ISIDORE
QUANTUM

QUANTUM RECKONING

SECURING FINANCE BEFORE THE COLLAPSE

WHITE PAPER

Executive Summary

The global financial system stands at the precipice of an irreversible disruption. The very cryptographic foundations securing $6.8 trillion in daily financial transactions—from SWIFT and ACH to mobile payments and blockchain protocols—are facing an existential threat from quantum computing.

Quantum risk is no longer theoretical. The International Monetary Fund warns that quantum computers will "crack many of the current encryption algorithms and threaten financial stability" across mobile banking, FinTech, and digital currencies. Public Key Infrastructure (PKI)—the foundation of online trust—can be dismantled by Shor's algorithm, making RSA and ECC instantly obsolete. Even more concerning, encrypted data harvested today may be decrypted in the future through "harvest now, decrypt later" attacks, potentially exposing years of sensitive transaction logs, contracts, and personal data to adversarial actors.

The World Economic Forum (WEF) underscores the urgency, stating that "most organizations are woefully unprepared for the quantum-powered future, particularly in terms of cybersecurity." A dangerous gap exists between innovation and cyber resilience, especially in sectors like finance that are often the earliest to adopt new technologies.

Developed in partnership with the NSA and now deployed across land, air, sea, and space, Isidore Quantum® stands as the world's first commercial, AI-enhanced, post-quantum encryption platform built for scale. Rather than simply patching existing PKI vulnerabilities, the platform replaces the outdated model entirely.

Unlike Quantum Key Distribution (QKD), which is fiber-dependent, expensive, and impractical for mobile or edge applications, Isidore operates seamlessly over existing IP, cellular, satellite, and even MIL-STD-1553 tactical networks. No certificates, key loaders, or manual provisioning are needed. Real-time self-healing, rekeying, and zeroization are powered by an AI engine trained on 8 trillion threat signals from Microsoft.

Contents

The financial world ignored the early signals of the 2008 crisis until it was too late. We are seeing those signals again—

Key Findings and Market Call to Action

For banking and FinTech organizations, this means:

- Zero-trust encryption at sub-millisecond latency
- AI-based anomaly detection and autonomous key lifecycle management
- Deployment-ready in under 30 minutes on existing infrastructure
- 60% lower total cost of ownership than legacy HAIPE and PKI stacks

The global financial system stands at the precipice of an irreversible disruption. The very cryptographic foundations securing $6.8 trillion in daily financial transactions—from SWIFT and ACH to mobile payments and blockchain protocols—are facing an existential threat from quantum computing.

This is not theoretical. Isidore is already protecting CubeSats in orbit and classified Defense operations. Over $700M are in the procurement pipeline across sectors, including financial networks.

International Monetary Fund (IMF), and WEF reports make one fact unmistakable: financial institutions that delay adopting quantum-resilient encryption risk the same fate as firms that ignored the rise of algorithmic trading—swift and irreversible disruption by faster, more advanced competitors.

Key findings include:

- Q-Day is approaching faster than predicted. By 2026, asymmetric encryption may be vulnerable even to hybrid classical systems

- NIST and NSA have already deprecated RSA and ECC in favor of Commercial National Security Algorithms (CNSA) Suite 2.0 algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium). PKI is no longer viable for future systems.

- Over $1.2 trillion in cybersecurity upgrades will be required by 2027, with 20 billion devices needing post-quantum upgrades

- Financial institutions face the highest exposure, due to high-value transaction volumes, long-term data sensitivity, and dependency on asymmetric encryption for everything from wire transfers to authentication.

- The financial world ignored the early signals of the 2008 crisis until it was too late. We are seeing those signals again—only this time, the threat is mathematical, irreversible, and global.

- Banks, FINTECH platforms, and regulators must act now to begin migrating to quantum-resilient encryption. Leading the transition ensures a position as one of the digital fortresses of tomorrow. Delaying invites obsolescence and exposure as digital ruins in the post-quantum era.

Isidore Quantum® is not a theory. It is field-tested, regulation-aligned, export-authorized, and built to scale.

Q-Day is not a myth. It’s a countdown.

