Please visit
www.Qdayready.com

Qday Ready

May-June 2025

Welcome to this month's roundup of exciting developments in the quantum computing world!

Has the Quantum Era Begun?

Quantum computing has long been a promising frontier, but recent breakthroughs suggest that the era of practical quantum applications may finally be upon us. With quantum processors achieving unprecedented milestones in speed and accuracy, the conversation has shifted from theoretical potential to tangible impact.

Researchers and industry leaders are now exploring how quantum computing can revolutionize fields like cryptography, drug discovery, and materials science, signaling that the quantum era may already be in motion.

Here are five major quantum computing announcements from big tech in 2025:

IBM's 1,386-Qubit Chip – IBM unveiled its latest quantum processor, codenamed Condor, which boasts 1,386 qubits, surpassing previous expectations for scalability and coherence.

Google's Breakthrough in Quantum Error Correction – Google Quantum AI made significant strides in error correction, improving qubit fidelity and bringing the industry closer to fault-tolerant quantum computing.

PsiQuantum's Photonic Quantum System Progress – PsiQuantum integrated quantum modules into conventional semiconductor manufacturing, advancing its goal of building a million-qubit photonic quantum computer.

Microsoft's Topological Qubit Milestone – Microsoft achieved a breakthrough in topological qubits, a long-pursued approach that could lead to more stable and fault-tolerant quantum systems.

Growth of Quantum-as-a-Service (QaaS) – Cloud-based quantum computing services expanded significantly, with platforms like AWS Braket, Azure Quantum, and IBM Quantum making quantum hardware more accessible to startups and researchers

Quantum Computing Standards 2025

Quantum computing standards in 2025 have evolved to address security, interoperability, and scalability as the technology moves toward broader commercial adoption. Here are some key developments:

1.**Post-Quantum Cryptography Standards** – The National Institute of Standards and Technology (NIST) has selected HQC as a backup algorithm for post-quantum encryption, complementing ML-KEM to ensure long-term security against quantum attacks.

2.**Global Policy Frameworks** – Organizations like the OECD are working on guidelines for responsible quantum technology development, focusing on privacy, digital security, and ethical innovation.

3.**Cybersecurity Preparedness** – Reports indicate that while quantum computing presents revolutionary opportunities, many businesses remain unprepared for the cybersecurity risks it introduces.

Quantum computing's impact won't arrive with a flashy product launch or widespread retail availability, but rather through a quiet transformation across industries, according to Vimal Kapu and Rajeeb Hazra in their latest Time Magazine article. Featured in the publication's latest issue, the authors argue that quantum technology is already generating value behind the scenes, enhancing scientific research, healthcare, logistics, and finance.

Quantum computing is not just a tool—it is a national capability. Countries that lead will attract talent, secure the data, and define how this new technology is regulated, protected, and deployed. Those that lag in investing in quantum computing may find themselves playing catch-up in cybersecurity, energy

modeling, drug development, and defense applications. This is not hypothetical, nor is it about a light bulb moment. It is happening now, and it has been ramping up over the past decade.

The commercial era of quantum computing has begun, they suggest, as advancements in quantum hardware and software accelerate at an astonishing pace similar to the early days of classical computing. Recent announcements from major tech firms highlight breakthroughs in quantum capabilities, reinforcing the growing momentum in the field.

The message is clear: **the quantum revolution is no longer a distant future—it is happening now**.

Amaravati's Quantum Valley Tech Park- a boost for Quantum Computing in India

In a groundbreaking move for India's quantum computing landscape, IBM, Tata Consultancy Services (TCS), and the Government of Andhra Pradesh have announced a collaborative effort to establish the country's largest quantum computer at the upcoming Quantum Valley Tech Park in Amaravati.

The facility will feature an IBM Quantum System Two, powered by a 156-qubit Heron processor, marking a significant leap in India's quantum capabilities. As part of the National Quantum Mission, the initiative will focus on developing real-world quantum applications and algorithms across key sectors, including life sciences, cryptography, and sustainable manufacturing.

The project aims to create a hub for cutting-edge research and innovation, fostering collaboration between industry and academia. IBM will provide hardware and cloud-based quantum access, while TCS will spearhead the development of hybrid architectures integrating CPUs, GPUs, and quantum systems.

Andhra Pradesh Chief Minister Chandrababu Naidu highlighted the state's ambition to become a global leader in quantum technology, anticipating that the Quantum Valley Tech Park will attract international investment, generate high-skill jobs, and drive breakthrough solutions beyond classical computing limits.

