



Payments
Innovation
Alliance®

Protecting Payments in the Quantum Era

What You Need to Know

Protecting Payments in the Quantum Era

What You Need to Know

The computing world is on the cusp of a paradigm shift that is unlocking unprecedented computational power. Fueled in part by the advent of quantum computing, this revolution promises to transform how organizations operate and solve complex problems. Quantum computing leverages the principles of quantum mechanics to process information in fundamentally new ways, offering a different computational approach that promises to tackle challenges and solve problems currently intractable for classical computers.

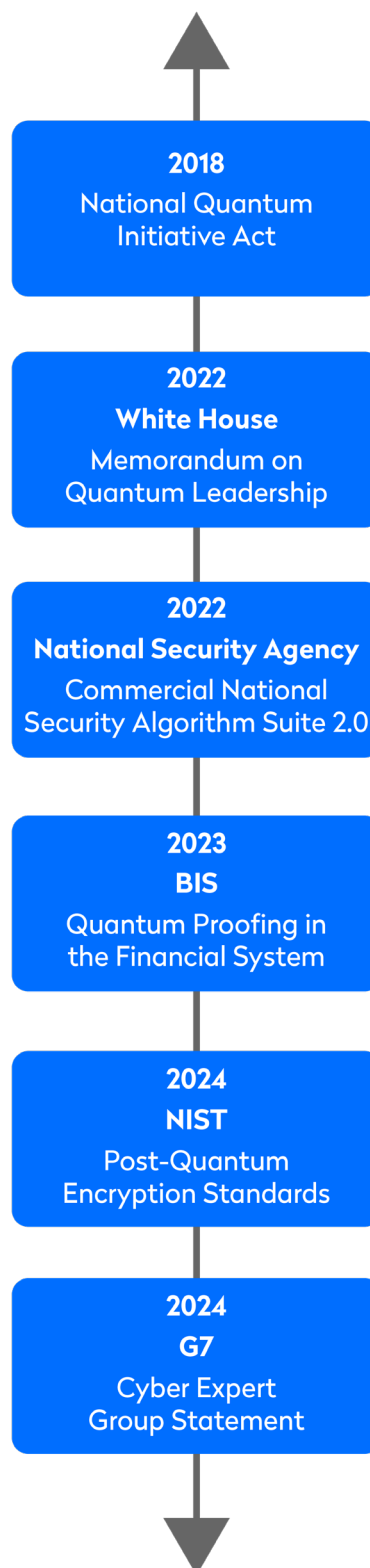
By the decade's end, quantum computing could impact computing strategies across industries, providing substantial innovation in finance, payments, fraud detection, anti-money laundering detection and behavioral analysis. Quantum computing may influence innovation in machine learning, optimization, sustainability and more. Working in conjunction with classical computers and cloud-based architectures, quantum computing could even address problems we have not yet imagined. The opportunities for society and the economy are enormous.

However, quantum computing is a double-edged sword and presents significant threats to the current data storage and communication cryptography used across industries, including the payments sector. The implications are important as the arrival of quantum computing threatens the core cryptography used to secure website connections, banking transactions, email exchanges, virtual private networks (VPNs), e-commerce, digital signatures and more. This topic has recently come to the forefront as new cryptographic standards have been identified by the U.S. National Institute of Standards and Technology (NIST) and released to safeguard against these threats.

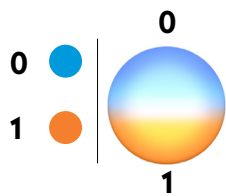
In support of this initiative, NIST released a fact sheet to help businesses understand how quantum computing will impact cybersecurity and to urge them to start planning for future-proof cryptographic standards. The fact sheet advises companies to form a team to identify all technologies at risk from quantum threats and prepare for the upcoming NIST guidelines on secure cryptographic practices in the quantum era. And in August 2024, NIST published [standardized post-quantum encryption standards](#).

Major Initiatives on Quantum Threats

Click on timeline events for original source documents.



