ESJ Social Sciences   Peer-reviewed

A Quantum-Safe, Interoperable, and Decentralized Payment Infrastructure for the Post-Classical Era as a Strategic Framework for Secure Global Transactions

Md. Abul Mansur
Nuspay International Inc., United States

Doi:10.19044/esj.2025.v21n19p17

Submitted: 26 May 2025
Accepted: 11 July 2025
Published: 31 July 2025

Cite As:
Mansur, A.M. (2025). *A Quantum-Safe, Interoperable, and Decentralized Payment Infrastructure for the Post-Classical Era as a Strategic Framework for Secure Global Transactions.* European Scientific Journal, ESJ, 21 (19), 17. https://doi.org/10.19044/esj.2025.v21n19p17

Abstract

The rise of quantum computing introduces a profound threat to existing digital security frameworks, particularly those that underpin modern payment systems. Current cryptographic standards, such as RSA, ECC, and ECDSA are susceptible to being broken by quantum algorithms like Shor's and Grover's, jeopardizing the confidentiality, authenticity, and integrity of transactions across financial networks. This study presents a comprehensive investigation into the design, feasibility, and architecture of a universal quantum-safe payment platform capable of processing all types of digital transactions, ranging from mobile money and bank transfers to blockchain-based and card payments through existing delivery channels on a decentralized infrastructure. The research synthesizes current developments in post-quantum cryptography (PQC), including lattice-based, hash-based, and code-based algorithms, and evaluates their suitability for real-time financial systems. The proposed platform incorporates a permissioned distributed ledger, API-level compatibility with legacy financial protocols, and an identity-governed, modular architecture that enables cryptographic agility and policy compliance. Through architectural modeling and critical analysis, this research provides a forward-looking blueprint for building quantum-resilient financial infrastructure. It concludes that while performance and governance hurdles remain, quantum-safe payment networks are both technically feasible and urgently necessary. This work aims to equip stakeholders, especially fintech firms, banks, and regulatory bodies, with a detailed roadmap for transitioning to secure, interoperable, and scalable payment systems in the quantum era.

Keywords: Quantum computing, post-quantum cryptography, payment systems, blockchain, decentralized ledger, digital finance, cryptographic agility, lattice-based encryption, financial security, PQC

Introduction

Quantum computing brings a major change in how we process information. It can solve complex problems that current computers cannot. However, it also creates a serious threat to cybersecurity. Quantum computers can break public-key cryptographic systems used to protect financial data, digital identities, and secure communications. Today's digital payment systems, such as mobile wallets, banking APIs, and crypto networks, rely on RSA, elliptic curve cryptography (ECC), and similar methods. These systems are considered secure because current computers can't break them easily. But quantum algorithms like Shor's can quickly solve problems that these cryptosystems depend on. This makes most of today's encryption methods unsafe in the face of quantum attacks (Deloitte, 2020).

Motivation: The Quantum Threat

The integrity of financial systems rests upon the assumption that digital transactions cannot be forged, modified, or eavesdropped upon by malicious actors. However, quantum computing directly undermines this trust. If an adversary were to gain access to a scalable quantum computer, they could compromise not only the confidentiality of encrypted payment messages but also the authenticity of digital signatures used to authorize transfers, verify identities, and maintain distributed ledgers (Entrust, 2025). As early as 2022, government agencies and standards bodies began issuing warnings and mandates to prepare for a post-quantum era. The U.S. National Institute of Standards and Technology (NIST) initiated a six-year project to develop and standardize post-quantum cryptographic algorithms (NIST, 2022), while central banks and international consortia launched pilot initiatives to evaluate the impact of quantum-safe encryption on payment infrastructure (BIS, 2023a). The potential economic impact of failing to act is enormous: a compromise of high-value financial systems like RTGS networks or SWIFT could cause cascading losses and trust erosion in global finance (World Economic Forum, 2024).

Research Objectives

This research aims to explore and design a universal quantum-safe digital payment platform capable of processing all forms of digital transactions, ranging from mobile money to banking transfers and digital currencies, through existing delivery channels within a decentralized architecture. The objectives include:

- Analyzing the quantum computing threat to existing cryptographic systems used in payments;
- Reviewing and comparing post-quantum cryptographic algorithms suitable for financial applications;
- Assessing industry pilots and regulatory frameworks addressing the quantum threat;
- Proposing a multi-layered, quantum-resilient architecture integrating decentralized ledger technology (DLT);
- Identifying the technical and regulatory challenges of transitioning to quantum-safe systems.
- Demonstrating a use case of a real-time cross-border payment conducted on a quantum-resistant network.

These objectives collectively support the strategic goal of equipping stakeholders in the financial and cybersecurity sectors with the frameworks and tools necessary to future-proof digital payments in a quantum-disrupted world.

Scope and Relevance

The scope of this study is centered on digital payment systems and the cryptographic mechanisms they employ. It encompasses peer-to-peer transactions, retail payments, card-based authentication, interbank settlement mechanisms, and emerging platforms such as central bank digital currencies (CBDCs) and blockchain networks. While the focus is technical, regulatory and economic considerations are also included due to their role in enabling or constraining technological adoption. This research does not cover other quantum-secure fields like secure multi-party computation or post-quantum authentication tokens, except where directly relevant to financial transactions. Given the predicted timeline for quantum computer development estimated at 8 to 15 years to threaten RSA-2048 and ECC (Utimaco, 2024), the relevance of preemptive preparation cannot be overstated. Institutions that fail to begin migration efforts today may find themselves vulnerable in the near future, especially considering the “Harvest Now, Decrypt Later” model, where intercepted data today could be decrypted post facto using future quantum resources (NACHA, 2024).

Methodological Approach

This research employs an applied analytical method, leveraging a synthesis of scholarly literature, standards documents, pilot project results, and technical specifications to design a viable architecture. A case study analysis of BIS's Project Tourbillon and related initiatives is used to ground theoretical proposals in practical insights. Architectural models are evaluated based on criteria such as cryptographic robustness, integration feasibility with existing systems, and compliance with regulatory mandates. The design framework is conceptualized in modular layers to reflect modern financial infrastructure while allowing cryptographic agility and protocol upgrades. The approach further incorporates a security-by-design principle, ensuring that post-quantum protections are embedded into every transaction stage from API calls and identity verification to consensus mechanisms and ledger storage.

Literature Review

As the specter of quantum computing grows nearer, an increasing body of research is being produced to understand its potential impact on digital infrastructures. For the payments sector, where trust, speed, and cryptographic integrity are non-negotiable, this literature reveals deep vulnerabilities and urgent paths toward post-quantum resilience. In this section, we examine (1) the foundational cryptographic systems at risk, (2) the mechanics of quantum algorithms and their effect on digital security, (3) the families of post-quantum cryptographic (PQC) algorithms, (4) comparative performance analysis for financial applications, and (5) existing industry and government-led initiatives aimed at mitigating these threats.

Cryptographic Foundations at Risk

Modern payment networks, whether online banking, card authorization, or blockchain-based platform,s are underpinned by public-key cryptography. Schemes such as RSA and elliptic curve cryptography (ECC) enable secure key exchanges, digital signatures, and message confidentiality. Their security relies on mathematical problems like integer factorization (RSA) and the discrete logarithm problem (ECC), which are computationally infeasible to solve using classical computers. However, these foundational assumptions collapse under quantum computation (Deloitte Insights, 2020). A major risk arises from the fact that most TLS (Transport Layer Security) connections, including those used by banks and fintech APIs, rely on RSA/ECDSA for handshake and authentication. If these keys are compromised by a quantum attacker, even encrypted sessions could be decrypted retroactively. Similarly, digital signature schemes used in blockchain transactions (e.g., ECDSA in Bitcoin) become forgeable once the public key is exposed on-chain, potentially leading to asset theft (Scientific Reports, 2023).

Quantum Algorithms and Their Impact

Two primary quantum algorithms directly threaten current cryptographic protocols:

- Shor's algorithm enables efficient factorization of integers and computation of discrete logarithms, breaking RSA, DSA, and ECC (Shor, 1994).
- Grover's Algorithm accelerates brute-force attacks on symmetric key systems, effectively halving their security level (Grover, 1996).

Shor's algorithm is especially dangerous, as it can retroactively compromise encrypted traffic or signed transactions once a quantum computer becomes capable of handling sufficient qubits. This underpins the urgency of preparing for what many researchers term Q-Day, the point at which cryptographic protections fail at scale (NACHA, 2024).

