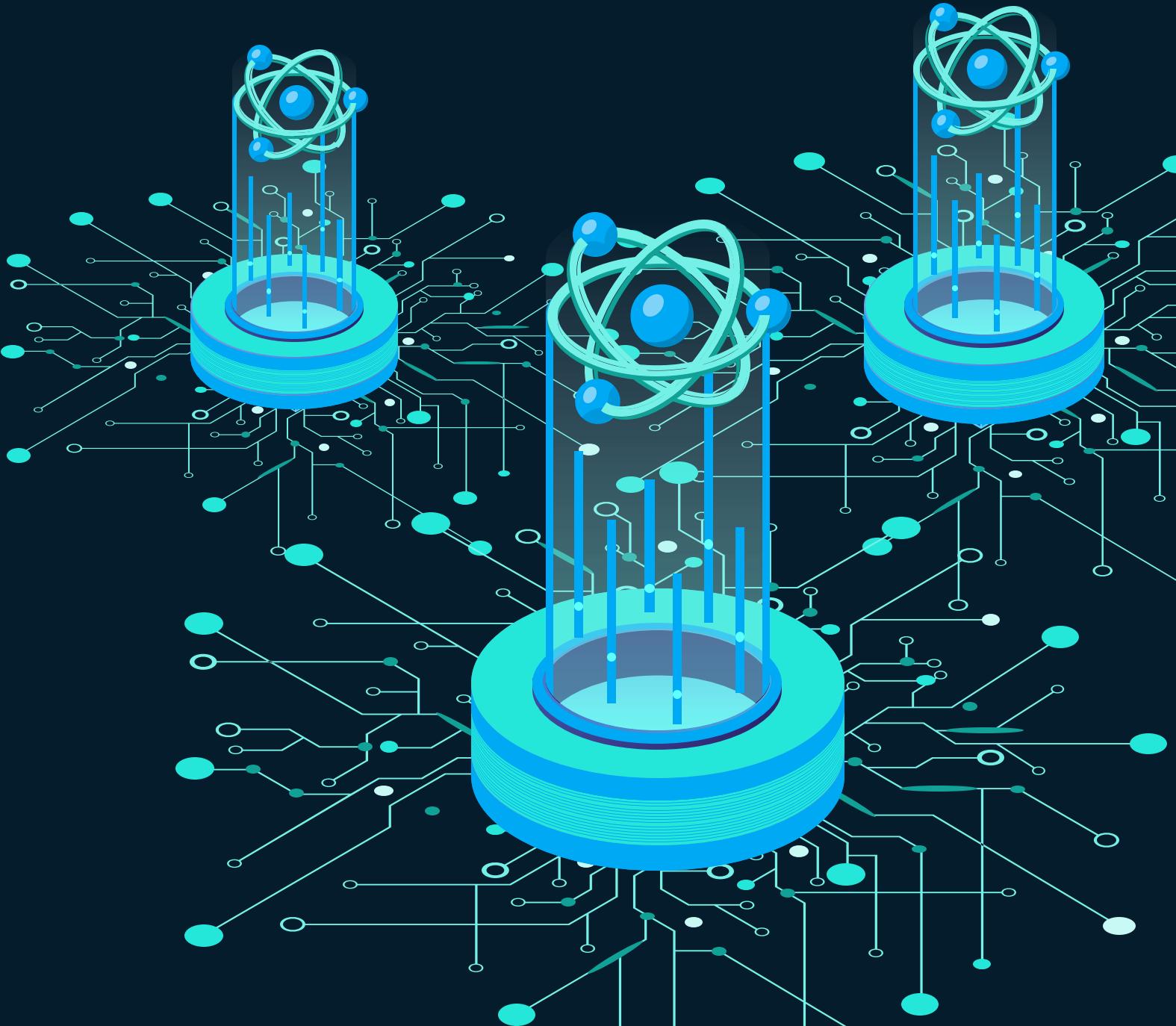


Quantum Technology Monitor

June 2025



What can you find in this report?



An overview of the continuously evolving quantum technology (QT) market—including investments, competitive landscape, and economic activities—covering quantum computing (QC), quantum communication (QComm), and quantum sensing (QS); see page 4 for definitions of these areas



Overview of the **maturity of the QT ecosystem and the use of QT in the broader industry context**, based on current application of the technology and patent and publication activity



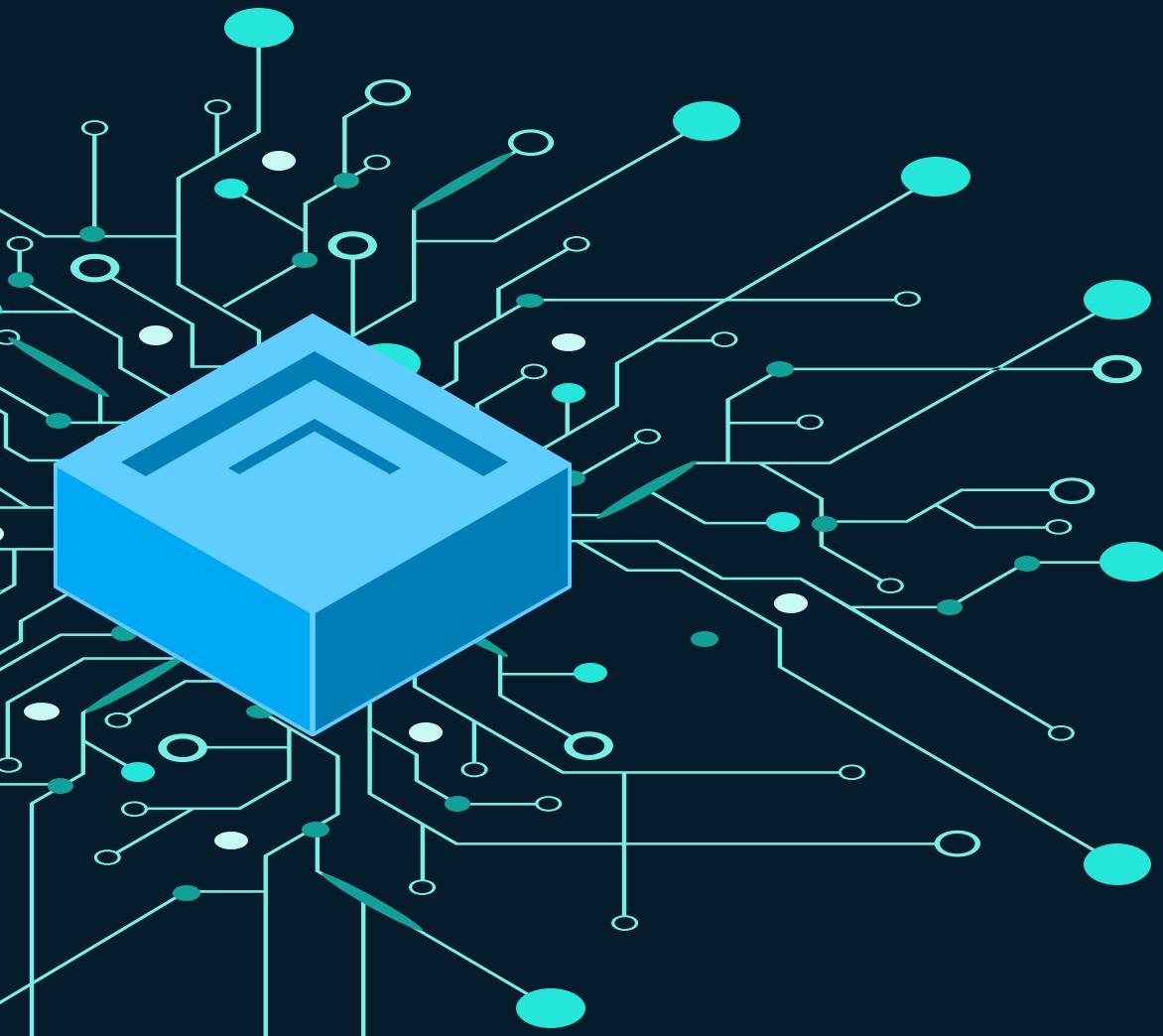
Definitive and exhaustive list of start-ups, investment, and economic activities in the QT space

Note: *Quantum Technology Monitor 2025* is based on research from numerous data sources (including, but not limited to, Crunchbase, expert interviews, PitchBook, *Quantum Computing Report*, S&P Capital IQ, and McKinsey analysis); minor data deviations may exist due to updates of the respective databases; data captured is up to and including March 2025.

Sections of the Monitor

- Technological innovations and breakthroughs in QT, including view on intellectual property (IP) and publications
- Revised internal market size and value at stake
- Updated insights on the private and public investment landscape
- QT innovation clusters and QC start-ups
- QC value chain, particularly on equipment and component manufacturers
- Deep dive into QComm
- QT impact on cutting-edge technology, including AI and machine learning, robotics, sustainability and climate tech, and cryptography and cybersecurity

Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

Quantum technology encompasses the three subfields of computing, communication, and sensing.

Quantum computing

A new computing paradigm leveraging the laws of quantum mechanics to provide significant performance improvement for certain applications and enable new territories of computing compared to existing classical computing



Quantum communication

The secure transfer of quantum information across distances and could ensure security of communication even in the face of unlimited (quantum) computing power¹

Quantum sensing

A new generation of sensors, based on quantum systems, that provide measurements of various quantities (eg, electromagnetic fields, gravity, time) and are orders of magnitude more sensitive than classical sensors

1. Quantum cryptography draws on the exchange of a secret key to encrypt messages based on the quantum mechanical phenomenon of entanglement. Unlike classical cryptographic protocol, it is in principle not possible to "eavesdrop" on messages exchanged with quantum cryptography without detection. However, early implementations have been shown to have some weaknesses—eg, due to physical implementations of the protocols.

A quantum computer leverages quantum mechanics, making it very powerful.

Why is quantum computing so powerful?

It leverages the phenomena of quantum mechanics:

- **Superposition**: The possibility of quantum systems to not be in a single defined state (left or right, up or down, etc)
- **Entanglement**: The possibility of two or more (even physically separate) systems to form an inseparable combined state
- **Interference**: The potential of quantum states to combine

Which problems can a quantum computer solve?

- **Linear algebra (machine learning and AI)** for, eg, reduction of large data for better decisions, predictions, and automation
- **Simulation** of quantum systems and processes—eg, molecular processes, material sciences, and life sciences
- **Mathematical optimization** with algorithms that can enable near real-time optimization for, eg, financial modeling
- **Factorization (security) of large numbers with exponential speedup**—eg, to break mainstream encryption protocols

What do potential use cases look like?



Automotive

Linear algebra for battery optimization: Efficiently predict the lifetime of batteries



Pharma and chemicals

Simulation of molecules: Simulate molecular processes for drug discovery



Finance

Optimization of collaterals: Consider more collaterals and solve with higher accuracy



Security

Factorization: Use quantum random number generators to enhance security

Key messages: Quantum Technology Monitor 2025

Section



Innovation and break-throughs



Market size and value at stake



Investment landscape



Clusters and start-ups



Value chain



Deep dive into QComm



QT impact on cutting-edge technologies

Key messages

Breakthrough announcements in 2024 from tech players and start-ups show major advances in quantum control, specifically in error correction toward reliable and stable QC

QC companies began a shift toward revenue generation, earning an estimated \$650M–\$750M in 2024, and are expected to surpass \$1B by the end of 2025

Start-up investments in QT grew by ~50% YoY to \$2B in 2024, with public funding showing a significant increase (19 pp¹) from 2023

Start-ups are increasingly consolidating into clusters, with emerging hubs in Asia and growing clusters in the US at state level

In 2024, most new start-ups emerged in components and application software, with a value shift moving from components toward application software

Q-Day will be a pivotal shift in security, requiring early adoption of QComm, with ~\$1B total market size in 2023 driving market growth at 22–25% CAGR

QT is a key enabler within the broader disruptive tech ecosystem, offering powerful synergies with other emerging innovations

1. Percentage points.

Source: Contino; Crunchbase; expert interviews; Craig Gidney and Martin Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, April 2021; Hyperion research 2022; Sc20 HPC market results and new forecasts; S. Mandal et al., "Implementing Grover's on AES-based AEAD schemes," *Sci Rep*, in *Nature*, Sep 10, 2024; IP analytics; Nature Index; Oxford Economics; Patsnap; PitchBook; press search; *Quantum Computing Report*; roundtable discussions; S&P Capital IQ; Statista; Gabriel Popkin, "The internet goes quantum," *Science*, 2021, Volume 372, Number 6546; Lareina Yee, Michael Chui, Roger Roberts, and Mena Issler, "McKinsey Technology Trends Outlook 2024," McKinsey, July 16, 2024; McKinsey analysis

Innovation and breakthroughs: Breakthroughs in 2024 include major advances in error correction toward a new era of reliable QC.

Key insights on breakthroughs



Shift toward qubit stability

As scalability and reliability become central to quantum system development, quantum control is increasingly recognized as a strategic priority throughout the ecosystem—from hardware to software integration—ensuring stabilization and error mitigation

Big announcements from key players

In 2024, tech natives—including Google, IBM, and Microsoft—continued to progress in quantum innovation, announcing breakthroughs in processor performance and scalability

Focus on quantum error correction

Quantum error correction emerged as a central focus (eg, Atom Computing, Google, QuEra, and Riverlane), underscoring that effective error correction is no longer optional; it's essential to ensure stability and accuracy using error-correction algorithms



Source: Company websites; expert interviews; IP analytics; Nature Index; Patsnap, accessed March 2025

Patents and scientific publications



Activity on granted QT patents rose **~13%** YoY in 2024, with US leading on total number of QT patents granted

China leads in number of scientific publications (within physical sciences), with **~42%** of total publications and a 7-pp increase in **share of global publications** from 2023 to 2024

Quantum patent applications

QComm

US has **~43%** of global patent applications, driven by the efforts of national labs (eg, NIST) and research institutes

QS

US has **~45%** of global patent applications, largely driven by defense and military priorities

QC

China holds the global lead in QC-specific patent applications with **~32%** of global patent filing activity, ahead of US at **~22%**

Market size and value at stake: QC companies began a shift toward revenue generation, earning an estimated \$650 million to \$750 million in 2024.

