Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Finance as Critical Infrastructure: Embedding Post-Quantum Cryptography in Digital Finance Architectures

Rahul Bhatia
Senior IEEE Member, Independent Researcher, United Kingdom
Corresponding Author: Rahul Bhatia, **E-mail**: : rahul.bhatia20@ieee.org

| ABSTRACT

Quantum computing presents both transformative potential and unprecedented risk. Financial systems, which rely on RSA, ECC, and other public-key cryptography, are especially vulnerable to quantum-enabled attacks. For the United States—where the IRS, Treasury, Federal Reserve, Medicare, and unemployment programs collectively manage trillions of dollars annually—the implications are profound. This paper argues that finance must be treated as critical national infrastructure and proactively secured against the quantum threat. Post-Quantum Cryptography (PQC), as being standardized by NIST, offers the technical foundation for resilience. However, successful adoption requires more than technical substitution—it demands an architecture-led redesign. Drawing on the Finance Architecture Strategy Technology (FAST™) framework, which embeds compliance and fraud prevention into design, and the Digital Finance Reference Architecture (DFRA™), a modular blueprint for cloud-native, scalable transformation, we propose a roadmap for embedding PQC into digital finance. This includes PQC integration within cloud ERP platforms such as SAP S/4HANA, hybrid cryptography strategies during transition, and governance models that align with OMB A-123 and DHS critical infrastructure protection. By combining PQC with structured frameworks, the U.S. can safeguard financial flows against future quantum adversaries, protect public trust, and reinforce its leadership in global digital governance. This work positions digital finance architecture as both an economic enabler and a national security priority, demonstrating how U.S. financial systems can be future-proofed for the quantum era.

| KEYWORDS

Critical Infrastructure; Post-Quantum Cryptography; Digital Finance Architectures

| ARTICLE INFORMATION

ACCEPTED: 04 July 2025 **PUBLISHED:** 20 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.134

1. Introduction

The financial system is one of the most critical components of national infrastructure. In the United States, trillions of dollars flow annually through the Internal Revenue Service (IRS), the U.S. Treasury, the Federal Reserve, Medicare, Medicaid, and state-level distribution programs. These flows enable the delivery of healthcare, social security, education, infrastructure investment, and emergency relief. Trust in this system rests on its integrity, confidentiality, and resilience. Today, these assurances are guaranteed by cryptographic protocols such as RSA and elliptic curve cryptography (ECC), which secure banking transactions, tax filings, and public sector fund transfers.

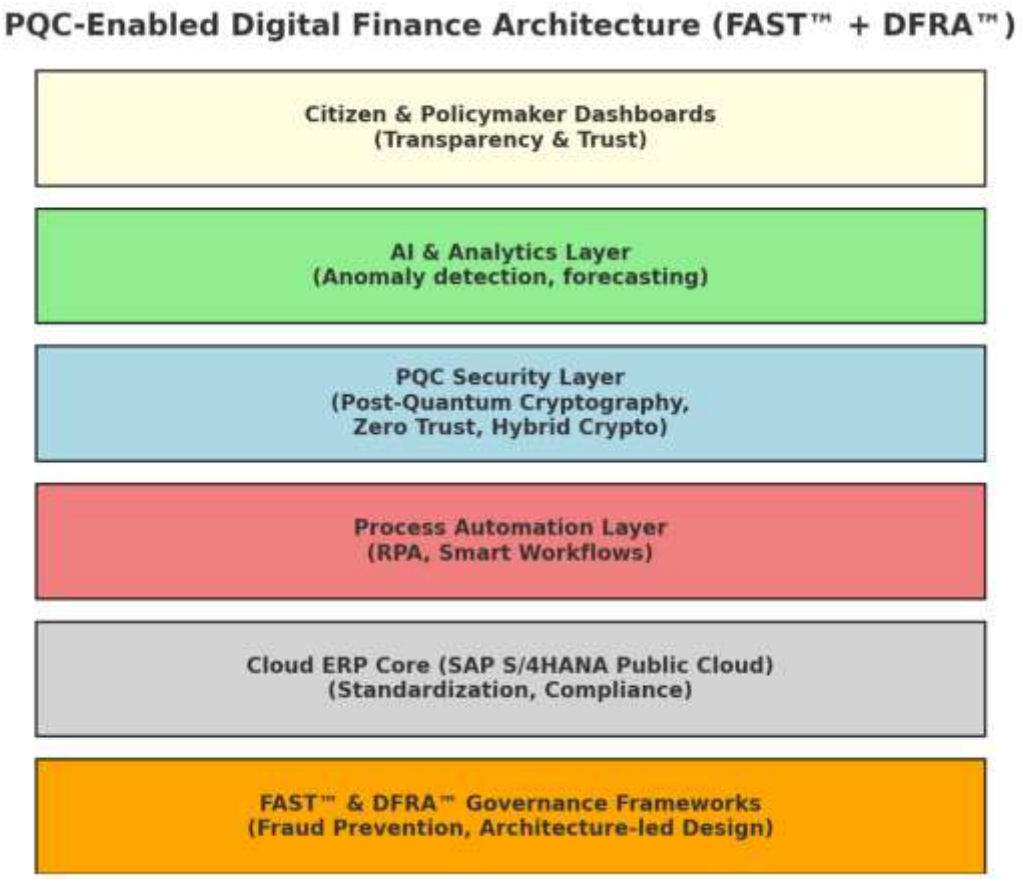
However, the emergence of quantum computing threatens to undermine this foundation. Quantum algorithms, particularly Shor's algorithm, have the capability to break RSA and ECC in polynomial time, rendering much of today's encryption obsolete [1]. While large-scale quantum computers may not yet exist, the threat is not theoretical. State and non-state adversaries are already engaging in "harvest now, decrypt later" strategies [5], storing sensitive financial data with the expectation that future quantum breakthroughs will allow decryption. This places the confidentiality of taxpayer records, banking transactions, and long-term contracts at risk—even before quantum machines are operational.