Introduction

The global financial system is entering a period of unprecedented vulnerability. For decades, public key cryptography—primarily RSA and elliptic curve algorithms—has served as the invisible architecture of digital trust. Encryption methods underpinning credit card payments, stock trades, digital identities, core banking systems, and decentralized finance platforms now face obsolescence. The very algorithms that enabled modern finance are approaching a point of collapse.

At the center of the disruption lies the emergence of quantum computing. Once limited to academic theory, quantum processors are now progressing rapidly, fueled by billions in government and private investment. Machines built on quantum principles are not simply faster—they represent a fundamentally different class of computation. Quantum algorithms, especially Shor’s, have the capability to break widely used asymmetric encryption within minutes, threatening the confidentiality and integrity of digital transactions, financial markets, and global economic stability.

Institutions that delay their response risk falling victim to what the U.S. intelligence community calls the “harvest now, decrypt later” attack model—where encrypted financial data is intercepted today and cracked when quantum capabilities become available. The IMF and WEF both warn that most organizations are unprepared for the cryptographic upheaval ahead, particularly in the banking and FINTECH sectors where risk, liability, and exposure are highest.

The purpose of this white paper **is to sound the alarm**—and present a clear path forward. Urgency surrounds the need to transition to quantum-resistant encryption, and Isidore emerges as the leading solution. As the first commercially deployed, NSA-aligned encryption platform designed specifically for the quantum era, Isidore Quantum has been field-tested across land, sea, air, and space. Built to replace vulnerable certificate-based systems, the platform delivers zero-trust encryption at scale—well before Q-Day arrives.

By combining insights from global financial policy leaders and technical validation across critical infrastructure, this paper equips decision-makers in banking, FINTECH, and regulatory agencies with a roadmap to protect their institutions—and the trust their industries are built on.

The Problem

The foundation of global financial security is under imminent threat from quantum computing.

For over 40 years, financial institutions have depended on public key cryptography—specifically RSA and elliptic curve algorithms (ECC)—to safeguard the integrity of online banking transactions, credit card processing, digital asset custody, SWIFT messages, and interbank authentication. Cryptographic systems were developed under the assumption that no existing algorithm could reasonably break them within practical timeframes using classical computing power.

Quantum computing nullifies that assumption.

Breakthroughs in quantum hardware and algorithms—particularly Shor's algorithm—are rapidly compressing timelines that were once believed to be decades away. A single cryptanalytically relevant quantum computer (CRQC) could decrypt sensitive data protected by RSA or ECC within minutes. The result would be the collapse of the financial system's encryption infrastructure, exposing trillions of dollars in assets, confidential communications, and customer identities to breaches, fraud, and manipulation.

Compounding the risk is the current inaction. Despite urgent warnings from the U.S. National Institute of Standards (NIST) and Technology (NIST), the IMF, and the WEF, most financial institutions have neither begun migrating to quantum-resistant encryption nor inventoried their cryptographic dependencies. Meanwhile, adversaries are already executing "harvest now, decrypt later" campaigns—collecting encrypted data in anticipation of future decryption capabilities.

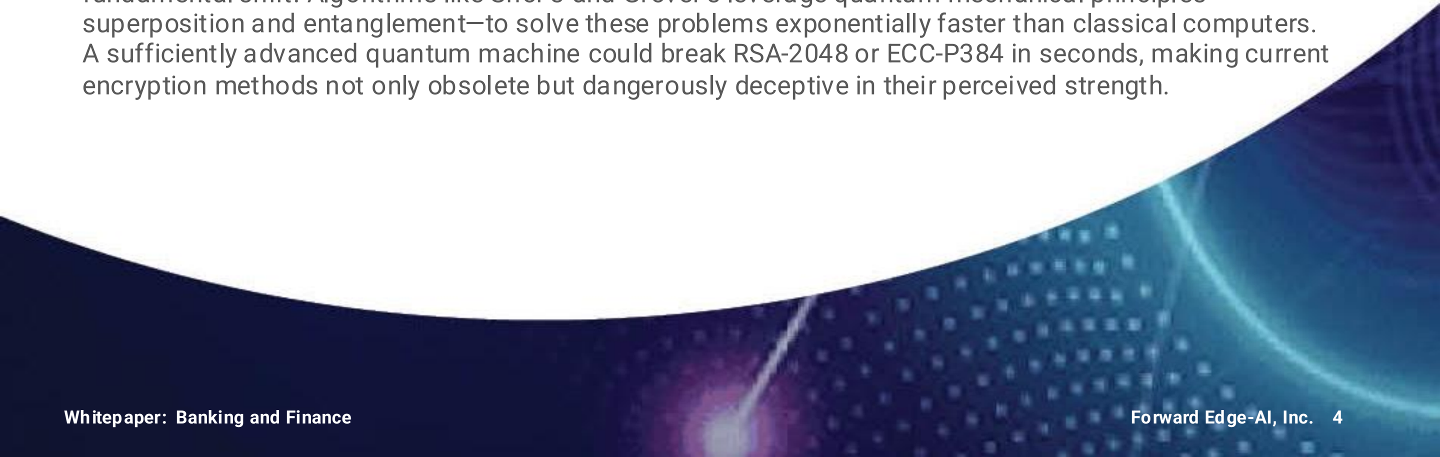
The financial system cannot afford to wait for Q-Day to act.