Families of Post-Quantum Cryptographic Algorithms

In response to these risks, the cryptographic community has developed several families of PQC algorithms. These are based on hard mathematical problems believed to resist quantum attacks:

- Lattice-based Cryptography (e.g., Kyber, Dilithium, Falcon): Relies on the hardness of lattice problems like Learning With Errors (LWE). Efficient and versatile, NIST selected Kyber (encryption) and Dilithium (digital signatures) as primary standards (NIST, 2022).
- Hash-based Signatures (e.g., SPHINCS+): Build secure signature schemes from cryptographic hash functions. Offers strong security guarantees but larger signatures (Utimaco, 2024).
- Code-based Cryptography (e.g., McEliece): Uses error-correcting codes; well-studied but suffers from large public key sizes.
- Multivariate Quadratic Systems (e.g., Rainbow): Once promising, but several schemes have been broken or retired from consideration (Utimaco, 2024).
- Isogeny-based Cryptography (e.g., SIKE): Originally favored for small key sizes, but recently compromised by classical cryptanalysis (Castryck et al., 2022).

Each family has trade-offs in terms of key size, computational efficiency, and deployment feasibility. NIST's current standards prioritize lattice-based and hash-based solutions due to their maturity and performance profiles (NIST, 2024) (Castiglione, Esposito, & Loia, 2024).

Comparative Analysis of PQC for Payments

Digital payment platforms require cryptographic algorithms that are not only quantum-safe but also fast, scalable, and compatible with constrained environments like smart cards and mobile apps. Among NIST's selections:

- Kyber is optimal for key encapsulation in TLS and VPNs due to small ciphertexts and fast computation.
- Dilithium offers strong digital signature performance, with moderate key and signature sizes (~2.5 KB), suitable for transaction signing.
- Falcon produces much smaller signatures (~0.5 KB) than Dilithium, but requires floating-point operations and a more complex implementation.
- SPHINCS+ has large signature sizes (10–40 KB) and slower signing, which limits its use in high-throughput payments but makes it a good fallback for certificate systems.

Code-based and multivariate schemes remain niche due to their inefficiencies or security setbacks. Table 1 summarizes the main characteristics of these algorithms for payment use cases.

Table 1: Summary Comparison of PQC Algorithms for Payment Applications

Algorithm	Type	Key Size	Signature Size	Speed (sign/verify)	Suitability
Kyber	Lattice	~1 KB	~1 KB	Fast	High
Dilithium	Lattice	~1.3 KB	~2.5 KB	Fast	High
Falcon	Lattice	~1 KB	~0.5 KB	Medium	Moderate
SPHINCS+	Hash	~32 KB	~20 KB	Slow	Backup
McEliece	Code	~200 KB	N/A	Medium	Limited

Industry and Government Initiatives

Several pilot projects and government directives are already paving the way for quantum-safe payments:

- BIS Project Leap (2023) tested hybrid classical/post-quantum encrypted communications between central banks using Kyber and Dilithium, demonstrating secure real-world payment message transmission (BIS, 2023a).
- Project Tourbillon implemented privacy-preserving, lattice-based blind signatures in a retail CBDC pilot, showing that anonymity and quantum safety can coexist, albeit with a 5× increase in latency and 200× drop in throughput (BIS, 2023b).

- Banco Sabadell conducted a practical migration assessment of cryptographic systems in partnership with Accenture, finding that crypto-agility middleware can enable PQC adoption without replacing legacy infrastructure (Accenture, 2024).
- FS-ISAC and G7 Cyber Experts Group have called for an immediate inventory of cryptographic assets and the development of PQC migration plans in financial institutions (FS-ISAC, 2024; G7, 2024).
- The Quantum-Resistant Ledger (QRL) has run a hash-based quantum-safe blockchain since 2018, illustrating that full-stack PQC in value transfer systems is viable, even if limited in throughput (QRL, 2024).

These efforts form a growing consensus: the quantum threat is real, and a proactive, phased transition to PQC is the only viable response. They also validate that integration is possible even in high-complexity financial networks.

Methodology

This research employs a multi-pronged analytical methodology to design and validate a universal quantum-safe payment platform. Given the interdisciplinary nature of the problem spanning cryptography, distributed systems, financial architecture, and regulatory policy, our approach integrates structured literature synthesis, case study evaluation, conceptual modeling, and feasibility assessment grounded in real-world constraints. The methodology is framed to address not only theoretical robustness but also practical deployment considerations.

Research Design (Applied Analytical Method)

The central research method is an applied analytical framework that synthesizes cryptographic, architectural, and economic insights from recent scholarly and institutional studies. We begin with a comprehensive literature review of existing quantum risks and post-quantum cryptographic standards. From this, we derive the criteria for quantum-resilient payment platforms encompassing key attributes such as cryptographic agility, scalability, interoperability, latency, and compliance. The study focuses on conceptual design, where the architecture of the proposed platform is developed layer by layer, integrating technical, operational, and governance components. Each element is evaluated for quantum resilience and interoperability with legacy financial systems. By structuring the research into functional modules (e.g., cryptographic services layer, API integration, DLT core), the platform can be analyzed and validated component-wise and as a holistic system.

Case Study Analysis (e.g., BIS Project Tourbillon)

To ground this research in practical application, we incorporate case study analysis of recent quantum-safe payment trials, especially from high-trust institutions such as the Bank for International Settlements (BIS) and central banks participating in its innovation hub. Of particular relevance are:

- Project Leap (2023): A cross-border experiment between Banque de France and Deutsche Bundesbank that evaluated hybrid encryption of payment messages using Kyber and Dilithium. This study serves as evidence of feasibility in a regulated environment with legacy infrastructure (BIS, 2023a).
- Project Tourbillon (2023): A retail CBDC initiative focused on maintaining payer anonymity while implementing lattice-based blind signatures. This case study is critical for understanding PQC's performance and privacy trade-offs in real-time retail use (BIS, 2023b).
- Banco Sabadell PQC Pilot (2024): A commercial case demonstrating how legacy banking infrastructure can transition to PQC using middleware, without wholesale architectural changes. It informs our integration and migration strategies (Accenture, 2024).

Insights from these case studies shape our technical design and risk mitigation strategies. They also validate certain assumptions about latency, throughput, and regulatory viability.

Architectural Modeling and Simulation Review

The proposed architecture of the quantum-safe platform is modeled conceptually using modular systems engineering principles. Each subsystem cryptographic core, ledger design, API gateway, smart contract logic, and identity management, is mapped with specific cryptographic dependencies and performance expectations. Simulated transaction flows are analyzed to understand latency impacts, signature size propagation, and validator workload. For example, PQC signature sizes (e.g., 2–3 KB for Dilithium) are evaluated in the context of network bandwidth, block size, and storage overhead. Latency benchmarks from BIS Tourbillon are used to forecast system responsiveness and guide performance optimizations.

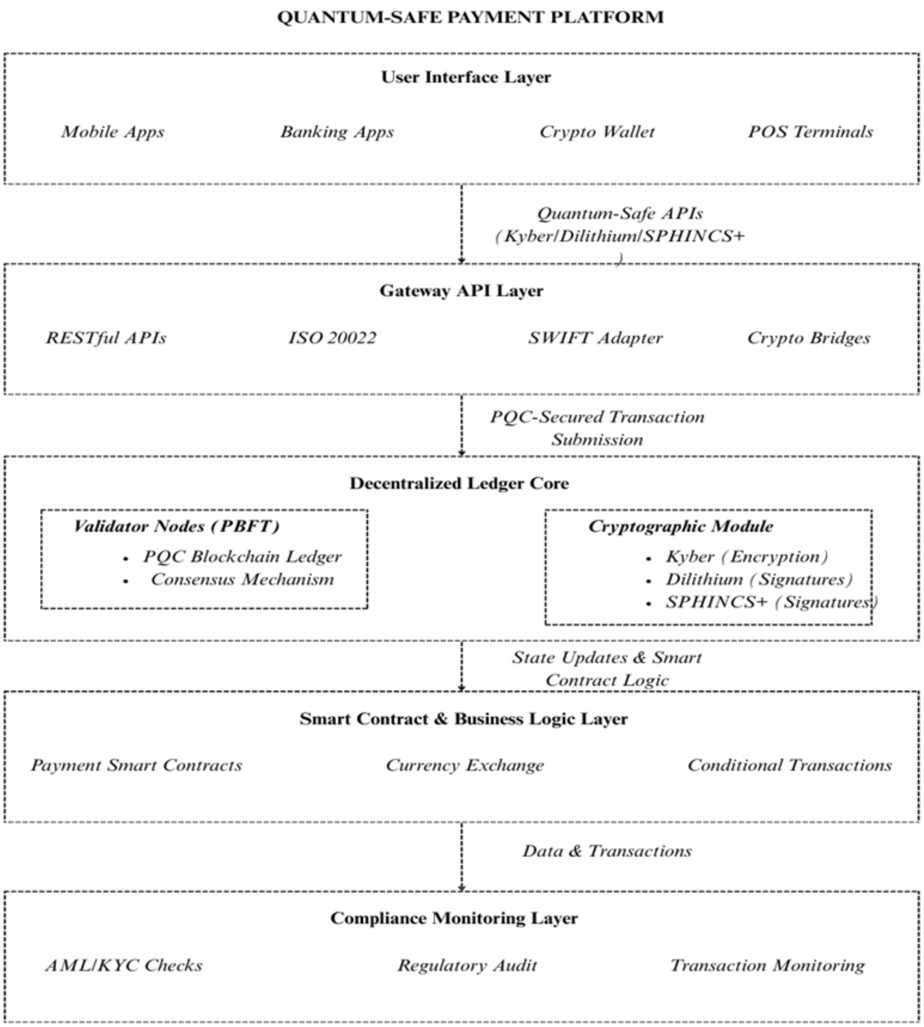

Figure: Conceptual Architecture of the Quantum-Safe Payment Platform

We plan a data flow analysis to visualize how a typical payment (e.g., mobile money to bank account) traverses the system and how PQC is applied at each point: key exchange, signature validation, transaction finality, and audit trail confirmation.