For the U.S., the implications are profound. Financial infrastructure is already a high-value target for cybercriminals and hostile nation-states, as demonstrated by large-scale fraud in pandemic relief programs [3] and cyber intrusions such as the SolarWinds breach [16]. The quantum era amplifies these risks by introducing a structural vulnerability in the very cryptographic fabric upon which digital finance is built. Without proactive preparation, the integrity of U.S. financial systems could be compromised, eroding public trust, destabilizing the economy, and weakening the dollar's role as the world's reserve currency.

To address this, the National Institute of Standards and Technology (NIST) has been leading the Post-Quantum Cryptography (PQC) Standardization Project since 2016, identifying algorithms such as CRYSTALS-Kyber (encryption) and CRYSTALS-Dilithium (digital signatures) as promising candidates [2]. Yet standardization alone is insufficient. Embedding PQC into digital finance architectures requires an enterprise-level, architecture-led approach that balances security, scalability, compliance, and operational continuity.

This paper argues that PQC adoption must be treated not as a technical substitution but as a national infrastructure redesign. Building on two proprietary frameworks—the Finance Architecture Strategy Technology (FAST™) framework, which embeds fraud prevention and compliance into system design, and the Digital Finance Reference Architecture (DFRA™), a modular blueprint for cloud-native transformation—we propose a roadmap for securing U.S. financial systems in the quantum era. By integrating PQC into cloud ERP systems such as SAP S/4HANA, layering AI-driven fraud detection, and aligning with DHS's critical infrastructure protection framework [8], financial systems can be future-proofed against emerging quantum threats.

In short, quantum computing transforms the conversation around financial cybersecurity from incremental upgrades to existential redesign. Just as roads, grids, and defense systems are considered national infrastructure, so too must financial systems be re-architected to withstand the quantum threat. This paper outlines the risks, technology enablers, and policy alignment required to embed PQC into U.S. digital finance—ensuring that every transaction, from tax filings to Medicare reimbursements, remains secure in the quantum era.



2. The Quantum Threat to Financial Systems

The quantum era poses an unprecedented challenge to the digital security of financial systems. While quantum computing promises breakthroughs in optimization, materials science, and healthcare, its most immediate impact will be in **cryptanalysis**—

the ability to break cryptographic algorithms that underpin global financial infrastructure. For the United States, whose economy relies on secure digital transactions, this represents not just a technical risk but a matter of **national security**.

2.1 Vulnerability of Current Cryptographic Standards

Most modern financial systems rely on **public-key cryptography** for secure communications and authentication:

- **RSA (Rivest-Shamir-Adleman):** Widely used in digital certificates, banking protocols, and tax systems.
- **ECC (Elliptic Curve Cryptography):** Powers TLS protocols in online banking, cryptocurrency wallets, and secure APIs.
- **Diffie–Hellman:** Used for key exchanges in financial messaging systems.

Quantum computing introduces a fatal flaw. **Shor's algorithm** can factor large integers and compute discrete logarithms exponentially faster than classical algorithms [1]. In practical terms, once a sufficiently powerful quantum computer is developed, **RSA and ECC will be rendered obsolete**. Financial transactions, tax filings, and digital signatures based on these systems would no longer be trustworthy.