Banks, FINTECH companies, and regulators urgently need a transition strategy to post-quantum cryptography that is deployable, scalable, and compliant with emerging national and international standards. The absence of such a plan presents a systemic vulnerability—one that will grow exponentially in risk, cost, and complexity the longer it goes unaddressed.

Background

The financial sector is one of the earliest and most enthusiastic adopters of encryption technologies, using cryptographic protocols to facilitate secure digital payments, authenticate user identities, protect interbank transfers, and safeguard billions in daily capital flows. Protocols such as RSA, ECC, and TLS underpin nearly every component of modern banking infrastructure—from online banking portals and trading platforms to APIs powering FINTECH ecosystems.

Cryptographic systems in use today derive their security from the mathematical difficulty of problems such as integer factorization and discrete logarithms. Quantum computing, however, introduces a fundamental shift. Algorithms like Shor's and Grover's leverage quantum mechanical principles—superposition and entanglement—to solve these problems exponentially faster than classical computers. A sufficiently advanced quantum machine could break RSA-2048 or ECC-P384 in seconds, making current encryption methods not only obsolete but dangerously deceptive in their perceived strength.



Recognizing this, NIST and NSA have initiated a sweeping overhaul of national cryptographic standards. RSA and ECC are being deprecated and replaced by post-quantum cryptographic algorithms such as CRYSTALS-Kyber and Dilithium, now formalized under the CNSA 2.0 Suite for National Security Systems.

However, transitioning the financial sector to these new standards is a monumental challenge. Most existing systems are built around centralized PKI, which requires complex key management, human intervention, and is ill-suited for rapid or mobile deployment. The overhead, latency, and cost associated with upgrading legacy cryptographic stacks pose significant barriers for financial institutions—especially given the absence of commercially viable, quantum-resistant alternatives.

Solution

Developed through a joint effort with the NSA, Isidore is the first all-domain, AI-enhanced, CNSA 2.0-compliant encryption platform engineered for real-world, operationally constrained environments. PKI is bypassed entirely through autonomous key lifecycle management and a zero-trust architecture, enabling encryption without reliance on certificates, key loaders, or centralized infrastructure. With deployments spanning air, land, sea, and space—including a SpaceX-launched CubeSat and DARPA drone vessels—Isidore has been rigorously field-tested, demonstrating resilience and readiness for immediate use in critical environments.

By combining NSA-grade cryptographic algorithms with real-time AI-based anomaly detection and autonomous self-healing, Isidore provides a scalable, affordable path to quantum resistance—one that financial institutions can deploy now, not years from now.

The research is clear. The threat is imminent. The infrastructure is fragile. And the technology to protect it already exists.

Isidore — Operational Quantum Resilience for Finance

To meet the urgent need for post-quantum cybersecurity in the financial sector, Forward Edge-AI introduces Isidore—a next-generation encryption platform engineered to replace legacy PKI and deliver immediate, scalable protection against quantum-enabled threats.

Isidore moves beyond theory. Aligned with NSA standards and compliant with CNSA 2.0, the platform has been field-tested across air, land, sea, and space. No other commercial quantum-resistant encryption solution offers the same level of operational readiness across disconnected, mobile, and high-performance environments—especially in financial systems where downtime, latency, and complexity cannot be tolerated.