Quantum technology market size scenarios in 2035 and 2040

Based on existing development road maps and assumed adoption curve

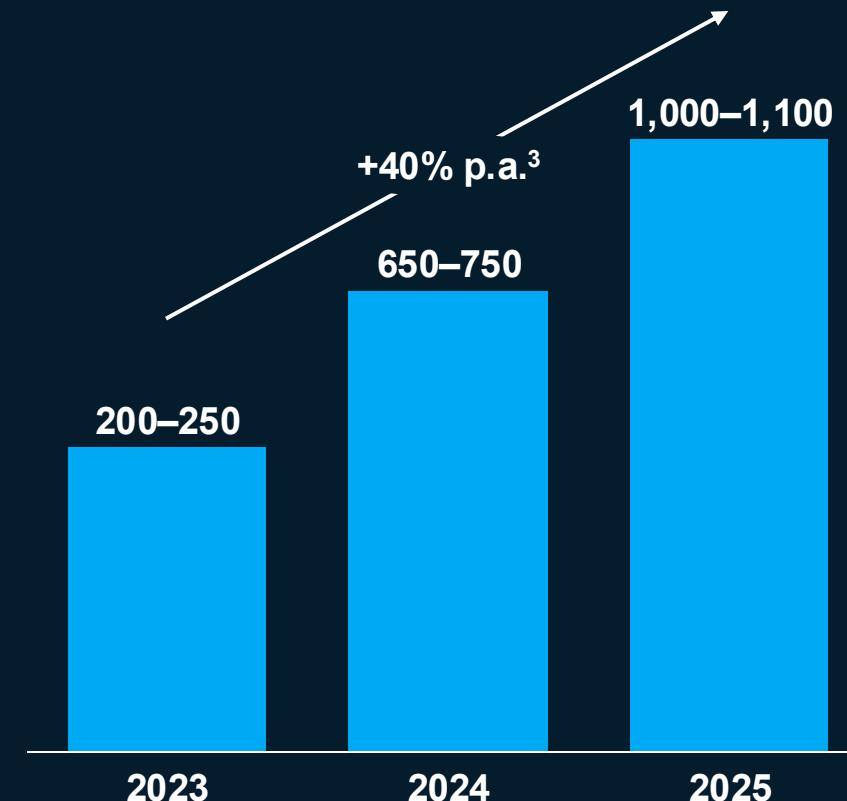
	QC	QComm	QS ¹
2035	\$28B–\$72B	\$11B–\$15B	\$7B–\$10B
2040	\$45B–\$131B	\$24B–\$36B	\$18B–\$31B

Potential economic value² from QC in 2035:

~\$0.9T–\$2.0T

Potential value driven by four industries by 2035: global energy and materials, pharmaceuticals and medical products, financial industry, and travel, transport, and logistics

Revenue estimates of QC companies,
\$ million



1. Approach for QS updated through clusters of use cases based on recent development, announcements, and breakthroughs.

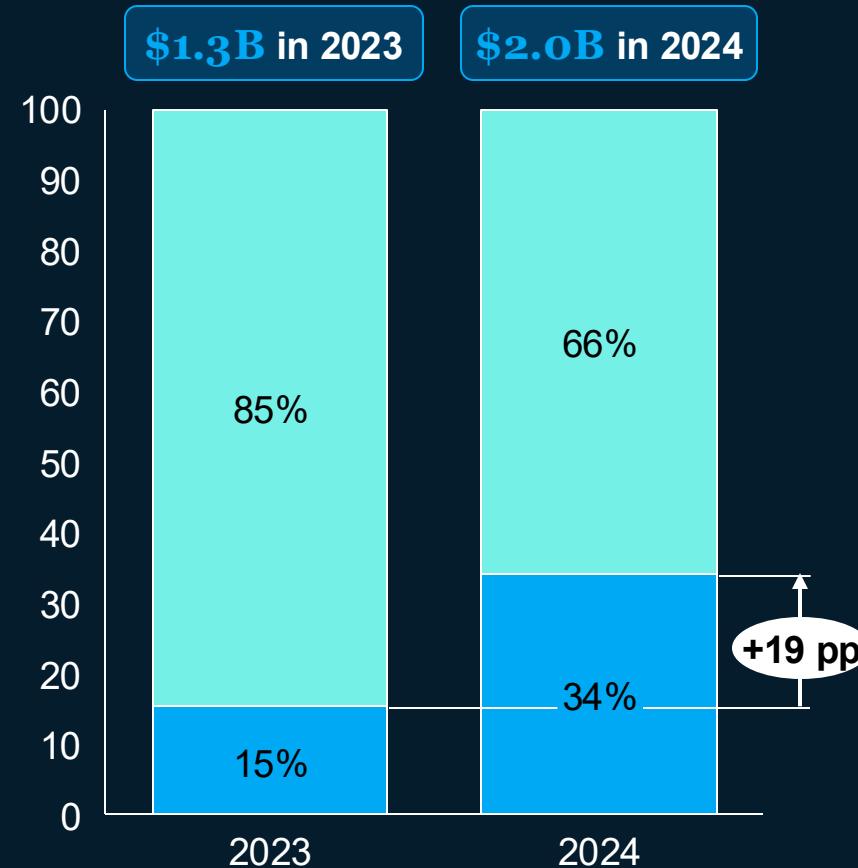
2. Economic value is defined as the additional revenue and saved costs that the application of QC can unlock.

3. Per annum.

Investment landscape: Funding for QT start-ups in 2024 nearly doubled year over year, to \$2 billion.

Total investment,
public vs private

■ Private ■ Public



Total number of
start-ups founded

+42% YoY

Geographic factors driving start-up creation:

EU fragmentation: 8 of 19 newly founded quantum start-ups originated in the EU, reflecting the EU's continuing push to start new companies rather than focusing only on mature start-ups

Asia accelerating: Asian countries are rapidly catching up (with 5 of 19 start-ups), driven by increased government support and strategic partnerships aimed at scaling quantum technologies

Public announcements

Government announcements totaled **\$1.8B** in 2024, with early 2025 investments already exceeding **\$10.0B**—driven largely by Japan's **\$7.4B** quantum investment—indicating a breakout year for the sector



Funding breakdown

Quantum computing accounts for ~80% of total quantum investments, with superconducting technologies receiving the highest funding, followed by photonic networks



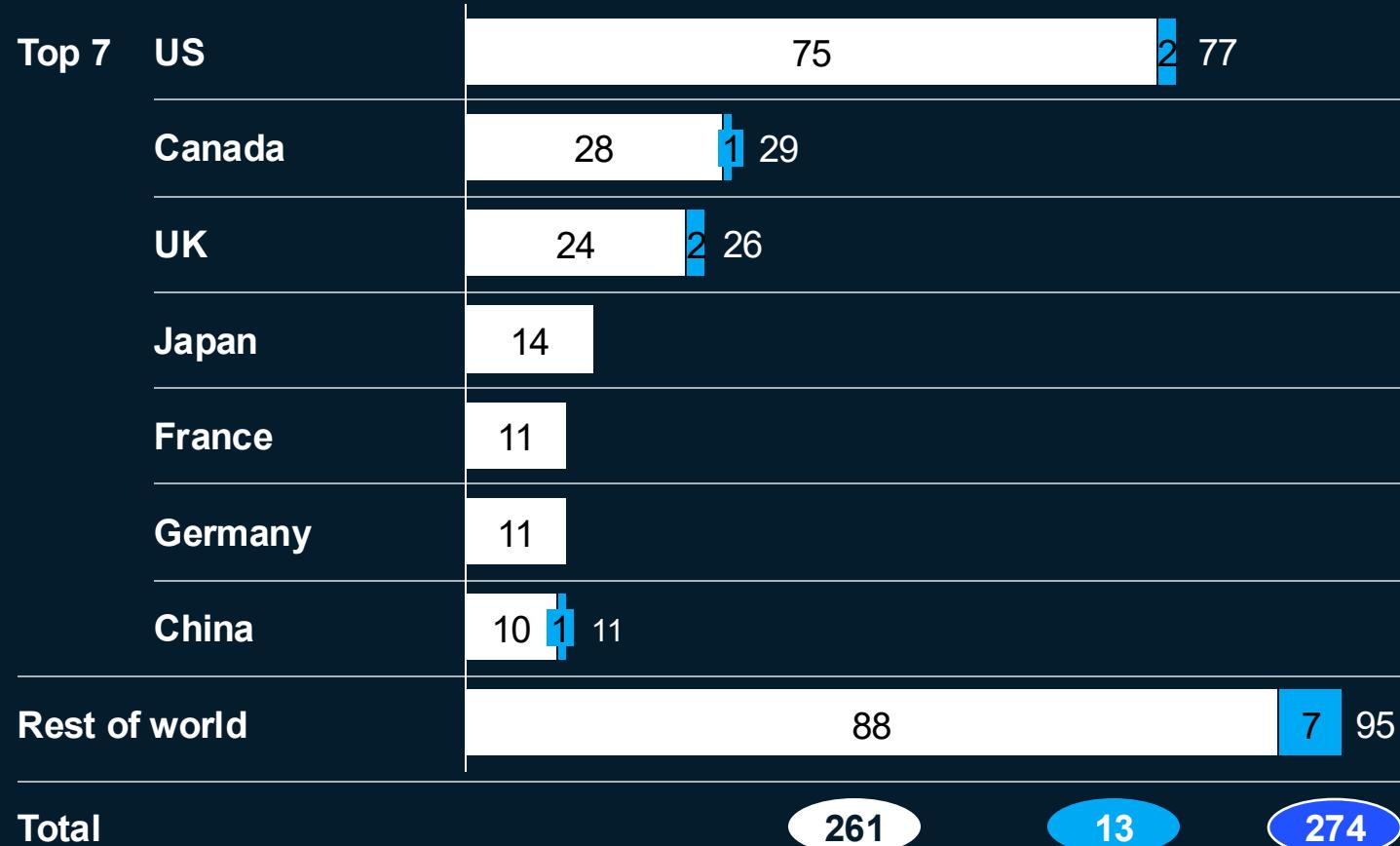
Funding by start-up stage

Funding is shifting away from scaling quantum start-ups as investors focus on early innovation and mature start-ups (~70% of total investment), driven by a desire to maximize return on innovation or reduce risk



Clusters and start-ups: Start-ups are increasingly consolidating into clusters, with emerging hubs in Asia and growing clusters in the US.

QC start-ups



■ Number of companies, end of 2023

■ Additional companies in 2024

■ Total number of companies

Emerging clusters



Tel Aviv

Tel Aviv hosts Israel's leading academic institutions and start-ups, which focus on QT development across the tech stack

Seoul

Seoul hub connects local universities and research organizations with emerging start-ups and industry players

Abu Dhabi

Abu Dhabi is emerging as a QT hub, supported by institutions such as TII and Khalifa University, with a focus on AI and quantum innovations

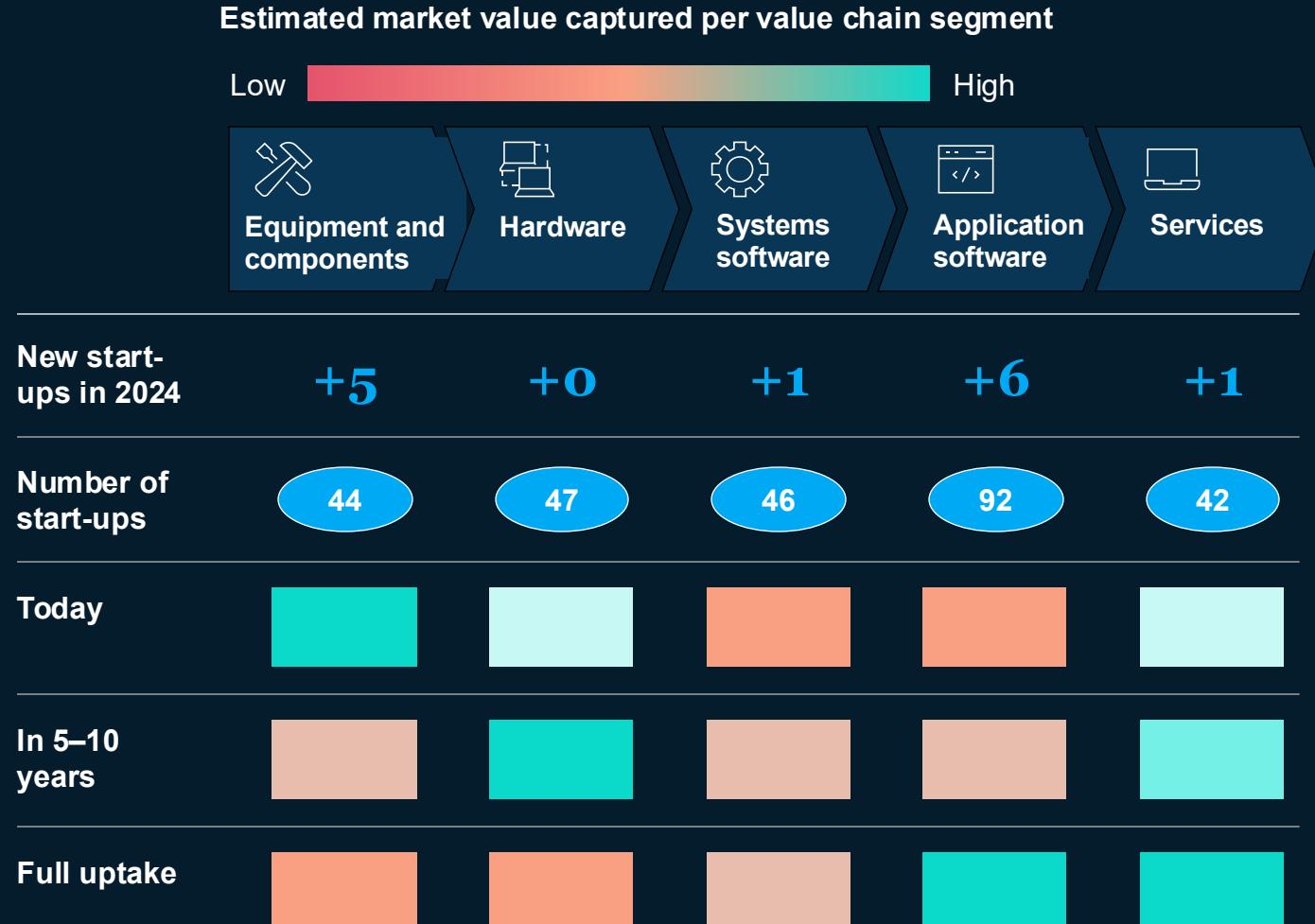
Established clusters



US quantum initiatives, including federal and state-level investments, have accelerated the emergence of key QT clusters:

- Illinois committed \$500M in 2024 to support quantum infrastructure and partnerships
- Maryland launched an initiative in early 2025, aiming to catalyze over \$1B in public-private investments

Value chain: Most new start-ups are emerging in equipment and components and application software.



Key insights

- In the hardware segment, big tech players (eg, AWS, Google, IBM, and Microsoft) are making substantial investments, underscoring both the segment's foundational importance and the capital intensity it demands
- The equipment and components segment has the largest value today, but this is expected to shift toward application software and services over the next decade
- Equipment and components attract investment attention due to lower-risk opportunities, caused by the hardware player-agnostic nature of the segment
- Equipment and components and application software account for a majority of new start-ups in 2024 (11 of 13), indicating a focus from emerging companies

QComm: Q-Day will introduce a pivotal shift in security, requiring early adoption of QComm and driving market growth.

Q-Day definition

The point at which quantum computers can break classical encryption, exposing sensitive data and creating an urgent need for quantum-safe security measures



Impact after Q-Day

Sensitive data using legacy encryption (including critical private information) becomes vulnerable, leading to potentially large economic and societal disruption



Q-Day drivers

Primary Q-Day driver is innovation affecting system performance, significantly affected by funding, talent, player breakthroughs



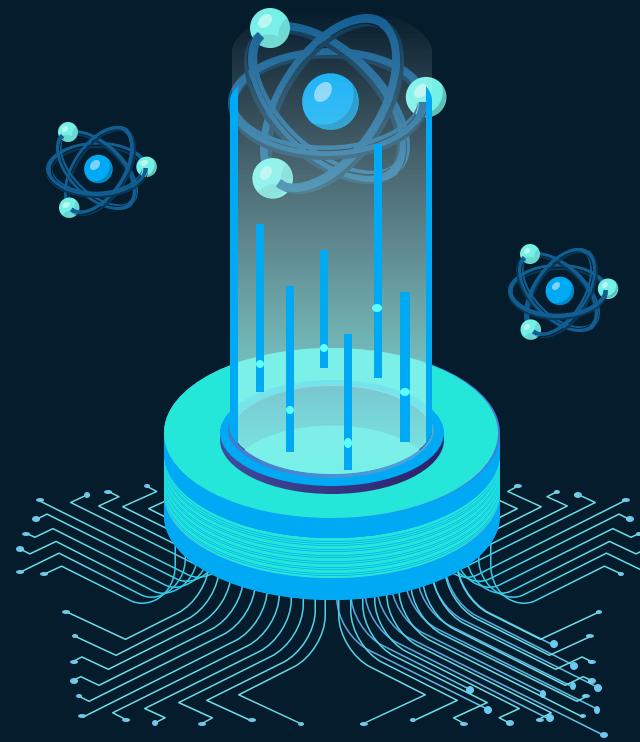
Key insights



Q-Day could be a critical shift in security strategies, requiring early adoption and potential partnerships with early movers in QComm and networks

Total QComm market size was ~\$1.0B in 2023 and is projected to reach \$10.5B–\$14.9B by 2035 with a CAGR of 22–25%

Governments are expected to hold the largest customer share, at 62–66% as of 2023; private sector involvement is projected to grow rapidly



Source: Alice & Bob; Crunchbase; expert interviews; Google; Craig Gidney and Martin Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, April 2021; IBM; literature review; Microsoft; PitchBook; press search; Quantinuum; *Quantum Computing Report*; QuEra; S&P Capital IQ; Gabriel Popkin, "The internet goes quantum," *Science*, 2021, Volume 372, Number 6546; McKinsey analysis

QT impact on cutting-edge technologies: QT is a key enabler within the broader disruptive tech ecosystem, offering powerful synergies.

