NIGHTDRAGON

MARKET REPORT:
QUANTUM

June 2025

www.nightdragon.com

Table of Contents

Foreword

Quantum computing stands at the threshold of revolutionizing industries, national security, and the very architecture of computing itself. Once a theoretical frontier, quantum is fast becoming a strategic imperative for both enterprise and government organizations. Driven by breakthroughs in hardware, the rapid evolution of artificial intelligence, and the maturation of cloud infrastructure, quantum technology is now transitioning from research labs into real-world use cases with profound implications.

The pace of innovation in the quantum ecosystem is accelerating rapidly. New startups are pushing the boundaries of what's possible, from developing quantum-native algorithms to creating modular, cloud-integrated hardware. Meanwhile, enterprise and cloud providers are testing hybrid quantum-classical solutions and embedding early quantum capabilities into AI workflows. Universities are expanding training programs, and cross-disciplinary collaboration is driving forward research in everything from materials science to quantum networking. This momentum is transforming quantum from an experimental curiosity into a dynamic innovation platform with the potential to reshape how problems are solved across sectors.

While organizations are eager to harness quantum's potential for accelerated drug discovery, next-generation artificial intelligence, logistics optimization, and secure communications, they must also navigate a fragmented hardware landscape. What's certain is that regardless of which hardware approach "wins", companies like Classiq, who are enabling us to code quantum software, migrate classical applications to quantum, and more, are at the cusp of transforming it all.

Quantum computing is no longer a distant possibility—it is a near-term reality. This report aims to help decipher the current state of the market, the forces shaping its future, and the critical actions required to prepare for a world where quantum is central to innovation, security, and global competitiveness.

Dorin Baniel
Principal & Head of EMEA Investments,
NightDragon

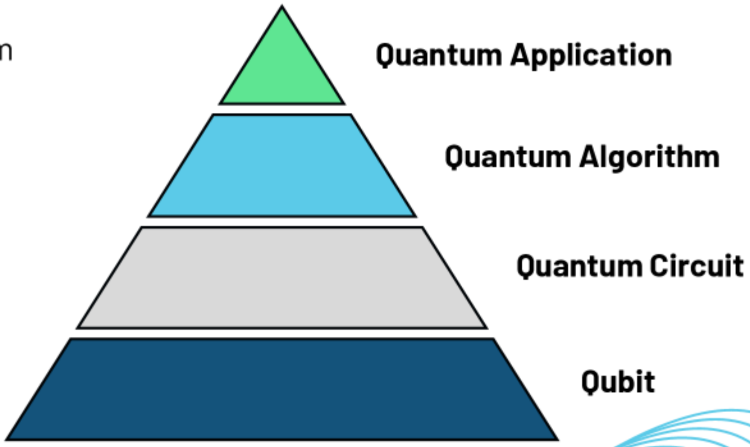
NIGHTDRAGON

The Foundation

To provide context before we begin, the following pages introduce key terminology essential for understanding and navigating the quantum landscape. We also introduce Shor's Algorithm and Grover's Algorithm, the two foundational quantum algorithms that demonstrate how quantum computers can outperform classical computers for specific types of problems.

Quantum Computing - A new era of computation based on quantum mechanics, processing information in fundamentally different ways compared to classical computing - using qubits that can perform complex calculations simultaneously, driving exponential results.

The core layers of quantum computing fall similar to a pyramidal structure:

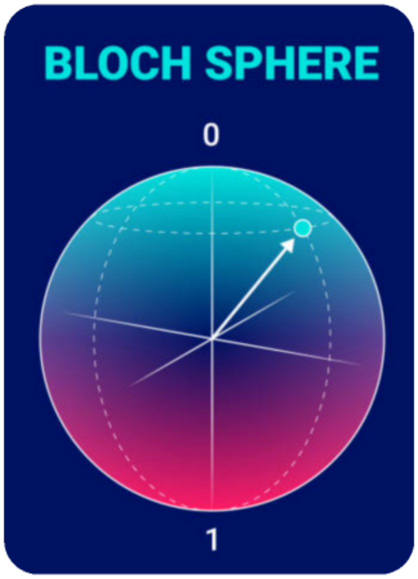


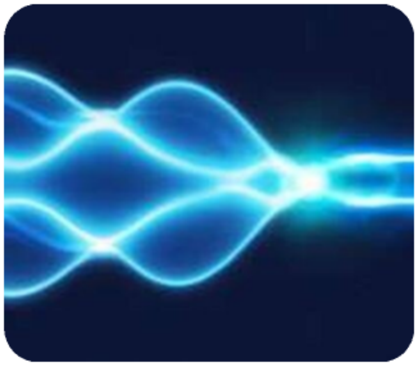
Qubit - Just like the basic unit of information for a classical computer is a bit, the basic unit of information for a quantum computer is a qubit. Unlike a classical bit, which can only be 0 or 1, a qubit can be both 0 and 1 at the same time thanks to a quantum property called superposition. This allows quantum computers to process vastly more information in parallel than classical computers. We dive deeper into this on the next page.

The foundational principles of quantum computing (qubits) are the quantum mechanic concepts below. They represent the core differences between classical and quantum systems.

SUPERPOSITION **EXPLORES**, ENTANGLEMENT **CONNECTS**, INTERFERENCE **SELECTS**.