Quantum Computer Achieves Historic Breakthrough, Outperforms Supercomputer in Optimization Task

In a landmark achievement, researchers at the University of Southern California (USC), led by Daniel Lidar, have demonstrated the first-ever decisive victory of a quantum computer over a supercomputer in a real-world optimization task. Using quantum annealing, the quantum system outperformed classical methods in solving complex spin-based problems, proving superior scalability as challenges grew more intricate. This breakthrough highlights quantum computing's practical advantages in industries like finance, logistics, and scientific research, where near-optimal solutions are more valuable than perfect ones. The milestone marks a critical shift from theoretical promise to real-world utility, paving the way for broader adoption of quantum technology in solving large-scale optimization challenges.

Qday Ready -Preparing for the Quantum Era

NIST Introduces Backup Encryption to Protect Banks from Quantum Threats

In a proactive move to safeguard financial data from future quantum computing threats, the National Institute of Standards and Technology (NIST) has introduced HQC (Hamming Quasi-Cyclic) as a backup encryption protocol. This secondary standard complements ML-KEM, the first post-quantum encryption standard finalized in August, ensuring continued security if vulnerabilities arise.

Financial institutions face growing concerns that quantum computers could eventually break current encryption systems, jeopardizing transactions and sensitive data. Industry experts, including the Financial Services Information and Sharing Center (FS-ISAC), emphasize the need for encryption agility, allowing banks and payment processors to swiftly adapt to new cryptographic defenses.

Dustin Moody, who leads NIST's post-quantum cryptography project, stressed that HQC strengthens security without replacing ML-KEM, reinforcing financial resilience in the quantum era. As quantum computing advances, institutions must embrace flexible encryption strategies to stay ahead of emerging threats.

Japan Unveils 256-Qubit Quantum Computer, Advancing Practical Applications

In a major leap for quantum computing, Fujitsu and research institute RIKEN have unveiled a 256-qubit superconducting quantum computer, quadrupling the capacity of their previous 64-qubit system. Developed at the RIKEN RQC-FUJITSU Collaboration Center in Saitama Prefecture, the machine is among the most powerful globally, marking a significant step toward solving complex scientific and industrial challenges.

Funded by Japan's Ministry of Education, Culture, Sports, Science, and Technology (NEXT), the system enhances quantum processing capabilities, enabling breakthroughs in pharmaceutical research, quantum error correction, and AI-driven optimization. The machine will be integrated into Fujitsu and RIKEN's hybrid quantum computing platform, combining classical supercomputers with quantum processors for advanced problem-solving.

Starting in Japan's first fiscal quarter, companies and research institutions worldwide will gain access to the platform, fostering cross-industry collaboration and accelerating quantum software development. Experts highlight its potential to drive innovations in drug discovery, cryptography, climate modeling, and artificial intelligence, reinforcing Japan's position as a global leader in quantum technology.

Being Qday Ready

Q-Day refers to the anticipated moment when quantum computers become powerful enough to break the encryption systems that currently secure our digital communications, financial transactions, and sensitive data. These encryption systems, such as RSA and ECC (Elliptic Curve Cryptography), rely on the difficulty of factoring large numbers or solving discrete logarithms—tasks that classical computers find nearly impossible within a reasonable timeframe. However, quantum computers, using algorithms like Shor's algorithm, could perform these tasks exponentially faster, rendering traditional encryption methods obsolete.

The implications of Q-Day are profound. It could compromise the security of everything from online banking and e-commerce to government communications and critical infrastructure. This is why there is an urgent need to transition to quantum-resistant cryptographic methods, also known as post-quantum cryptography, to safeguard data against future quantum threats.

.

China's Quantum Cryptology Breakthrough Raises Urgent Security Concerns

Chinese researchers have achieved a major milestone in quantum cryptology, successfully factoring a 90-bit RSA integer using a D-Wave Advantage quantum computer. Led by Professor Wang Chao of Shanghai University, the breakthrough challenges previous assumptions about quantum decryption capabilities and accelerates concerns over global data security.

The development brings the world closer to "Q-Day"—the hypothetical moment when quantum computers can break widely used encryption systems, potentially exposing financial transactions, government communications, healthcare records, and private data. Experts warn that this advancement intensifies the international race to develop post-quantum cryptography, urging governments and corporations to accelerate preparations before quantum machines outpace current safeguards.

