KPMG

Are you ready for a quantum leap?

Get up to speed on a game-changing computer technology

KPMG Technology Risk Insights

The quantum revolution is coming – and sooner than you think.

Tech giants such as IBM,[1] Google,[2] Microsoft,[3] and Honeywell[4] are focusing on building solutions in quantum computing. Over the past few years, IBM has increased the size of its quantum computer from 27 to 433 qubits.* The company is aiming for 10,000 to 100,000 qubits or more in 2026.[5]

* Qubits are the basic unit of information in quantum computing.

Honeywell has made significant progress in demonstrating real-time quantum error-correction and achieving significant computational advantages.[6] Nation states are also driving massive growth in quantum development.

Quantum computing is expected to revolutionize fields such as artificial intelligence and machine learning, cryptography, pharmaceutical research, manufacturing, cybersecurity, finance, and logistics by solving problems in just a few hours or minutes that would take classical computers billions of years to solve.

Like many tools and technologies, quantum computing can be both used and misused. It poses a significant threat to cybersecurity because it can break currently used encryption algorithms, potentially putting sensitive information at risk.

Now is the time for organizations to properly understand and prepare for quantum computing, helping them to leverage the advantages and manage the disruptions that quantum computing will inevitably bring to our world.

What is quantum computing?

Classical computing—also known as binary computing—relies on bits, which exist in one of two states at any point in time. Qubits exist in multiple states simultaneously. This property allows quantum computers to perform calculations on many different inputs in parallel, reducing the time required to solve certain problems.

Quantum parallel processing is also supported by superposition, which involves how particles exist in multiple states simultaneously until they are observed. This allows for phenomena such as quantum entanglement, where two particles become linked in such a way that the state of one particle affects the state of the other, regardless of the distance between them.

[1] IBM, "Secure your enterprise for the quantum era," May 2023

[2] Google, "Explore the possibilities of quantum," October 2019

[3] Microsoft, "Accelerate the pace of science," April 2023

[4] Honeywell, "Honeywell quantum solutions," June 2020

[5] "IBM Quantum breaks 100 qubit mark," IBM blog, November 2021. See also "IBM's roadmap for scaling quantum technology," IBM blog, September 2020

[6] Ryan-Anderson, C., et al., "Realization of real-time fault-tolerant quantum error correction," July 2021. See also Chertkov, Eli, et al., "Holographic dynamics simulations with a trapped ion quantum computer," August 2022

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS000457

Additionally, quantum algorithms can take advantage of interference between different qubit states to cancel out unwanted results and amplify the desired ones, further increasing their efficiency.

In many respects, quantum computing is still in the early stages of development and faces significant technical challenges. One such challenge is maintaining the delicate quantum states of qubits and minimizing errors. Quantum systems are also extremely susceptible to interference. Changes in temperature, vibrations, gamma rays, and a myriad of other variables can cause decoherence in a quantum state. Advancements in error correction will be required before quantum systems at scale will be developed. Additionally, quantum computers are not always faster than classical computers for every task and may require specialized algorithms to fully leverage their capabilities. Not every problem is a candidate for quantum optimization or quantum speed increases. Quantum systems are uniquely suited for solving multi-variable problems that collapse to a single answer i.e., the Traveling Salesman Problem. For problems that have multiple solutions, classical systems will still be required.

Applications for quantum computing

Quantum computing represents a significant advancement in computing technology with the potential to solve problems that are currently beyond the reach of classical computing. The use of quantum computing will improve processes in finance, logistics, transportation, and materials science. It will help optimize supply chain management, portfolio management, route planning, and the discovery of new materials with desirable properties. Examples of organizations leveraging quantum computing include optimizing new materials for electric vehicle batteries, folding proteins, and new pharmaceutical products.

In the hands of bad actors, quantum computing has the potential to break some of the most widely used cryptographic protocols used to secure communications and transactions on the internet.

In addition, organizations face potential cyber risk from harvest-now-decrypt-later attacks, in which attackers steal encrypted information and wait a few years until advances in quantum computing will make it easy to crack.

However, quantum-safe (or postquantum) cryptography provides cryptographic algorithms that are resistant to attacks from quantum computers. In addition, quantum key distribution uses the principles of quantum mechanics to provide highly secure encryption keys.

In December 2022, the Biden administration passed the Quantum Computing Cybersecurity Preparedness Act,[8] which directs federal entities to begin their preparations for migration to postquantum cryptography. Federal organizations are required to understand their cryptographic footprint and begin planning to replace susceptible equipment. Numerous Nation States have adopted Harvest Now, Decrypt Later (HNDL) strategies with the intention of decrypting information when quantum systems reach viability. The Mosca theorem provides organizations a method for understanding when they need to begin their cryptographic transitions.

X = Security shelf life (how long do you need your data to remain secure)

Y = Migration time (how long will it take to migrate your data and systems to quantum safe cryptographic processes)

Z = Collapse time (the number of years before a quantum computer with the scale to break current encryption protocols exists)

If X + Y > Z organizations need to worry.