Superposition	A qubit can be in a superposition — a mix of 0 and 1 at the same time — meaning it can represent multiple states simultaneously. This lets quantum computers explore many possibilities at once, enabling powerful parallel calculations. • 1 qubit = can explore 2 states at once • 2 qubits = can explore 4 states at once • 3 qubits = can explore 8 states at once However, environmental noise (like heat or vibrations) can easily disrupt superposition, causing errors or loss of quantum behavior. The current hardware challenge is having enough logical qubits (error-corrected, reliable qubits) for useful quantum processing.
Entanglement	When two or more qubits become entangled, the state of one instantly affects the other — even at a distance. You can encode much more information with fewer qubits because of the shared entangled state. • 2 classical bits → 1 of 4 states at a time • 2 entangled qubits → all 4 states at once Every added qubit doubles the possible states: • 1 qubit = 2 states • 2 qubits = 4 states • 3 qubits = 8 states • 4 qubits = 16 states • 100 qubits = more states than atoms in the universe
Interference	Interference is when the different paths that a quantum system could take combine to strengthen or cancel each other out. Quantum computers set up superpositions, then use interference to amplify the correct answers and cancel out the wrong ones. It's how quantum algorithms steer the system toward correct solutions. Without interference, superposition would just be random chaos.



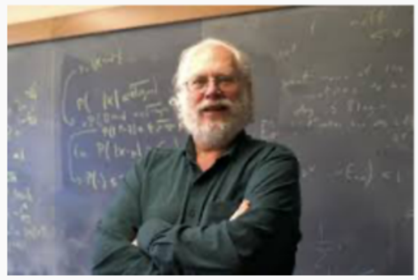


THE PIONEERING COMPUTER SCIENTISTS

Peter Shor and Lov Grover are pioneering computer scientists who made foundational contributions to quantum computing through their algorithms. Shor's Algorithm and Grover's Algorithm gave scientific proof that transformed the idea of quantum computing from theory into an engineering problem.

Shor's Algorithm (1994) - The quantum algorithm for ***directly finding the prime factors of an integer (factoring) in polynomial time***, something that is computationally impossible for a classic computer. This, in essence, showed that quantum computers could do something classically impossible, like breaking encryption. RSA encryption relies on the difficulty of factoring large primes to keep its security and this is the base of cryptography in today's world. Shor's Algorithm undermines RSA's security assumptions, driving the need for post-quantum cryptography (PQC) to ensure security in the quantum era.

After Shor's Algorithm was created, suddenly governments, companies, and researchers realized quantum computers could change security, finance, communication, and more. This triggered a turning point in quantum research and the beginning of large amounts of funding in the space.



Grover's Algorithm (1996) - The quantum algorithm foundation for ***searching for solutions inside an unsorted pile of possibilities.***

Classical	Grover's Algorithm
Search by One	Search using quantum superposition and interference
Time needed = N tries for N items	Time needed = square root of N

Grover's Algorithm was the basis for Quantum Advantage – even if you cannot break encryption, every day problems can and will be solved much faster. Examples include optimizing delivery routes, scheduling flights, matching medical data, investment portfolio optimization and trading, speeding up and enhancing machine learning,

Key Terms

Application Layer	Quantum Readiness	The preparedness of organizations (or technologies) to integrate and leverage quantum computing	Critical for businesses and governments to stay competitive as quantum technologies mature and disrupt industries
Algorithm Layer	Quantum Noise	Random disturbances that affect quantum states, typically from environment interactions	Limits the reliability and lifespan of qubits; overcoming noise is key for practical quantum computing
	Error Correction	Methods to protect quantum information from errors due to decoherence and other quantum noise	Essential for building scalable, fault-tolerant quantum computers
	PQC (post-quantum cryptography)	Cryptographic algorithms designed to be secure against attacks by quantum computers	Ensures long-term security of sensitive information, even after powerful quantum computers emerge that could break today's encryption
	Quantum Advantage	When a quantum computer solves a problem faster than any classical computer could	Proof that quantum computers can outperform classical ones, justifying investment and advancing applications
Circuit Layer	Gate	Basic building blocks of quantum circuits, manipulating qubits through specific operations	Enable complex algorithms; precision and fidelity of gates directly impact computational power
Qubit Layer	Superposition	Qubit can be 0 and 1 at once	Explore many possibilities simultaniously
	Entanglement	Qubits become deeply linked and act as one system	Create complex, powerful connections between qubits
	Interference	Quantum paths combine to strengthen the right answers and cancel the wrong ones	Steer computation towards the correct solution
	Logical Qubit	A qubit built from many physical qubits to correct errors and behave reliably	Enables scalable, fault-tolerant quantum computing by protecting against noise and decoherence

The Opportunity

THE QUANTUM GLOBAL ARMS RACE

The global race to harness quantum computing is intensifying as its promise to solve once-intractable problems becomes more tangible. From drug discovery and logistics optimization to financial modeling and national defense, quantum offers transformative potential that classical computing simply cannot match. However, this promise brings with it an urgent need: organizations must move quickly or risk falling behind in what may be the next era-defining technology race—much like AI before it.