Selected technologies based on *McKinsey Technology Trends Outlook*

Nonexhaustive

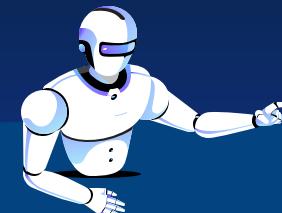
AI and machine learning

Play a central role in accelerating quantum software and benefit significantly from the computational power quantum computers could offer



Robotics

Drives automation in quantum manufacturing and potentially benefits from quantum technology through enhanced computing power, optimized software applications, secure communication and authentication, and improved navigation and sensing precision



Sustainability and climate tech

Demand energy-efficient and high-impact solutions, making them both beneficiaries and drivers of innovation in quantum technologies—with significant benefits from boosted computing power, algorithm optimization, and molecular simulation

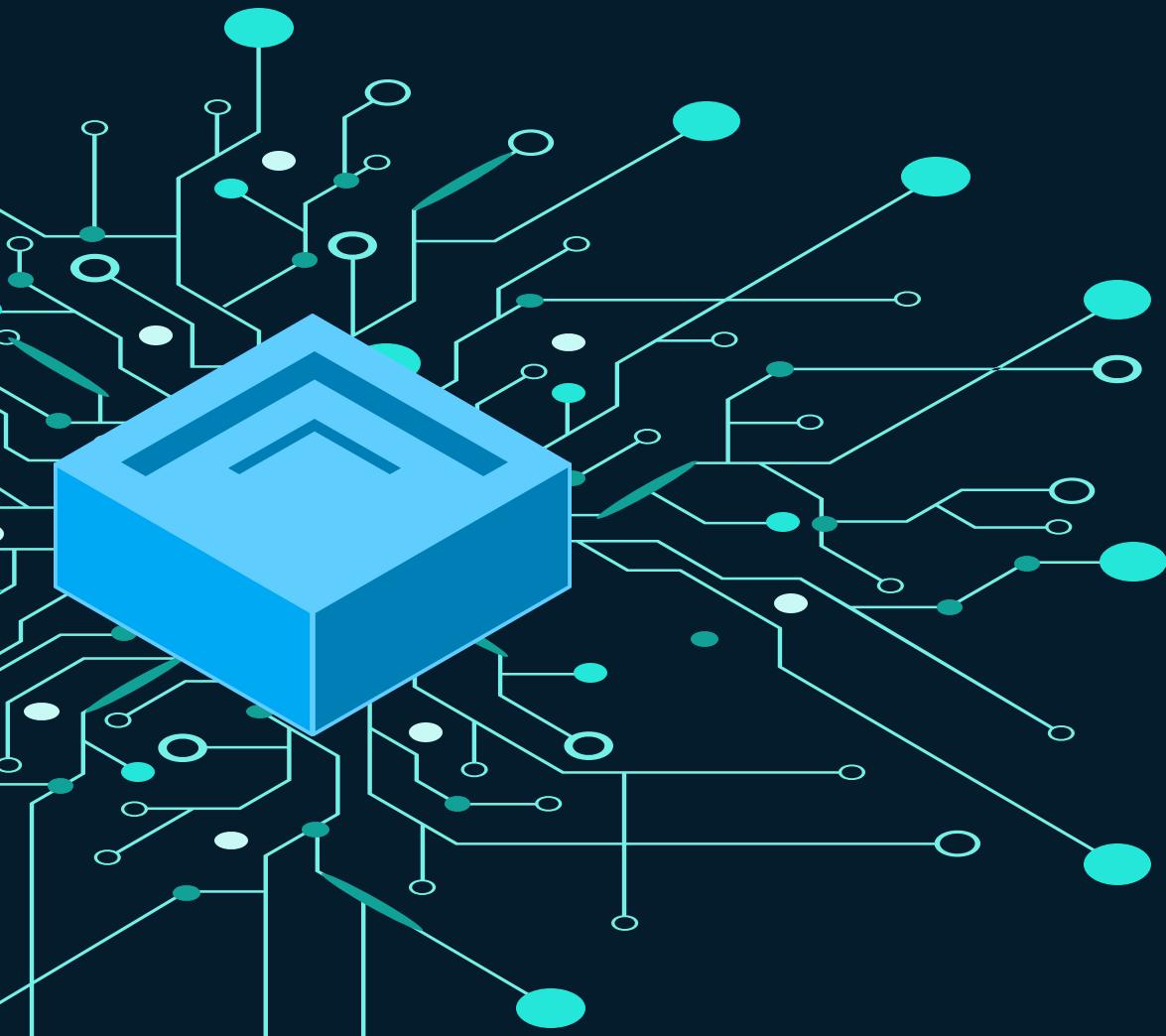


Cryptography and cybersecurity

Face both existential risks and transformative opportunities from quantum capabilities, making this a potential critical area of impact



Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

Key players are reaching groundbreaking milestones, reshaping the QC ecosystem toward scalable logical qubits (1/3).

Selected QC announcements

Nonexhaustive



Photonic networks



Superconducting circuits



Spin qubits



Neutral atoms



Trapped ions



Topological qubits

Company	Innovation and claim	How it works	What it means	Publication ¹
Google	Demonstrated 1 logical qubit with a fidelity of ~99.86% (ie, 0.143% error) for a distance-7 surface code (a specific configuration of qubits used for quantum error correction), using 105 physical qubits	The Willow processor is a 105-qubit superconducting QC processor enabling logical qubits. By encoding logical qubits across increasingly large patches of physical qubits, it illustrates exponential suppression of error rates, a key prediction of quantum error-correction theory	Google showcases how the error rate can be suppressed exponentially as more physical qubits are added using error-correction algorithms, paving the way for logical qubit computations	“Quantum error correction below the surface code threshold”
AWS	Encoded 1 logical qubit in 5 physical cat qubits for data and 4 ancilla qubits for syndrome detection (ie, 9 physical qubits total), with a fidelity of ~98.35% (ie, ~1.65% error rate) for a distance-5 code, slightly better than a smaller distance-3 code (fidelity of ~98.25%, error rate of ~1.75%)	Superconducting quantum circuit combines bosonic cat qubits with ancillary transmons to create logical qubit memory, reducing the number of physical qubits required relative to more conventional superconducting (typically rely on large number of transmons for error correction) qubits and correcting cat-qubit phase-flip errors	AWS chip showcases how cat qubits can be combined with transmon qubits to achieve logical qubits with fewer physical qubits, potentially creating a more efficient way of producing quantum computing hardware	“Hardware-efficient quantum error correction using concatenated bosonic qubits”
IBM	Prepared logical “magic state” in 4 physical qubits (non-Clifford resource state) on a 27-qubit Falcon chip with fidelity above the breakeven point (ie, higher than a single physical qubit’s fidelity) using a distance-2 code	Superconducting quantum circuit is being prepared in so-called magic states (ie, states able to complete a universal set of logic gates) Preparing high-fidelity “magic states” is thus essential (in this case, better than for the individual physical qubits)	High-fidelity “magic states” are essential as they reduce the number of physical qubits required to produce large-scale quantum computing architectures	“Encoding a magic state with beyond break-even fidelity”

1. Publication name as published on ArXiv.

Key players are reaching groundbreaking milestones, reshaping the QC ecosystem toward scalable logical qubits (2/3).

Selected QC announcements

Nonexhaustive



Photonic networks



Superconducting circuits



Spin qubits



Neutral atoms



Trapped ions



Topological qubits

Company	Innovation and claim	How it works	What it means	Publication ¹
Microsoft  Topological qubit	Claimed the world's first quantum chip powered by a new topological core architecture that it expects to realize quantum computers capable of solving meaningful, industrial-scale problems in years, not decades	The Majorana 1 chip employs nanowires arranged in a specific configuration, each hosting Majorana modes to potentially form a single qubit. These configurations can potentially be connected across the chip, allowing for a scalable and modular design	The Majorana 1 chip aims to overcome the challenges of quantum decoherence and error correction that have hindered previous quantum computing efforts and paves the way to large-scale qubits	"Interferometric single-shot parity measurement in an InAs-Al hybrid device"
QuEra  Logical qubit	Two high-fidelity logical qubits were demonstrated using a reconfigurable neutral atom array of up to 280 physical qubits , achieving improved gate performance by improving the surface code from distance-3 to distance-7 (specific configuration of qubits for quantum error correction)	This achievement was made possible through advancements in error-correction techniques and the development of innovative logical qubit architectures. By improving the fidelity, QuEra has demonstrated the feasibility of more accurate and reliable quantum computations	QuEra chip demonstrates a programmable quantum processor operating with up to 280 physical qubits, indicating neutral atom platform is scalable toward systems with large numbers of logical (physical) qubits	"Logical quantum processor based on reconfigurable atom arrays"

1. Publication name as published on ArXiv.

Key players are reaching groundbreaking milestones, reshaping the QC ecosystem toward scalable logical qubits (3/3).

Selected QC announcements

Nonexhaustive



Photonic networks



Superconducting circuits



Spin qubits



Neutral atoms



Trapped ions



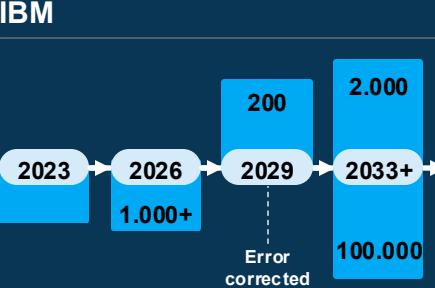
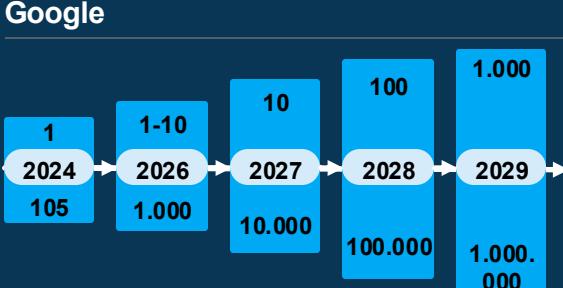
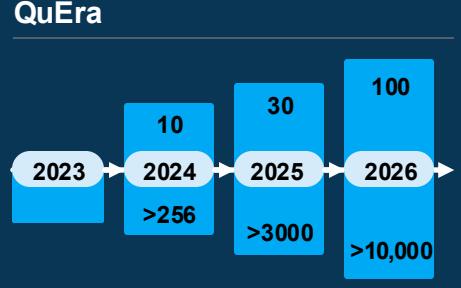
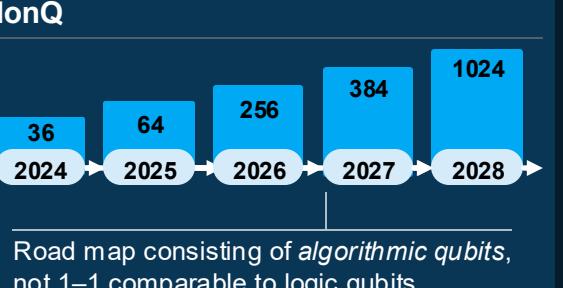
Topological qubits

Company	Innovation and claim	How it works	What it means	Publication ¹
Pasqal  <i>Logical qubit</i>	Developed hybrid quantum-classical algorithm that detects conical intersections —critical points where two potential energy surfaces of a molecule cross. These intersections are pivotal in photochemical processes such as vision and photosynthesis	Pasqal's method uses the company's quantum computer to detect conical intersections in molecules, key points where energy surfaces cross and chemical reactions often happen. The algorithm works by using a quantum circuit to track how the molecule's quantum state changes	Pasqal's method provides a practical quantum algorithm for identifying critical features in molecular systems, paving the way for more efficient simulations of complex chemical processes.	"A hybrid quantum algorithm to detect conical intersections"
Quantinuum  <i>Post-selection</i>	Fault-tolerant teleportation of 1 logical qubit with a logical process fidelity of 97.5% encoded with 7 data and 3 ancilla qubits (out of a 30-ion device), using the Steane code	Trapped ion qubits (mix of data and ancilla qubits) are used for fault-tolerant teleportation of logical qubits (however, no logical gate operations conducted)	The system showcases fault-tolerant teleportation for trapped ions, as teleportation enables reliable information transfer and entanglement distribution across qubits, critical for scalable QC	"High-fidelity and fault-tolerant teleportation of a logical qubit using transversal gates and lattice surgery on a trapped-ion quantum computer"
Atom Computing  <i>Logical qubit</i>	24-qubit logical entangled state encoded in 48 qubits on a 256-atom neutral-array processor ran a 28-logical-qubit Bernstein–Vazirani algorithm with error rates better than using 28 physical qubits (ie, showcasing error suppression) using a distance-2 code	Neutral atom quantum processor consisting of 256 Ytterbium atoms leveraged to encode a 24-qubit logical entangled state and showcasing error suppression Surface-2 codes used provide a proof of concept, showcasing how logical states can be error suppressed	Array of neutral atoms showcases error suppression (despite small error codes), illustrating how neutral atoms can be a promising modality toward logical qubits	"Logical computation demonstrated with a neutral atom quantum processor"

1. Publication name as published on ArXiv.

Leading quantum computing companies have road maps toward scalable universal QC.

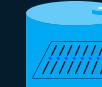
Nonexhaustive

Technology	Photonic networks	Superconducting (SC) circuits	Spin qubits	Neutral atoms	Trapped ions	
Qubit description	Occupation of a photonic waveguide	Difference in energy states of Cooper pairs between two sides of a Josephson tunnel junction	Electron spins of different materials; eg, an electron trapped within a silicon quantum dot or a color center in an insulator, controlled by laser light or microwave radiation	Internal energy levels of neutral atoms trapped by laser fields	Internal energy levels of ions trapped by electromagnetic fields	
Physical qubit count ¹	216 Xanadu	1.121 IBM 105 Google 16 Alice & Bob	84 Rigetti 64 Fujitsu	12 Intel	256 QuEra 1.110 Pasqal 1.180 Atom Computing 1.600 Inflection	36 IonQ 56 Quantinuum 20 Alpine Quantum Technologies
Example road map ¹	IBM 	Google 	QuEra 	IonQ 		
Logical qubits						
Physical qubits						

1. Qubit counts and road maps are selected based on available public announcements and available information as of February 2025.

Quantum control plays a key role in advancing quantum modalities and overcoming their challenges.

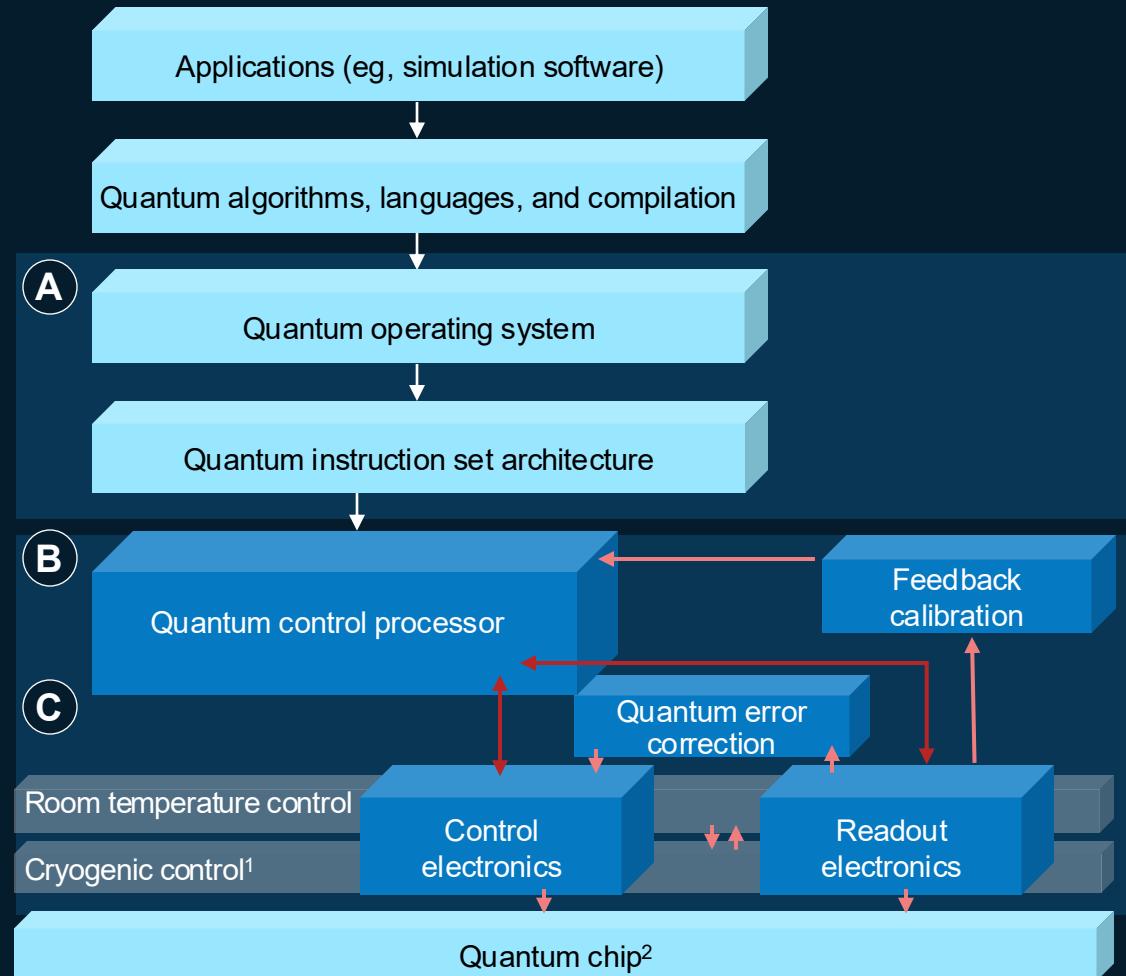
Nonexhaustive

 Qubit modality	Photonic networks	 Superconducting (SC) circuits	 Spin qubits	 Neutral atoms	 Trapped ions
Challenges of modality in control and readout	Manipulation of light paths, polarization, and phase Detection of single photons	Creation of microwave pulses used for control and readout Integration of control electronics inside cryostat to meet performance demands	Creation of microwave pulses used to induce coherent rotations of the spin states in silicon (often enhanced by voltage-controlled nanomagnets that create localized magnetic fields)	Manipulation and trapping of atoms using focused laser beams (optical tweezers) Capturing emitted light from atoms with camera for readout	Manipulation of ions through microwave control, using waveguides Drive qubits through photonic control using lasers
Cryogenic control	Not required	Required	Required	Some solutions	Some solutions
Technology-specific control challenges	Develop scalable high-precision laser systems while minimizing the use of active components	Build a scalable control architecture and improve calibration methods (eg, move from wiring to single flux quantum (SFQ) chip control)	Adapt SFQ chip control to spin qubits because they are smaller in size than superconducting (SC) qubits, and SFQ size matches the SC scale	Develop higher-powered lasers for individual qubit control, while also reducing photon loss	Optimize space in vacuum chamber as high number of individually controlled qubits must be placed here



Most specialized control vendors focus on superconducting and spin qubits, with plans to expand their offerings to other modalities in the near term

Quantum control can combine three techniques across the tech stack to increase the robustness of qubits.