How Isidore Solves the Problem

1. Bypasses Vulnerable PKI Architectures

Traditional encryption systems depend on centralized PKI—certificates, key loaders, and manual provisioning processes—that are fundamentally misaligned with the requirements of quantum-resilient security. Isidore removes those dependencies altogether. Through ephemeral keying, autonomous lifecycle management, and zero-trust architecture, the platform ensures no node, session, or device is implicitly trusted.

2. Implements NSA-Approved Quantum-Resistant Algorithms

Isidore integrates the full suite of CNSA 2.0 algorithms:

- CRYSTALS-Kyber for key encapsulation
- CRYSTALS-Dilithium for digital signatures
- AES-256 and SHA-384/512 for symmetric encryption and hashing

Algorithms in use have been validated by NIST and mandated by the NSA for deployment in National Security Systems—providing strong assurance of cryptographic durability against quantum-enabled attacks.

3. AI-Powered Threat Detection and Self-Healing

At its core, Isidore includes a Machine Learning engine trained on over 8 trillion security signals from Microsoft, enabling:

- Real-time anomaly detection
- Cyber-immune response to emerging threats
- Autonomous rekeying or zeroization upon tamper detection

Such capability enables financial institutions to detect and respond to threats in advance of compromise, significantly reducing overall risk exposure.

4. Plug-and-Play Deployment Across Financial Infrastructure

Isidore operates across:

- IP, Ethernet, fiber, wireless, CAN Bus, and SATCOM
- Edge devices, datacenters, cloud platforms, and air-gapped networks
- Legacy systems without requiring infrastructure overhauls

Such flexibility empowers financial institutions to deploy post-quantum security in minutes, avoiding operational disruption and minimizing integration costs.

5. Cost-Efficient, Subscription-Based Model

Unlike traditional systems requiring $100,000+ capital investment, Isidore is available through:

- Hardware units priced from $500–$10,000
- SaaS subscriptions from $368–$500/month per device

A 60% lower Total Cost of Ownership (TCO) makes quantum resilience attainable for institutions of every size—from local community banks to global investment firms.

Benefits to the Financial Sector

- Protects against quantum decryption of financial transactions
- Enables compliant migration from RSA and ECC to CNSA 2.0 standards
- Reduces operational overhead by eliminating PKI complexity
- Extends encryption to mobile, remote, and disconnected endpoints
- Strengthens customer trust by ensuring continuity and resilience

Isidore is a strategic shield that enables banks, FINTECH firms, and regulators to transition confidently into a quantum-threatened world without waiting for experimental solutions or expensive infrastructure overhauls.

The quantum clock is ticking. Isidore is ready now.

Supporting Evidence: Proven Performance and Strategic Validation

Isidore has been rigorously tested, field-validated encryption platform trusted by defense agencies, critical infrastructure operators, and technology partners worldwide. Its proven performance across real-world environments provides the financial sector with a clear, deployable path to quantum resilience.

1. Industry Recognition and Strategic Endorsements

Developed in collaboration with the NSA and aligned with the Commercial National Security Algorithm Suite (CNSA 2.0), Isidore integrates post-quantum cryptographic standards—including CRYSTALS-Kyber and Dilithium—as required for National Security Systems and soon, commercial financial networks.

- Validation by Microsoft, Lumen Technologies, and Cubic Corporation included independent testing of Isidore's performance under high-throughput, real-time constraints using industry-grade systems from Spirent, Juniper, and Nokia. Evaluations confirmed:
    - ○ Sub-millisecond encryption latency
    - ○ Dual-VLAN zero-trust capability
    - ○ Superior throughput compared to legacy MACsec and IPsec devices

2. Field-Proven Across All Domains

Isidore is the only commercial quantum-resistant encryptor successfully deployed in air, land, sea, and space:

- **Space:** Launched aboard SpaceX Transporter-13 in March 2025, Isidore secured Rogue Space Systems’ Barry-2 CubeSat, marking the first use of quantum-resistant encryption in a CubeSat application.
- **Sea:** Deployed aboard the Defense Advanced Research Projects Agency’s (DARPA) NOMARS autonomous vessel for securing command and control systems in long-duration, unmanned maritime operations.