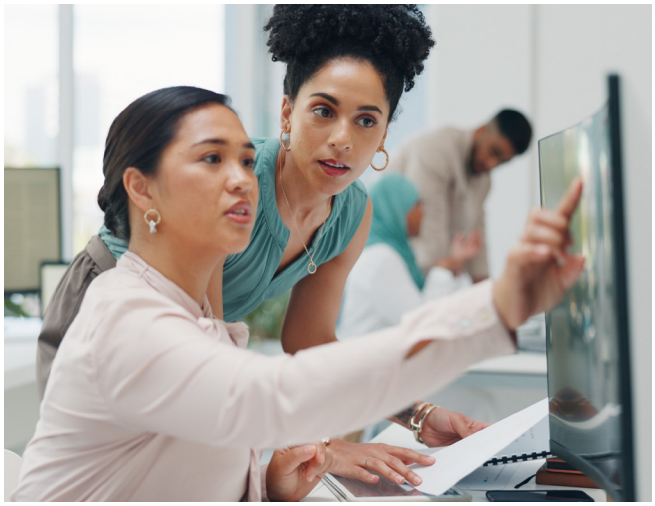
Matters of security

A classical computer would take about 2 million years to break the industry-standard RSA-1024 security algorithm. A quantum computer can break it in a few minutes.[7]

[7] Petrenko, A., Applied Quantum Cryptanalysis, April 2023

[8] H.R.7535 - Quantum Computing Cybersecurity Preparedness Act, December 2022

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS000457



Example: Organization 1

X = 15 Years (data must remain secure)

Y = 5 Years (time required for the organization to transition to Post Quantum Cryptography (PQC))

Z = 10 Years (technological leaps create viable quantum computers at scale)

15 + 5 > 10

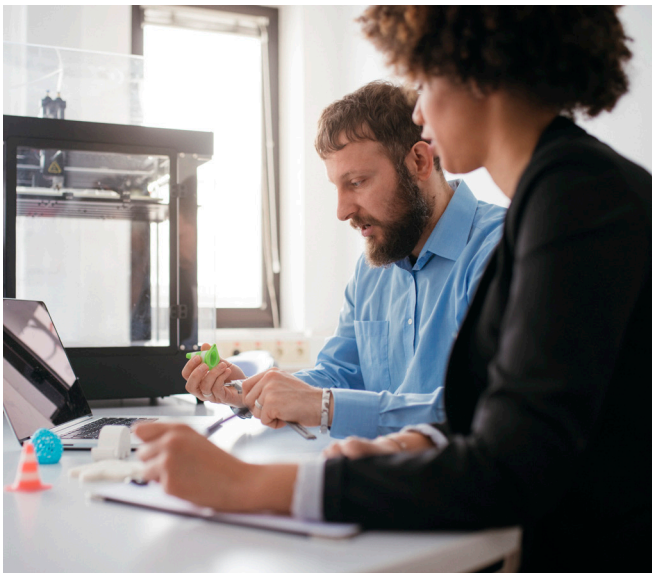
20 > 10

In this case, even if the organization started their transition to PQC now, existing data and data created prior to Y being achieved would be vulnerable to HNDL.

Quantum computing in action

KPMG has worked with organizations on a number of quantum computing projects in areas such as antenna placement, field service optimization, power grid design, value-at-risk optimization, and budget optimization.

For example, a client in the financial services sector wanted to find an optimal hedging strategy that would help minimize risk for one of its investment portfolios. KPMG professionals recast the minimization problem into a mathematical form that supported the examination of a larger solution space. As a result, the client realized a 10 percent value-at-risk improvement compared to its existing approach.



Look before you leap

We cannot stress enough the need for organizations to begin their preparations for a postquantum world. This will be a significant undertaking, requiring support throughout the organization and a plan to address cost, scheduling, actions, and time. Organizations must also be prepared to adopt new government data-protection standards such as the National Institute of Standards and Technology (NIST) Post Quantum Initiative.

First steps for leveraging the potential advantages of quantum include working with third-party consultants to help identify potential cases for quantum optimization in the following areas:

- **Education**, bringing management and staff up to speed on quantum computing
- **Discovery**, identifying areas most likely to gain a quantum advantage

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS000457

- **Quantum candidate benchmarking**, compared to existing solutions
- **Production and value realization**, bringing the most promising benchmarks to life and realizing their value.

First steps for protecting the organizations intellectual property, data and security includes working with third-party consultants to migrate to quantum safe in the following areas:

- **Inventory**, understanding the cryptographic processes used in the organization and applications utilizing insecure algorithms
- **Discovery**, finding the cryptographic processes which will need to be improved or replaced
- **Quantum Safe**, achieving organizational alignment with PQC standards and continuous cryptographic improvement.

The theory of quantum computing has been around for more than 40 years, but we still have work to do before a fully realized, scalable quantum computer with error correction becomes a reality. That time is fast approaching, however, and organizations that prepare now will gain the most in the years ahead.

The KPMG Technology Risk Modernization – Center of Excellence

The threat landscape in today's volatile environment continues to evolve shifting attack vectors and variable risks. As digital transformations accelerate in business functions at a record pace, our Technology Risk service network has launched a new Center of Excellence on Technology Risk Modernization to provide insights and help organizations evolve their capabilities to respond to digital acceleration, cloud transformation, and emerging technologies.

Learn more here.

Contact us

Dr. Aaron C. Kemp
Director, Advisory Technology Risk
T: 404-222-3000
E: aaronkemp@kpmg.com

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

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS000457