantum cryptography," *J. Anal. Sci. Technol.*, vol. 15, no. 1, 2024, doi: 10.1186/s40543-024-00416-6.

[33] M. Mehic, E. Dervisevic, P. Fazio, and M. Voznak, "Virtual quantum key distribution network ecosystem: the national Czech QKD network," *IEEE Netw.*, vol. 39, no. 3, pp. 173–179, 2025, doi: 10.1109/MNET.2025.3540705.

[34] Y. Jiang, "Post-Quantum Cryptography: Mathematical Foundations and Future Challenges," *Theor. Nat. Sci.*, vol. 125, no. 1, pp. 65–72, 2025, doi: 10.54254/2753-8818/2025.gl25401.

[35] C. G. Kinyua, "'The impact of quantum computing on cryptographic systems: urgency of quantum-resistant algorithms and practical applications in cryptography,'" *Eur. J. Inf. Technol. Comput. Sci.*, vol. 5, no. 1, pp. 1–10, 2025, doi: 10.24018/ejcompute.2025.5.1.146.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[36] S. Sadeghi, V. Chouhan, M. Aldarwbi, A. Ghorbani, A. Chow, and R. Burko, "Securing financial sector applications in the quantum era: a comprehensive evaluation of NIST's recommended algorithms through use-case analysis," *Elsevier*, vol. 288, no. May 2024, p. 128243, 2025, doi: 10.1016/j.eswa.2025.128243.

[37] P. Maitireni, V. Ncube, B. Ndlovu, and T. Sibanda, "Quantum computing cryptography: systematic review of innovations, applications, challenges, and algorithms," *J. Inf. Syst. Informatics*, 2025, doi: 10.63158/journalisi.v7i4.1331.

[38] J. Senor, J. Portilla, and G. Mujica, "Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18778–18790, 2022, doi: 10.1109/JIOT.2022.3162254.

[39] H. Shiu, C. Yang, Y. Tsai, W. Lin, and C. Lai, "Maintaining Secure Level on Symmetric Encryption under Quantum Attack," *Appl. Sci.*, 2023, doi: 10.3390/app13116734.

[40] F. Raheman, "From standard policy-based zero trust to absolute zero trust (AZT): a quantum leap to q-day security," pp. 252–282, 2024, doi: 10.4236/jcc.2024.123016.

[41] S. Ahmed, A. Ahad, and S. Subhan, "Decoherence Impediments in Quantum Computing and Fundamental Challenges of Quantum Error Correction," *Asian J. Res. Comput. Sci.*, vol. 18, no. 12, pp. 228–239, 2025.

[42] A. B. A. Mohamed, E. M. Khalil, M. F. Yassen, and H. Eleuch, "Two-qubit local fisher information correlation beyond entanglement in a nonlinear generalized cavity with an intrinsic decoherence," *Entropy*, vol. 23, no. 3, pp. 1–13, 2021, doi: 10.3390/e23030311.

[43] Z. Ye, R. Song, H. Zhang, D. Chen, C. Cheung, and K. Huang, "A Highly-efficient Lattice-based Post-Quantum Cryptography Processor for IoT Applications," vol. 2024, no. 2, pp. 130–153, 2025, doi: 10.46586/tches.v2024.i2.130-153.

[44] G. Song, K. Jang, S. Eum, and M. Sim, "NTT and Inverse NTT Quantum Circuits in CRYSTALS-Kyber for Post-Quantum Security Evaluation," *Appl. Sci.*, 2023, doi: 10.3390/ app131810373.

[45] R. Azarderakhsh, M. Sadat, and A. Tehrani, "Integrating Post-Quantum Cryptography (PQC) with Quantum Key Distribution (QKD): Challenges and Considerations," in *Proc. of SPIE*, 2025, pp. 1–6. doi: 10.1117/12.3055954.

[46] J. Lee, T. G. Kang, K. Cho, and D. Hyun, "New Parameter Sets for SPHINCS + ∗," *Inst. Electron. Inf. Commun. Eng.*, no. 6, pp. 890–892, 2021, doi: 10.1587/transinf.2019EDL8223.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[47] A. A. Moosa, "Performance evaluation of post quantum digital signature algorithms over WDM optical communication system," *J. Opt. Commun.*, pp. 1–21, 2025, doi: 10.1515/joc-2025-0104.

[48] J. Junquera-Sanchez, C. Hernando-Ramiro, O. Gamallo-Palomares, and J.-A. Gomez-Sanchez, "Assessment of Cryptographic Approaches for Quantum- Resistant Galileo OSNMA," vol. 71, no. March, 2024, doi: 10.33012/navi.648.

[49] D. Fallnich, C. Lanius, S. Zhang, and T. Gemmeke, "Efficient ASIC Architecture for Low Latency Classic McEliece Decoding Code-Based Cryptography," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2024, no. 2, pp. 403–425, 2024, doi: 10.46586/tches.v2024.i2.403-425.