- **Land & Air:** Operational across classified Army and Air Force networks, as well as with Special Operations Command, and US Space Force mission profiles.

Deployments across varied domains validate Isidore's survivability and cryptographic performance in high-threat environments—the same conditions under which financial infrastructure must remain secure amid cyber or geopolitical instability.

3. Commercial Demand and Adoption Traction

- A robust delivery pipeline across defense, telecom, and critical infrastructure sectors—representing over $700 million in projected revenue including SaaS contracts.
- Over 1,000 stakeholder interviews conducted with CIOs, CISOs, US military, and compliance leaders across the government, financial services, insurance, and FINTECH to align Isidore's deployment strategy with regulatory and operational requirements.
- Zero ITAR/EAR restrictions, enabling international deployment—critical for global banks and payment processors with cross-border infrastructure.

Cost and Risk Reduction vs. Legacy Solutions

Feature	Isidore	Traditional PKI Systems	QKD Solutions
Deployment Time	Under 30 minutes	Weeks to months	12–18 months
TCO (5 yrs)	↓ 60%	High (Cert. Mgmt., PKI)	Extremely High
Mobility & Edge Use	Fully supported	Limited	Not viable
Real-time AI Defense	Yes	No	No
Scalability	Plug-and-play	Fragmented	Not ready

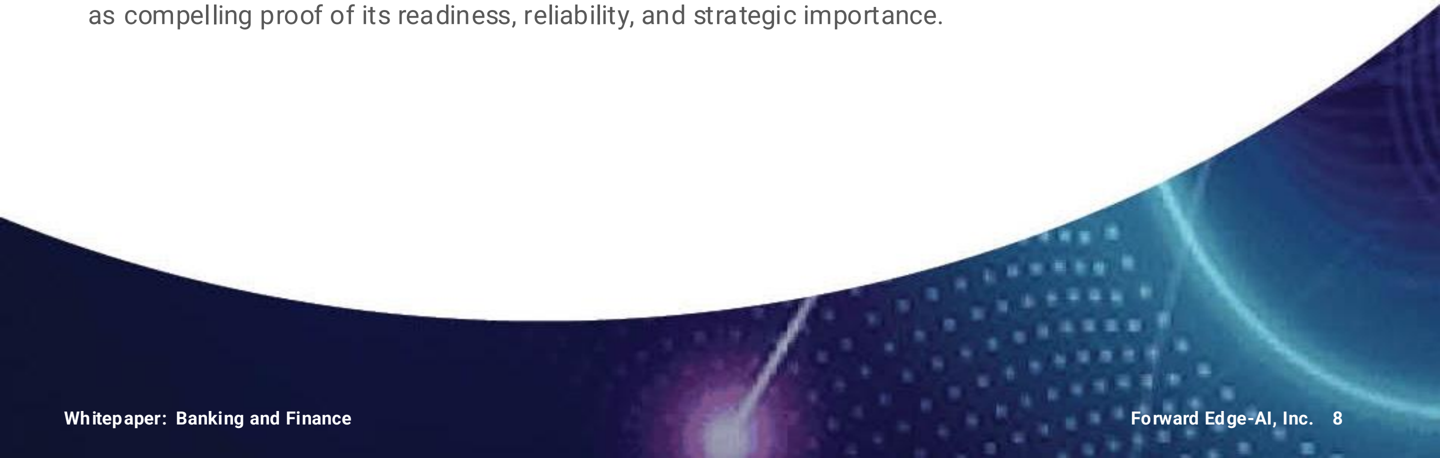
Isidore's plug-and-play architecture ensures immediate utility without costly infrastructure upgrades—making it ideal for financial institutions needing zero-downtime migration paths.

5. Alignment With Global Cybersecurity Roadmaps:

- Fully compliant with NIST's Post-Quantum Cryptography Standardization Program
- Supports U.S. Executive Orders 14028 and 14158 on quantum risk mitigation and AI integration
- Meets NSA requirements for Commercial Solutions for Classified (CSfC)
- Integrates with Microsoft Sentinel, Defender, and Azure security signals for enterprise threat correlation

Summary

Whether safeguarding an AI-driven CubeSat or securing financial clearinghouses, Isidore has demonstrated cryptographic integrity, operational flexibility, and AI-driven cyber resilience in the most demanding conditions. Its adoption by defense leaders, telecom giants, and classified programs serves as compelling proof of its readiness, reliability, and strategic importance.