The proposed infrastructure for quantum-safe cross-border remittance leverages a multilayered, decentralized platform architecture, emphasizing robust security through post-quantum cryptography (PQC). It incorporates specialized layers starting from the user interface—such as mobile money apps and banking applications—down through secure gateway APIs and into a decentralized ledger core utilizing advanced PQC algorithms, including Kyber, Dilithium, and SPHINCS+. This decentralized core integrates cryptographic modules and smart contracts to execute transactions securely, while a dedicated compliance monitoring layer ensures strict adherence to AML and KYC regulatory standards. Such infrastructure is strategically designed to mitigate quantum-computing threats, maintaining transaction security and trustworthiness in a post-classical cryptographic environment (Nwaga & Idima, 2024).

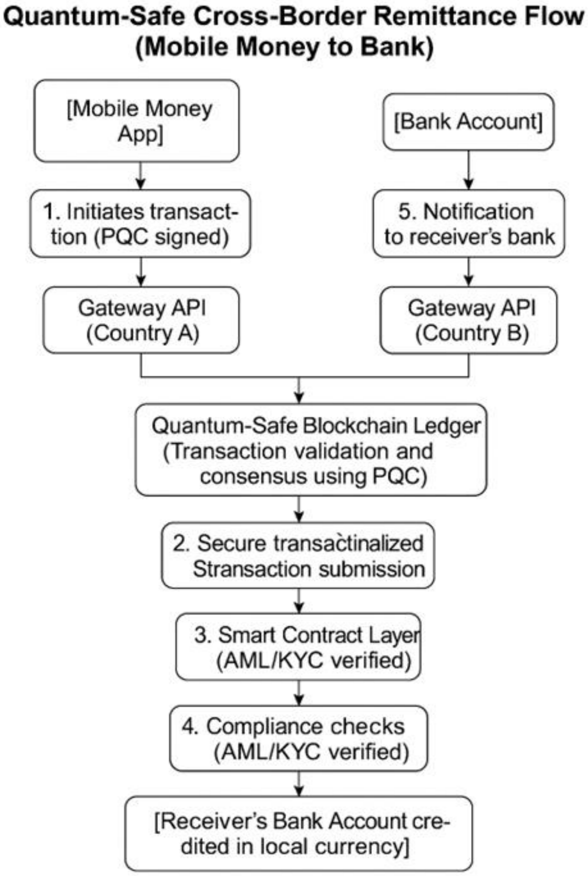
Quantum-Safe Cross-Border Remittance Flow
(Mobile Money to Bank)
[Mobile Money App]
1. Initiates transact-tion (PQC signed)
Gateway API (Country A)
[Bank Account]
5. Notification to receiver's bank
Gateway API (Country B)
Quantum-Safe Blockchain Ledger (Transaction validation and consensus using PQC)
2. Secure transactinalized Stransaction submission
3. Smart Contract Layer (AML/KYC verified)
4. Compliance checks (AML/KYC verified)
[Receiver's Bank Account cre-dited in local currency]

Figure: Conceptual Architecture of the Quantum-Safe Cross-Border Remittance Flow (Mobile Money to Bank)

This illustrates a practical application of this infrastructure in a quantum-safe cross-border remittance scenario, originating from a mobile money account in the sender’s country and concluding with credit to a bank account in the receiver’s country. The diagram visually details each transaction step, beginning from the initiation of a PQC-secured request at the sender's mobile interface. This transaction securely traverses the gateway API and is validated by the quantum-safe decentralized ledger. Post-validation, smart contracts facilitate foreign exchange conversions and enforce business logic rules. Compliance modules subsequently perform critical AML/KYC checks, ensuring regulatory compliance. Finally, the verified transaction is securely communicated to the receiving bank through APIs, resulting in successful crediting of funds in local currency, thus demonstrating the secure, efficient, and compliant cross-border financial transaction in a quantum-threatened future.

Limitations and Scope Control

Several limitations are inherent in this research:

- Lack of empirical hardware benchmarking: While this paper draws on published pilot data and simulations, it does not conduct real-world PQC deployment due to resource and infrastructure constraints.
- Evolving standards: NIST PQC standards are still maturing. This paper focuses on first-generation algorithms (Kyber, Dilithium, SPHINCS+), acknowledging that new schemes may emerge post-publication (NIST, 2024).
- Jurisdictional variance: Regulatory requirements differ across countries. This study assumes a generalizable regulatory framework aligned with global standards (e.g., FATF, ISO 20022, PSD2) but does not delve into localized compliance laws.
- Selective focus: This work concentrates on quantum threats to payment systems, not broader sectors such as identity management, quantum-resistant messaging, or hardware-based quantum security (e.g., quantum key distribution), except where payment-relevant.

Despite these limitations, the research provides a thorough conceptual foundation and operational roadmap for building a quantum-resilient digital payment network. The layered methodology ensures that each element from cryptographic protocol selection to legacy integration is critically analyzed and contextually grounded.

Quantum Threats in Digital Payment Systems

The advent of quantum computing represents a paradigm shift with far-reaching consequences across digital infrastructures, and the payment ecosystem stands as one of its most vulnerable sectors. Payments, by their nature, involve the exchange of value, sensitive information, and irrevocable commitments, factors that demand cryptographic certainty. Most of the cryptographic primitives currently securing these operations were not designed with quantum capabilities in mind. As such, the emergence of cryptographically relevant quantum computers introduces a multifaceted threat to the digital payment infrastructure (Turpu, 2024).

Vulnerabilities in TLS, Blockchain, and Banking APIs

The most immediate threat from quantum computing lies in its ability to undermine the foundational public-key cryptography (PKC) used in securing communication channels and digital identities. Transport Layer Security (TLS), the backbone of secure communication over the internet, typically uses RSA or elliptic-curve Diffie–Hellman (ECDH) for key exchange and authentication (Mansoor, Afzal, Iqbal, & Abbas, 2025). In the context of banking APIs and fintech integrations, TLS ensures the confidentiality and authenticity of transmitted data (Das, 2025). However, once quantum computers can efficiently run Shor's algorithm, they can break RSA and ECC by factoring or computing discrete logarithms exponentially faster than classical machines (Shor, 1994). This would allow an adversary to decrypt past recorded TLS sessions and impersonate legitimate financial institutions. Blockchain systems are equally vulnerable. For instance, cryptocurrencies like Bitcoin use the ECDSA signature scheme (Weinberg, Petratos, & Faccia, 2024). Once a public key is revealed, such as when a transaction is made, a quantum-capable adversary could derive the corresponding private key and steal funds. The security assumption behind ECDSA is completely broken in a post-quantum context (Deloitte Insights, 2020). Moreover, blockchain consensus mechanisms that rely on cryptographic signatures (e.g., validator authentication in proof-of-stake systems) could also be compromised, leading to governance failures and double-spending attacks. Banking APIs, mobile wallets, and cloud-based financial services typically rely on digital certificates (issued under PKI systems) to authenticate users and services. These certificates, again, use RSA or ECC-based keys (Agrawal, 2024). Once these keys are vulnerable, attackers can forge certificates, impersonate service providers, and intercept or alter financial transactions (NACHA, 2024). This opens the door not only to financial theft but to large-scale systemic disruption of trust in payment networks.

The "Harvest Now, Decrypt Later" Model

Even before quantum computers become practically usable, there exists a credible and pressing threat in the form of the "Harvest Now, Decrypt Later" (HNDL) attack model. In this model, malicious actors today can intercept and store encrypted payment data, be it TLS-secure API traffic, encrypted financial messages, or blockchain transaction records with the intention of decrypting it in the future once quantum capabilities mature. This threat model is particularly concerning for financial institutions because many types of financial data have long lifespans. For example, banking records, account information, and transaction logs may need to be kept secure and confidential for decades. A breach in the future, even if the data was captured years earlier, could expose historical financial behavior, account details, and personally identifiable information (PII). Institutions that have not adopted quantum-safe encryption would be unable to retroactively protect such data (BIS, 2023a). Moreover, the widespread reuse of keys such as static server keys for TLS or certificate-based identities further exacerbates the problem. If even one long-lived key is compromised, all past messages encrypted under it become vulnerable. This presents an existential risk to regulatory frameworks like the Payment Card Industry Data Security Standard (PCI-DSS) and GDPR, which mandate stringent protection of user data (NACHA, 2024).