THE NEED FOR MORE COMPUTE

At the core of this urgency lies the need for radically greater computational power. Classical systems are nearing their physical and economic limits, especially in domains that demand vast data processing, probabilistic modeling, or multidimensional optimization. Quantum systems, leveraging principles like superposition and entanglement, promise a new paradigm—where simulations of molecules, optimization of logistics networks, and modeling of complex systems could become exponentially faster and more precise.

THE GOVERNMENT ARMS RACE

Governments around the world have recognized the strategic importance of quantum computing and are investing heavily to secure a technological lead. This is especially apparent in the unfolding "quantum arms race," with countries such as the United States, China, and members of the European Union channeling billions of dollars into national quantum initiatives. These efforts aim to establish domestic quantum expertise, secure critical infrastructure, and ensure that adversaries do not gain a first-mover advantage in exploiting quantum capabilities, particularly in the realms of cybersecurity and intelligence.

"HARVEST NOW, DECRYPT LATER"

We must understand that the same tools that promise to revolutionize industries could also be weaponized by malicious actors. One of the most frequently cited concerns is the threat quantum computing poses to current encryption standards. Algorithms such as RSA and ECC, foundational to modern internet security, could be rendered obsolete by a sufficiently powerful quantum computer. This has sparked intense interest in post-quantum cryptography, as organizations race to get quantum ready. Many adversaries today are executing the "harvest now, decrypt later" approach – data is intercepted and stored today to be decrypted in the future, compromising confidential information across governments, businesses, and individuals. Classiq, our newest portfolio company, is helping address these critical challenges.

THE BOTTOM LINE:

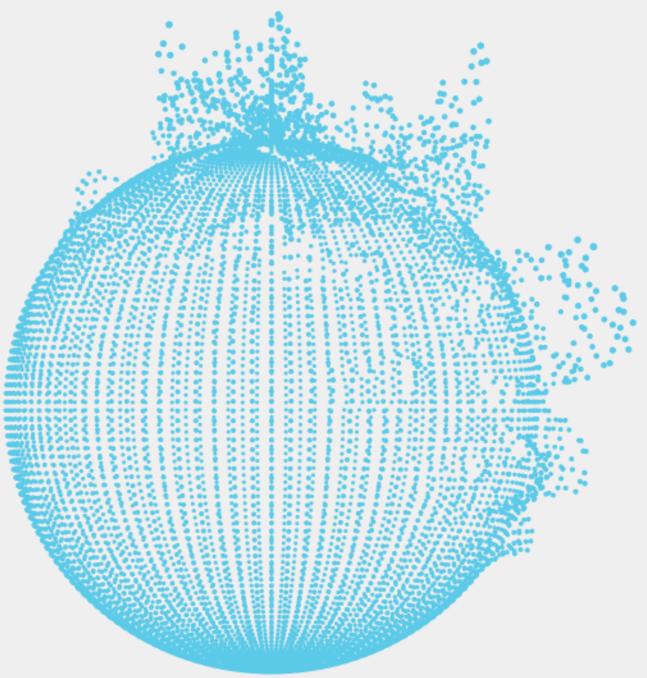
As the quantum era approaches, stakeholders must navigate a landscape filled with both promise and peril. Understanding and preparing for these challenges is essential—not only to capitalize on quantum's transformative potential, but also to defend against the threats it may introduce.

Quantum Will Change Modern-Day Cybersecurity

As quantum computing advances, so does its potential to upend the foundations of modern cybersecurity. At the core of today's digital infrastructure lie cryptographic algorithms such as RSA, elliptic curve cryptography (ECC), and Diffie-Hellman key exchange protocols. These methods are designed around mathematical problems—like integer factorization and discrete logarithms—that are practically unsolvable by classical computers within a reasonable time frame. For instance, factoring a 2048-bit RSA key using a classical machine would take billions of years. However, a sufficiently powerful, error-corrected quantum computer could break it in mere hours or days using Shor's algorithm.

The implications of this are profound. Once quantum computers reach that threshold, RSA encryption will be rendered obsolete, digital signatures will no longer be trustworthy, and secure communications over VPNs, HTTPS, and even software updates could be compromised. In anticipation of this "Q-Day," adversaries are already believed to be harvesting encrypted data today with the intent to decrypt it later, once quantum capabilities are sufficient—a tactic known as "store now, decrypt later."

This looming threat has triggered a global, coordinated response. The U.S. National Institute of Standards and Technology (NIST) is leading the charge on post-quantum cryptography (PQC), a class of cryptographic algorithms designed to be resistant to quantum attacks. NIST's ongoing competition to standardize PQC algorithms has entered its final stages, with several candidates now being tested for implementation across government and commercial systems.



Quantum Will Change Modern-Day Cybersecurity

In parallel, governments worldwide are doubling down on quantum-readiness through national quantum initiatives, many of which include cybersecurity as a top priority. Regulatory bodies and intelligence agencies, including CISA and the NSA, have issued roadmaps urging organizations to begin planning for cryptographic migration. This is a particularly pressing concern for industries handling sensitive, long-lived data such as healthcare, finance, defense, and critical infrastructure.

Cloud providers are also taking proactive steps. Technology giants like Google, AWS, and Microsoft are already integrating PQC into their cloud APIs and testing encrypted communication protocols that will remain secure in a post-quantum world. These early efforts are vital in ensuring that the digital ecosystem can withstand the disruptive capabilities of quantum computing.