1. Only relevant for superconducting and spin qubit technology.

2. Some qubit technologies do not require a chip—eg, neutral-atom quantum control arranges qubits in array.



Biggest area of improvement identified



Analog signals



High-speed digital



Error mitigation: Reduces errors through control software at the interface to control hardware; several players integrate error mitigation at this point using software-based, algorithmic post-processing calculations that leverage additional quantum processing unit (QPU) overhead to improve robustness



Error suppression: Aims to lower the rate at which errors occur in quantum systems at the lowest levels close to the hardware, at the control level, or through software suppression; ie, through pre-processing calibration, optimization, or reversible (coherent) error reduction without increase in run time or overhead



Error detection and error correction: Is key for quantum robustness as error detection and correction are two sides of the same coin enabled by redundancy of physical qubits (ancilla qubits) in defining logical qubits

The path to fault-tolerant QC requires robustness to mitigate noise and enable effective error correction.

A set of solutions that can work together to reduce noise



Quantum robustness could conquer noise and decoherence through the following:

<i>Technique</i>	<i>Timing</i>	<i>Overhead</i>	<i>Tech stack</i>
 Error suppression	Pre-processing	No overhead	Close to hardware
 Error detection and error correction (QEC)	Real time	Qubit overhead	Middleware and hardware
 Error mitigation	Post-processing	QPU overhead	Middleware and software

Deep dive: Error-correction solutions can be evaluated across six key criteria to provide a holistic view of performance.

Criteria to assess quantum error-correction solutions



Modality support

Compatibility of the error-correction method with different quantum hardware technologies, such as superconducting qubits, trapped ions, or photonic qubits



Code distance

Measurement of the minimum number of physical qubit errors required to corrupt a logical qubit irreparably. Higher code distances indicate greater error resistance and stronger fault tolerance



Architecture support

Alignment with specific qubit connectivity patterns, such as nearest-neighbor or more flexible connectivity, which affects the feasibility of implementing the method on certain quantum processor architectures



Scaling of QEC

Criterion gauging how effectively the error-correction method can be expanded to larger quantum systems while maintaining manageable resource requirements and robust performance



Qubit overhead

Evaluation of the number of physical qubits needed to represent a single logical qubit; higher overhead indicates more qubits are required to achieve fault tolerance, affecting scalability



Advancement in recent years

Measurement of progress made in research, development, and implementation of the error-correction method, highlighting how far the solution has evolved toward practical deployment

QS announcements revolve around industry use cases rather than academic breakthroughs, moving toward commercialization.

Selected QS announcements

Nonexhaustive

Company	Innovation	How it works	What it means	Announcement ¹
NASA	Demonstrated an ultracool quantum sensor in space (onboard the International Space Station) for the first time	Using a quantum sensor capable of detecting weak electromagnetic signals	Enables space missions to use QT to, eg, track water on Earth, explore the composition of moons and other planets, or probe cosmic phenomena	“NASA demonstrates ‘ultra-cool’ quantum sensor for first time in space”
Q-CTRL	Overcame GPS denial through quantum navigation , outperforming traditional systems in areas with no GPS signal	Using quantum magnetometers and proprietary software for detection of small magnetic variations	Provides reliable navigation solutions in environments where GPS is unavailable	“Q-CTRL overcomes GPS-denial with quantum sensing, achieves quantum advantage”
SandboxAQ	Launched commercial real-time navigation system powered by AI and quantum sensing	Leveraging proprietary AI algorithms, powerful quantum sensors, and the Earth's crustal magnetic field to create a geomagnetic navigation system	Provides an unjammable, all-weather, terrain-agnostic, real-time navigation solution in situations where GPS signals are unavailable or denied	“SandboxAQ announces AQNav—world's first commercial real-time navigation system powered by AI and quantum to address GPS jamming”
Quantum Diamonds	Developed quantum device tailored to semiconductor chip failure analysis using diamond-based quantum microscopy	Leveraging diamond-based quantum microscopy to detect and localize faults in integrated circuits by extracting electrical current information across multiple layers	Addresses challenges in semiconductor fabrication, improving yields and accelerating production ramp-up	“Launch of the world's first commercial quantum device for semiconductor failure analysis”

1. Based on publicly available data on the websites of NASA Jet Propulsion Laboratory, QCTRL, SandboxAQ, and Quantum Diamonds.

Key insights



- QS announcements are industry-driven and commercial, in contrast to, eg, academic breakthroughs in QC (often missing immediate commercial applications)
- QS commercialization is driven by maturity of the field as multiple use cases are already realized
- QS is spread across multiple industries and use case clusters; however, its adoption is expected to accelerate as QC and QComm mature and make progress toward commercialization

IP analysis shows a 13 percent year-over-year increase in patent grants; US companies lead in QComm and QS patent applications.

Key message

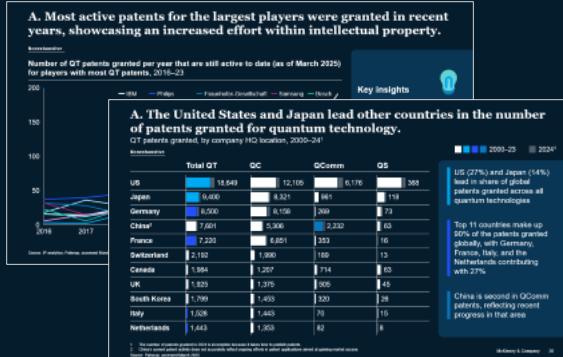
A. Patents granted¹

The activity of patents granted increased in 2024 (13% YoY)

IBM and Google are leading on number of granted patents

US companies are leading patent-granted activity across QT with highest growth in QComm

Analyses



B. Patent applications²

While US companies lead in overall QT patent applications, China leads in QC and consistently ranks second across overall QT

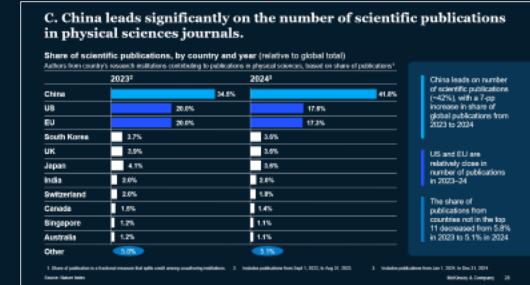
In QComm, US companies own 43% of patent applications



C. Publications

China leads in scientific publications with ~42% of the total and a 7-pp share of global publications from 2023 to 2024

US and EU relatively close (~17% in 2024, ~20% in 2023) in terms of publications through 2023–24

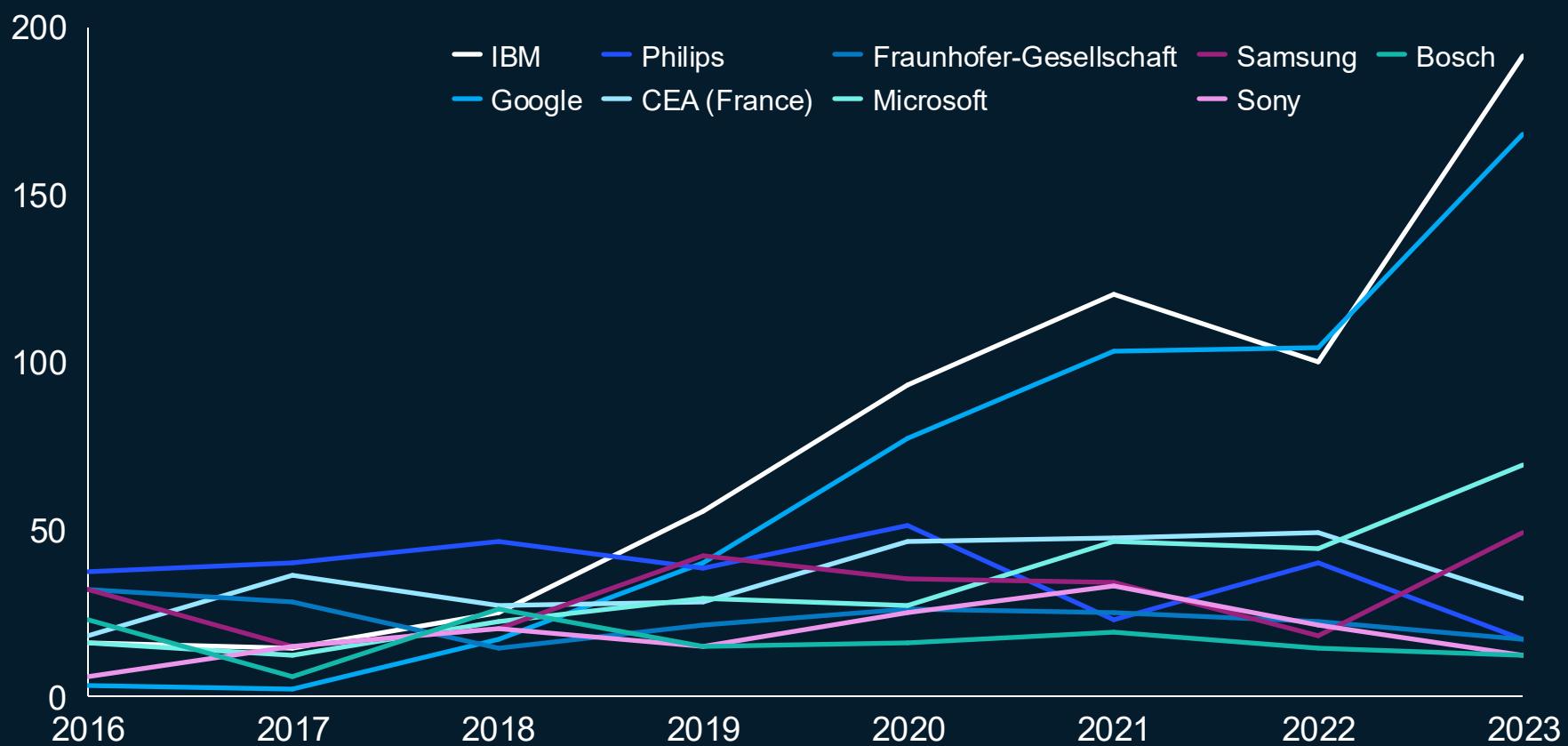


1. The approved outcome of a patent application, giving the inventor exclusive legal rights. Only granted patents are legally recognized and enforceable in the industry.
2. The first step in patenting an invention. It is a formal request to a patent office, including detailed documentation of the invention's design, function, and originality.

A. Most active patents for the largest players were granted in recent years, showcasing an increased effort within intellectual property.

Nonexhaustive

Number of QT patents granted per year that are still active to date (as of March 2025) for players with most QT patents, 2016–23



Key insights

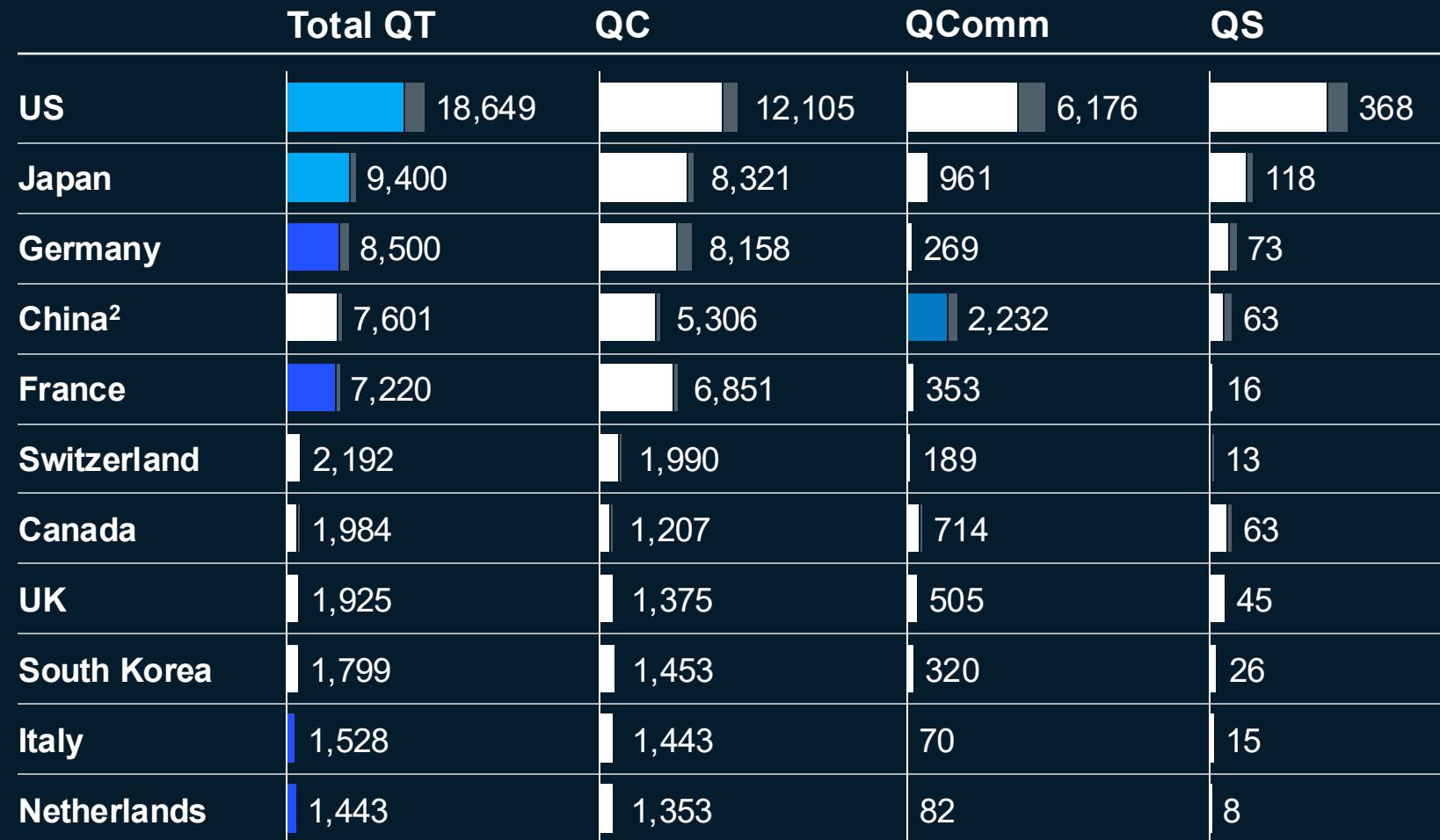
- IBM and Google saw a significant increase in the number of patents granted in 2023, illustrating an increased effort in IP
- Contrary to trend, CEA and Philips experienced the largest decrease in granted patents from a peak in 2022