This document is a primer on quantum computing, explaining key concepts and how it differs from classical computing. It explores the potential applications of quantum computing in the financial sector, particularly in payments, highlighting the opportunities for innovation and efficiency. The document also addresses the significant threats quantum computing poses to current cryptographic standards, using the four-corners model¹ to illustrate these vulnerabilities in payment networks. Finally, it discusses recent developments in quantum technologies, the urgent need for quantum-safe cryptographic solutions and proactive next steps to prepare leaders in the payments industry for the quantum era.



How Quantum Works: Bits vs. Qubits

The foundation underlying classical computing is the bit, a unit of information that can exist in two distinct states, 0 or 1, which we call a binary state. This simple representation enables data storage and manipulation and has served us well for decades. In contrast, quantum computing is a form of computation that utilizes core principles of quantum mechanics, characteristics referred to as superposition, entanglement, and interference, to perform complex calculations and process vast amounts of information that promises to be much faster than classical computers. While these concepts are essential for understanding why quantum computing differs, it is understandable if they initially seem complex.

Superposition

Instead of using traditional bits (0s and 1s) to represent information, quantum computers use quantum bits, or qubits, which can exist in multiple states simultaneously thanks to superposition. A traditional bit is like a spinning coin that lands definitively as either heads or tails. A qubit is able to reflect heads or tails but adds the ability to remain in both states while the coin is spinning, offering a third representation of information. The qubit will remain in both states until it is observed, at which point it is “forced” to collapse into a defined outcome.

Superposition enables a qubit to store all the possible values of the quantum state. This superposition property creates an exponentially more significant computational processing advantage over classical computers.

Entanglement

Entangled qubits can become linked and instantaneously affect each other's state, regardless of the distance separating them. Entanglement means that measuring one entangled particle will instantly determine the state of its partner, even if they are light-years apart. Entangled particles form a single unified system called a superposition of states and enable the simultaneous evaluation of all possible outcomes of a given calculation, further increasing computational capacity.

Interference

A third aspect of quantum computing that plays a vital role in quantum-based algorithms is the notion of interference, which increases the probability of the desired outcome and reduces the likelihood of the non-desired outcome of algorithms in a quantum computer. Imagine two stones tossed into a pond, each creating ripples in the water. Some ripples combine to form more significant ripples, while others cancel each other out.

Quantum processors harness this property, which occurs when the waves of two or more particles overlap, creating a phenomenon known as constructive or destructive interference. When the waves overlap, they constructively interfere, resulting in a more substantial wave. Conversely, when the peak of one wave meets the trough of another, they destructively interfere, canceling each other out.

¹ Retail Payment Systems IT Examination Booklet, Federal Financial Institutions Examination Council, 2016, page 5.

Combined, the properties of superposition, entanglement and interference make quantum computing a different paradigm of processing that can solve complex problems more efficiently. Quantum computing uses specialized hardware and algorithms that use quantum mechanics to solve complex problems that classical computers or supercomputers cannot solve quickly enough.

Quantum Applications: Finance and Payment Improvements

Quantum computing holds immense promise for the financial sector because it processes complex computations much faster than classical systems. This speed and efficiency may improve fraud detection, risk management, payment network routing and algorithmic trading, ultimately contributing to enhanced customer experience and increased profitability. Quantum algorithms can also potentially optimize portfolio allocation and asset pricing strategies, providing banks with enhanced insights for informed decision-making. Other use cases will extend to finance, payment networks, fraud detection, anti-money laundering detection and behavioral analysis by efficiently simulating economic scenarios and variables, providing deeper insights into financial risks and opportunities.

In payments and finance, quantum computers' strength in solving complex optimization problems is already being applied to the central bank clearing problem² and improving financial logistics, such as routing payments more efficiently in global banking networks—tasks that are challenging for classical computers. Moreover, they promise to improve fraud detection, as quantum sorting algorithms allow for faster processing of complex financial data and better detection and mitigation strategies.