2.2 Risks to Financial Infrastructure

The U.S. financial system relies on cryptography at every layer of its infrastructure:

- **Payment Systems:** SWIFT, ACH, Fedwire, and card networks all use encryption for secure communication. A quantum-capable adversary could disrupt settlements or forge payment instructions.
- **IRS and Treasury Systems:** Tax filings, refunds, and intergovernmental fund transfers rely on secure data exchanges that would be vulnerable.
- **Healthcare Payments:** Medicare and Medicaid transactions, already subject to fraud, would face heightened exposure to interception and tampering [6].
- **Banking and Fintech APIs:** Authentication and secure data exchange rely on ECC. A quantum compromise would endanger everything from mobile payments to open banking.

In short, every dollar that moves through the U.S. economy depends on cryptographic assurances that will collapse in the face of quantum adversaries.

2.3 Blockchain and Digital Assets

Beyond traditional finance, blockchain-based systems such as cryptocurrencies, central bank digital currencies (CBDCs), and distributed ledgers used for financial settlement also rely on ECC.

- **Bitcoin and Ethereum:** Both depend on elliptic curve digital signatures (ECDSA). Quantum attacks could forge signatures, seize wallets, and undermine trust in the system [4].
- **Stablecoins and CBDCs:** As the U.S. explores digital dollar prototypes, failure to embed PQC could render next-generation payment infrastructure insecure from inception.
- **Smart Contracts:** Manipulation of cryptographic keys would allow attackers to override contractual agreements encoded on-chain.

Given the increasing adoption of blockchain in both private and public finance, this represents a systemic risk that cannot be ignored.

2.4 "Harvest Now, Decrypt Later" Threat

The quantum threat is not confined to the future. Today's adversaries can intercept and store encrypted financial data with the expectation of decrypting it once quantum computers become available [5].

- **Long-Term Sensitive Data:** Tax records, healthcare reimbursements, and financial contracts often require confidentiality for decades.
- **State Adversaries:** Nation-states with advanced cyber capabilities are believed to already be collecting encrypted financial traffic.

- **Strategic Risk:** A future decryption event could expose years of historical financial data, undermining trust in institutions.

This "time-delayed breach" risk is especially acute in government finance systems, where sensitive data (e.g., IRS tax returns, Social Security payments) must remain confidential well into the future.

2.5 U.S. Financial Exposure in Context

The U.S. financial system's global role magnifies its exposure:

- **Reserve Currency Dependence:** As issuer of the world's reserve currency, the U.S. dollar, the integrity of U.S. financial systems underpins global trust in the monetary order.
- **Cross-Border Settlements:** International transactions routed through U.S. institutions could become prime targets for quantum adversaries.
- **Public Sector Programs:** Pandemic-related stimulus fraud already highlighted systemic weaknesses [3]; a quantum threat could multiply risks.

Unlike localized cyber incidents, quantum vulnerabilities threaten the **structural foundations of trust** in U.S. finance. If left unaddressed, the result could be destabilization of both domestic and global markets.

2.6 Implications

The implications of these vulnerabilities are stark:

1. **Loss of Trust:** Without secure cryptography, citizens and markets may lose faith in government and financial institutions.
2. **Systemic Disruption:** Payments, settlements, and tax collection could be disrupted at scale.
3. **National Security Threat:** Adversaries could weaponize quantum capabilities to destabilize the U.S. economy.
4. **Erosion of Dollar Dominance:** If U.S. systems are compromised, the dollar's reserve currency status could be challenged.

The quantum threat therefore transforms cybersecurity in finance from a **technical concern to an existential one**.

3. The Case for Post-Quantum Cryptography (PQC)

The adoption of post-quantum cryptography (PQC) in financial systems is not just about replacing vulnerable algorithms—it is about **re-architecting the financial core** of national infrastructure. For decades, RSA and elliptic curve cryptography (ECC) have underpinned secure tax filings, Treasury transfers, Medicare reimbursements, and intercompany settlements. Yet these protocols are mathematically exposed to Shor's algorithm and will not withstand the computational capabilities of quantum machines [1].

In the U.S. context, the stakes are exceptionally high. Trillions of dollars flow annually through systems such as the IRS, U.S. Treasury, and Medicare. Many of these run on fragmented, legacy platforms with limited scalability. If RSA and ECC collapse without PQC-ready replacements, the impact would not be incremental but **systemic**—compromising payments, benefits distribution, and even international confidence in the U.S. dollar.