Socioeconomic Impact of Inaction

Failing to act on the quantum threat could have dire socioeconomic consequences. At the systemic level, the breakdown of trust in financial transactions could lead to a loss of faith in digital commerce, banking platforms, and payment systems. Imagine a scenario where attackers forge digital signatures on interbank payment instructions. The results could include unauthorized fund transfers, cascading defaults due to mistrusted settlement instructions, and liquidity crises in clearing systems. Studies suggest that a successful quantum attack on high-value payment systems like the U.S. Federal Reserve’s Fedwire could cause economic contractions of over 10% of GDP due to the loss of transactional trust (World Economic Forum, 2024). In retail scenarios, the compromise of consumer-facing applications such as mobile wallets or contactless cards would erode confidence in digital payments and could drive regression to cash-based economies. This would disproportionately affect regions where digital inclusion has only recently been achieved.

In global trade, quantum threats could disrupt supply chains by targeting financial messages exchanged over SWIFT or ISO 20022 standards. A compromised SWIFT infrastructure, even for a short duration, would paralyze international payments and settlements. Furthermore, if adversarial nation-states or state-sponsored entities develop a quantum advantage first, it could lead to geopolitical imbalances in financial power and economic security. The reputational damage to institutions that fall victim to quantum-era breaches would be severe, both in customer trust and regulatory penalties. Legal liability, class-action lawsuits, and heightened scrutiny from financial regulators would follow. Hence, preparing for quantum threats is not just a technical necessity but a strategic imperative for long-term financial stability. The threats posed by quantum computing to digital payments are systemic, far-reaching, and imminent. From protocol-level vulnerabilities to long-term data privacy breaches, quantum capabilities challenge the very assumptions that secure modern financial ecosystems. Organizations must adopt a forward-looking stance, transitioning to quantum-safe cryptography, auditing cryptographic assets, and establishing governance frameworks that anticipate the next cryptographic revolution. As the literature and pilot studies clearly show, the time to act is not when quantum computers arrive, but now during the preparation window that remains open.

Post-Quantum Cryptographic Solutions

The emerging threat landscape shaped by quantum computing has necessitated a re-evaluation of cryptographic foundations across the digital ecosystem. In response, the cryptographic community, supported by standardization bodies such as the National Institute of Standards and Technology (NIST), has developed a set of post-quantum cryptographic (PQC) algorithms designed to resist known quantum attacks. These algorithms are not merely theoretical constructs; they are practical tools currently being standardized, implemented, and piloted across payment networks, with a growing body of research and trials validating their feasibility. This section explores the major families of PQC algorithms with specific attention to their applicability in real-time, high-volume financial environments. Each family is assessed in terms of security assumptions, performance metrics (key size, signature size, computational cost), maturity, and integration potential in payment platforms.

Lattice-Based Cryptography

Lattice-based cryptography has emerged as the most promising family of quantum-resistant algorithms for both encryption and digital signatures. These algorithms derive their security from hard problems in high-dimensional lattices, such as the Learning With Errors (LWE) or Shortest Vector Problem (SVP), which remain hard even in the presence of quantum adversaries (Alkim et al., 2016).

NIST’s primary selections for its PQC standardization process were lattice-based:

CRYSTALS-Kyber for encryption and key encapsulation
CRYSTALS-Dilithium and FALCON for digital signatures

These algorithms offer a favorable balance between performance and security. Kyber, for example, enables secure key exchange with compact keys (~1 KB) and ciphertexts and is fast enough to support TLS handshakes in payment APIs. Similarly, Dilithium produces moderate-sized signatures (~2.7 KB) and public keys (~1.3 KB) while avoiding complex floating-point operations, making it easier to implement in constrained environments (NIST, 2024). FALCON offers even smaller signatures (~0.8 KB) but requires more complex implementations and hardware floating-point support.

In real-world financial scenarios, lattice-based schemes are well-suited to:

Signing interbank transactions and instructions
Authenticating user identities and wallet keys
Securing API communications between payment gateways and processors
Enabling secure key exchange in TLS and VPNs for data in transit

The financial sector has begun piloting lattice-based solutions. For instance, the BIS Tourbillon project implemented lattice-based blind signatures for CBDC payments with privacy features (BIS, 2023b). While the project noted increased latency and reduced throughput (5× slower processing and 200× drop in TPS), ongoing optimizations and hardware acceleration are expected to mitigate these issues over time.

Hash-Based and Code-Based Cryptography

Hash-based cryptography is another mature and well-understood approach. These schemes rely on the pre-image resistance of secure hash function primitives believed to withstand quantum attacks, barring Grover's algorithm ,which only provides a quadratic speedup. NIST selected SPHINCS+, a stateless hash-based digital signature scheme, as an alternative standard (Hülsing et al., 2020). While hash-based signatures are theoretically robust and straightforward to analyze, their practical deployment faces challenges:

Large signature sizes (10–40 KB)
Slower signing operations compared to lattice schemes

In payment systems, hash-based signatures are best suited for applications where long-term integrity and robustness are paramount, and where signature size is less of a constraint. For instance:

Signing critical software updates for payment hardware
Issuing root certificates in a quantum-safe public key infrastructure (PKI)
Authenticating interbank messages where bandwidth is ample

Code-based cryptography, epitomized by the Classic McEliece scheme, offers extremely conservative security. McEliece has withstood decades of cryptanalysis and is resistant to both classical and quantum attacks. Its primary drawback lies in its massive public key sizes (up to hundreds of kilobytes), which makes it ill-suited for high-frequency transactions or resource-constrained devices (Bernstein et al., 2008).

Nonetheless, in payment infrastructures, code-based schemes can be viable for:

Encrypting bulk archival data
Root key storage in high-security modules
Specialized one-time communication (e.g., initial device onboarding)

Isogeny- and Multivariate-Based Cryptography

Isogeny-based and multivariate quadratic equation-based cryptography were initially promising avenues for PQC due to their compact key sizes and fast operations. However, both families have suffered major cryptanalytic setbacks in recent years. For example, the SIKE (Supersingular Isogeny Key Encapsulation) scheme was completely broken in 2022 by a classical attack, undermining its assumed hardness (Castryck & Decru, 2022). Similarly, Rainbow, a leading multivariate signature scheme, was broken in practice shortly before NIST was to standardize it. These collapses have severely limited the deployability of these algorithm families in mission-critical applications like payments. Given the current state of cryptanalysis, isogeny- and multivariate-based schemes are not recommended for production deployments in payment platforms. However, academic research continues, and future iterations may address existing vulnerabilities.

Hybrid Schemes for the Transition Period

A practical challenge in migrating to PQC is ensuring backward compatibility with existing systems and preserving security during the transition. To this end, hybrid cryptographic schemes are recommended. These schemes combine classical and quantum-safe algorithms in a single transaction or session. For example:

Dual TLS key exchange using both ECDHE and Kyber
Transactions signed with both ECDSA and Dilithium (dual signature fields)

This ensures that data remains secure as long as one of the two algorithms remains unbroken. Hybrid schemes are already being tested in protocols like TLS 1.3 (Open Quantum Safe Project) and are particularly useful for:

Protecting data-in-transit against HNDL threats
Allowing phased migration of systems and devices
Gaining regulatory and institutional confidence in PQC deployment

Institutions such as JPMorgan and Banco Sabadell have already piloted hybrid deployments, illustrating the feasibility of dual-crypto architectures in complex financial networks (Accenture, 2024; JPMorgan, 2022). In conclusion, post-quantum cryptographic solutions offer a comprehensive set of tools to secure payment systems in the face of quantum adversaries. Lattice-based algorithms provide a balance of efficiency and security suitable for most payment operations. Hash- and code-based schemes offer specialized robustness for archival or infrequent use cases. While isogeny and multivariate cryptosystems have yet to reach production readiness, the combination of lattice and hash-based methods, coupled with hybrid strategies, enables immediate transition paths. Financial institutions should begin deploying PQC in critical systems, prioritize cryptographic agility, and participate in standards alignment to future-proof digital payments in the quantum era.

Proposed Quantum-Safe Payment Platform Architecture

In response to the growing risks posed by quantum computing and the urgent need for cryptographic agility, this section introduces a comprehensive architecture for a universal quantum-safe payment platform. The platform is designed to process all forms of digital payments, including mobile wallets, bank transfers, cards, and cryptocurrencies via existing delivery channels, while embedding quantum-resistant cryptographic primitives at every layer (Agrawal, 2024). The architectural model leverages decentralized technologies, modular design, and industry-compliant interfaces to ensure both forward compatibility and practical deployment feasibility.