[50] F. Raheman, "The Future of Cybersecurity in the Age of Quantum Computers," *Futur. Internet*, vol. 14, no. 11, 2022, doi: 10.3390/fi14110335.

[51] L. Astrizi, Thiago and R. Custódio, "Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption," *Sensors*, vol. 24, no. 22, pp. 1–38, 2024, doi: 10.3390/s24227300.

[52] M. Abbasi, F. Cardoso, P. Váz, and J. Silva, "A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments," *Cryptography*, pp. 1–27, 2025, doi: 10.3390/cryptography9020032.

[53] T. Ngwenya and B. Ndlovu, "A Systematic Review of Post-Quantum Cryptography for Healthcare Data Protection : Performance , Readiness , and Deployment Challenges," *J. Appl. Informatics Comput.*, vol. 10, no. 1, pp. 134–149, 2026, doi: 10.30871/jaic.v10i1.11836.

[54] G. Surla and R. Lakshmi, *Quantum Cryptography Analysis for Secure Data Communication in Multi-Core Environment*, no. Icacecs. Atlantis Press International BV, 2023. doi: 10.2991/978-94-6463-314-6_20.

[55] R. T. Avireneni, "Quantum-Resilient Middleware Architecture for Secure Federated API Integration in Enterprise Cloud Ecosystems," *Eur. Mod. Stud. J.*, vol. 9, no. 4, pp. 700–714, 2025, doi: 10.59573/emsj.9(4).2025.67.

[56] K. Csenkey and N. Bindel, "Post-quantum cryptographic assemblages and the governance of the quantum threat," *J. Cybersecurity*, vol. 9, no. 1, pp. 1–14, 2023, doi: 10.1093/cybsec/tyad001.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[57] S. Sokol, "Navigating the Quantum Threat Landscape : Addressing Classical Cybersecurity Challenges," *J. Quantum Inf. Sci.*, pp. 56–77, 2023, doi: 10.4236/jqis.2023.132005.

[58] N. A. Karim, O. A. Khashan, and H. Kanaker, "Online Banking User Authentication Methods : A Systematic Literature Review," *IEEE Access*, vol. 12, no. January, pp. 741–757, 2024, doi: 10.1109/ACCESS.2023.3346045.

[59] E. O. Sodiya, U. J. Umoga, O. O. Amoo, and A. Atadoga, "Quantum computing and its potential impact on U . S . cybersecurity : A review : Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets," *Glob. J. Eng. Technol. Adavnces*, vol. 18, no. 2, pp. 49–64, 2024.

[60] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, "Improving Software Quality in Cryptography Standardization Projects," in *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 2022, pp. 19–30. doi: 10.1109/EuroSPW55150.2022.00010.

[61] P. Das -, "Quantum Computing in Payments Security: Preparing for the Post-Quantum Era," *Int. J. Sci. Technol.*, vol. 16, no. 1, pp. 1–17, 2025, doi: 10.71097/ijsat.v16.i1.2712.

[62] M. Zhang *et al.*, "Research on Development Progress and Test Evaluation of Post-Quantum Cryptography," *Entropy*, vol. 27, no. 2, pp. 1–15, 2025, doi: 10.3390/e27020212.

[63] P. Vareta, H. Muzenda, T. Nyamupaguma, and B. Ndlovu, "The Rise of Quantum Computing and its Impact on Cybersecurity," *Indones. J. Comput. Sci.*, vol. 14, no. 6, pp. 10072–10102, 2025, doi: 10.33022/ijcs.v14i6.5040.

[64] S. Dahiya, Yeshwardhan, S. Pandey, D. Patel, and A. Kulkarni, "Advancing security in digital transactions using quantum cryptography," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 47s, pp. 36–48, 2025, doi: 10.52783/jisem.v10i47s.9214.

[65] A. Ghimire, "Quantum computing in US banking: the future of fraud prevention and financial crime detection," *Glob. J. Emerg. AI Comput.*, vol. 1, no. 2, pp. 31–50, 2025, doi: 10.70445/gjeac.1.2.2025.31-50.

[66] P. Rathika, S. Vidhya, T. Jayaprakash, P. Nagasaratha, C. Sincija, and L. Guangda, "Adaptive Quantum Cryptography : A Scalable Framework for Quantum – Resistant Security in Next – Generation IoT Networks," *CompSci AI Adv.*, vol. 2, no. 1, pp. 50–61, 2025, doi: 10.69626/cai.2025.0050.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[67] L. Velasco *et al.*, "Scenarios for Optical Encryption Using Quantum Keys †," *Sensors*, vol. 24, no. 20, 2024, doi: 10.3390/s24206631.