The Bank for International Settlements (BIS) has initiated a project called “quantum leap”³ along with central banks of France and Germany. The objective of this project is to safeguard the financial system from quantum threat. They have done first phase of testing between the central banks.

However, the industry players in US financial system need to be aware of this threat and plan accordingly.

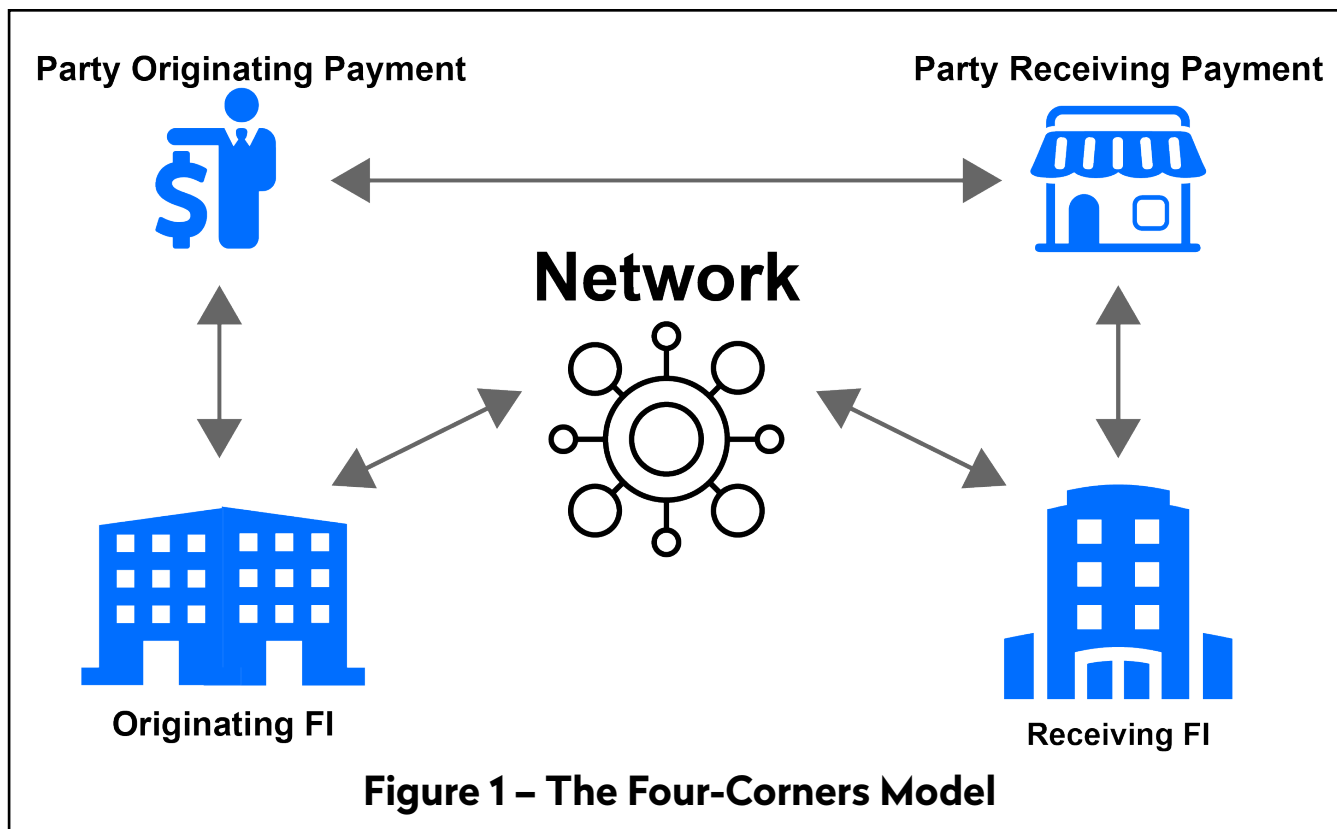


The Quantum Threat

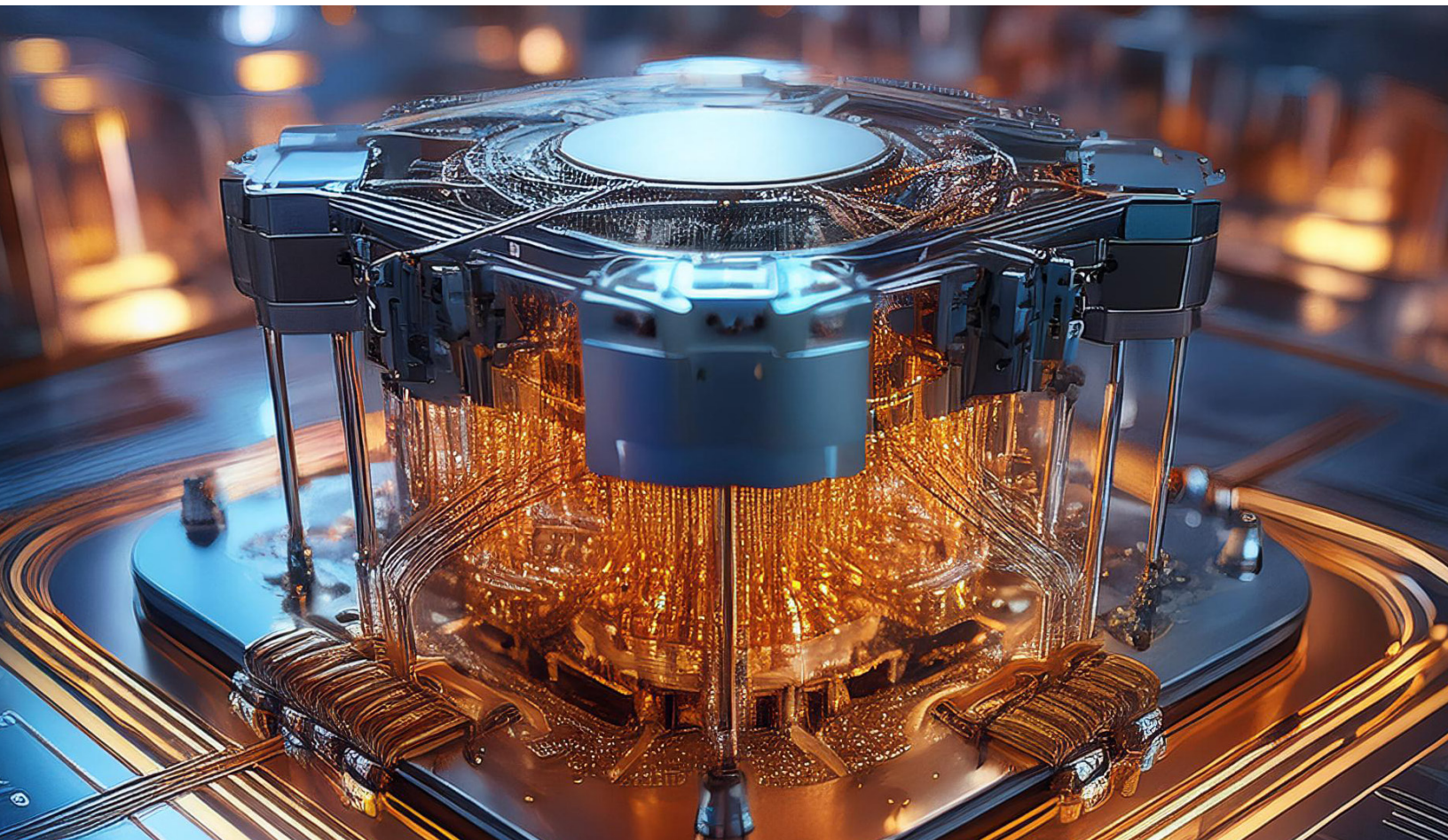
The financial industry's digital infrastructure and communications heavily rely on cryptography to safeguard sensitive digital information. Whether to securely store customers' personally identifiable information (PII), access the internet through a VPN, or ensure the integrity of a payment placed on a mobile application, cryptographic algorithms play a central role in many critical functions within the financial system. Cryptography is embedded in almost every finance application, including data storage and transmission, communication links with identity verification and securing most internet-based operations.