3.1 The Inevitability of Quantum Risk

Quantum research has advanced rapidly, with IBM, Google, and global competitors achieving breakthroughs in error correction and qubit stability. While estimates for breaking RSA-2048 range between 10–20 years [1,5], the "harvest now, decrypt later" threat means the risk horizon has already begun [5]. Sensitive IRS data, Treasury transactions, and healthcare claims intercepted today could be decrypted once quantum systems mature, exposing decades of financial history.

This inevitability means that PQC must be embedded now, not as a future upgrade, but as a **strategic redesign of financial systems**.

3.2 Legacy Constraints and the Cost of Delay

The U.S. financial infrastructure is heavily constrained by legacy ERP systems. The IRS still relies on COBOL-based mainframes built in the 1960s [4]. Medicare and Medicaid operate on fragmented claims platforms [6]. State treasuries use a patchwork of ERP environments, many of which lack interoperability.

Retrofitting PQC into such heterogeneous environments will be costly, complex, and disruptive. Every year of delay increases the backlog of systems requiring transition and leaves more encrypted data vulnerable to "store now, break later" threats.

This is where **SAP S/4HANA Public Cloud** becomes central. As a modern, cloud-native ERP, it provides:

- **Continuous innovation:** Automatic upgrades allow seamless integration of PQC standards once finalized by NIST [2].
- **Standardization:** Harmonized financial processes across federal and state levels, reducing fragmentation.
- **Scalability:** A platform capable of handling trillions in transaction volumes with embedded security.
- **Interoperability:** APIs and integration frameworks that support hybrid cryptography models during transition [6].

The cost of inaction is not only fiscal—it risks leaving the U.S. financial system unprepared for a wholesale cryptographic collapse.

3.3 PQC in Architecture-Led Finance Transformation

PQC implementation cannot be treated as a bolt-on encryption patch. It must be integrated within a **layered digital finance architecture**:

- **Governance layer:** Compliance and fraud prevention frameworks (e.g., OMB A-123, GAO guidelines) must require PQC-secured transactions as part of standard controls.
- **ERP core (SAP S/4HANA Public Cloud):** PQC algorithms should secure tax collection, fund distribution, general ledger entries, and intercompany settlements at the system-of-record level.
- **Process automation layer:** RPA-driven reconciliations and workflows must authenticate with PQC keys to prevent interception.
- **Analytics layer:** Budget forecasting and fraud detection models should run within PQC-protected environments.
- **Presentation layer:** Real-time dashboards for Treasury and policymakers must ensure PQC-secured data integrity.

This layered integration ensures PQC not only protects data in transit but also strengthens the resilience of the entire financial ecosystem.

3.4 Finance as Critical Infrastructure

Financial systems are as vital as power grids or transportation networks. They underpin every aspect of governance, from payroll to healthcare funding. The Department of Homeland Security already classifies finance as critical infrastructure [8]. In the quantum era, this must translate into tangible investment in PQC deployment across national finance systems.

By embedding PQC within **SAP S/4HANA Public Cloud deployments**, the U.S. can ensure that its financial backbone—IRS, Treasury, Medicare, state treasuries—is modernized and future-proofed. This positions finance not only as secure infrastructure but as **resilient digital infrastructure**, capable of withstanding next-generation threats.