Platform Objectives and Design Principles

The primary objective of the proposed platform is to establish a secure, interoperable, and scalable payment infrastructure that resists quantum-era threats while maintaining the flexibility to integrate with legacy financial systems. To meet this goal, the architecture adheres to the following key principles:

- Quantum Resilience: All cryptographic operations, including digital signatures, key exchanges, and identity validation, must employ post-quantum cryptographic algorithms approved or recommended by international standardization bodies like NIST.
- Decentralization and Redundancy: To avoid single points of failure and centralized vulnerabilities, the platform uses permissioned distributed ledger technology (DLT) operated by a consortium of trusted entities (e.g., banks, fintechs, central banks).
- Legacy Compatibility: The architecture must allow seamless integration with existing systems (e.g., ISO 20022 messaging, REST APIs, SWIFT), enabling a smooth transition for institutions and end-users.
- Cryptographic Agility: To allow future upgrades, the system must support pluggable cryptographic primitives, with metadata indicating the algorithms in use for each transaction or communication.

- User Transparency: While underlying cryptographic protocols will evolve, the user-facing experience (e.g., mobile payments, bank transfers) must remain intuitive and consistent.

Functional Layers: From API to Ledger Core

The architecture is structured into distinct functional layers, each responsible for a specific aspect of the system's operations.

User and Channel Integration Layer

This layer interfaces with external payment systems and user applications. It includes:

Mobile banking apps
E-commerce payment gateways
Point-of-sale systems
Internet banking portals
Cryptocurrency wallets

These endpoints communicate with the platform via standardized APIs. Crucially, these channels are protected using quantum-safe TLS (e.g., Kyber for key exchange, Dilithium for mutual authentication).

API and Gateway Layer

To ensure backward compatibility, the API and gateway layer performs protocol translation and message formatting. It supports:

ISO 20022 (PACS, CAMT) for banks
RESTful or gRPC APIs for fintechs
EMV/NFC interface translation for card processors

Each message is authenticated and secured using a combination of post-quantum digital signatures and symmetric encryption. A digital signature using CRYSTALS-Dilithium or FALCON confirms authenticity, while AES-256-GCM ensures confidentiality (Utimaco, 2024).

Distributed Ledger Core

The ledger core serves as the transaction recording and consensus layer. It is a permissioned blockchain with the following attributes:

- Validator nodes run by consortium members (banks, central banks, regulated fintechs)
- PBFT or HotStuff consensus, with validator messages signed using PQC
- Account-based or UTXO-based model, depending on implementation preference

Each transaction is signed using PQ digital signatures. Blocks include Merkle trees hashed with quantum-safe functions like SHA-384 or SHA3-512. Validator nodes authenticate one another using post-quantum certificates, possibly anchored in a decentralized identity framework.

Cryptographic Services Layer

This cross-cutting layer includes:

- Quantum-Safe Key Management: Key generation and storage using hardware security modules (HSMs) supporting PQC
- Public Key Infrastructure (PKI) or decentralized identity (DID) systems using SPHINCS+ or Dilithium for long-term certificates
- Multi-signature schemes and threshold signatures, allowing high-security operations (e.g., corporate approvals or interbank transfers)
- Hybrid signature engines, enabling dual-algorithm transactions during migration phases

Smart Contract and Application Layer

Where programmable logic is required (e.g., conditional payments, currency exchange, escrow), this layer supports smart contracts. These contracts must use PQC-aware cryptographic opcodes and can include:

PQ signature verification
Zero-knowledge proofs (e.g., PQ-secure zk-SNARKs for privacy)
Atomic swaps with hash-locking using quantum-safe hashes

The platform may provide precompiled contracts or native opcodes for PQC operations to reduce gas and latency costs.

Cryptographic Services and Key Management

Key management is central to quantum-safe infrastructure. The platform introduces a quantum-safe key lifecycle involving:

- Key provisioning: Devices (e.g., mobile apps, ATMs) receive keys from certified PQC-enabled CAs or issuers.
- Key rotation policies: Avoiding excessive reuse of signatures by rotating keys regularly (especially relevant for lattice and hash-based schemes).
- Recovery and revocation: Compromised keys can be revoked using quantum-safe certificate revocation lists or ledger-anchored proofs.

Where possible, multi-algorithm agility is built in. For example, a transaction format may include an algo_type field, specifying the signature algorithm used. This allows validators and clients to interpret and verify transactions under varying algorithm choices.

Smart Contracts and Payment Applications

Smart contracts extend the platform's capability to support complex payment scenarios, such as:

- Cross-border remittance logic
- Escrow or dispute resolution
- FX conversions using oracle feeds
- Compliance checks embedded into transaction logic

Contracts can verify PQC digital signatures, compute Merkle proofs, and validate zero-knowledge claims for privacy. Additionally, smart contracts may be used for programmable compliance, for example, preventing a transaction above a certain value unless approved by multiple signatories (multi-sig logic based on Dilithium threshold schemes).

The architecture ensures that smart contracts are extensible, formally verifiable, and sandboxed to prevent attacks, especially important in the financial context where logic bugs could have monetary consequences.

Table 1: Comparative Analysis of PQC Schemes for Platform Layers

Platform Layer	Recommended PQC Algorithm(s)	Key Advantages	Potential Limitations	Ideal Use-Cases
User Interface Layer	Dilithium, Falcon	Efficient digital signatures, moderate sizes	Slightly higher computational overhead	Mobile wallets, POS terminals, web apps
Gateway API Layer	Kyber, Dilithium	Fast encryption and signature verification	Increased message sizes	Secure API requests, session encryption
Decentralized Ledger Core	Dilithium, SPHINCS+	Robust long-term security, widely vetted	Larger signatures (SPHINCS+)	Blockchain consensus, transaction signing
Cryptographic Module	Kyber, Dilithium, SPHINCS+	Algorithm diversity, cryptographic agility	Complexity managing multiple schemes	Key management, PKI infrastructure
Smart Contract Layer	Dilithium, Falcon	Rapid verification, lower signature sizes (Falcon)	Implementation complexity (Falcon)	Payment logic, conditional transactions
Compliance Monitoring Layer	SPHINCS+, Dilithium	Highly secure, long-term quantum resistance	Signature size overhead	Regulatory audits, AML/KYC verification

Decentralized Ledger Integration

The core of a universal quantum-safe payment platform lies in its ledger infrastructure. A decentralized ledger offers a unified, tamper-resistant, and continuously available substrate for payment processing that minimizes reliance on central intermediaries. In this section, we explore the integration of decentralized ledger technology (DLT) with quantum-safe cryptographic primitives to ensure a robust and scalable foundation for next-generation payments.

PQC-Enabled Blockchain Model

The integration begins by replacing classical cryptographic primitives used in existing blockchains, primarily RSA and ECDS,A with post-quantum cryptographic (PQC) algorithms. Given the existential vulnerabilities of public key cryptography in a post-quantum world (Deloitte, 2020), this transition is foundational.

A permissioned blockchain architecture is preferred due to its ability to enforce performance, governance, and compliance guarantees while retaining decentralization through consortium governance (BIS, 2023a). The blockchain operates with:

- Dilithium/Falcon-based signature schemes for signing transactions and validator messages
- Kyber or hybrid key exchanges for node-to-node encrypted communication
- SHA-3-384 or SHA-512 for hashing block contents and building Merkle trees
- SPHINCS+ for long-term identity credentials or certification anchors

Unlike public blockchains like Ethereum or Bitcoin, which still rely on ECDSA and SHA-256, the proposed system avoids exposing public keys until necessary and ensures that even old transactions cannot be retroactively forged or decrypted.

Each transaction submitted to the blockchain must be:

- Digitally signed using a PQ signature algorithm (e.g., Dilithium3 for general use, Falcon for low-bandwidth contexts)
- Accompanied by metadata indicating the algorithm used, its version, and a reference to the user’s post-quantum public key

Validators, upon receiving transactions, verify signatures using standardized PQC libraries, apply application-specific logic (e.g., balance checks, authorization), and participate in consensus voting, all secured by PQ signatures.

Consensus Mechanisms and Signature Verification

Consensus is the backbone of ledger trust. For a high-throughput, low-latency payment system, Byzantine Fault Tolerant (BFT) protocols are ideal. Protocols like Practical Byzantine Fault Tolerance (PBFT) or HotStuff are widely adopted in financial-grade DLTs due to their deterministic finality and bounded communication complexity.

Each round of consensus involves:

- A leader proposing a block
- Other nodes verifying transactions and voting via PQ signatures
- Aggregation of at least 2/3 validator approvals before finalizing a block

These messages are signed using PQ signature schemes (e.g., Dilithium), which, while heavier than ECDSA, are manageable in networks with limited validator counts (typically <100). The additional CPU and network overhead can be mitigated by:

- Signature batching and pipelining
- Use of GPU/FPGAs for PQC operations
- Selective fast paths for low-value or internal transactions

For instance, Tourbillon, a BIS pilot, successfully used a lattice-based signature system in a permissioned blockchain setting, despite latency and throughput hits (BIS, 2023b). Engineering solutions such as signature aggregation (where possible) and parallel verification can improve these metrics significantly.

