KPMG

Quantum computing:
Preparing for the future

Quantum computing: Opportunities are coming

Quantum computing is set to revolutionize multiple industries by offering unparalleled computational power and advanced problem-solving capabilities. In finance, quantum algorithms can transform risk management, portfolio optimization, and fraud detection. Financial institutions will be able to process complex models and large datasets at unprecedented speeds, leading to more accurate predictions and more informed decision-making. Cryptographic security will also be dramatically enhanced, safeguarding sensitive transactions and data from increasingly sophisticated cyber threats. In healthcare, quantum computing will accelerate drug discovery and the development of personalized medicine by rapidly analyzing complex molecular and genetic data. The technology sector will see new frontiers in artificial intelligence and machine learning, enabling the analysis of vast and intricate datasets and driving innovation. Breakthroughs in materials science and logistics optimization will drive efficiencies and foster the development of advanced products. Across industries—from manufacturing to climate modeling—quantum computing will provide a significant competitive edge, placing organizations at the forefront of technological advancement and ushering in the next wave of digital transformation.

Healthcare

Quantum computing offers immense potential in revolutionizing healthcare through accelerated drug discovery and personalized medicine. By simulating molecular structures and biological processes at unprecedented speeds, researchers can identify new drug candidates more rapidly and accurately, leading to faster development of treatments and cures for complex diseases. This capability extends to personalized medicine, where quantum computing can analyze genetic data to tailor treatments to individual patients' unique profiles, enhancing efficacy and reducing adverse effects.

Supply chain

Quantum computing may dramatically enhance supply chain management and logistics optimization. With its ability to solve complex optimization problems and process vast amounts of data in real time, quantum computing can identify the most efficient routes, predict disruptions, and optimize inventory levels. This can lead to significant cost savings, improved delivery times, and increased operational efficiency, providing a competitive advantage to organizations in manufacturing, retail, and distribution.

Finance

In finance, quantum computing will detect and prevent fraud with unprecedented accuracy by analyzing complex transaction patterns and identifying anomalies in real time. Quantum algorithms will optimize investment portfolios and manage financial risks more effectively, leading to better decision-making and enhanced profitability. In insurance, quantum computing will enhance risk assessment and underwriting processes by processing vast amounts of data, leading to more accurate predictions and personalized insurance products, thereby improving customer satisfaction and operational efficiency.

Technology, media, and telecommunications

Quantum computing is poised to redefine capabilities within the technology, media, and telecommunications sector by enhancing data processing and analysis. In technology, quantum computing can accelerate advancements in artificial intelligence, enabling machines to learn and adapt more efficiently, which drives innovation in software development and cloud computing services. For media companies, quantum algorithms can analyze consumer data at scale, leading to highly personalized content delivery and more effective advertising strategies. Telecommunications will benefit from enhanced network optimization and more efficient data routing, improving connectivity and service delivery for consumers. The sector as a whole will see increased cybersecurity with quantum-resistant encryption methods to protect sensitive data and communications from evolving threats.

Industrial manufacturing

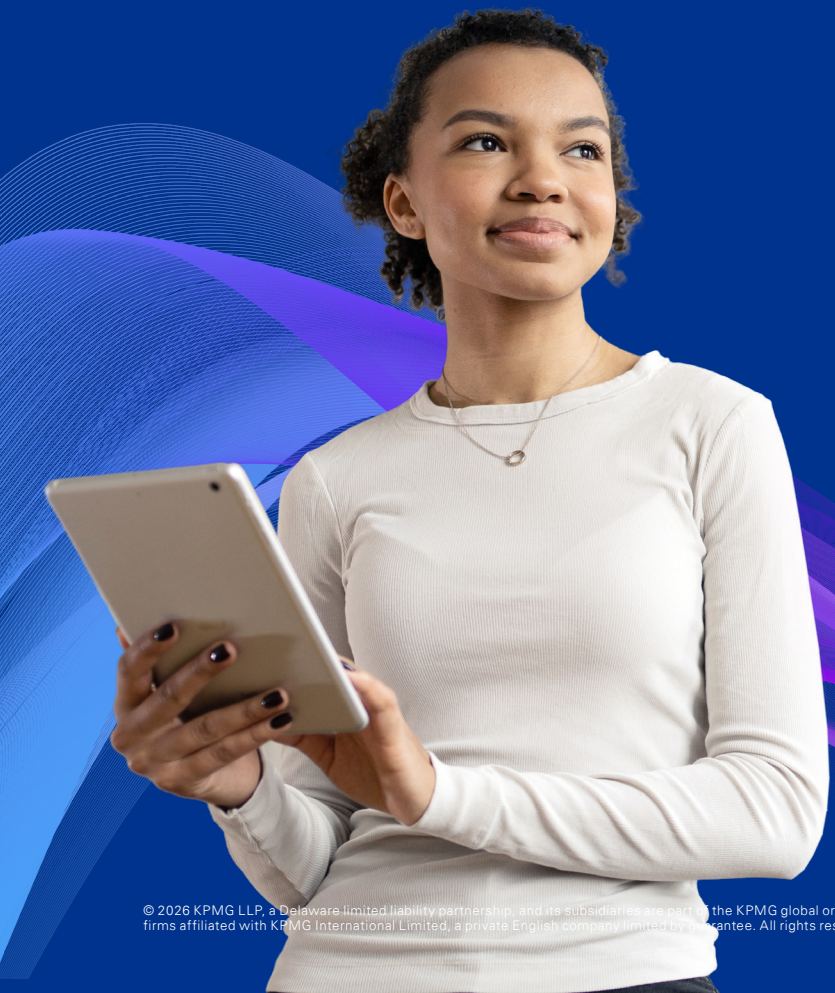
Quantum computing offers transformative potential in industrial manufacturing by optimizing complex supply chains and manufacturing processes. By solving intricate optimization problems rapidly, quantum computing can enhance production efficiency, reduce waste, and minimize costs, leading to higher-quality product development and faster time-to-market. The capability to model and simulate material behaviors at the atomic level can spur innovation in developing new materials with improved properties, enhancing the durability and functionality of manufactured goods. Manufacturers can further leverage quantum computing to predict maintenance needs and reduce downtime in production lines, improving operational efficiency.