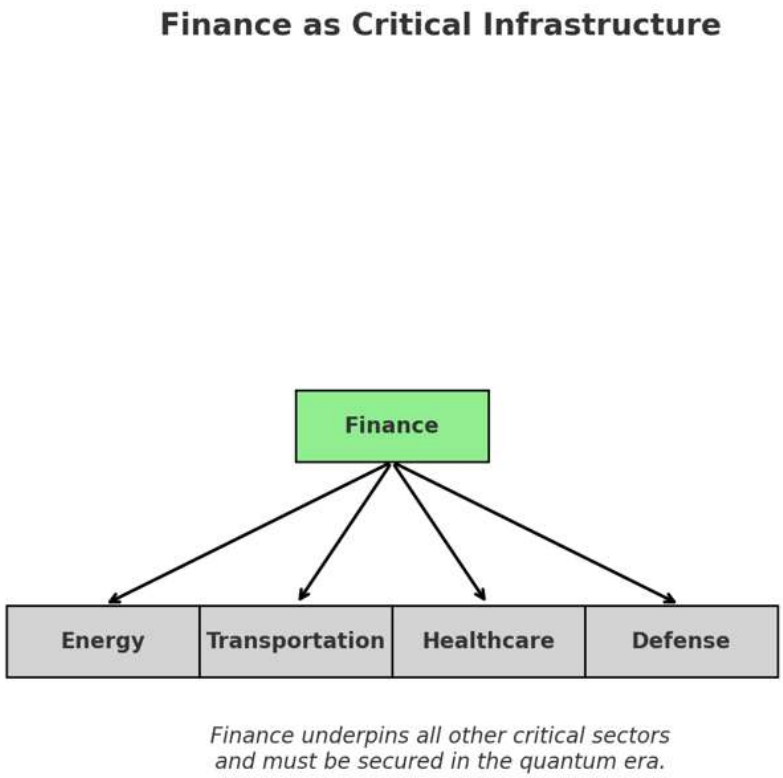


Fig: Finance as Critical Infrastructure

3.5 Strategic Leadership in Global Finance

Through the NIST PQC standardization project [2], the U.S. is already shaping the future of cryptography. But leadership is not achieved through theory—it is realized through **real-world adoption**. By integrating PQC into cloud ERP systems such as SAP S/4HANA Public Cloud, the U.S. can set a global benchmark for how financial infrastructures transition to the quantum era.

This would reinforce trust in the U.S. dollar, secure global settlements routed through American institutions, and demonstrate that **finance can be re-architected as national infrastructure**, secured not only against current cyber threats but also against quantum adversaries.

3.6 Implications

The case for PQC is clear:

1. **Quantum disruption is inevitable** — current cryptography will fail.
2. **Legacy constraints amplify cost** — delay worsens technical debt.
3. **Architecture-led redesign is required** — PQC must be embedded across all financial layers.
4. **Finance must be treated as infrastructure** — securing fund flows is a national security imperative.
5. **SAP S/4HANA Public Cloud is the enabler** — a modern ERP capable of embedding PQC at scale.
6. **U.S. leadership depends on action** — PQC integration must begin now to maintain global financial trust.

4. Embedding PQC in Digital Finance Architectures

The transition to post-quantum cryptography (PQC) cannot be approached as a stand-alone encryption upgrade. It requires an **architecture-led strategy** in which PQC is systematically integrated across the layers of financial infrastructure, from the ERP core to citizen-facing dashboards. This approach ensures that PQC does more than secure data in transit; it enhances resilience, transparency, and trust in the entire financial system.

Drawing on layered finance transformation models such as the **Digital Finance Reference Architecture (DFRA™)** and compliance-driven principles embedded in the **Finance Architecture Strategy Technology (FAST™) framework**, PQC adoption can follow a structured path that is scalable, interoperable, and future-proof.

4.1 Governance and Compliance Layer

At the top of the design, PQC must be codified as a **governance requirement**. Financial controls defined in **OMB Circular A-123** and GAO's high-risk cybersecurity assessments [9,17] should be updated to mandate quantum-resilient encryption for all financial transactions. In practice, this means:

- Embedding PQC-based signatures in tax filing systems (e.g., IRS e-filing).
- Ensuring Treasury fund transfers require PQC-authenticated approvals.
- Using PQC-secured audit trails to strengthen fraud investigations.

In FAST™, this aligns with the **compliance-first principle**, embedding PQC as a **mandatory financial control** rather than a discretionary IT feature.

4.2 ERP Core Layer (SAP S/4HANA Public Cloud)

The **ERP core** represents the foundation of financial operations. SAP S/4HANA Public Cloud, already used for Treasury, grants, and public sector management, provides a scalable environment where PQC can be embedded natively.

Key ERP applications that must be PQC-secured include:

- **General Ledger & Fund Distribution:** All postings and transfers should use PQC-based digital signatures.
- **Accounts Payable/Receivable:** Vendor and citizen payments must be validated with PQC-secured certificates.
- **Intercompany Settlements:** PQC ensures that cross-entity reconciliations cannot be tampered with.
- **Treasury & Cash Management:** High-value transfers protected with PQC-based key exchanges.

SAP's continuous upgrade cycle in the cloud ensures that once NIST PQC standards are finalized [2], they can be deployed without disruptive, large-scale migrations. In DFRA™, this forms the **foundational security layer**.

4.3 Process Automation Layer

Routine but critical financial processes—such as reconciliations, approvals, and compliance reporting—must also transition to PQC. Robotic Process Automation (RPA) systems are increasingly used in Treasury operations and state-level finance. By embedding PQC into their authentication, these workflows can be protected from interception or manipulation.

Examples include:

- Automated reconciliation between Treasury and state accounts.
- PQC-secured workflows for Medicare claim approvals.
- PQC-enforced access control for RPA bots in accounts payable processing.