Interoperability and Bridging to Legacy Systems

True payment ubiquity requires seamless interoperability with existing financial infrastructure. This includes:

- SWIFT messages (ISO 20022 and legacy MT)
- National ACH and RTGS systems
- Mobile money operators using proprietary APIs or telecom integrations
- Card networks (EMVCo and PCI DSS systems)
- Public blockchains (e.g., Bitcoin, Ethereum)

The platform implements interoperability gateways, which:

- Receive classical cryptographically signed messages from legacy systems
- Authenticate them using existing mechanisms (e.g., TLS + JWT or OAuth2 tokens)
- Re-sign or wrap the transactions using PQC before ledger inclusion

- Translate response data back to legacy formats (e.g., ISO 20022 PACS.008 to bank system)

During the transition phase, the system may also support dual-signature transactions, whereby legacy and PQ signatures are both required for validation. This protects against “harvest-now, decrypt-later” attacks during early adoption (NACHA, 2024).

In cross-chain contexts, atomic swaps using hash-locks and bridging contracts can allow tokenized representations of external assets (e.g., wrapped BTC, or synthetic fiat tokens) to exist within the platform, all secured with PQ signatures.

Governance and Identity Systems

Governance is vital for maintaining trust and ensuring regulatory compliance in decentralized infrastructures. The platform proposes a hybrid governance model, combining:

- A consortium council composed of major financial stakeholders (central banks, PSPs, card schemes)
- A technical advisory board responsible for cryptographic standards and software updates
- A compliance panel to audit protocol adherence and respond to legal inquiries

Each participant, whether a user, node, or institution has a unique quantum-safe digital identity, managed via:

- A post-quantum PKI system for certificate-based authentication
- A Decentralized Identity (DID) layer using blockchain-resident identity mappings
- Role-based permissions and transaction scopes (e.g., regulator nodes can observe but not write, PSP nodes can initiate payments, etc.)

The identity infrastructure ensures that all participants can:

- Prove their legitimacy cryptographically
- Revoke compromised credentials instantly
- Maintain pseudonymity when needed (e.g., for retail users), while still satisfying regulatory requirements such as Know Your Customer (KYC) or Anti-Money Laundering (AML) policies (FS-ISAC, 2024)

It is acknowledged that the platform focuses on software-defined solutions, while quantum computing itself is a fundamentally hardware-centric paradigm based on phenomena such as quantum entanglement, tunneling, and photon-based interactions. Nevertheless, post-quantum cryptography seeks to preempt quantum threats by designing algorithms secure even when attacked by hardware-capable quantum machines. PQC is a defensive software response to the prospective offensive capability of quantum hardware (Turpu, 2024; Das, 2025).

Implementation Challenges and Considerations

Developing and deploying a universal quantum-safe payment platform is not merely a cryptographic challenge but a multidisciplinary endeavor that intersects with system engineering, regulation, user experience, and infrastructure planning. This section outlines the key implementation challenges and provides insights into how each can be mitigated through architectural foresight, protocol design, and stakeholder collaboration. The proposed platform assumes deployment within dedicated servers or cloud-native infrastructures hosted in highly secure environments. This aligns with current cybersecurity best practices, especially when integrating post-quantum cryptographic (PQC) toolchains that require secure key management, memory isolation, and tamper-proof computation modules. Server-grade hardware with hardened operating systems will be essential in ensuring that the PQC primitives are not vulnerable to side-channel attacks or state recovery mechanisms.

Performance and Scalability

Post-quantum cryptographic algorithms, especially lattice-based and hash-based schemes, introduce significant computational and bandwidth overhead compared to classical counterparts. For instance, a Dilithium signature can be between 2.5 KB and 4 KB, compared to a 64-byte ECDSA signature, and verification can consume millions of CPU cycles (NIST, 2024). The architecture supports major operating environments Microsoft, Linux, and iOS, using language-agnostic APIs and portable cryptographic libraries. However, this heterogeneity introduces challenges in vulnerability management. Legacy protocols, fragmented update cycles, and dependency on platform-specific entropy sources may affect PQC module integrity. A centralized vulnerability disclosure program and regular PQC patch rollouts will be vital for operational resilience (Castiglione et al., 2024).

Performance Bottlenecks:

- Signature size inflates transaction payloads, increasing block size and network traffic.
- The computation cost for signing and verifying degrades transaction throughput.
- Consensus rounds become more communication-intensive due to larger authentication payloads.

Mitigation Strategies:

- Hardware acceleration: Deploy FPGA- or GPU-based cryptographic modules to offload PQC operations (Johnson & Murchison, 2019).
- Pre-signing and caching: Allow wallets to generate signatures ahead of time for likely transactions.
- Signature batching and aggregation: Combine multiple signatures in consensus blocks, where supported.
- Sharding and regional subnetworks: Distribute load across zones (e.g., domestic vs. cross-border payment ledgers).
- Layer-2 scaling: Implement off-chain channels or rollups for high-frequency retail payments, similar to the Lightning Network.

Despite early pilot concerns (e.g., Project Tourbillon's 5× latency hit and 200× throughput drop), incremental software and hardware optimization can drastically reduce these figures (BIS, 2023b).

Latency and Real-Time Payment Needs

Users and merchants demand instantaneous payment confirmation, particularly for retail and contactless payments. PQC introduces additional signing and verification steps, which can delay processing.

Latency-Sensitive Areas:

- Point-of-sale (POS) authorization
- Mobile wallet transfers
- ATM withdrawal confirmations

Solutions:

- Use optimistic confirmation models: provide provisional approval immediately while final settlement occurs in the background.
- Tiered validation: lightweight real-time checks followed by full PQC verification asynchronously.
- Fast-finality consensus protocols (e.g., PBFT, HotStuff) that can confirm transactions in under 1–2 seconds.

Additionally, PQC algorithms like Falcon provide shorter signatures (compact ~700-byte range), suitable for bandwidth-constrained or latency-sensitive environments such as mobile SIMs and cards (NIST, 2024).

Regulatory Compliance (e.g., AML, KYC)

In a decentralized system, compliance enforcement must be integrated without compromising decentralization or privacy.

Challenges:

- Regulatory bodies demand traceability, identity verifiability, and auditable records.
- Some jurisdictions require data localization and transactional record retention.
- Zero-trust environments make it hard to centrally enforce rules.

Design Responses:

- Implement programmable compliance logic (e.g., smart contracts that block large payments without AML checks).
- Utilize zero-knowledge proofs to satisfy conditions (e.g., KYC-passed) without revealing private user data.
- Develop privacy zones: sub-networks where transaction visibility is role-based (e.g., regulator nodes can decrypt selected fields).
- Comply with evolving regulatory guidance (e.g., Financial Action Task Force on virtual assets).

A regulator’s observer node can audit consensus and access compliance data via encrypted backdoors (governed by legal warrants) while user-facing systems preserve privacy and usability.

Hardware and Cryptographic Agility

A significant challenge in PQ migration is the heterogeneity of hardware, particularly in embedded environments such as:

- Smart card chips
- Mobile SIMs
- POS terminals
- ATM security modules

These devices often lack the processing power or memory footprint to handle large PQC key sizes and heavy operations.

Roadmap for Hardware Migration:

- Develop dual-stack support: allow continued use of ECDSA in these devices while wrapping communications in PQC (e.g., a POS sends an ECDSA transaction, which is then re-signed by the issuer bank using Dilithium before submission to the ledger).
- Promote vendor adoption: encourage chipset makers to support Kyber, Dilithium, SPHINCS+ in HSMs and secure elements (Accenture, 2024).
- Introduce quantum-safe SDKs for mobile wallets and banking apps with hybrid crypto support.

Furthermore, cryptographic agility must be embedded into the platform's design: if a PQC scheme is later deprecated (as SIKE and Rainbow were), the system must support algorithm swapping without breaking the transaction chain (Utimaco, 2024).

Privacy and Zero-Knowledge Strategies

While quantum-safe cryptography secures transaction authenticity and confidentiality, privacy remains a complex domain, especially in decentralized systems that are inherently transparent.

Privacy Tensions:

- Public ledgers expose transaction flows.
- Financial data must be both auditable and confidential.
- PQC privacy technologies are still emerging.

Approaches:

- Use quantum-resistant zero-knowledge proofs (zk-SNARKs) based on hash primitives (e.g., Poseidon) rather than number-theoretic assumptions.
- Implement blind signature mechanisms (e.g., lattice-based) for anonymous digital cash.
- Adopt selective disclosure protocols for regulators, allowing compliance checks without full public transparency.
- Design privacy tiers: consumer-to-consumer payments may be private, while institution-to-institution flows are visible.

The BIS Project Tourbillon validated a working prototype of private quantum-safe CBDC using blind lattice-based signatures (BIS, 2023b). Similar techniques can be scaled for broader privacy-sensitive use cases in our platform (De Haro Moraes, Pereira, & Grossi, 2024).