Ultimately, quantum computing's promise must be matched with vigilance. Preparing now for post-quantum security is not just prudent—it's essential to protect the integrity of global digital systems before the threat becomes reality.

"Having spent decades in defense and aerospace, I've witnessed firsthand how emerging technologies can reshape national security paradigms. Quantum computing represents the most significant strategic inflection point since the advent of satellite communications. The organizations that master quantum-secured communications and quantum-enhanced sensing today will define the security architecture of tomorrow."

- RUSS MATIJEVICH, CEO, Matijevich International LLC

The Evolution

Quantum computing holds transformative potential for both enterprise and government organizations, promising capabilities that extend far beyond the limits of classical systems. As industries seek solutions for increasingly complex challenges—whether it's optimizing global supply chains, simulating advanced materials, or defending against evolving cyber threats—quantum technology offers the ability to unlock insights and solve problems that were previously impossible or prohibitively time-consuming.

Quantum systems use quantum mechanics including entanglement, superposition, and interference, to model natural and engineered systems more accurately, evaluate probabilities more effectively, and process data with unprecedented efficiency. This has incredibly powerful implications, enabling breakthroughs in materials science, artificial intelligence, cybersecurity, pharmaceuticals, finance, defense, and more.

2016-2023: 0 to 50 to hundreds of logical qubits

2016
IBM launched IBM Q, the 1st cloud-based access to a real quantum computer

2017
Google announces 72-qubit processor

2018
Qiskit, NISQ born

2019
Google's 53-qubit processor solved a sample problem in 200 seconds vs. 10,000 years for traditional computing

2020
Honeywell & Cambridge formed Quantinum

China solves boson sampling problem with Jiuzhang

2021
IBM unveils 127-qubit processor

2023
IBM unveils 433-qubit processor

2023-2025: Error Correction & Quantum Advantage

- Microsoft, Azure Quantum launch hybrid quantum-classical workflow tools
- Hyperscalers focus helping enterprises ready for quantum future
- D-Wave partners with AWS Braket
- Google reveals progress with error-corrected logical qubits
- Quantinuum achieved record-low error rates
- Quantum gets market traction: Sandbox.AQ ($500M+) PsiQuantum ($940M+) IonQ ($95M in bookings)

2028-2029: Commercial Scale

- Error corrected commercial quantum computers (500, 1000+ logical qubits)
- Largest funding round to date, with $110M invested in Classiq

The quantum market itself is undergoing a major transformation, moving from an era dominated by hardware experimentation toward a more layered ecosystem that includes both hardware and software. While progress on the hardware front is accelerating, the landscape remains fragmented. Multiple technological approaches—superconducting qubits, trapped ions, photonics, and others—are being pursued, with no clear "winner" yet. Although some corporates have projected Quantum Advantage by 2026-2028, like IBM, the lack of a dominant platform creates uncertainty for organizations planning long-term investments.

This fragmentation presents a significant opportunity: the emergence of a software layer that abstracts the underlying hardware and enables developers to build applications without needing to bet on a specific hardware modality. Just as classical computing benefited from standardized operating systems and programming environments, quantum software platforms that are hardware-agnostic will be critical to driving adoption and enabling innovation. These platforms can serve as the interface between developers and quantum machines, facilitating code portability, optimization, and deployment across various quantum backends.

The real value of quantum computing will ultimately be defined by its practical daily use cases:

SAMPLING AND SEARCH APPLICATIONS
Quantum algorithms can rapidly search and sample from large, unstructured databases, which has implications for big data analytics and intelligence gathering.