China's latest quantum achievement serves as a wake-up call for global cybersecurity efforts. As quantum computing progresses, the urgency to reinforce encryption standards grows, ensuring that digital infrastructure remains secure in an era where traditional cryptographic defenses may no longer be enough.

Quantum Computers Could Threaten Satellite Security

According to Panagiotis (Panos) Vlachos a PhD Researcher in Post-Quantum Cryptography at the Queen's University Belfast, satellites serve as the hidden backbone of modern technology, enabling GPS navigation, air travel, telecommunications, and disaster response. However, the rise of quantum computing poses a potential risk to their security.

Designed to operate for decades, satellites rely on encryption systems that must withstand not only today's cyber threats but also future advancements, including those from quantum computers. Unlike traditional computers, quantum machines leverage the principles of quantum physics to process information in entirely new ways.

Though quantum computers have yet to reach their full potential, experts anticipate they will revolutionize computing once technological challenges are overcome. If unprepared, satellite security systems could become vulnerable, underscoring the urgent need for quantum-resistant encryption to safeguard critical infrastructure for the future.

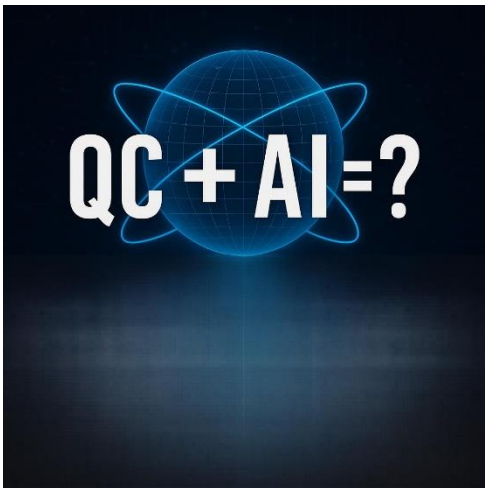
Now, A Quantum Secured Video Call?

In a major breakthrough for quantum communications, researchers from the Universities of Bristol and Cambridge have successfully demonstrated the UK's first long-distance ultra-secure data transfer, including the nation's first quantum-secured video call.

The team developed a quantum communications network using standard fibreoptic infrastructure but leveraging quantum key distribution (QKD) for enhanced security. The network employs two QKD schemes: encryption keys hidden within particles of light and distributed entanglement, where quantum particles remain intrinsically linked.

To showcase its capabilities, the researchers conducted a live quantum-secure video call, transferred encrypted medical data, and enabled secure remote access to a distributed data centre. The data was successfully transmitted over a 410-kilometre fibre link between Bristol and Cambridge, marking a significant step toward next-generation cybersecurity.

Quantum-Inspired AI Poised to Challenge Traditional Large Language Models



As large language models (LLMs) like ChatGPT and Gemini dominate the AI landscape, researchers are exploring whether quantum computing principles could unlock new efficiencies and reasoning capabilities beyond classical AI. Dynex, a Liechtenstein-based company, has introduced its Quantum Diffusion Large Language Model (qdLLM), which was recently named a finalist at the SXSW 2025 Innovation Awards.

Dynex claims qdLLM can generate AI outputs faster and more efficiently than traditional transformer-based models by leveraging quantum diffusion principles, potentially reducing computational overhead and energy consumption. Unlike classical LLMs, which rely on massive datasets and computing resources, quantum-inspired models aim to deliver lighter, more scalable architectures with lower costs and faster inference.

Despite challenges in scaling quantum-inspired AI to match today's leading LLMs, researchers believe these innovations could reshape the future of AI, offering more sustainable and intelligent systems. If successful, quantum principles may provide a breakthrough in efficiency, complexity, and scalability, positioning quantum-inspired AI as a serious contender in the next generation of intelligent computing.

The Future of Intelligence

With great power comes great uncertainty. If Quantum AI reached its full potential, it could surpass human intelligence in ways never before imagined.

Would it remain a tool for progress, or would it challenge the very nature of human decision-making?

Governments and corporations were already racing to develop quantum-enhanced AI systems capable of solving problems beyond classical limits.

Quantum AI could revolutionize cryptography, making current encryption obsolete while simultaneously creating unbreakable security protocols. It could optimize global supply chains, predict financial markets with unprecedented accuracy, and even accelerate the search for extraterrestrial life.

Want to learn more and stay updated about exciting developments in quantum computing?

Subscribe to our monthly newsletter at www.QdayReady.com

Please visit www.QdayReady.com