A. The United States and Japan lead other countries in the number of patents granted for quantum technology.

QT patents granted, by company HQ location, 2000–24¹

Nonexhaustive



2000–23 2024¹

US (27%) and Japan (14%) lead in share of global patents granted across all quantum technologies

Top 11 countries make up 90% of the patents granted globally, with Germany, France, Italy, and the Netherlands contributing with 27%

China is second in QComm patents, reflecting recent progress in that area

1. The number of patents granted in 2024 is incomplete because it takes time to publish patents.

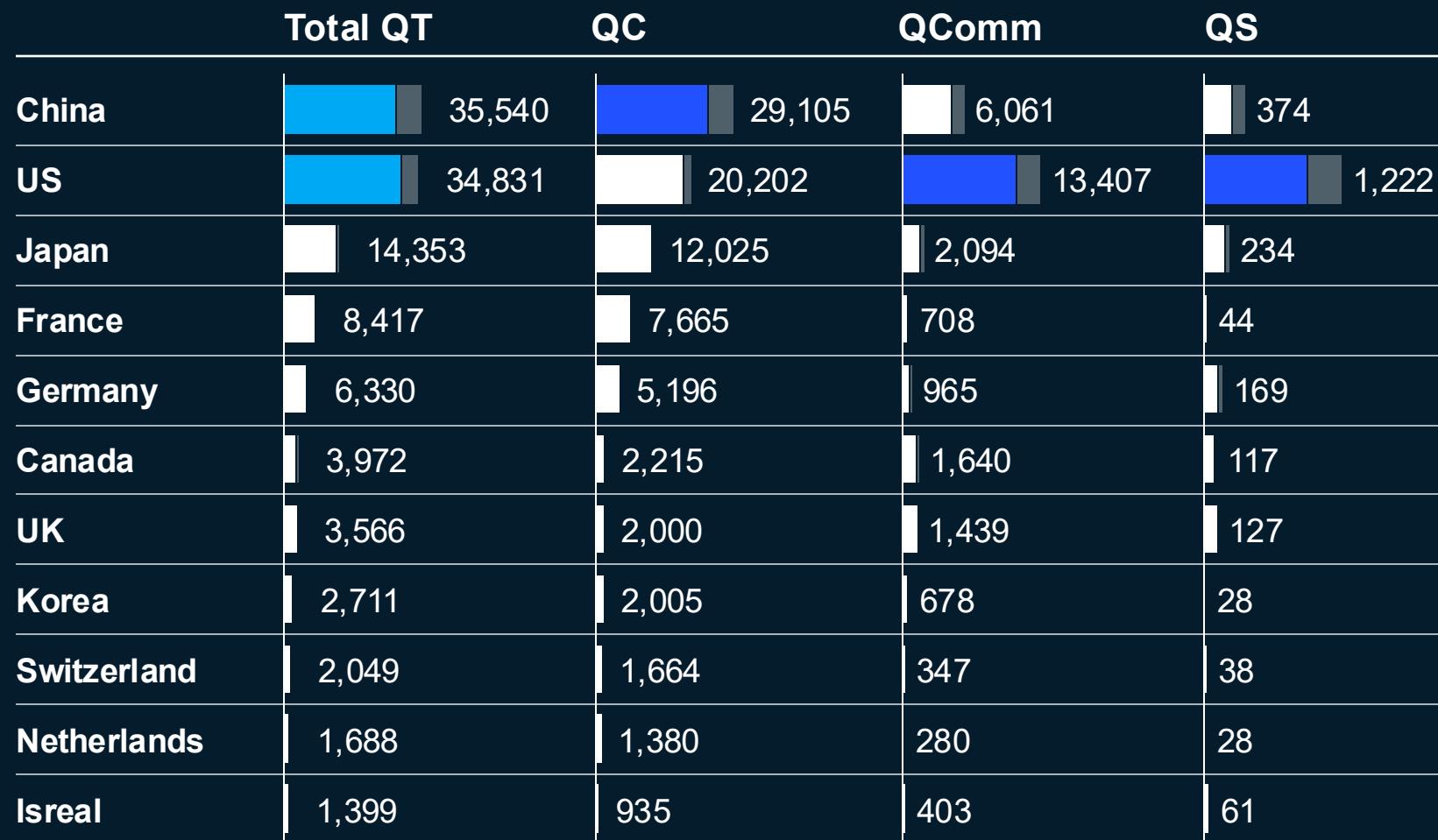
2. China's current patent activity does not accurately reflect ongoing efforts in patent applications aimed at gaining market access.

Source: PatSnap, accessed March 2025

B. The United States and China lead other countries in the number of quantum technology patent requests filed.

QT patent applications, by company HQ location, 2000–2024

Nonexhaustive



2000–23 2024

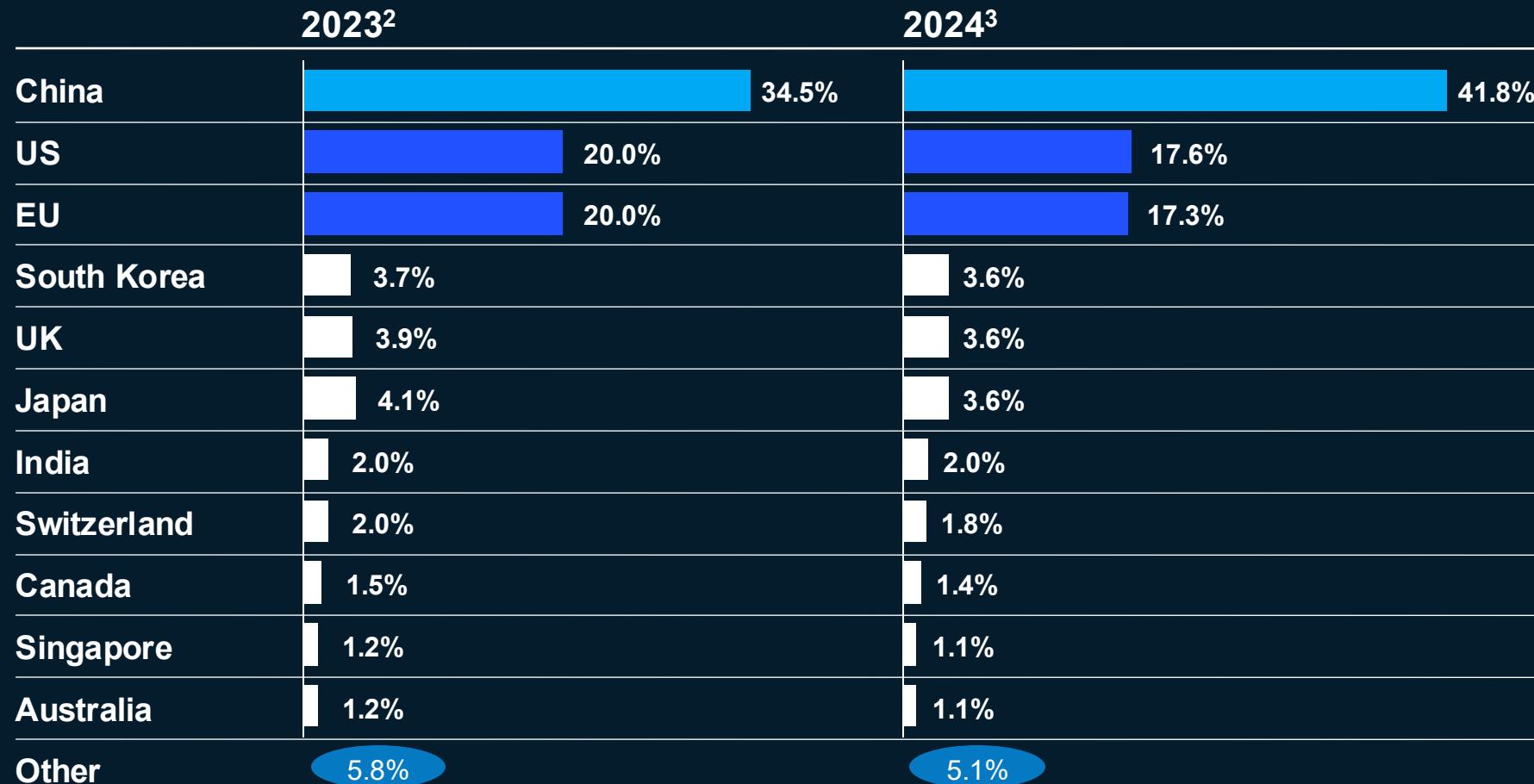
US and Chinese companies lead global QT patent applications, filing >50% of total global applications (~28% each)

US companies lead significantly in number of QComm and QS patent applications; Chinese companies lead in number of QC applications

C. China leads significantly on the number of scientific publications in physical sciences journals.

Share of scientific publications, by country and year (relative to global total)

Authors from country's research institutions contributing to publications in physical sciences, based on share of publications¹



China leads on number of scientific publications (~42%), with a 7-pp increase in share of global publications from 2023 to 2024

US and EU are relatively close in number of publications in 2023–24

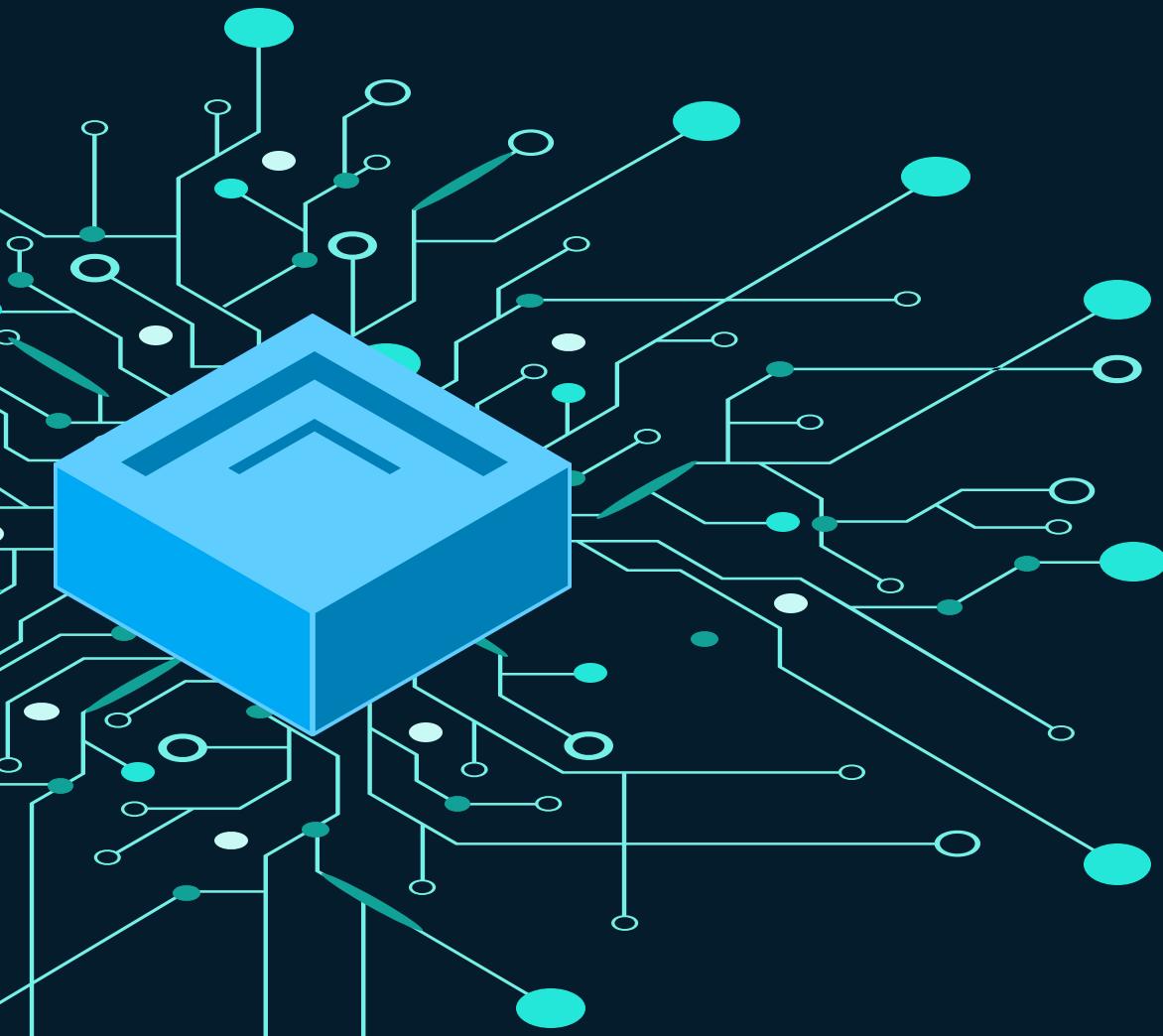
The share of publications from countries not in the top 11 decreased from 5.8% in 2023 to 5.1% in 2024

1. Share of publication is a fractional measure that splits credit among coauthoring institutions.

2. Includes publications from Sept 1, 2022, to Aug 31, 2023.

3. Includes publications from Jan 1, 2024, to Dec 31, 2024.

Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

To quantify the impact of QT, internal market size and value at stake were considered.



Internal market size

Market size of QT infrastructure, hardware, software, and services (ie, entire tech stack for quantum technologies)

QT tech stacks include:

- Physical components
- Assembled hardware
- Embedded and application software
- Networking (eg, cloud infrastructure)



Value at stake

Economic value from impact of quantum technologies on non-QT industries along the respective value chains

Example industries:

- Finance
- Pharmaceuticals
- Energy and materials

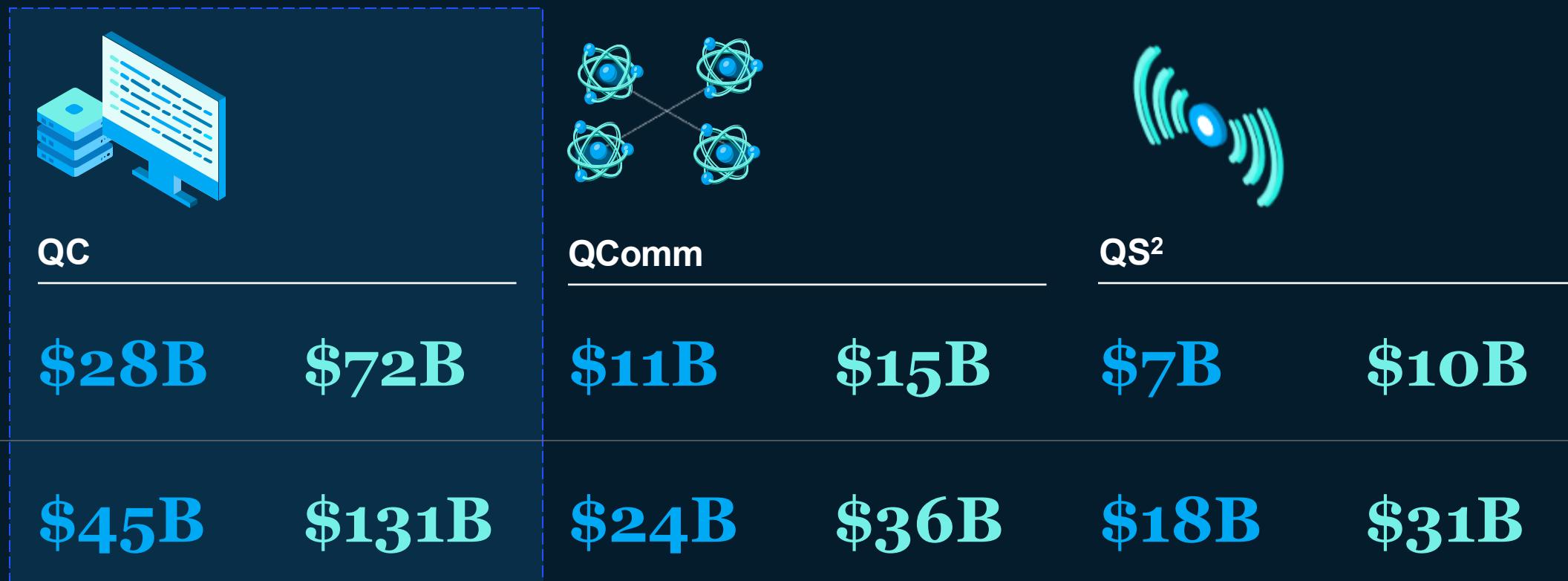
Example value chain components:

- R&D
- Logistics and distribution

The total internal market for quantum technology could reach an estimated \$198 billion by 2040.