This integration ensures that automation is not a new vulnerability but a secure efficiency enabler.

4.4 Security Layer: PQC Integration

This is the **core layer where PQC algorithms are embedded**. Leveraging NIST finalists such as CRYSTALS-Kyber (encryption) and CRYSTALS-Dilithium (digital signatures) [2], financial systems can secure:

- **Data in transit:** Treasury ↔ IRS ↔ State systems communication.
- **Data at rest:** Taxpayer and healthcare records stored in ERP databases.
- **Digital signatures:** All approvals, fund releases, and contracts validated with PQC keys.

During transition, hybrid cryptography (RSA/ECC + PQC) may be necessary [6]. SAP S/4HANA APIs can support this by enabling interoperability while ensuring gradual migration.

4.5 Analytics and AI Layer

PQC also protects financial intelligence. Predictive analytics, revenue forecasting, and fraud detection models rely on sensitive financial and behavioural data. If exposed through quantum decryption, adversaries could manipulate models or compromise oversight.

Embedding PQC in analytics ensures that:

- Treasury's predictive revenue models remain secure.
- AI-driven fraud detection operates on uncompromised datasets.
- Machine learning pipelines in cloud environments remain resilient to future quantum attacks.

This aligns with DFRA™'s **analytics and insight layer**, ensuring resilience in decision-making.

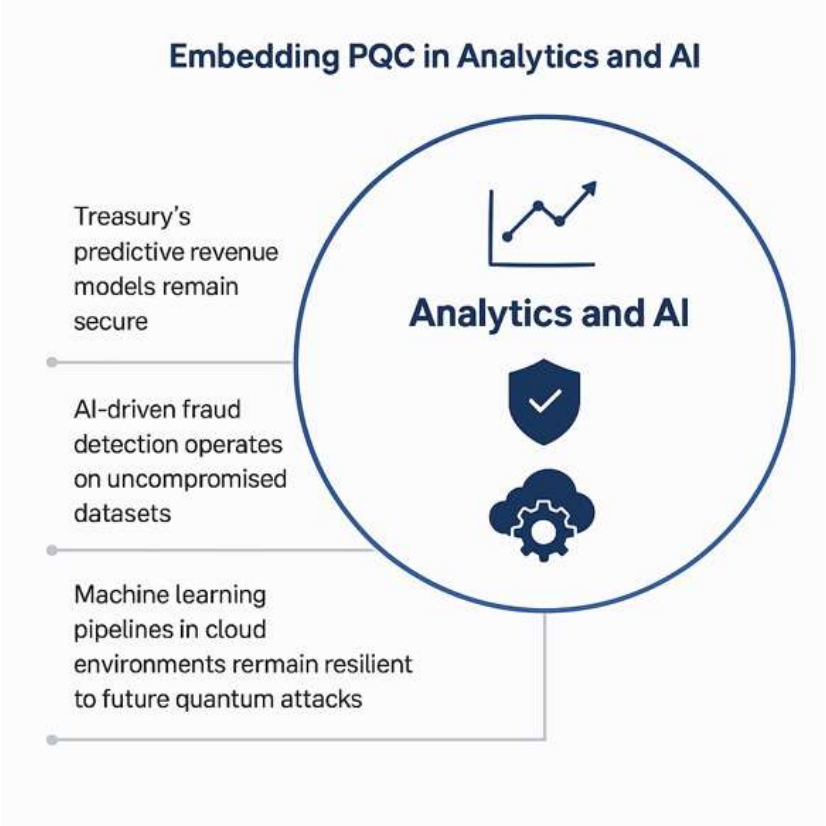


Fig: Embedding PQC in Analytics and AI

4.6 Transparency and Citizen Dashboards

Finally, PQC must extend to **citizen-facing portals and policymaker dashboards**. These platforms, used to track government budgets, benefit disbursements, and tax obligations, depend on real-time integrity of data.

By securing dashboards with PQC:

- Citizens gain confidence that their tax and benefit data is protected.
- Policymakers receive tamper-proof, real-time financial intelligence.
- Transparency initiatives (e.g., CARES Act fund tracking) can withstand even advanced cryptographic threats.

This matches the **trust and transparency dimension** of FAST™, ensuring accountability at the point of public interaction.

4.7 Integrated Architecture Model

When embedded across these layers, PQC transforms digital finance into a **quantum-resilient architecture**:

- **Governance-first controls (FAST™)** define PQC as a compliance mandate.
- **ERP core (SAP S/4HANA Public Cloud)** delivers scalability and standardization.
- **Process automation (RPA)** reduces inefficiency while remaining secure.
- **PQC security layer** provides quantum-safe encryption and signatures.
- **Analytics and dashboards** extend resilience to decision-making and transparency.