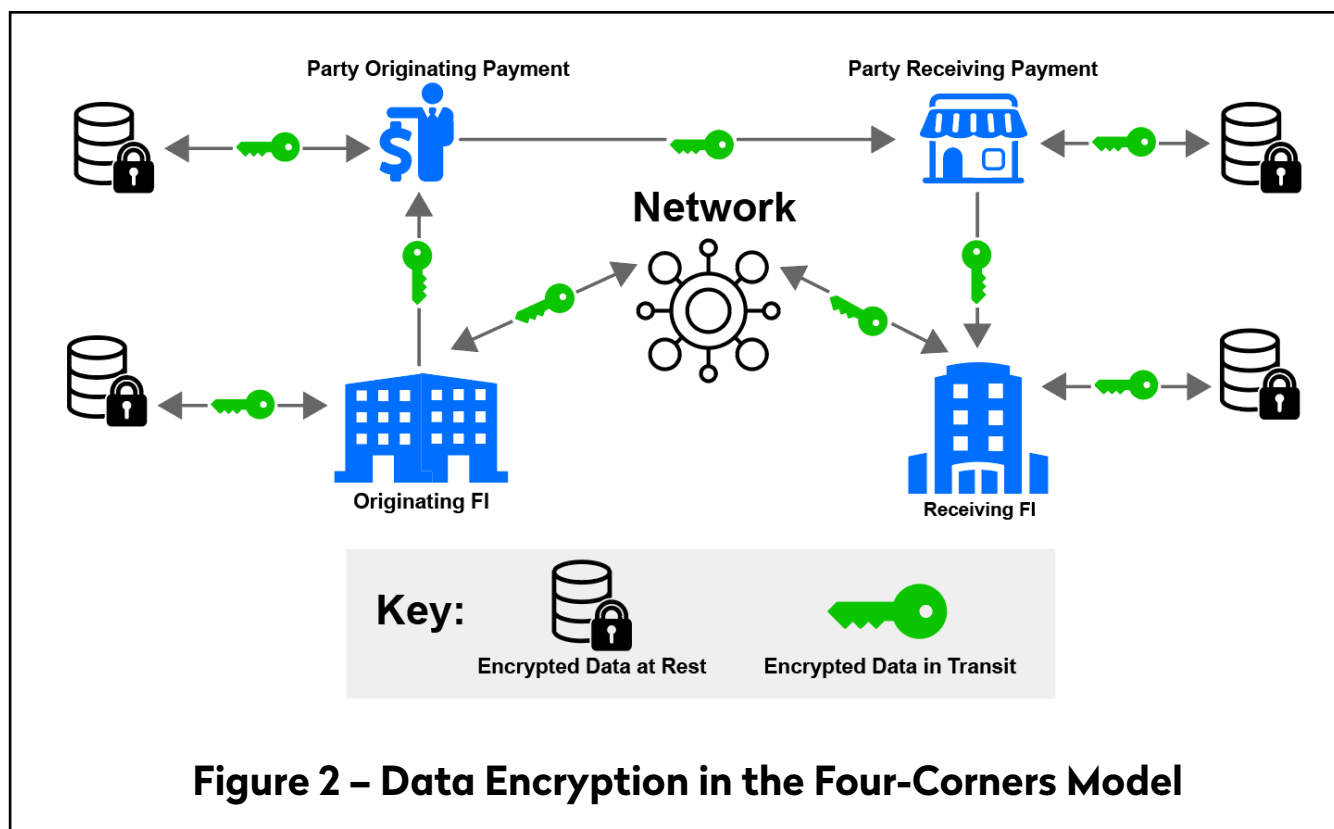
² [Improving the Efficiency of Payments Systems Using Quantum Computing.](#)

³ [BIS Quantum Proofing in the Financial System.](#)



In assessing the threat of quantum computing specific to payments, it is helpful to consider the four-corners model. This model broadly generalizes different payment networks, with the corners being: the party originating the payments instruction; the originating financial institution (FI); the receiving FI; and the party receiving the payments instruction, as illustrated in the figure above.