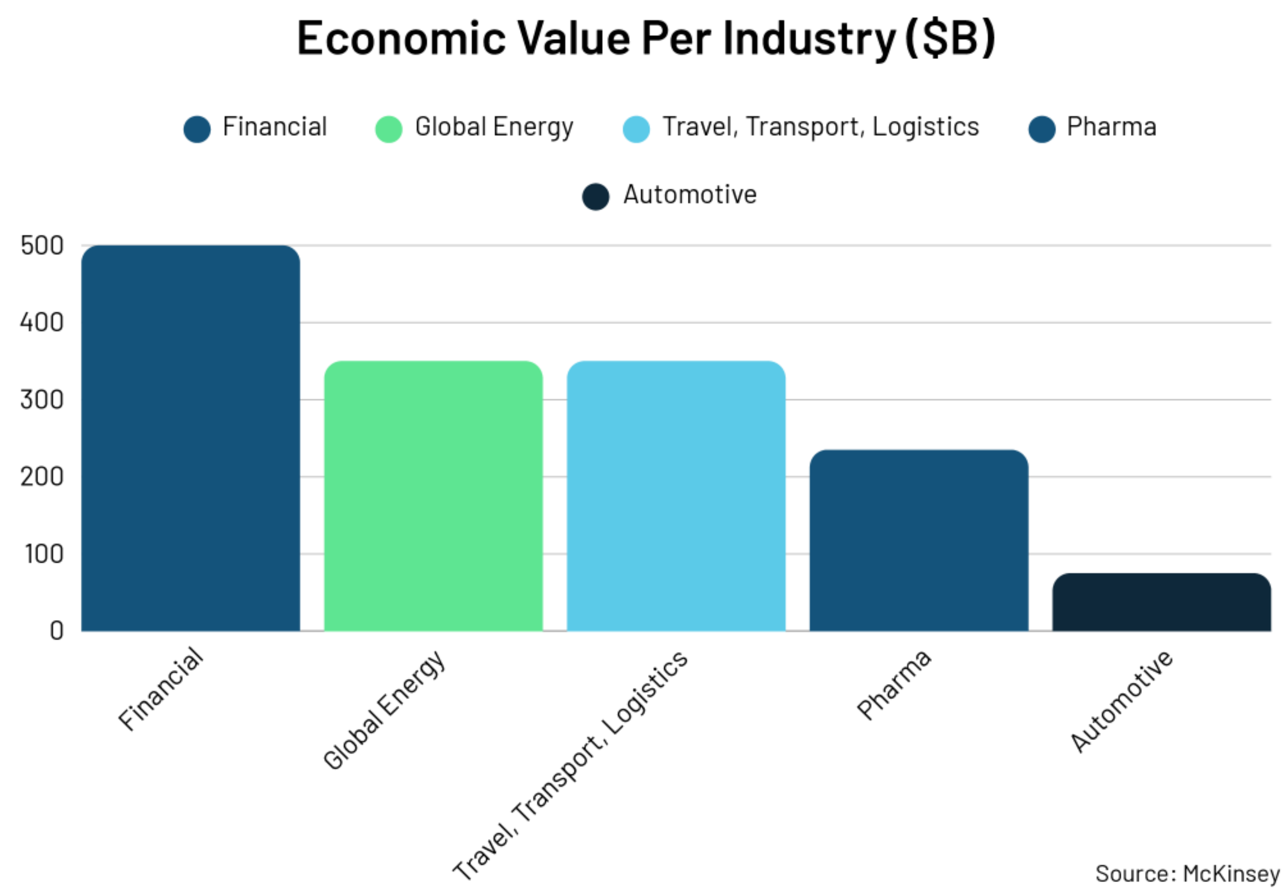
PHARMACEUTICALS
Accurately simulating molecular interactions and calculating energy spectra can drastically shorten the drug discovery lifecycle.

MILITARY AND DEFENSE
Quantum technology can enhance ultra-secure communication, support advanced navigation systems that do not rely on GPS, and enable detection systems capable of identifying stealth threats like submarines or aircraft.

ARTIFICIAL INTELLIGENCE
Quantum methods can enhance the training of AI models, improve generative model sampling, and reduce computational costs for complex neural networks.

OPTIMIZATION
Quantum computing can address highly complex optimization problems—such as fuel usage, vehicle routing, or scheduling—in ways that outperform classical heuristics.

CYBERSECURITY
Quantum-accelerated algorithms can bolster classical cybersecurity approaches, enabling more accurate threat detection, anomaly identification, and file simulation across distributed systems.



Source: McKinsey

As quantum hardware matures and a flexible software stack emerges, organizations that position themselves now will be best equipped to harness the full scope of what quantum computing can offer. With thoughtful investment and strategic focus, the quantum opportunity could redefine the technological foundation of the modern enterprise and reshape the capabilities of government and defense institutions.

The Market

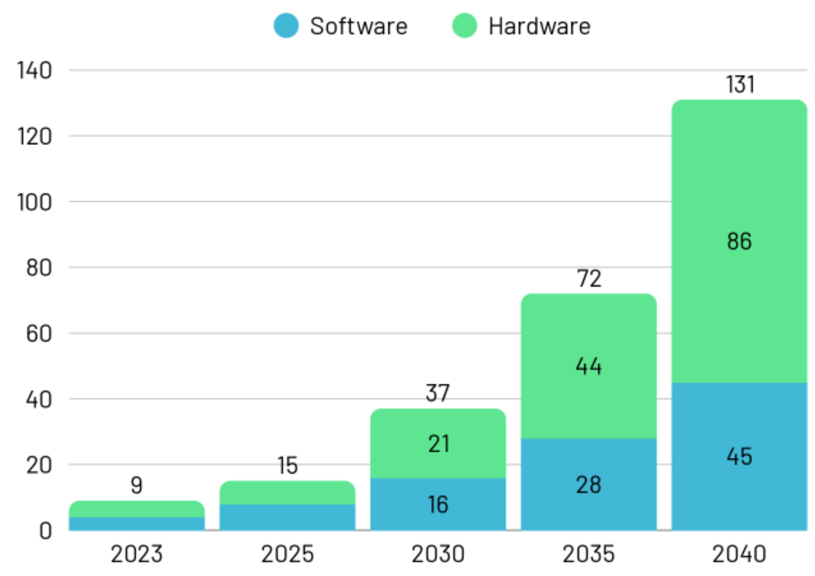
RAPID MARKET GROWTH

The quantum computing market is on the cusp of explosive growth, driven by a convergence of technological breakthroughs, geopolitical urgency, and strategic investments from both public and private sectors. As hardware capabilities continue to improve—bringing the field closer to utility-scale quantum systems—there is a corresponding acceleration in software development, infrastructure integration, and workforce readiness. What's more, we are also seeing now the integration of AI to enhance quantum algorithm performance and reduce time-to-value, and a broader market shift toward scalable, cloud-delivered computing solutions.

As we reach an inflection point with these technologies, we're seeing a corresponding jump in actions from governments to invest heavily in quantum research as part of a broader technological arms race, while cloud hyperscalers and enterprise IT providers are also rapidly evolving to offer hybrid classical-quantum computing environments. This shift is unlocking new commercial opportunities and pushing quantum from experimental labs into real-world applications.