The financial system's quantum defense must be proactive—not reactive. Isidore delivers that defense today.

Conclusion

The global financial system is approaching a pivotal moment. Quantum computing is not a distant concern—it is a near-term disruptor with the potential to unravel the cryptographic foundations of banking, FinTech, capital markets, and digital asset ecosystems. Legacy encryption methods such as RSA and ECC, long considered secure, are mathematically guaranteed to fail once quantum capabilities mature.

Warnings from the IMF, World Economic Forum, and NSA are clear: quantum threats are accelerating, and most institutions remain dangerously unprepared. The cost of inaction is not theoretical—it includes systemic data breaches, irreversible financial fraud, legal liabilities, and the erosion of public trust.

Isidore delivers a decisive solution as the first commercially available, NSA-aligned, AI-powered encryption platform purpose-built for the post-quantum era. Field-tested across the harshest operating domains—space, sea, air, and cyber—the platform provides:

- Quantum-resistant encryption using CNSA 2.0 algorithms, including CRYSTALS-Kyber and Dilithium
- Zero-trust, PKI-free architecture, eliminating certificates, key loaders, and human error
- AI-driven anomaly detection and autonomous threat response
- Rapid deployment without infrastructure overhauls
- 60% lower total cost of ownership than legacy solutions
- Scalability across financial systems, from core banking to edge devices and cloud APIs

With over $700M units in the procurement pipeline, active deployments in classified missions, and partnerships with Microsoft, Lumen, Cubic, and SpaceX payload integrators, Isidore Quantum is more than ready—it's already securing tomorrow's most vulnerable systems.

The takeaway is urgent but simple:

Financial institutions must act now to safeguard digital trust in a quantum world.
Isidore is the only solution engineered to meet this challenge today.

In a race against quantum decryption, speed, scale, and security win.
Isidore Quantum delivers all three.

The financial system’s quantum defense must be proactive—not reactive. Isidore delivers that defense today.

Conclusion

Quantum computing presents a rapidly accelerating and existential threat to the cryptographic foundations of the global financial system. PKI—including RSA and ECC encryption protocols—supports nearly all secure digital transactions, from banking APIs to blockchain-based assets. Algorithms like RSA and ECC are mathematically guaranteed to collapse under the power of CRQCs, which can leverage Shor’s algorithm to decrypt sensitive financial data within minutes.

The threat is no longer hypothetical. The IMF and WEF have confirmed that financial systems face heightened risk due to the enduring sensitivity of transaction records and the industry's dependence on asymmetric cryptography. Even more concerning, adversaries are already conducting “harvest now, decrypt later” campaigns—stockpiling encrypted data with the intent to break it once quantum computing becomes viable.

By 2027, U.S. mandates will require critical infrastructure to adopt post-quantum standards. Yet transitioning away from PKI—an entrenched system spanning decades—could take years. Most institutions remain dangerously unprepared.

Isidore offers a decisive, field-tested alternative purpose-built for the post-quantum era. Developed in collaboration with the NSA and fully compliant with CNSA 2.0, Isidore replaces PKI with a protocol-agnostic, zero-trust architecture. Data is encrypted directly at the physical layer, removing dependence on certificates, key loaders, and manual provisioning. Operational readiness is what sets Isidore apart:

- Sub-millisecond latency, even in tactical or mobile environments
- AI-based anomaly detection trained on 8 trillion threat signals
- Autonomous key rotation and zeroization
- No infrastructure overhaul required—works across IP, CAN Bus, SATCOM, and legacy networks
- 60% lower total cost of ownership compared to traditional HAIPE or PKI stacks

Isidore has already secured assets in every operational domain: satellites, maritime systems, and classified ground networks. Over $700 million in active procurement pipelines across defense, finance, and telecom sectors further underscores market confidence.

Key Takeaway:

Quantum computers are on track to break the encryption securing global financial systems by 2026—rendering billions in daily transactions, digital identities, and stored data vulnerable overnight. Institutions that fail to transition now face irreversible breach, legal liability, and systemic collapse. Isidore is the only NSA-aligned, AI-powered encryption platform ready to replace PKI today—without downtime, without certificates, and without waiting for Q-Day to strike.