Use Case Demonstration

To validate the technical and architectural concepts proposed in this study, we present a real-world use case demonstration involving a cross-border remittance scenario. This scenario highlights how a quantum-safe decentralized payment platform can enable secure, interoperable, and regulation-compliant transactions across borders, channels, and financial systems while preserving performance, auditability, and post-quantum resilience.

Scenario Overview: Mobile Wallet to Bank Transfer (Cross-Border)

Consider a user in Kenya who wants to send money from their mobile money wallet (e.g., M-Pesa) to a merchant's bank account in Germany.

Traditionally, this transaction would traverse multiple intermediaries: mobile operator, local bank, remittance aggregator, foreign exchange bureau, SWIFT messaging, and the recipient bank, incurring fees and delays. With our quantum-safe decentralized payment network, this same transaction is executed securely, transparently, and rapidly across a unified platform.

Transaction Workflow (Step-by-Step)

1. User Authorization & Key Binding

The sender's mobile wallet app interfaces with the platform via a quantum-safe SDK that integrates a Dilithium keypair. Upon account registration, the user's identity is linked with a post-quantum public key using a decentralized identity (DID) credential issued by their mobile money provider. The wallet app signs the transaction request using the user's private key.

2. Transaction Creation

The user initiates a transfer: "Send 10,000 Kenyan Shillings (KES) to merchant@examplebank.de (EUR equivalent)."

The mobile money provider's API gateway receives this request and translates it into the platform's transaction schema. The transaction object includes:

- Sender's address (tied to Dilithium public key)
- Recipient's address (tied to the recipient bank's custodian node)
- Amount, currency, timestamp
- Optional memo or invoice ID
- Digital signature from sender (PQC)

3. API Gateway & Currency Conversion

The API gateway checks KYC compliance, verifies the signature, and forwards the transaction to the platform. If currency conversion is required, the gateway interfaces with an on-chain FX contract or a liquidity provider. Conversion rates are retrieved from authenticated price oracle feeds, signed using SPHINCS+ for authenticity.

4. Submission to Ledger

The validated and signed transaction is submitted to the PQC-secured ledger. The validator nodes verify:

- Signature authenticity (Dilithium verification)
- Sufficient balance in sender's account
- Recipient identity validity
- Transaction limits, sanctions screening (via compliance contract)

5. Consensus and Finality

Using a HotStuff-based consensus protocol, the validator nodes sign the block proposal containing this transaction using their PQC keys. Upon 2/3 quorum, the block is finalized. This process takes under 2 seconds due to the permissioned architecture.

6. Settlement and Notification

The recipient's German bank receives a notification via its node interface that funds (in EUR) have been credited to its on-platform custody account. The bank updates its internal core ledger via API integration and reflects the amount in the merchant's actual bank account. The sender receives a confirmation in their mobile app.

7. Regulatory Audit and Proof

The transaction metadata (including time, origin, FX rate, and compliance flags) is recorded in an auditable Merkle proof. Regulators with permissioned observer nodes can independently verify:

- That the transaction passed AML/KYC checks
- That currency conversion used authentic data
- That no tampering occurred post-submission

This flow achieves cryptographic end-to-end security under quantum threat models. No part of the transaction key exchange, digital signature, or ledger commitment relies on classical vulnerable cryptography. Moreover, the user retains a standard mobile interface experience, while the institutions maintain regulatory oversight.

Stakeholder Roles

- User: Holds a mobile wallet with PQ key integration; initiates the transaction.
- Mobile Money Provider: Onboards the user, verifies identity, and signs transactions as needed.
- Payment Platform: Performs core ledger operations, FX, consensus, and compliance enforcement.
- Recipient Bank: Receives funds, credits merchant account, and participates in ledger validation.
- Regulator: Audits the transaction trail using observer nodes and zero-knowledge verifications if required.
- Liquidity Provider: Offers real-time FX services on-chain, protected by post-quantum signature mechanisms.

Audit Trail and Compliance Record

The ledger maintains:

- A signed transaction receipt, verifiable via PQC tools
- A hash-anchored compliance log, detailing AML checks passed
- A zero-knowledge proof of origin (optional) to protect user privacy while enabling audit

This system aligns with guidance from global regulators (e.g., G7 Cyber Expert Group, FSB) who demand cryptographic agility and verifiability in cross-border payment innovations (FSB, 2023).

Strategic Discussion and Roadmap

Building a universal quantum-safe payment platform is an ambitious yet necessary endeavor that requires strategic planning across technical, institutional, and regulatory domains. This section outlines a phased roadmap for deployment, discusses ecosystem readiness, and provides actionable recommendations for key stakeholders including central banks, fintechs, and financial regulators. The goal is to transition global payments to quantum-resilient rails before cryptographically relevant quantum computers (CRQCs) arrive estimated within the next 10–15 years (World Economic Forum, 2024).

Phased Deployment Strategy

Given the complexity and scale of global payment systems, a staged rollout allows gradual adoption while mitigating risk and building confidence.
Phase 1: Immediate Preparations (Year 1–2)

- Cryptographic Inventory: Institutions conduct a detailed audit of cryptographic components across payment APIs, communication channels (TLS/VPN), authentication systems, and internal messaging layers.
- Hybrid Pilots: Begin integrating PQC algorithms (e.g., Kyber, Dilithium) in non-critical channels, such as internal VPNs, bank-to-bank test environments, and sandbox APIs using hybrid modes.
- Stakeholder Consortia Formation: Form industry consortia under regulatory supervision (e.g., central banks or BIS Innovation Hub) to coordinate strategy, reference architecture, and pilot parameters.
- Regulatory Alignment: Collaborate with compliance bodies to define legal status of PQ signatures, ledger finality, and digital identities under financial laws.

Phase 2: Prototype Network Launch (Year 2–4)

- Deploy a limited-scope quantum-safe DLT network with 5–10 participating institutions processing test payment flows (e.g., interbank clearing, payroll disbursements, or controlled remittances).
- Integrate core features: PQ identity system, validator consensus with post-quantum signatures, and API gateways supporting ISO 20022 messages.
- Validate latency, scalability, and auditability; implement metrics to track TPS, finality time, and transaction cost.
- Collaborate with national and cross-border payment operators to run simulations comparing current infrastructure and PQ network behavior.

Phase 3: Real-World Corridor Deployment (Year 4–6)

- Choose a payment corridor (e.g., Kenya–Germany, Philippines–UAE) with engaged institutions and implement full-stack PQ infrastructure in production volumes.
- Introduce tokenized fiat currencies, verified user wallets, mobile API support, and real-time currency conversion with compliance features.
- Evaluate economic benefits (cost reduction, faster settlement) and performance against legacy systems.
- Start onboarding large PSPs and regional banks to increase transaction diversity.

Phase 4: Gradual Legacy Replacement (Year 6–10)

- As PQC standards are formalized (e.g., FIPS certification, EMV updates), move to full PQC mandates for high-value payments, central bank operations, and critical financial infrastructure.
- Use the platform as a settlement backbone for card networks, ACH systems, and government disbursement programs.
- Explore embedding CBDCs or stablecoins on the platform, facilitating atomic swaps, programmable money, and privacy-preserving regulatory mechanisms.
- Formalize exit plans for vulnerable cryptographic algorithms set a cutoff date for RSA/ECC retirement in payment systems.

This roadmap aligns with the notion of crypto-agility and ensures quantum-safe protections are in place before real quantum threats materialize (Entrust, 2025).

Stakeholder Readiness and Collaboration Models

Effective migration to quantum-safe payments hinges on coordinated participation across public and private sectors. Each actor has a unique role:

- Central Banks: Provide legal and operational guidance; possibly run validator nodes; issue digital fiat or CBDC over the network; fund research; coordinate pilot corridors (De Haro Moraes, Pereira, & Grossi, 2024).
- Commercial Banks and PSPs: Transition infrastructure (e.g., APIs, signing modules, encryption libraries); implement wallet and interface changes; participate in node operation.
- Fintechs and Wallet Providers: Rapid adopters of PQC SDKs; bridge services for users and merchants; push PQ features (e.g., faster payments, transparency) as competitive advantages.
- Standardization Bodies (NIST, ISO, ETSI): Finalize PQC specs; define secure parameters; create PQC-compatible protocols (e.g., updated ISO 8583, EMV).
- Developers and Startups: Innovate privacy-preserving smart contracts, bridges to legacy networks, and tools for key management, auditing, and cryptographic agility.

To ensure a common operational model, a governance framework should be established that:

- Defines minimum compliance and operational standards (e.g., signing key lifecycle, API security).
- Certifies node software implementations and cryptographic modules.
- Manages cryptographic updates (e.g., replacing or retiring algorithms).
- Provides dispute resolution mechanisms for smart contract misbehavior or regulatory escalations.

Recommendations for Institutions

Drawing from research and pilot observations, we outline targeted recommendations:

- Start Migration Early: Begin replacing classical crypto now where feasible TLS tunnels, internal APIs, backup certificates (Accenture, 2024).
- Adopt Hybrid Cryptography: Until full PQC systems mature, use hybrid modes (e.g., ECDSA + Dilithium) in signatures and hybrid KEMs in TLS to preserve forward secrecy (NIST, 2024).
- Focus on Crypto Agility: Architect systems that can swap algorithms easily use metadata in transaction formats to specify algorithms; avoid hardcoded cryptographic primitives.