Deep dive to follow Conservative growth rate¹ Optimistic growth rate

QT market-size scenarios in 2035 and 2040



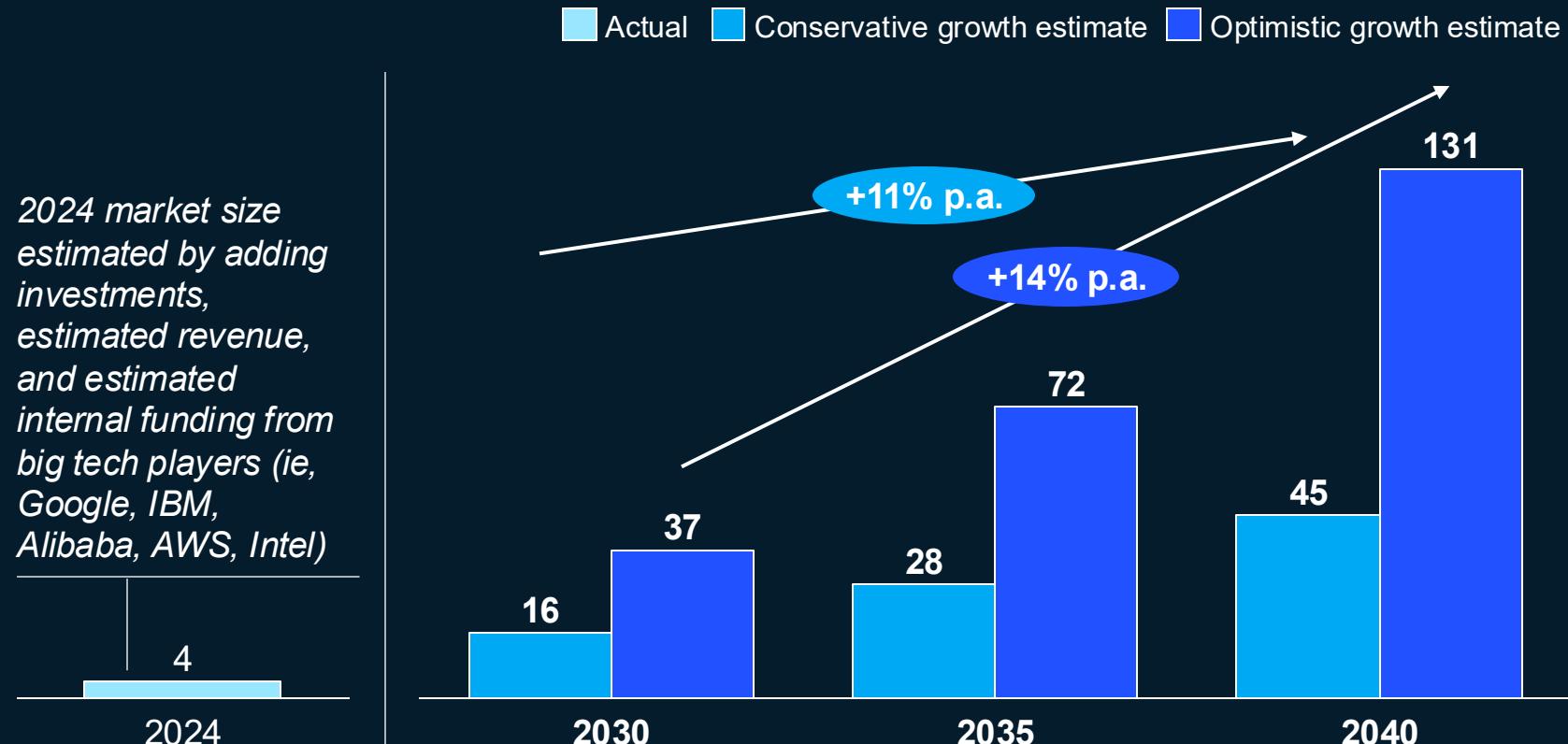
1. Based on existing development road maps and assumed adoption curves per technology.

2. Approach for QS updated through clusters of use cases based on recent development, announcements, and breakthroughs.

Source: Expert interviews; press search; McKinsey analysis

Deep dive: The QC market is expected to reach \$16 billion to \$37 billion by 2030 and \$45 billion to \$131 billion by 2040.

Expected market size (revenue plus external funding) in each scenario, \$ billion



Numbers include both funding and investment in QC and proceeds to quantum providers

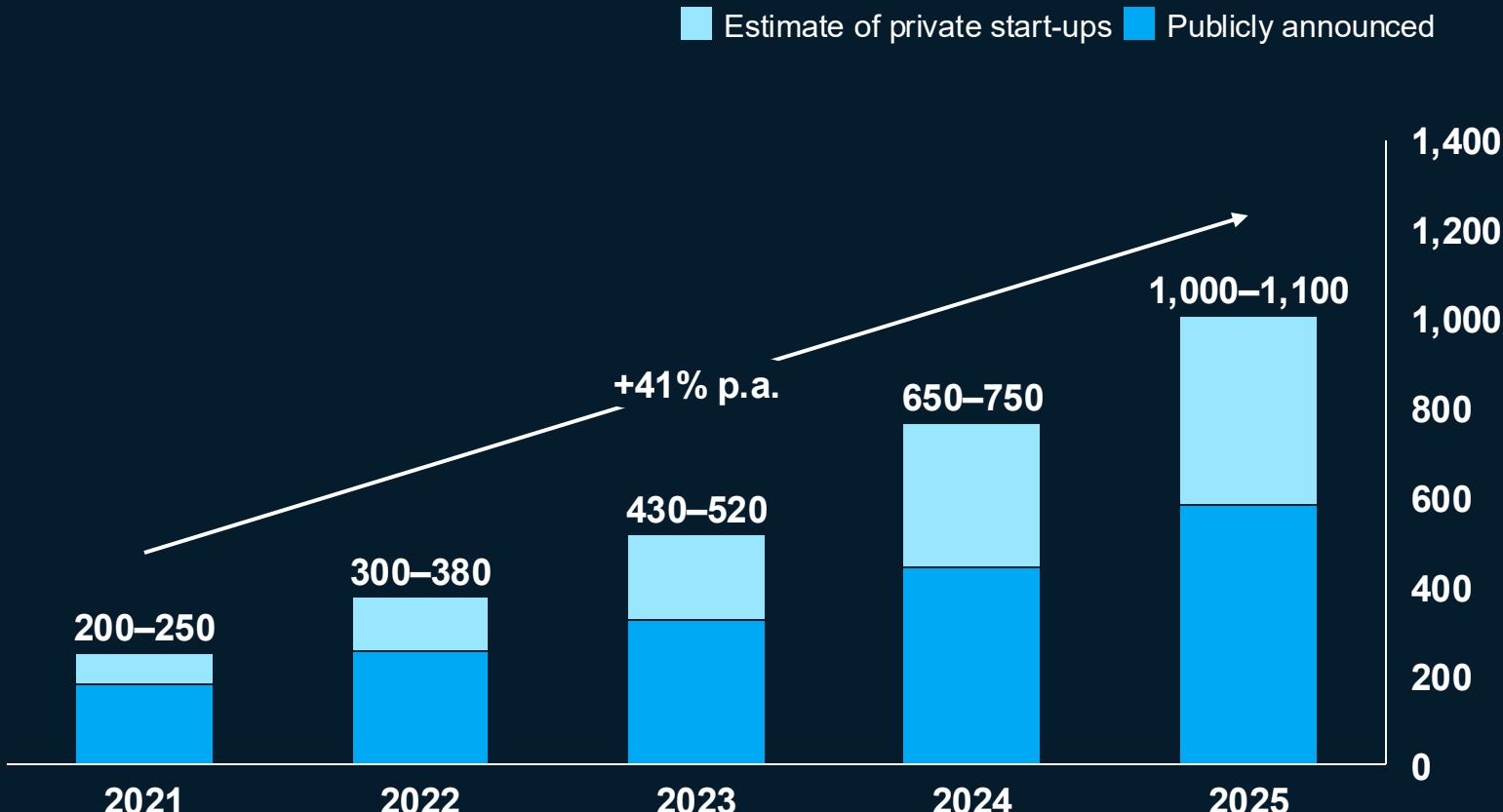
Key insights

- Expected overall market size of \$45B–\$131B in 2040, depending on assumed growth scenario
- Growth rates are expected to be 11–14% per year in the next decade
- The key difference between scenarios is the pace of solving today's challenges combined with higher demand in case of faster progress
- Industry capital expenditures in 2024 were ~32% of overall market size



Deep dive: Total revenue in QC reached \$650 million to \$750 million in 2024 and is expected to surpass \$1 billion in 2025.

Revenue estimates of QC companies, 2021–24, \$ million



Note: Estimated based on publicly announced revenues of QC start-ups and assuming 30–40% of total revenue is distributed among private companies with less than \$1M revenue according to market reports.

Source: Expert interviews; press search; McKinsey analysis

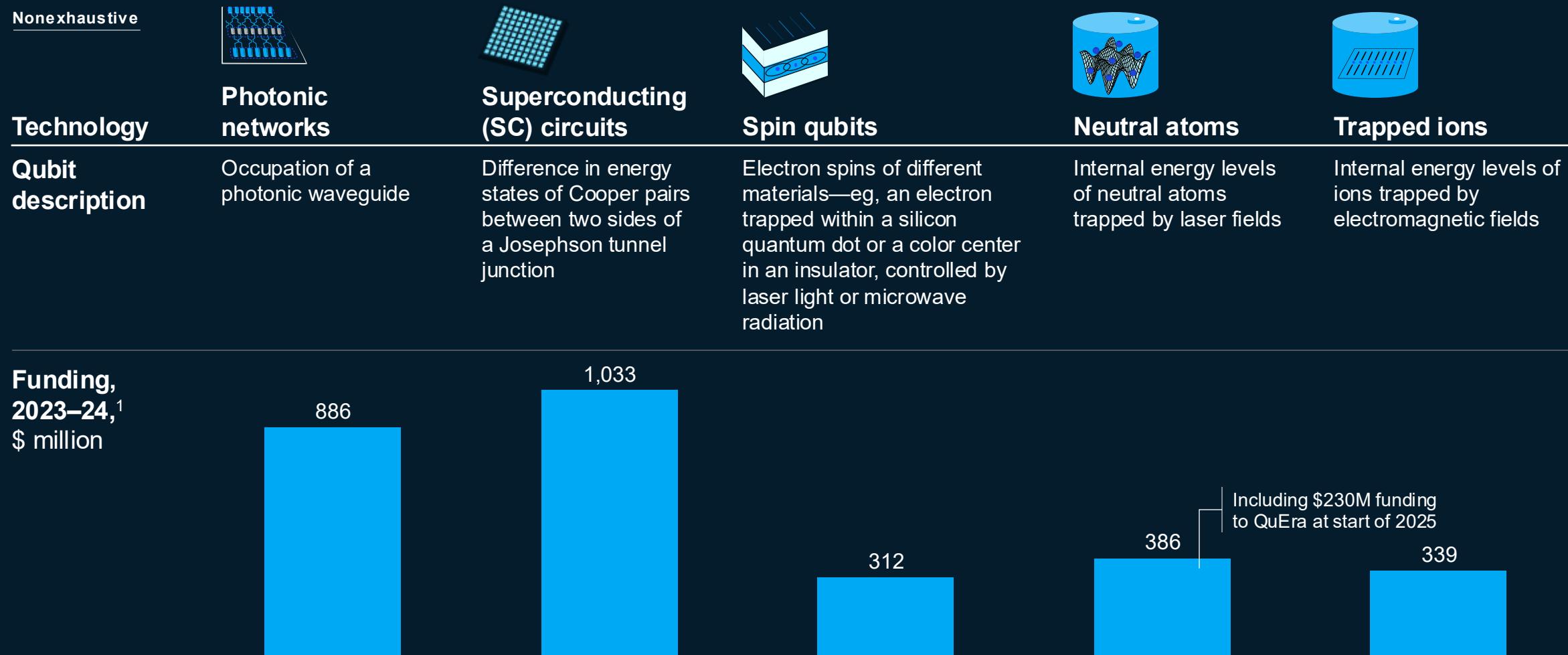
Key insights



Factors affecting revenue increase:

- Significant increase in revenue primarily driven by the growing deployment of quantum hardware (including cloud-based access), reflecting rising adoption across countries
- Increased government and defense sector funding have fueled the accelerating deployment of both quantum software and hardware solutions
- This estimate excludes system components

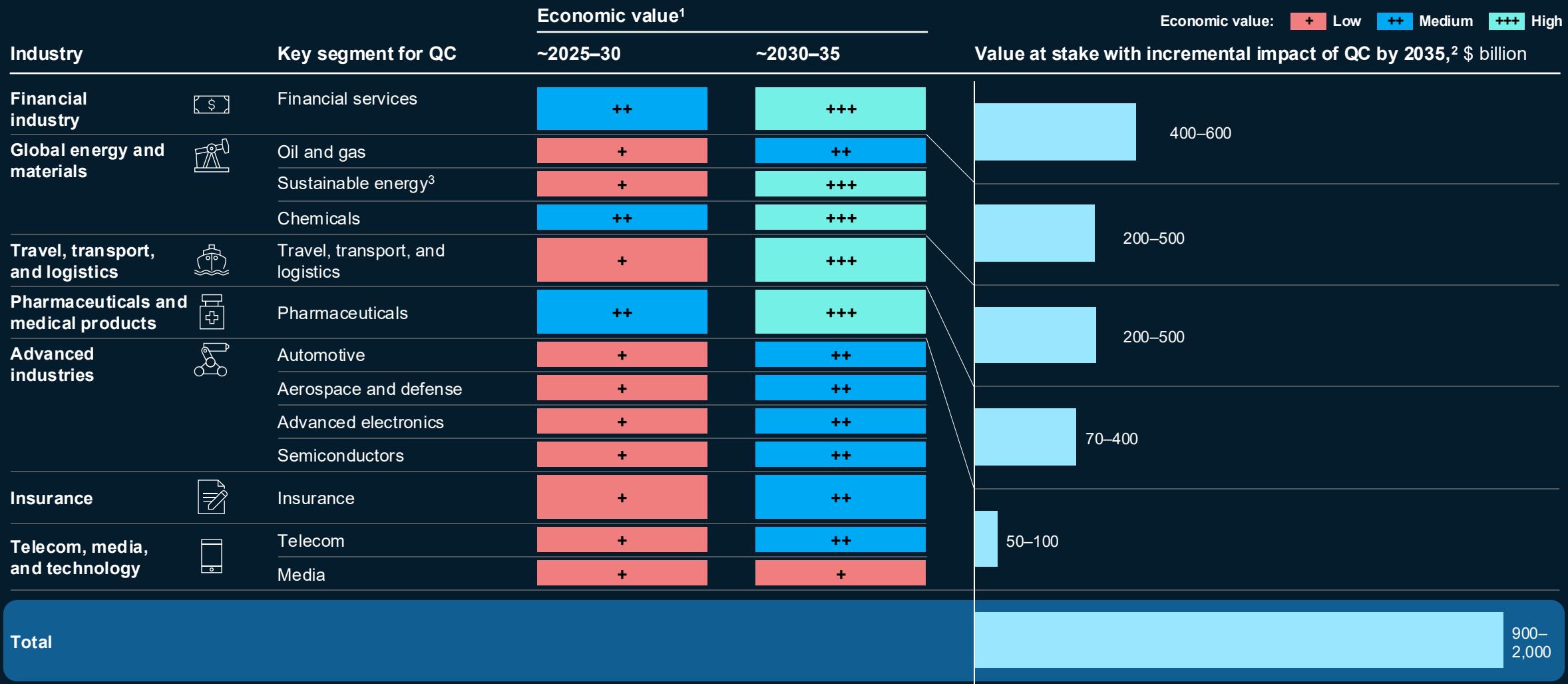
Deep dive: In QC, superconducting and photonic networks have raised the highest funding across quantum modalities.



1. Assumptions: \$100M funding per major player per year for SC circuits (Google, IBM, Alibaba, AWS); \$50M per medium players per year for spin qubits (Intel).

Source: Crunchbase; expert interviews; PitchBook; *Quantum Computing Report*; S&P Capital IQ; McKinsey analysis

Deep dive: QC presents a \$1 trillion to \$2 trillion use case opportunity, with rapid acceleration expected in the next five to ten years.