As illustrated in this graph, the quantum computing market is projected to reach $72 billion by 2035 and exceed $131 billion by 2040, with software expected to account for at least 25% of that value. The quantum software segment alone represents a $131B+ opportunity, one that is growing quickly as this market continues to mature.

Quantum Computing Market Growth ($B)

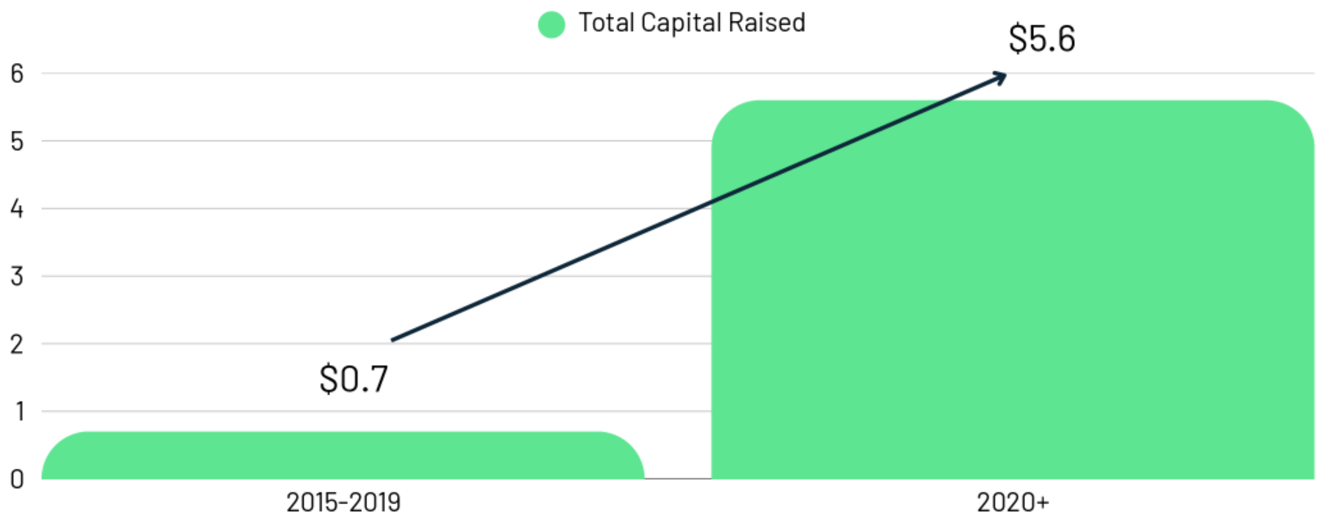


Source: McKinsey

INCREASED VENTURE INVESTMENT

Since 2020, venture capital investment in the quantum computing sector has surged, reflecting growing confidence in the technology's long-term potential and commercial viability. This explosion of funding has fueled rapid innovation across both hardware and software, supported a wave of new startups, and accelerated the maturation of the ecosystem.

Global VC Funding ($B)



Noteworthy 2025 Funding Rounds

QuEra Computing Inc.	$230M	Quantum Machines	$170M
Classiq	$110M	QCi Quantum Computing Inc	$100M
seeqc	$30M	QuantWare	$20M

INCREASED VENTURE INVESTMENT

Moreover, in 2025, there have been multiple new funds that are specializing in quantum investments. One, for example, is Qbeat, the fund founded by Dorit Dor, former CTO of Check Point, which aims to invest only in quantum technologies. Qbeat is a co-investor of NightDragon's in Classiq, alongside other great investors such as Entree, Norwest, Hamilton Lane, Team8, Phoenix, AWZ and more.

Most Active Investors in Quantum

KKR 17 transactions	EQT 16 transactions	CLEARLAKE 12 transactions	THOMABRAVO 10 transactions
Blackstone 8 transactions	PERMIRA 8 transactions	FP 8 transactions	Advent 7 transactions
TPG 7 transactions	VISTA EQUITY PARTNERS 7 transactions	Hellman & Friedman 5 transactions	INSIGHT PARTNERS 5 transactions

** As of June 2025

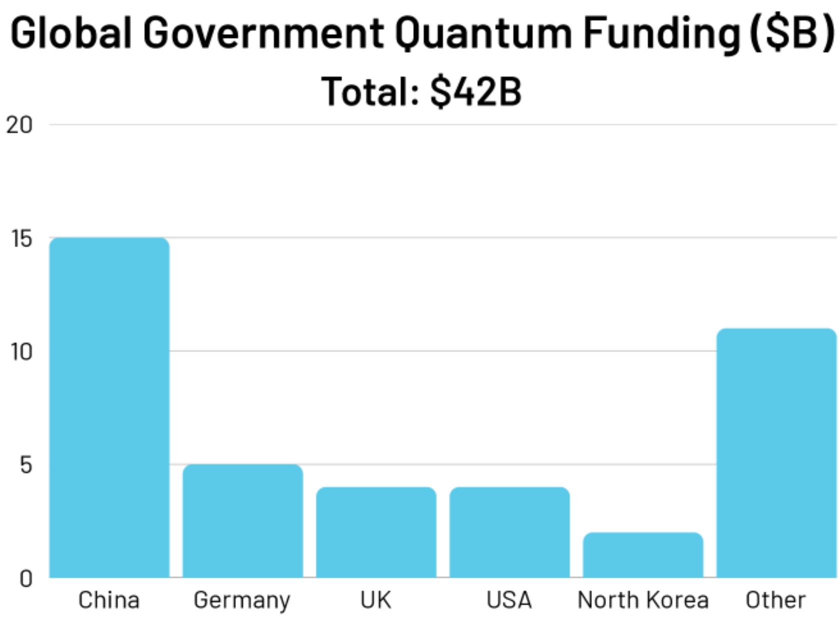
"Quantum technologies represent the next major revolution in computing — solving problems that classical computers simply cannot. With engineering hurdles being overcome and real-world use cases emerging, we're witnessing a rapid transition from academic research to commercial impact. That's why we co-founded Qbeat Ventures: to invest in and accelerate the rise of quantum innovation."