Call to Action: Secure Your Future Before 2027

The clock is ticking toward Q-Day—the moment quantum computers render traditional encryption obsolete. For financial institutions, FINTECH innovators, and digital custodians, the consequences of delay are catastrophic: compromised transactions, regulatory exposure, reputational collapse, and systemic risk to the global economy.

By 2027, U.S. federal mandates require all critical infrastructure and financial systems to adopt post-quantum encryption standards. Yet, migrating from vulnerable PKI-based systems to compliant, operationally viable alternatives takes years—not months. Transitioning safely and efficiently requires acting now, while time and trust remain on your side.

Isidore is your first-mover advantage.

It's not an experiment—it's an NSA-aligned, AI-powered platform already in use across national defense, space, and telecom networks. It's fast to deploy, scalable across environments, and affordable for institutions of any size.

Here's what to do next:

- Schedule a readiness assessment with the Isidore Quantum deployment team
- Inventory your cryptographic exposure across APIs, databases, and network layers
- Begin phased integration with a pilot deployment—no rip-and-replace needed
- Achieve CNSA 2.0 compliance ahead of the federal deadline
- Secure customer trust by leading the transition, not reacting to the breach

Waiting until 2027 is not a strategy—it's a liability. Transitioning now is leadership.

Let your institution be remembered not for how it reacted to Q-Day—but for how it anticipated it.

Contact Forward Edge-AI to begin your transition to Isidore today.
Because in the quantum era, trust must be engineered—not assumed.

About

Forward Edge-AI, Inc. is a U.S.-based technology company pioneering the development and deployment of secure, AI-powered, and quantum-resilient solutions for national security, critical infrastructure, and the financial sector. Founded with the mission to protect data-in-transit at global scale, Forward Edge-AI combines government-grade cryptography with advanced machine learning to deliver next-generation cybersecurity platforms ready for the quantum era.

At the heart of its innovation portfolio is Isidore, the world's first commercial, all-domain, post-quantum encryption solution. Developed in collaboration with the National Security Agency (NSA) and validated by strategic partners including Microsoft, Lumen Technologies, and Cubic Corporation, Isidore Quantum is actively protecting sensitive systems across land, sea, air, and space.

Mission

To accelerate the global transition to quantum-resilient cybersecurity by delivering AI-enhanced encryption solutions that are compliant, autonomous, and scalable—empowering public and private sectors to defend against emerging threats before they materialize.

Leadership

Forward Edge-AI is led by a seasoned executive team with deep expertise in cybersecurity, defense technology, AI, and regulated industries:

- **Eric Adolphe, Founder & CEO** – Serial entrepreneur, National Inventors Hall of Fame honoree, attorney, and NSA-licensed technology innovator
- **LTG (Ret.) Ross Coffman, President** – Former Deputy Commander, U.S. Army Futures Command
- **Dr. Benjamin Harvey, EVP of Advanced Research** – Former Chief of Data Science, NSA
- **Riaan Gouws, CTO** – Veteran systems architect with a focus on secure communications, AI, and cloud technologies

Together, the team has built a quantum-secure platform that's not only mission-ready—but market-ready.