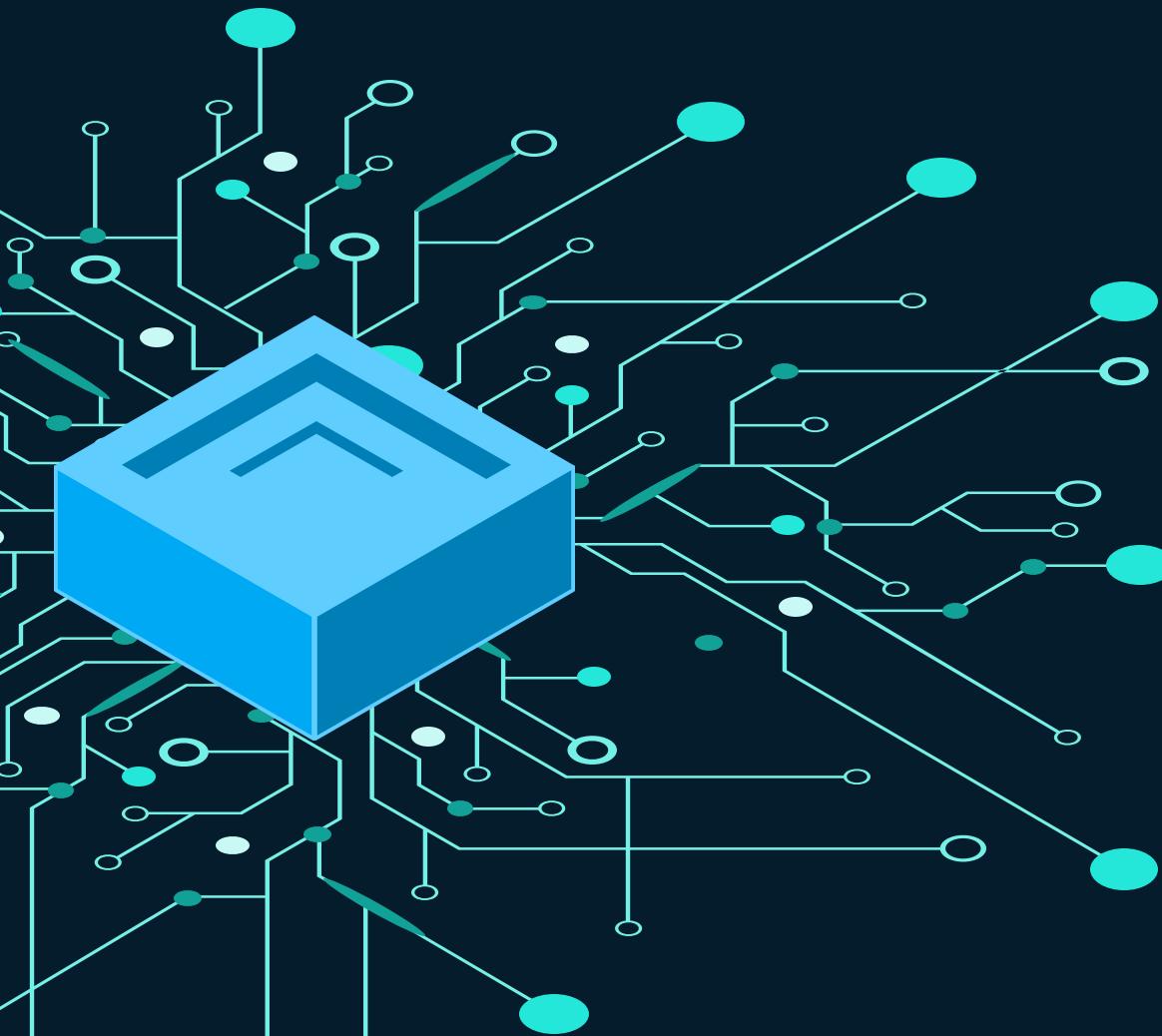
1. Economic value is defined as the additional revenue and saved costs that the application of QC can unlock. These industries are the most likely to realize this value earlier than other industries; therefore, they are examined in more depth.

2. Value estimates are approximative, not definitive projections for business value.

3. Sustainable energy market is expected to grow rapidly from 2022 to 2035. However, the 2035 market size is influenced by numerous factors and challenging to predict.

Source: Oxford Economics; McKinsey analysis

Contents



- Introduction
- Innovations and breakthroughs
- Market size and value at stake
- Investment landscape
- Private funding**
 - Public announcements
- Clusters and start-ups
- Value chain
- Deep dive into QComm
- QT impact on cutting-edge technologies
- Methodology and acknowledgments

QT start-up creation increased by 46 percent in 2024, with notable activity seen in the European Union and Asia.

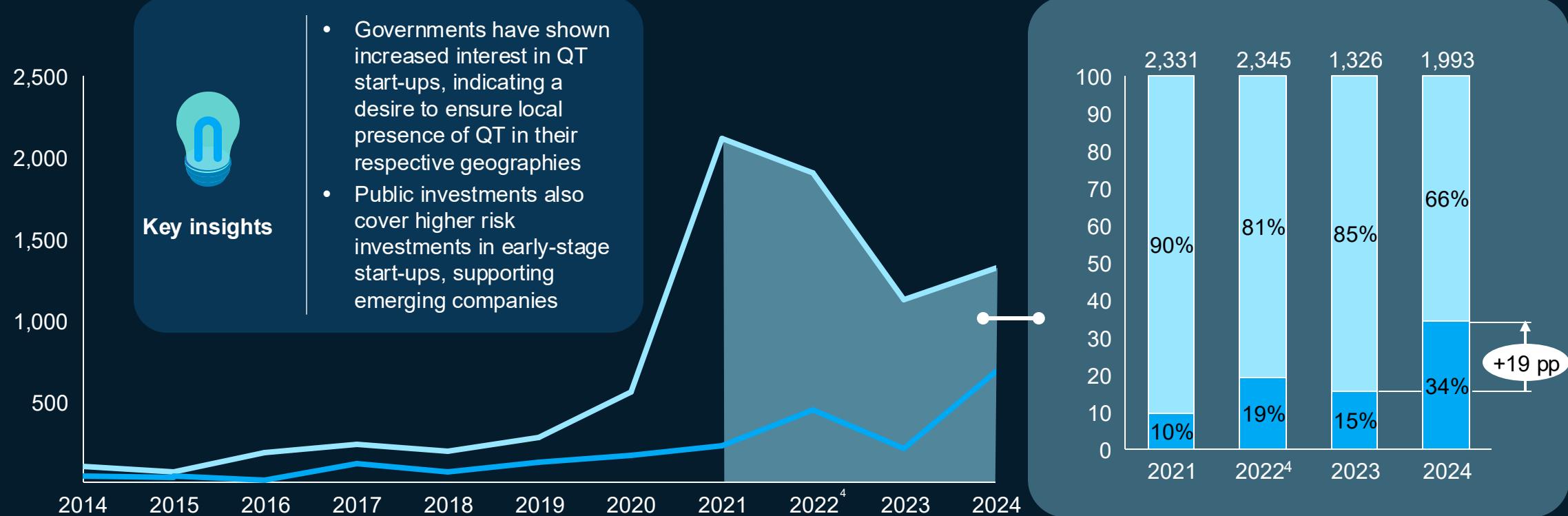


Total investments in quantum technology start-ups increased by about 50 percent year over year in 2024, reaching \$2 billion.



Public investment in quantum technology start-ups increased 19 percentage points from 2023 to 2024.

QT investments by funding type, 2014–24,¹ \$ million



1. Based on investment data recorded in PitchBook; actual investment likely higher (excludes investments with missing details on investment types); data availability on start-up investment in China is limited.

2. Includes investments from venture capital funds, hedge funds, corporations, angel investors, and accelerators.

3. Includes investments from governments, sovereign wealth funds, and universities.

4. Excludes other uncategorized funding data.

Source: PitchBook

McKinsey & Company

39

The combined value of the top two deals in 2024 was about \$925 million, representing almost half of the total deal value in 2024.

Top 10 investments in QT start-ups in 2024, by deal size (descending)

Company	Start-up HQ location	Segment	Deal size, \$ million	Deal type
1 PsiQuantum	US	Hardware manufacturing	624.63	Later-stage VC
2 Quantinuum	US	Hardware manufacturing	300.00	Early-stage VC
3 QunaSys ¹	Japan (US ³)	Hardware manufacturing	253.00	M&A
4 Zapata Computing ²	US	Systems software	190.00	Reverse merger
5 Q-CTRL	Australia	Systems software	113.97	Series B
6 Riverlane	UK	Systems software	82.13	Series C
7 Quantum Circuits	US	Hardware manufacturing	60.00	Series B
8 Quantum Source	Israel	Application software	50.00	Series A
9 Maybell	US	Component manufacturing	33.30	Series A
10 SEEQC	US	Hardware manufacturing	29.90	Series A2

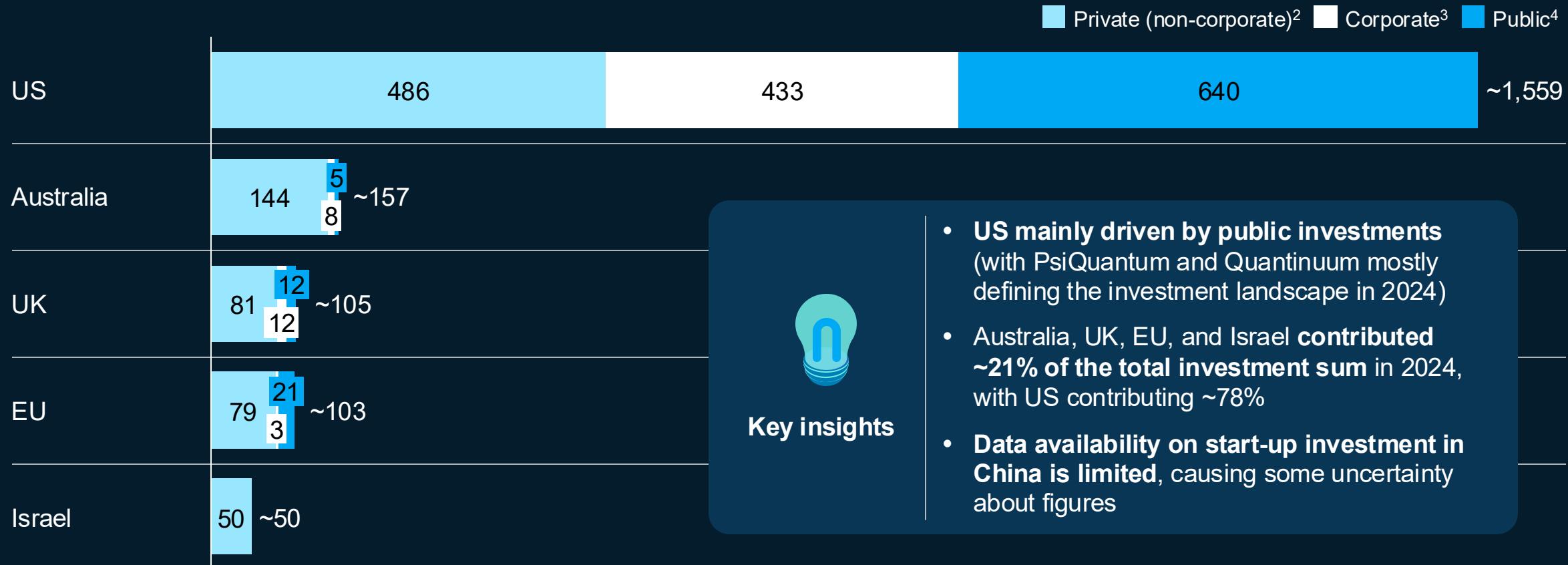
1. QunaSys, a Japanese innovator, announced a strategic partnership with Hon Hai Research Institute, affiliated with Foxconn.

2. In 2024, Zapata Computing Holdings Inc., a company specializing in quantum computing and generative AI solutions, ceased operations.

3. QunaSys's HQ is in Japan, but because the company is affiliated with Foxconn, it is counted as a US start-up in the analysis.

A majority of QT start-up investment in 2024 was directed toward US-based companies, primarily driven by government funding.

Total investment in QT by start-up location and primary investor type, 2024, \$ million¹



1. Based on public investment data recorded in PitchBook; actual investment likely higher (excludes investments with missing details on investment types); data availability on start-up investment in China is limited.

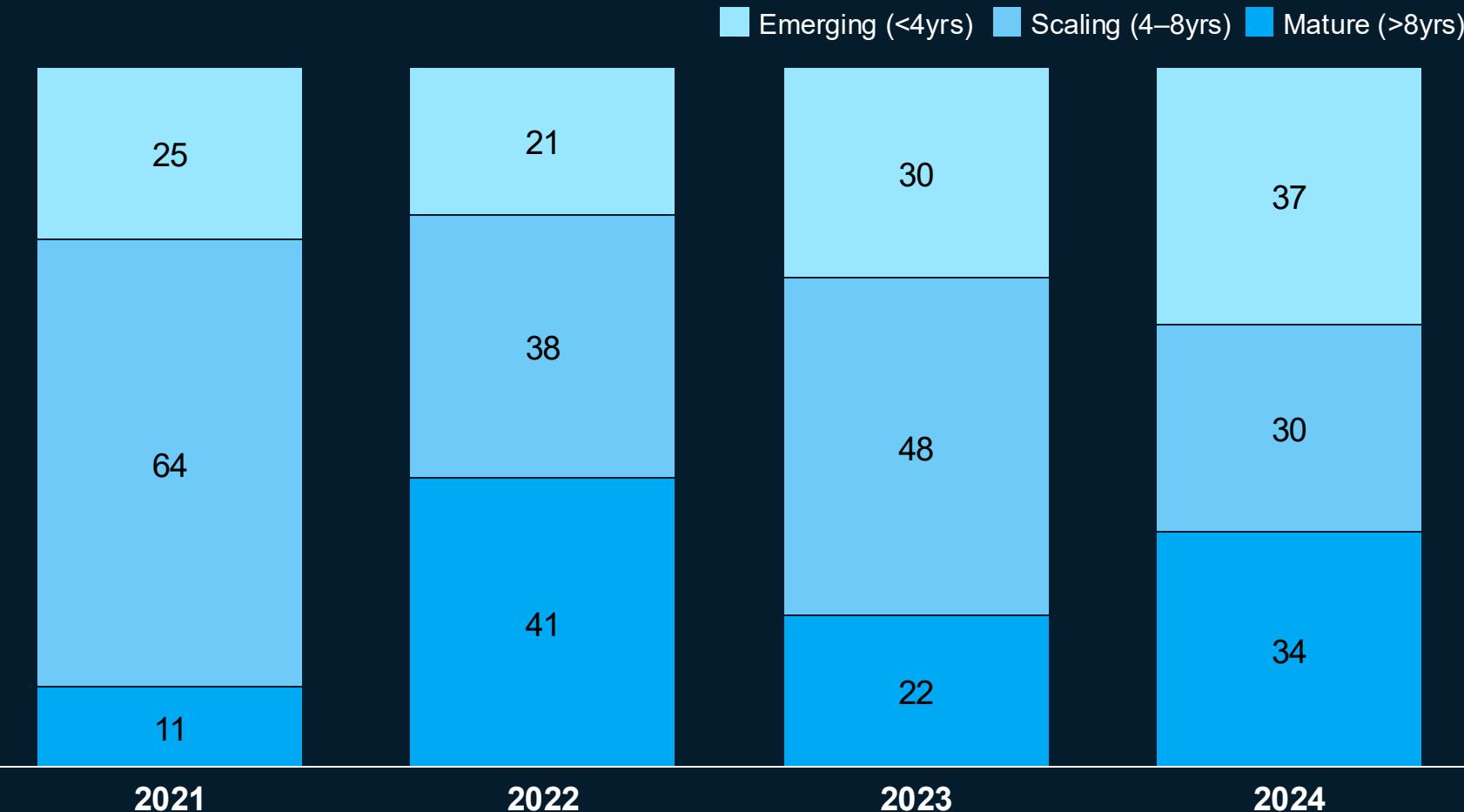
2. Investments from VC funds, hedge funds, angel investors, and accelerators.

3. Includes investments from corporations and corporate venture capital in external start-ups; excludes corporate investments in internal QT programs.

4. Includes investments by governments, sovereign wealth funds, and universities.

Funding is shifting away from scaling start-ups; investors are favoring emerging start-ups and mature companies with lower risk.