- DORIT DOR, PH.d, Co-founder, QBeat Ventures
Former CTO of Check Point. Dr. Dorit Dor was pivotal to the company's success. Since joining in 1995, she played a central role in its growth to today's $25B+ market cap.

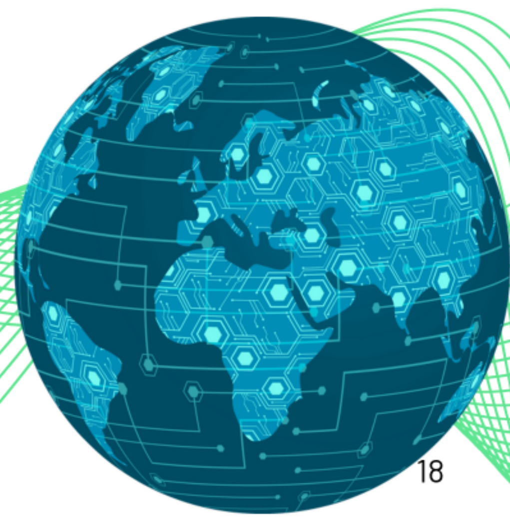
GOVERNMENTS WORLDWIDE IN QUANTUM ARMS RACE

Governments around the world are fueling a global quantum arms race, recognizing quantum technology as a top-tier strategic priority. To date, over $42 billion has been committed to quantum research and adoption, led by major national programs in China (with a $15B allocation), the USA, Germany, the UK, South Korea, and India. In the U.S., agencies like CISA, NIST, and the NSA are leading coordinated efforts to ensure the country is "quantum ready," particularly in securing critical systems against future threats. The graph below illustrates the growing wave of global government investment, underscoring the urgency and scale of national commitments to quantum dominance.

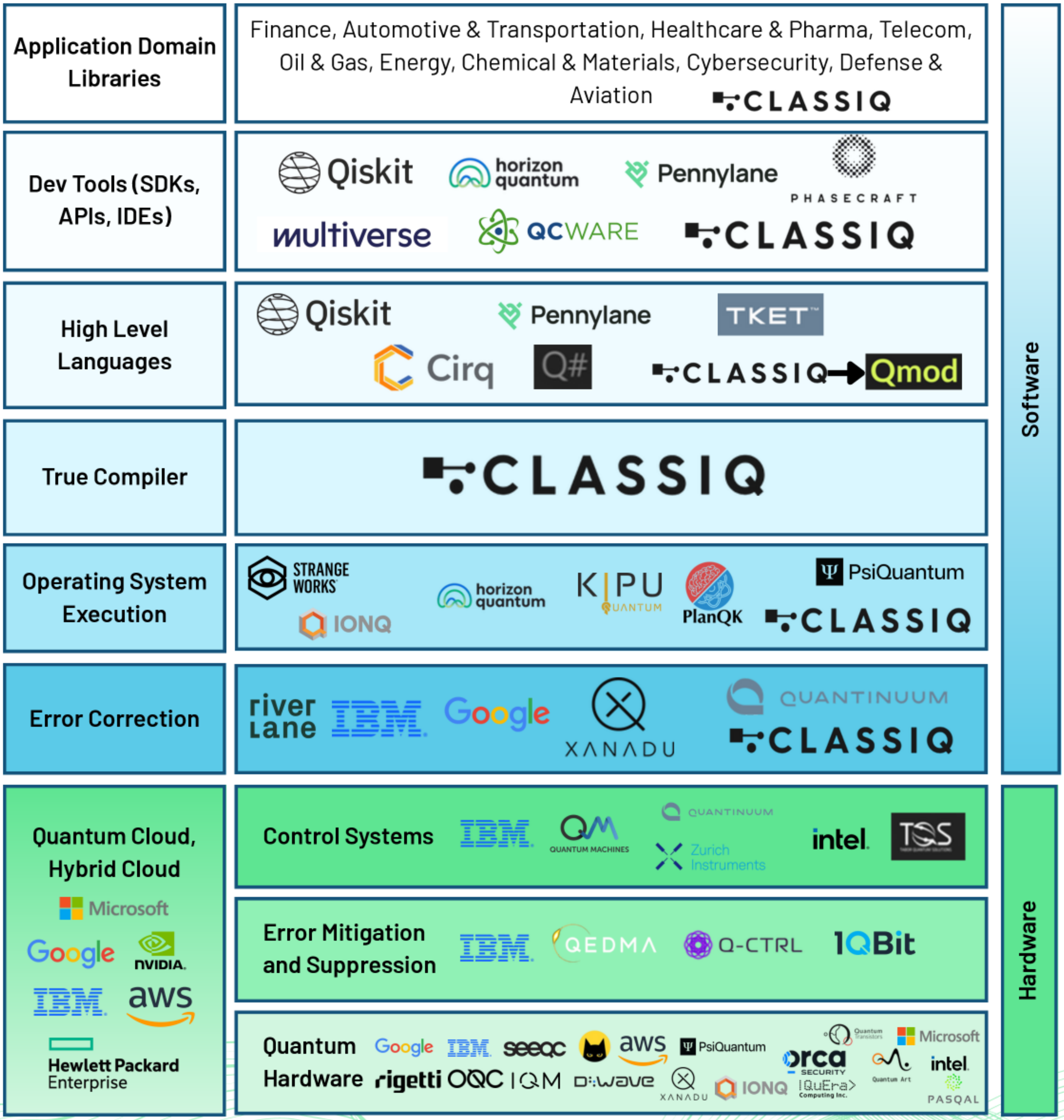
Part of what's driving the investment is warnings from groups like the U.S. Defense Intelligence Agency that quantum technologies are nearing battlefield readiness levels. Governments see a compelling reason to invest in order to maintain a strategic advantage on the global stage. Read more about this dynamic in the Quantum Insider.