- Invest in Performance R&D: Support research on signature aggregation, hardware acceleration, and protocol optimization (BIS, 2023b).
- Engage with Standardization Bodies: Ensure your feedback and use-cases are part of shaping global PQC payment standards.

These steps will position financial institutions to withstand future quantum attacks, improve interoperability, and capitalize on the efficiency gains of decentralized clearing.

Conclusion

The financial world stands at the edge of a historic transformation driven by the rise of quantum computing. With quantum algorithms capable of breaking the cryptographic foundations of existing digital payment infrastructures, the need to prepare is no longer speculative; it is a pressing and strategic imperative. This study has presented a comprehensive exploration of the threat landscape, evaluated the maturity of post-quantum cryptographic (PQC) solutions, and proposed a detailed, technically grounded design for a universal quantum-safe payment platform built upon decentralized architecture. Through an in-depth literature review, we analyzed the weaknesses of current protocols TLS, ECDSA, RSA and demonstrated how quantum computers, using algorithms like Shor's and Grover's, can compromise them. We outlined the families of PQC algorithms, particularly lattice-based schemes like Kyber and Dilithium that provide strong security guarantees under quantum threat models and meet the performance demands of real-time financial transactions (NIST, 2024). Our assessment extended beyond cryptographic primitives to encompass full-stack architectural needs: from API gateway integration, digital identity management, and consensus protocols, to smart contract logic and compliance oversight.

The proposed platform unifies diverse payment channels, bank wires, mobile money, card systems, and cryptocurrencies on a single, quantum-resilient ledger. The architecture emphasizes cryptographic agility, compliance interoperability, and performance engineering to ensure practical adoption. Importantly, the design embeds privacy safeguards, supports regulatory mandates, and offers a roadmap for incremental migration without disrupting existing financial operations. The use case demonstration of a cross-border remittance showcased the feasibility of deploying PQC-based digital signatures, key exchanges, and API-level integration in real-world flows. Furthermore, the strategic roadmap charts a realistic multi-phase path for rolling out this platform from hybrid pilots and institutional readiness audits to corridor-specific deployments and eventual mainstream adoption. Ultimately, the findings validate the technical and institutional feasibility of building a future-proof, universal, decentralized payment system. The cryptographic tools are ready, and the industry is increasingly aware of the risks. What remains is committed leadership, sustained research investment, and coordinated regulatory support.

The long-term implications of transitioning to a quantum-safe platform are profound. Beyond defending against quantum threats, such a platform can improve settlement efficiency, reduce operational costs, enhance interoperability, and foster trustless collaboration across borders. It redefines what "secure payments" mean in the 21st century, laying the foundation for resilient global commerce in the quantum age. As the "Q-Day" approaches, the day when quantum computers render current cryptography obsolete, institutions that act early will safeguard not just their infrastructure but the trust of their users and the stability of global finance. This research offers the blueprint to begin that journey, secure, decentralized, interoperable, and quantum-ready (Andriani, Bencivelli, & Castellucci, 2024).

Glossary

- AML (Anti-Money Laundering): Regulations and procedures aimed at preventing and detecting financial crimes like money laundering.
- API (Application Programming Interface): An Interface allowing software components to interact and exchange data securely and efficiently.
- Blockchain: Distributed ledger technology (DLT) where transaction records are stored in linked blocks across multiple decentralized nodes.
- Consensus Mechanism: An Algorithm enabling decentralized nodes within a blockchain network to agree on transaction validation and state updates.
- Cryptographic Agility: Capability of a system to rapidly adapt and integrate new cryptographic algorithms without major architectural changes.
- Decentralized Ledger: A distributed database spread across multiple nodes, eliminating central authority while enhancing data security and transparency.
- Dilithium: Post-quantum cryptographic algorithm based on lattice mathematics, primarily utilized for secure digital signatures.
- DID (Decentralized Identifier): A Digital identification system operating without a centralized issuing authority, empowering users with direct control of their identity data.
- Falcon: A lattice-based signature scheme optimized for efficiency and security against quantum computing attacks.

- HotStuff: An Efficient leader-based Byzantine Fault Tolerant (BFT) consensus algorithm designed to enhance scalability and transaction throughput.
- HSM (Hardware Security Module): A Physical computing device providing secure storage, generation, and management of cryptographic keys.
- ISO 20022: International messaging standard facilitating structured electronic communication between financial institutions.
- Kyber: Quantum-resistant encryption algorithm selected by NIST as part of its standardization efforts, based on lattice cryptography.
- KYC (Know Your Customer): Regulatory procedure involving verification of user identities to mitigate fraud and financial crime risks.
- Lattice-Based Cryptography: Quantum-resistant cryptographic techniques relying on mathematical lattice structures, effective against quantum attacks.
- PBFT (Practical Byzantine Fault Tolerance): Consensus algorithm enabling robust agreement among decentralized nodes, tolerant against malicious or faulty behaviors.
- POS (Point of Sale): Hardware and software interfaces enabling secure processing of retail payment transactions.
- Post-Classical Era: Future period dominated by quantum computing capabilities, requiring advanced cryptographic safeguards.
- Post-Quantum Cryptography (PQC): Cryptographic methods designed explicitly to remain secure against quantum-computer-enabled cryptanalysis.
- Quantum-Safe: Cryptographic solutions and practices capable of resisting attacks from quantum computing algorithms.
- RESTful API (Representational State Transfer API): An Architectural style for designing networked APIs that are lightweight and interoperable.
- Smart Contract: Self-executing digital contracts stored and executed automatically on blockchain platforms based on predefined conditions.
- SPHINCS+: Hash-based cryptographic signature algorithm providing robust, quantum-resistant digital signatures.
- SWIFT (Society for Worldwide Interbank Financial Telecommunication): Global network enabling secure financial communication between banks and institutions.
- TLS (Transport Layer Security): A Security protocol providing encrypted communication between systems over networks, securing data privacy and integrity.

- zk-SNARKs (Zero-Knowledge Succinct Non-interactive Argument of Knowledge): Cryptographic method allowing proofs of validity without revealing underlying sensitive information.

Conflict of Interest: The author reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The author did not obtain any funding for this research.

References:

1. Accenture. (2024). *Banco Sabadell explores adoption of PQC in banking infrastructure*.
2. Bank for International Settlements [BIS]. (2023a). *Project Leap: quantum-proofing the financial system.*
3. Bank for International Settlements [BIS]. (2023b). *Project Tourbillon: exploring privacy, security and scalability for CBDCs.*
4. Deloitte. (2020). *Quantum computers and the Bitcoin blockchain.*
5. Entrust. (2025). *The post-quantum era demands quantum-safe payments.*
6. Financial Services Information Sharing and Analysis Center [FS-ISAC]. (2024). *Quantum threat preparedness recommendations.*
7. National Institute of Standards and Technology [NIST]. (2024). *PQC final standardization: CRYSTALS-Kyber, Dilithium, Falcon, SPHINCS+.*
8. NACHA Payments Innovation Alliance. (2024). *Protecting payments in the quantum era.*
9. PQShield. (2025). *Identity and payments: Preparing for the quantum threat.*
10. Scientific Reports. (2023). *Quantum-resistance in blockchain networks.*
11. Utimaco. (2024). *Types of post-quantum cryptography public key schemes.*
12. World Economic Forum. (2024). *Safeguarding CBDC systems in the post-quantum age.*
13. Adeoye, S. (2025). *Blockchain-enabled, post-quantum cryptographic framework for securing electronic health records: A next-generation approach to healthcare data.*
14. Turpu, R. R. (2024). *Fortifying banking transactions: Harnessing post-quantum cryptography for next-generation security.*

15. Agrawal, S. (2024). *Harnessing quantum cryptography and artificial intelligence for next-gen payment security: A comprehensive analysis in distributed ledger environments.*
16. Nwaga, P., & Idima, S. (2024). *Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure.*
17. Das, P. (2025). *Quantum computing in payments security: Preparing for the post-quantum era.*
18. De Haro Moraes, D., Pereira, J. P. A., & Grossi, B. E. (2024). *Applying post-quantum cryptography algorithms to a DLT-based CBDC infrastructure: Comparative and feasibility analysis.*
19. Weinberg, A. I., Petratos, P., & Faccia, A. (2024). *Will central bank digital currencies (CBDC) and blockchain cryptocurrencies coexist in the post-quantum era?*
20. Andriani, C., Bencivelli, L., & Castellucci, A. (2024). *The quantum challenge: Implications and strategies for a secure financial system.*
21. Castiglione, A., Esposito, J. G., & Loia, V. (2024). *Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices.*
22. Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). *Securing the future: Exploring post-quantum cryptography for authentication and user privacy in IoT devices.*