This layered design ensures PQC adoption is not fragmented but holistic, embedding security into the very fabric of financial architecture.

5. Technology Enablers: SAP S/4HANA Public Cloud

The successful adoption of post-quantum cryptography (PQC) in U.S. financial systems depends on modern digital platforms capable of supporting rapid cryptographic change. Legacy ERP environments—such as the IRS's COBOL-based master files [4] and fragmented claims systems in Medicare and Medicaid [6]—cannot easily absorb the computational and architectural requirements of PQC. For this reason, SAP S/4HANA Public Cloud emerges as the central enabler for building a quantum-resilient financial infrastructure.

5.1 Cloud-Native Readiness

Unlike legacy on-premise systems that require large-scale custom upgrades, SAP S/4HANA Public Cloud is continuously updated by SAP. Once NIST finalizes PQC algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium [2], they can be deployed into cloud ERP environments through seamless updates. This ensures that cryptographic readiness is not a one-off upgrade but part of an ongoing innovation cycle.

5.2 Standardized Financial Processes

Fragmentation across U.S. financial systems—federal, state, and local—creates complexity in implementing uniform security measures. SAP S/4HANA Public Cloud provides standardized best-practice financial processes that can be applied across jurisdictions. Embedding PQC into these standardized processes ensures consistent protection of:

- General ledger postings at the Treasury and state levels.
- Fund allocations from federal to local entities.
- Accounts receivable/payable workflows in benefits and grants management.
- Intercompany settlements between government agencies.

Standardization reduces the risk of uneven PQC adoption and ensures a uniform security posture nationwide.

5.3 Scalability for National Finance

U.S. public finance operates at unmatched scale, handling trillions of dollars annually. SAP S/4HANA Public Cloud has been designed to manage high transaction volumes with embedded security. This scalability is critical when integrating PQC, which may require greater computational resources than RSA or ECC. By operating within a platform already optimized for scale, PQC can be implemented without creating bottlenecks in Treasury transfers, IRS processing, or Medicaid reimbursements.

5.4 Interoperability and Hybrid Cryptography

Transitioning to PQC will require hybrid cryptography—operating RSA/ECC alongside PQC algorithms during migration [6]. SAP S/4HANA Public Cloud supports secure API-based integration, allowing Treasury, IRS, and state systems to communicate securely while operating in mixed cryptographic environments. This interoperability is essential for maintaining continuity during the transition period and ensuring that critical systems remain functional and secure.

5.5 Compliance and Auditability

Compliance with OMB Circular A-123 and GAO audit recommendations requires that financial systems demonstrate effective internal controls [9,17]. By embedding PQC within SAP S/4HANA Public Cloud, every transaction—tax return, fund transfer, or Medicare claim—can be cryptographically verified and logged. This strengthens auditability, ensuring that future fraud investigations and oversight reviews have tamper-proof evidence secured by quantum-resistant algorithms.

5.6 Transparency and Citizen Trust

SAP S/4HANA Public Cloud also enables real-time dashboards and reporting, extending PQC benefits to transparency initiatives. Treasury dashboards can display PQC-secured fund flows across states, while citizen portals for tax and benefit tracking can assure users that their data is protected against future decryption risks. This transparency reinforces public trust in government finance systems at a time when digital security is under unprecedented scrutiny.

5.7 Strategic Platform for PQC Adoption

By centering PQC adoption within SAP S/4HANA Public Cloud, the U.S. creates a platform-based approach to national financial security:

- Federal and state entities migrate to a common ERP backbone.
- PQC algorithms are embedded into the system-of-record layer.
- Cryptographic standards are uniformly applied across processes.
- Compliance, transparency, and auditability are strengthened at scale.

This ensures that PQC adoption is not fragmented or reactive, but structured, scalable, and future-ready.

6. Risks and Considerations

- **Performance Overheads:** PQC algorithms are computationally heavier; ERP and financial systems must scale accordingly [2].
- **Interoperability:** PQC transition requires coordination across global financial networks (SWIFT, Fedwire).
- **Regulatory Gaps:** U.S. regulators (SEC, OCC, FDIC) have yet to issue PQC-specific mandates.
- **Awareness:** Many financial institutions underestimate the urgency of the quantum threat.

7. Policy and National Interest Alignment

7.1 National Security

Financial systems are critical infrastructure per DHS guidelines [8]. PQC adoption is central to securing this infrastructure against nation-state quantum threats.