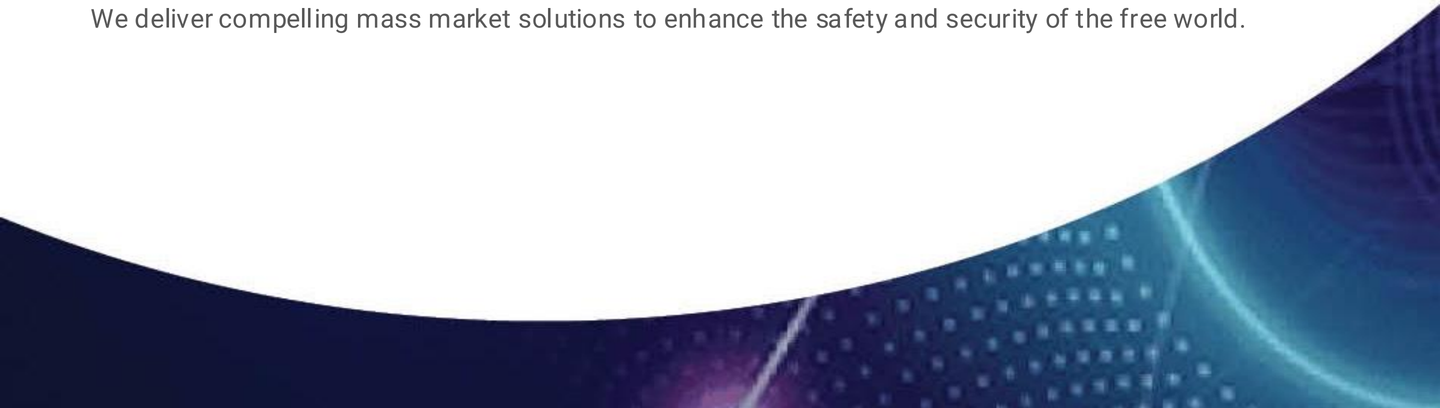
Contact Us

To schedule a quantum readiness assessment or learn more about transitioning your financial infrastructure with Isidore, contact:

Brandon@Forwardedge.ai

https://forwardedge.ai/isidore/

We deliver compelling mass market solutions to enhance the safety and security of the free world.



Appendix A: References

1. Deodoro, Jose, Michael Gorbanyov, Majid Malaika, and Tahsin Saadi Sedik. Quantum Computing and the Financial System: Spooky Action at a Distance? IMF Working Paper WP/21/71. International Monetary Fund, March 2021. https://www.imf.org/en/Publications/WP/Issues/2021/03/19/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-503014.

2. World Economic Forum. Embracing the Quantum Economy: A Pathway for Business Leaders. In collaboration with Accenture. January 2025. https://www.weforum.org/reports/embracing-the-quantum-economy.

3. Forward Edge-AI, Inc. Isidore Quantum vs. Quantum Key Distribution (QKD). White Paper, April 2025.

4. Forward Edge-AI, Inc. Securing Data-in-Transit with Quantum-Resistant Cryptography. White Paper, 2025.

5. Forward Edge-AI, Inc. Q-Day: Adapt or Perish – From Stirrups to Quantum Computing. Strategic White Paper, 2025.

6. Forward Edge-AI, Inc. FEAI Isidore Quantum Commercial Introduction Memorandum. April 2025.

7. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization Project. U.S. Department of Commerce. Accessed May 2025. https://csrc.nist.gov/projects/post-quantum-cryptography.

8. National Security Agency (NSA). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). U.S. Department of Defense, 2022. https://media.defense.gov/2022/Sep/07/2003075016/-1/-1/0/CNSA-SUITE-2.0-FACT-SHEET.PDF.

9. Lumen Technologies. Independent Test Results: Isidore Quantum Encryption Platform. Technical Evaluation Report, March 2025.

10. Forward Edge-AI, Inc. FEAI Quantum Encryption Platform: Investment Presentation. April 2025.

Appendix B: References

Acronyms

AES	Advanced Encryption Standard CQTS Cross-Quantum Technology Systems
CRQC	Cryptoanalytically-Relevant Quantum Computer CSfC Commercial Solutions for Classified
HiPS	High-Performance Superconducting Qubit Systems HNDL Harvest Now, Decrypt Later
LPS	Laboratory for Physical Sciences LWE learning-with-errors
NEQST	New & Emerging Qubit Science & Technology
NIST	National Institute of Science and Technology
NQCO	National Quantum Coordination Office
NSA	National Security Agency NSS National Security Systems
PKI	Public-key Infrastructure, asymmetric encryption scheme, two different keys are used to encrypt/decrypt PQC Post-Quantum Cryptography
PSK	Pre-shared key, symmetric encryption scheme, same key is used to encrypt/decrypt QC Quantum Computer
QCISS	Quantum Characterization of Intermediate-Scale Systems QIS Quantum Information Science
QiS	Qubits in Silicon Program
QR	Quantum-Resistant (algorithms)
QRC	Quantum-Resistant Cryptography
SHiFT	Stable High Fidelity Trapped Ion Systems SIS short integer solution
TCO	Total Cost of Ownership

.