Energy, natural resources, and chemicals

The energy, natural resources, and chemicals sector stands to gain significantly from quantum computing in areas such as resource exploration, energy production, and materials discovery. Quantum computing can analyze vast datasets to identify new energy reserves, optimize extraction processes, and improve resource allocation, enhancing efficiency and sustainability. In chemical engineering, simulating molecular interactions at a quantum level can accelerate the development of novel compounds and catalysts, leading to breakthroughs in environmental conservation and energy storage. Energy providers can use quantum computing to forecast consumption patterns more accurately and optimize grid distribution, reducing waste and improving resilience in energy supplies. Additionally, advancements in quantum encryption will strengthen the security of critical infrastructure and protect against cyber threats.

Postquantum cryptography: Managing risk

The migration to postquantum cryptography (PQC) is critically important for all organizations to maintain the security and integrity of their valuable data and personal information in the face of emerging quantum computing threats. Such threats could potentially break current cryptographic algorithms, exposing valuable data to unauthorized access. Starting the transition to PQC now is essential to safeguard against the "harvest now, decrypt later" threat model, where adversaries collect encrypted data with the intention to decrypt it once quantum capabilities become viable. Preparing proactively will not only protect your organization's information assets but also ensure compliance with upcoming regulatory requirements, fortify its defenses against future threats, and demonstrate a commitment to advanced security measures, thereby maintaining trust with their customers.



Cryptographic vulnerability

Quantum computers have the potential to break widely used cryptographic algorithms such as Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptic Curve Digital Signature Algorithm (ECDSA), which are currently deemed secure against classical computational methods. This vulnerability threatens the confidentiality and integrity of any data protected by these algorithms, necessitating the development and adoption of quantum-resistant algorithms.

Harvest now, decrypt later

Adversaries may actively collect encrypted data today with the intent to decrypt it in the future once quantum computing capabilities become available. This threat underscores the immediate need to transition to PQC to protect sensitive information that must remain confidential for years or even decades.

Infrastructure and system disruption

The transition to PQC algorithms involves major changes to cryptographic protocols, software libraries, hardware cryptographic modules, and public key infrastructures. Delaying this increases the risk of rushed changes, leading to disruptions and vulnerabilities in critical systems. Starting the migration promptly ensures a smoother and more secure transition.

Deprecation and end of life: The clock is ticking

Algorithm type	Algorithm/Standard	Deprecated by	Disallowed by
Digital signature algorithms	ECDSA 112 bits security strength	2030	2035
	ECDSA ≥ 128 bits security strength	-	2035
	EdDSA ≥ 128 bits security strength	-	2035
	RSA 112 bits security strength	2030	2035
	RSA ≥ 128 bits security strength	-	2035
	ECDSA (all parameter sets)	-	2035
	EdDSA (all parameter sets)	-	2035
	RSA (all parameter sets)	-	2035
Key establishment schemes	Finite field DH 112 bits security strength	2030	2035
	Finite field MQV 112 bits security strength	2030	2035
	RSA 112 bits security strength	2030	2035
	Finite field DH ≥ 128 bits security strength	-	2035
	Finite field MQV ≥ 128 bits security strength	-	2035
	RSA ≥ 128 bits security strength	-	2035
Symmetric cryptography	Symmetric standards at 112 bits security level	n/a	2030

What should organizations do to prepare?

KPMG LLP is ready help your organization prepare for the quantum era by providing strategic guidance and support in the following key quantum areas:

Quantum optimization: We assist your organization in the development to explore quantum computing use cases and potential benefits specific to your organization, driving innovation and competitive advantage.

PQC: We conduct a extensive evaluation of your current systems and processes to determine their preparedness for quantum computing integration, identifying potential areas of improvement and strategies to help ensure a smooth transition.

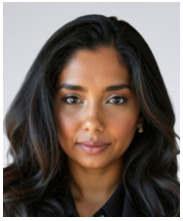
PQC migration: We support transitioning to PQC to protect sensitive data against future quantum threats, helping ensure your organization is ahead of the curve in safeguarding critical information.

Talent development: Provide training programs and workshops to upskill your workforce in quantum computing and associated technologies, building internal knowledge and preparing your team for the future of computing.

Quantum innovation: Facilitate partnerships with academic institutions, tech companies, and quantum computing experts, keeping you updated on advancements and enabling you to leverage the latest emerging approaches for strategic advantage.

Contact us

Dr. Aaron Kemp
US Quantum Lead,
KPMG LLP
T: 404-358-3138
E: aaronkemp@kpmg.com



Dr. Lekshmy Sankar
US Quantum Security Lead,
KPMG LLP
T: 303-495-8125
E: lekshmysankar@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**