7.2 Economic Competitiveness

A secure financial system ensures continued U.S. leadership in global finance. If compromised, trust in the dollar as the global reserve currency could erode.

7.3 Regulatory Alignment

Integrating PQC aligns with **OMB A-123** (risk management) and GAO's calls for strengthening cybersecurity in federal financial systems [9].

7.4 Global Leadership

By leading PQC adoption in finance, the U.S. can shape global standards and reinforce its role as a digital governance leader.

8. Conclusion & Recommendations

Quantum computing represents both an opportunity and an existential risk. For U.S. public and private finance, the risks dominate: without PQC, the nation's financial backbone could be compromised.

Recommendations:

1. **Immediate pilot programs** in IRS, Treasury, and Federal Reserve systems using hybrid cryptography.
2. **Mandates for PQC-readiness** in federal procurement for finance systems.
3. **PQC integration into SAP S/4HANA cloud ERP rollouts** across public sector finance.
4. **National Finance PQC Roadmap**, aligning federal, state, and private financial institutions.
5. **Citizen awareness initiatives** to build trust in quantum-secure digital finance.

By embedding PQC through frameworks like FAST™ and DFRA™, the U.S. can secure its financial systems, reinforce its role as the global financial leader, and prepare national infrastructure for the quantum era.

References

[1] Shor P. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE; 1994. p. 124–134.
[2] National Institute of Standards and Technology (NIST). *Post-Quantum Cryptography Standardization Project*. Gaithersburg, MD: NIST; 2023.
[3] U.S. Small Business Administration, Office of Inspector General. *Significant Weaknesses in SBA's Handling of COVID-19 EIDL and PPP*. Washington, DC: SBA OIG; 2022.
[4] Internal Revenue Service (IRS). *IRS Legacy Systems Modernization Report*. Washington, DC: IRS; 2023.
[5] Mosca M. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*. 2018;16(5):38–41.
[6] Bindel N, Brendel J, Fischlin M, Gonczarowski Y, Günther F, Janson C, et al. Hybrid key encapsulation mechanisms and applications. *Cryptology ePrint Archive*. 2019.
[7] SAP SE. *SAP S/4HANA Public Cloud for Public Finance*. Walldorf, Germany: SAP; 2022.
[8] U.S. Department of Homeland Security (DHS). *National Infrastructure Protection Plan (NIPP)*. Washington, DC: DHS; 2019.
[9] U.S. Government Accountability Office (GAO). *High-Risk Series: Cybersecurity of the Nation*. GAO-21-288. Washington, DC: GAO; 2021.
[10] U.S. Department of Homeland Security (DHS). *Critical Infrastructure Sectors*. Washington, DC: DHS; 2021.
[11] SAP SE. *Intelligent ERP: SAP S/4HANA Cloud Capabilities*. Walldorf, Germany: SAP; 2021.
[12] IBM Research. *AI for Fraud Detection in Public Finance*. Armonk, NY: IBM; 2022.
[13] Accenture. *Robotic Process Automation in Public Finance Modernization*. Dublin: Accenture; 2021.
[14] World Bank. *Blockchain and the Future of Public Sector Finance*. Washington, DC: World Bank; 2022.
[15] Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner R, Smith-Tone D. *Report on Post-Quantum Cryptography*. NISTIR 8105. Gaithersburg, MD: NIST; 2016.
[16] Cybersecurity and Infrastructure Security Agency (CISA). *Analysis of the SolarWinds Cyber Incident*. Washington, DC: CISA; 2021.
[17] U.S. Office of Management and Budget (OMB). *Circular A-123: Management's Responsibility for Enterprise Risk Management and Internal Control*. Washington, DC: OMB; 2016.
[18] Centers for Medicare & Medicaid Services (CMS). *Medicare Fraud & Abuse Reports 2022*. Baltimore, MD: CMS; 2022.
[19] Aggarwal D, Brennen GK, Lee T, Santha M, Tomamichel M. Quantum attacks on Bitcoin, and how to protect against them. *Ledger*. 2018;3:68–90.
[20] National Academy of Public Administration (NAPA). *Modernizing Federal Financial Infrastructure*. Washington, DC: NAPA; 2020.
[21] Brookings Institution. *Fraud in Pandemic Relief Programs: Scale, Patterns, and Lessons Learned*. Washington, DC: Brookings; 2022.
[22] Organisation for Economic Co-operation and Development (OECD). *Digital Government Index 2022: Shaping the Future of Public Finance*. Paris: OECD; 2022.