Source: BCG



Quantum Market Map



Credit: Classiq

Q&A with Nir Minerbi, Classiq CEO

To help CISOs, developers, and enterprise leaders better understand the evolving quantum landscape, we sat down with Classiq CEO Nir Minerbi to discuss what's next—from quantum-safe cryptography and cross-platform flexibility, to the convergence of quantum and AI, and the critical race for top-tier talent. Classiq recently closed the largest quantum funding round to date, a milestone moment for the industry and a round NightDragon was proud to be part of.

Nir Minerbi,
CEO & Co-Founder
Classiq

HOW SHOULD TECHNOLOGY AND CYBER LEADERS BE THINKING ABOUT QUANTUM AND WHAT STEPS SHOULD THEY TAKE TO PREPARE THEIR ORGANIZATIONS FOR IT?

Quantum computing is moving from theory to reality. CISOs need to prepare now by exploring quantum-safe cryptography and understanding where quantum will intersect with their systems. Early action ensures both security and a strategic edge.

CLASSIQ ALLOWS FOR UNIQUE 3RD PARTY SOFTWARE INTEGRATIONS WITH ALL MAJOR CSPS AND HPC HYPERSCALERS. WHY WAS IT IMPORTANT FOR CLASSIQ TO SUPPORT ALL HARDWARE OPTIONS NOW?

The quantum landscape is evolving rapidly. By staying hardware- and stack-agnostic, Classiq ensures customers can scale with flexibility and avoid vendor lock-in, no matter how the ecosystem shifts.

TELL US ABOUT THE RACE FOR QUANTUM TALENT. IF WE THOUGHT THE TALENT PROBLEM IN CYBER WAS BIG, HOW MUCH BIGGER IS IT GOING TO BE IN QUANTUM?

Quantum demands rare, cross-disciplinary expertise. We help close that gap by letting software developers build powerful quantum applications without needing to be quantum physicists.

HOW IS THE CONVERGENCE OF AI AND QUANTUM SHAPING THE FUTURE OF SOFTWARE DEVELOPMENT, PARTICULARLY IN AREAS LIKE GENERATIVE DESIGN OR OPTIMIZATION?

AI and quantum together will transform how we design and optimize systems. Quantum expands the solution space, and AI helps navigate it—enabling breakthroughs in fields like generative design and complex optimization.

NightDragon Perspective

At NightDragon, we invest in SecureTech companies that build the backbone of national security, data integrity, and critical infrastructure resilience. Quantum computing is rapidly emerging as a transformational force across these domains—redefining what's possible in cryptography, optimization, modeling, and more. While still early, the market is accelerating faster than many realize and the opportunity is massive, with potential to unlock $1–2 trillion in economic value by 2040.

We believe quantum software will be the defining layer of this ecosystem, much like operating systems did for classical computing. Hardware is evolving rapidly, but enterprises and governments alike need tools to develop, optimize, and deploy quantum applications across this fragmented and fast-changing landscape. Software will be the bridge—enabling interoperability, usability, and resilience in a complex quantum future.

That's why we recently invested in a company called Classiq, a pioneer in quantum software. The company's hardware-agnostic platform, high-level quantum modeling tools, and partnerships with major hyperscalers signal the type of technical depth and market foresight we believe will drive the space forward. We will continue to also monitor the market closely.

Quantum's implications extend far beyond computing performance—they touch on global cybersecurity, national sovereignty, and technological leadership. As with AI before it, quantum computing is not just a technological leap—it's a strategic imperative for innovation, security, and global leadership. We believe the companies leading this transition will define the next era of SecureTech, and we're proud to be at the forefront of that journey.

Contact

If you're building interesting technology in this sector or have a perspective, reach out to:

Dorin Baniel
Principal, Head of EMEA Investments
dorin@nightdragon.com

NIGHTDRAGON