In this model, quantum computing poses significant threats to the cryptographic foundations that secure transactions between and the storage at each corner. For example, a merchant's payment instructions could be intercepted and decrypted by quantum computers if not protected in transit by quantum-safe encryption, and the storage of the instructions by the receiving party could be compromised if not securely stored on their device. The diagram above illustrates the four-corners model and where data encryption occurs with data in transit or at rest. Decision-makers touching any corner or connection between them should consider how quantum computers will change their security landscape.

Modern public-key encryption protocols protect against most technological tools used by today's threat actors because classical computing could take hundreds (if not thousands) of years to decipher cryptography. Quantum computers will be capable of breaking these math-based asymmetric key cryptographic algorithms in a matter of seconds. Deciphering cryptography is possible because quantum computing can leverage specialized algorithms to significantly reduce the time to solve the mathematical problems underlying today's encryption. Quantum computers use superposition to simultaneously see across several potential solutions to an algorithm and select the correct one.



Research indicates a potential total of \$3.3 trillion in indirect losses.

The impact is potentially dramatic as bad actors could be able to decrypt exfiltrated data, forge digital signatures and fraudulently authenticate services. It is essential to state that no quantum computer is available today to crack the predominant cryptographic schemes currently being used. The consensus prediction is we can anticipate such quantum computing capabilities to emerge within this decade. However, the question of when quantum

computing will break cryptography is misleading, for it implicitly frames the threat to be sometime in the future. The threat is today; the impact is in the future. Data that is considered securely protected today is already compromised by a future quantum adversary using “harvest now, decrypt later” schemes.

Research by the Hudson Institute⁴ analyzes the economic impact on the quantum threat to Fedwire system. Their analysis demonstrates that a quantum hack would result in declines in annual real GDP ranging from over 10 percent in the baseline scenario to 17 percent in the maximum impact attack scenario. Furthermore, the results indicate that such a decline in aggregate output would comprise a total of between \$2 and \$3.3 trillion in indirect losses alone, as measured by GDP-at-risk.

All data - past, present and future - that is not protected using quantum-safe security will be at risk, and the longer we postpone the migration to quantum-safe standards, the more data will be at risk. The quantum computing era will unfold over time, but the need for quantum-safe solutions is immediate. Both the historic and current complexity of cryptosystems—even pre-quantum computing—can require many years of strategic planning, preparation, and remediation. Business, technology, and security leaders must now develop a quantum-safe strategy roadmap.

Recent Developments in Quantum Technologies

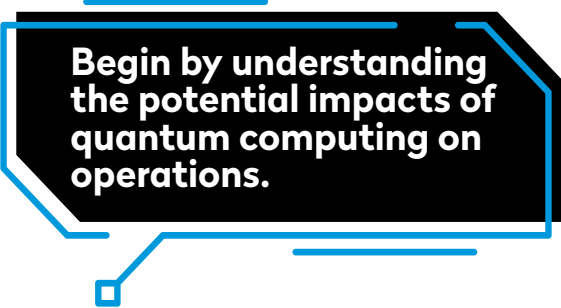
Quantum computing is a relatively new field, and challenges exist. Tracking the advance of quantum computing can be arduous as different vendors describe their progress using various metrics (e.g., logical or physical qubits, quantum volume, etc.). These measures will also vary by the type of quantum computer technology being used. Defining these units is beyond the scope of this paper. Still, one example of a metric to monitor is logical qubits, which many consider fundamental units of a scalable quantum computer. A logical qubit comprises multiple underlying physical qubits that act as a single qubit with lower error rates. One main challenge is qubits’ fragility, which can quickly lose their quantum properties due to slight disturbances. This phenomenon, called decoherence, makes error correction mechanisms essential for reliable quantum computation.

Another significant challenge is building scalable systems that contain and control large numbers of interconnected qubits. Connectivity is a sizable engineering challenge, as maintaining the precise environmental conditions required to stabilize qubits, such as extremely low temperatures and high vacuum levels, adds complexity and cost to these systems. There are additional hurdles to overcome in devising use cases and educating people on how to build and use quantum computers.

These challenges are being addressed. Companies are creating thousand-plus (1,000+) qubit computers (up from 433 in 2022), and two recent papers from IBM and Microsoft have shown dramatic improvements in error correction techniques. These advancements increase confidence that we will see helpful quantum computing within this decade. In addition, quantum systems are rapidly becoming computational tools, offering benefits to computing fields beyond quantum computing.

⁴ [Prosperity at Risk: The Quantum Computer Threat to the US Financial System](#)

To effectively integrate quantum capabilities, a hybrid computing architecture is needed to create quantum-centric supercomputers, which will incorporate quantum processors, classical processors, quantum communication networks and classical networks, all working together to transform how we compute in the future. Companies such as IBM are already developing this type of infrastructure and runtime environments, envisioning a future where quantum systems play a central role in high-performance supercomputing: [IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility](#).



Begin by understanding the potential impacts of quantum computing on operations.

Call to Action and Conclusion

As the quantum era approaches, leaders in the payments industry must prepare for the impending changes and challenges. The quantum threat to cryptographic security is real and imminent, potentially disrupting the very foundations of digital transactions. Ensuring this trust calls for immediate action to future-proof systems and ensure the continued protection of financial operations. Key steps to initiate include:

Awareness and Education	Increase awareness and understanding of quantum computing and its implications among stakeholders within your organization.
Identify and Prioritize Crown Jewels	Develop a comprehensive inventory of the organization’s most critical data and assets, considering both technical and business perspectives.
Risk Assessment	Conduct a thorough assessment of your current cryptographic infrastructure and that of your providers to identify vulnerabilities that quantum computers could exploit.
Adopt Quantum-Safe Cryptography	Begin transitioning to quantum-safe cryptographic algorithms as recommended by NIST and other cybersecurity authorities.
Collaborate and Innovate	Engage with NACHA’s Payments Innovation Alliance, industry peers, research institutions, and technology providers to stay abreast of the latest developments in quantum computing.
Strategic Planning	Develop a comprehensive quantum-safe strategy and roadmap that aligns with your organization’s timelines for technology upgrades, resource allocation, and contingency plans.

Quantum computing, though still in its early stages, holds transformative potential for the payments industry by redefining the limits of computational power. Quantum computing will complement classical computing by handling complex, specialized tasks that classical systems struggle with today. In the payments sector, this synergy could lead to unprecedented speed and security in processing transactions, opening possibilities for innovation and efficiency beyond our reach.

Financial services organizations are responsible for large volumes of confidential customer data and intellectual property. Because this data is high value and heavily regulated, a data breach at a financial institution can result in substantial material damages, reputational loss, and legal liability. Considering these risks, financial services organizations must proactively address evolving cybersecurity threats, particularly those related to the advent of quantum computing.

The payments industry's business, technology, and security leaders must take proactive steps to address the quantum threat. Begin by understanding the potential impacts of quantum computing on your operations and start planning for the necessary changes. By taking these steps, you can help safeguard the integrity of financial transactions and ensure the resilience of payments infrastructure in the quantum era. Let us commit to building a quantum-safe future starting today!

In the coming months, we will be releasing additional resources to help the industry better understand the complex issues surrounding quantum payments, including a list of the top things organizations need to know to prepare for the future.

Quantum Payments Project Team

This paper was developed by the Quantum Payments Project Team of Nacha's Payments Innovation Alliance.

Payments Innovation Alliance

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Quantum Payments Project Team to create educational materials on quantum computing as it relates to the payments industry. Visit [Quantum Payments Project Team](#) to learn more.