QT investment split based on founding years of start-ups in 2021–24,¹ %



1. Limited information available on activity in China.

Source: Expert interviews; press search; PitchBook; McKinsey analysis

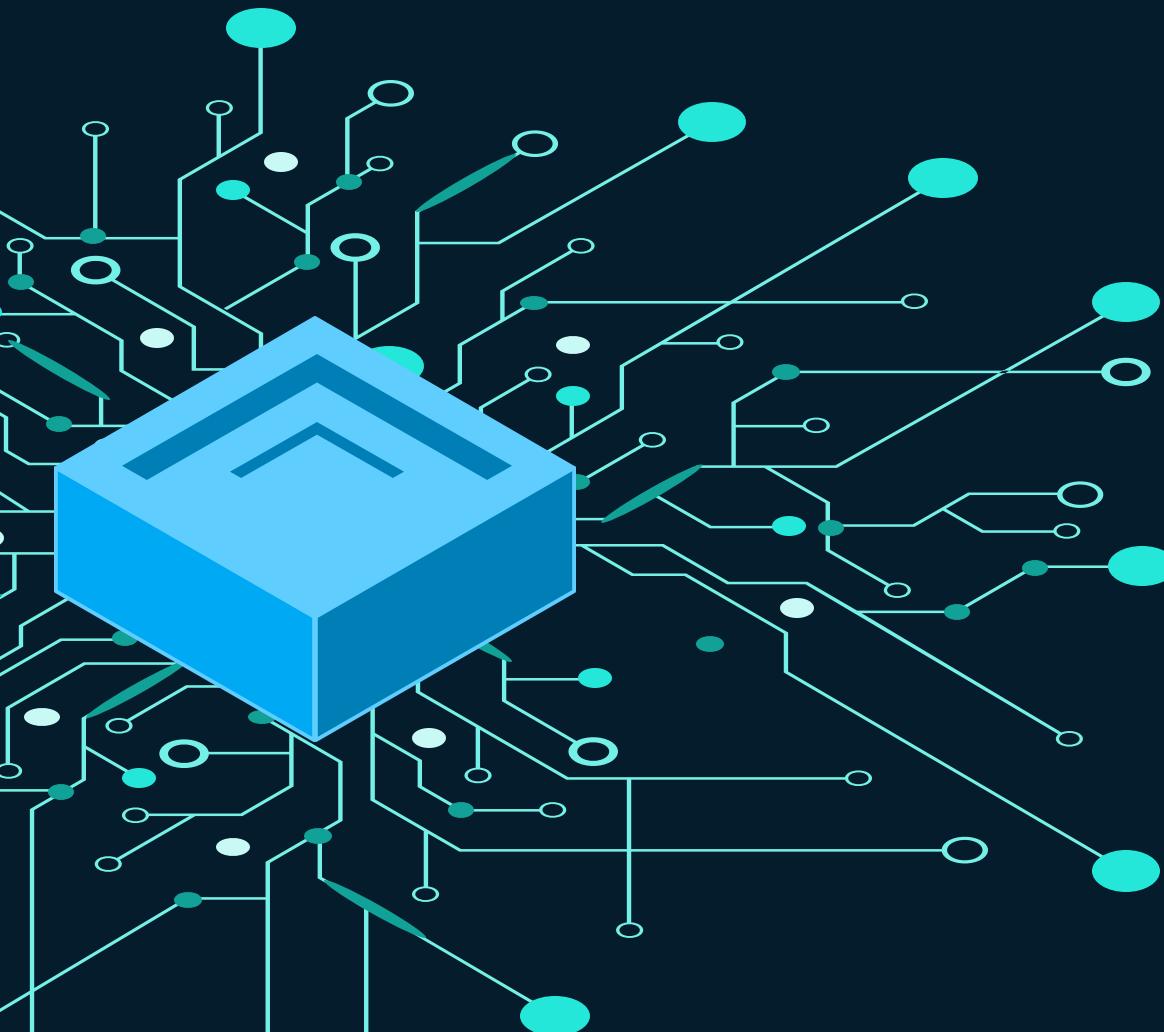
Key insights



Investments are shifting away from scaling start-ups toward emerging and mature start-ups:

- Investors are gravitating toward mature start-ups with validated technologies and revenue streams, reflecting a growing emphasis on risk mitigation and near-term returns
- Investors show strong appetite for emerging start-ups in Series A and B and those that are pioneering disruptive innovations, as investors seek first-mover advantages and higher expected ROI

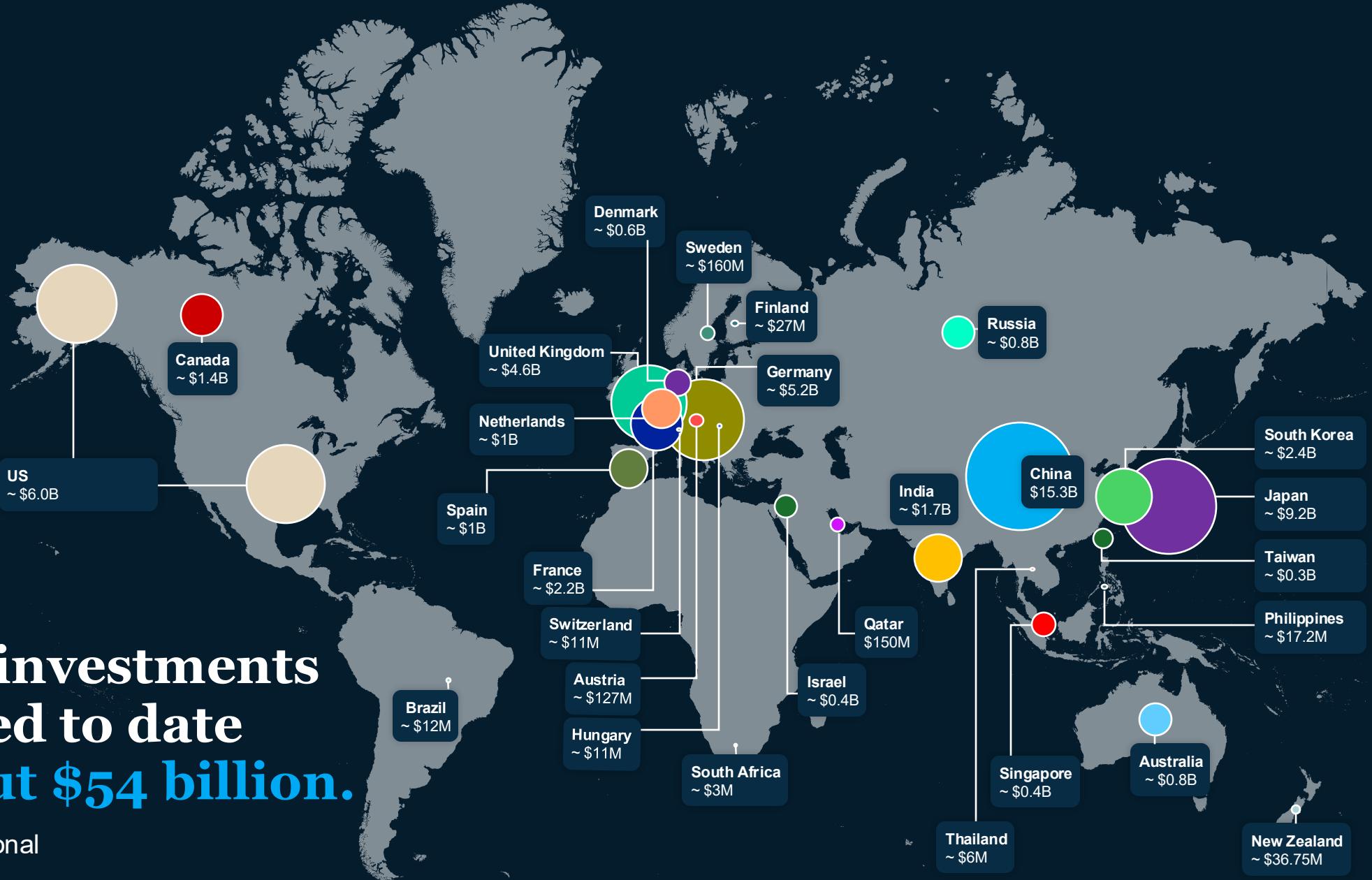
Contents



- Introduction
- Innovations and breakthroughs
- Market size and value at stake
- Investment landscape
 - Private funding
- Public announcements**
- Clusters and start-ups
- Value chain
- Deep dive into QComm
- QT impact on cutting-edge technologies
- Methodology and acknowledgments

National investments announced to date total about \$54 billion.

Estimated and directional



Note: Includes investments through April 2025. Limited transparency on commercial activity in China; excludes the recent \$136B announced investment toward emerging technologies due to unclear relevance for QT. Excludes \$680M Swedish investments toward research and innovation, and US–Swedish investment of \$40M toward next-generation networks, AI, quantum technology, and educational science within STEM areas. The boundaries and names shown on maps do not imply official endorsement or acceptance by McKinsey & Company.

Source: Press search

Announcements of public investments in QT reached \$10 billion in early 2025, with Japan accounting for nearly 75 percent.



Note: Figures may not sum to totals, because of rounding. Limited transparency on commercial activity in China; excludes the \$136B announced investment toward emerging technologies due to und clarity of relevance for QT; the ~\$15B investment is not shown here because it was announced before 2023. Excludes \$680M in Swedish investments toward research and innovation, and US–Swedish investment of \$40M toward next-generation networks, AI, quantum technology, and educational science within STEM areas. Also excludes Saudi Arabia's \$6.4B investment in 2022 toward future tech because no breakdown for quantum technology is present; excludes Qatar's (QIA) and Bpifrance's investment in Alice & Bob in 2025 due to missing breakdown of investment. Japan's investment is not exclusively directed toward quantum technology (includes next-generation chip design as well).

Public announcements surged to about \$10 billion in early 2025, led by major initiatives in Japan, Spain, and the United States.

Largest national and regional funding announcements; includes investments through Apr 2025

Nonexhaustive

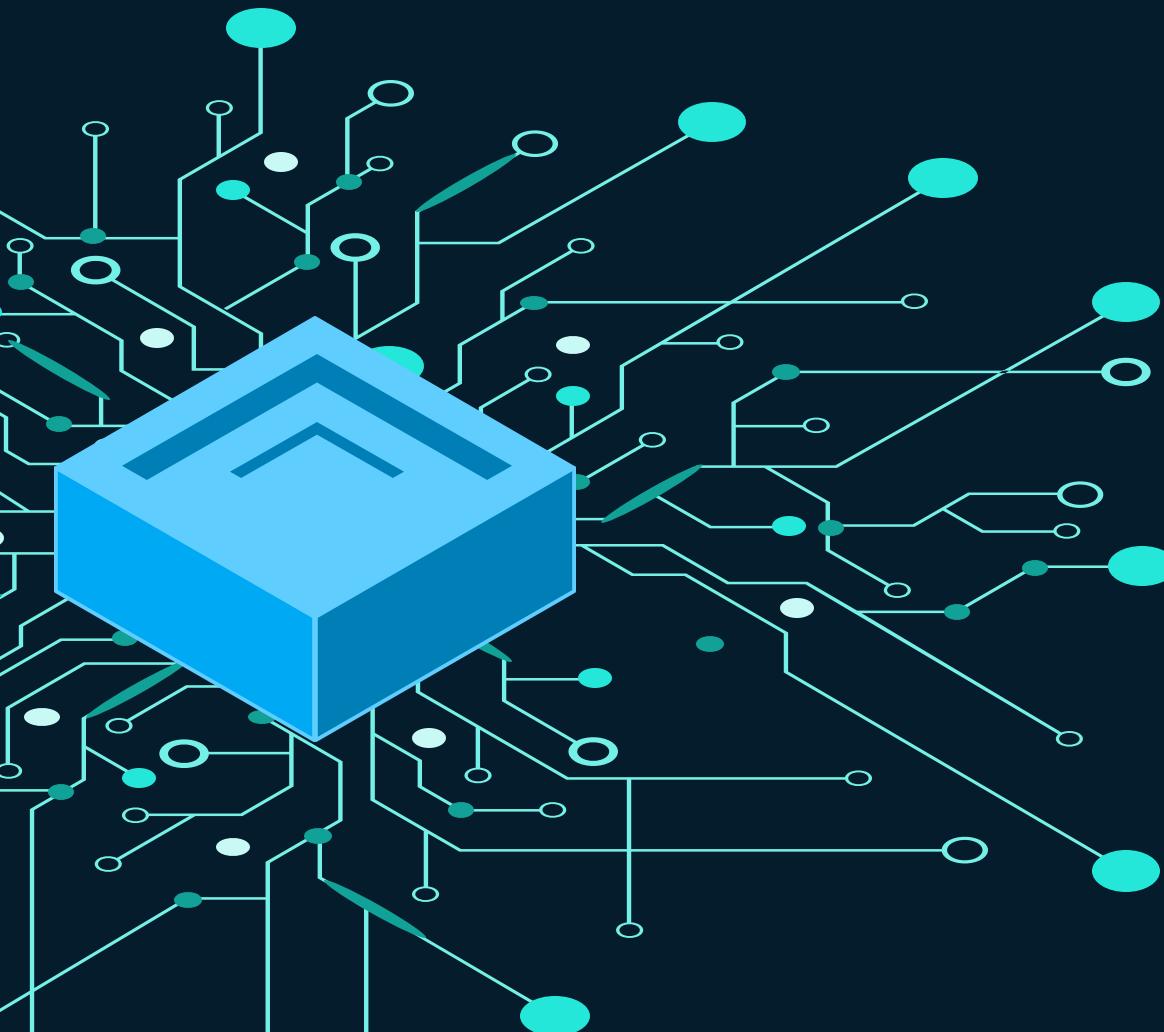
Announced in 2024 or Jan–Apr 2025

Announced before 2024

UK The UK government (Department of Science, Innovation, and Technology) announced \$130M in funding for five quantum research hubs in the UK	US US has multiple investments in QT, most significantly: \$500M from State of Illinois, \$625M from Department of Energy's Office of Science, and State of Maryland aiming to secure \$1B	Singapore Singapore announced National Quantum Strategy, covering ~\$222M investment toward QT research and talent over the next 5 years	Denmark Novo Holdings announced \$213M to support the development of a global QT innovation hub in Denmark <i>Note: Novo Holdings is an enterprise foundation with philanthropic objectives and thus not fully public</i>	China China has boosted government funding for quantum research and development to over \$15B, with applications in security, defense, and AI	UK The United Kingdom's National Quantum Strategy introduced new strategic goals for the next 10 years, including market growth stimulation, research, and talent, with additional investment worth \$3.1B	Canada The Canadian government launched its National Quantum Strategy with an announced \$360M investment in 2023	India The government of India announced the National Quantum Mission, which aims to seed, nurture, and scale up scientific and industrial R&D and create a vibrant and innovative ecosystem in QT, with \$730M in funding
Spain Spain announced its National Quantum Technology Strategy, dedicating \$900M toward 2030 to advance in quantum science	Canada Canada announced \$52M investment toward QT, covering QC, QComm, and QS	Australia The Australian Commonwealth and Queensland governments announced a \$620M financial package for PsiQuantum to build a utility-scale, fault-tolerant quantum computer in Brisbane	Japan The Japanese government announced \$7.4B for next-generation chip and QC research as part of its pledge to support semiconductor and AI development toward 2030	South Korea The South Korean government plans to invest \$2.3B in quantum science and technology by 2035, with a goal to become a leading player in QT	Netherlands The Netherlands' National Growth Fund allocated \$65M in funding to Quantum Delta NL in 2023. The organization is a main driver in the Netherlands' national ecosystem for quantum innovation	US In 2018 the US announced the National Quantum Initiative, which provides \$1.2B over five years for QT development.	France France has committed to establishing a leading position in the international QT race, with a \$1.3B investment announced in 2021

Note: Limited transparency on commercial activity in China; excludes the recent \$136B announced investment toward emerging technologies due to unclear relevance for QT.

Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

Existing quantum clusters continue to grow; growing investments support the development of emerging clusters.



Existing clusters; example organizations



Emerging clusters; example organizations

Key trends shaping the innovation of clusters for the quantum industry

Clusters continue to grow ...

Quantum clusters, usually anchored by research organizations, provide a critical mass of technology, talent, and infrastructure for cutting-edge advancements in QT

Existing larger (eg, Boston, Chicago) and smaller clusters are expected to continue to expand as the quantum industry matures

... while new clusters emerge and develop

As QT matures, growing commercial and public interest further drives growth of existing clusters—and development of new, emerging clusters

Companies often form partnerships or sponsor R&D at innovation clusters, providing funding and direct infrastructure for innovation clusters

Innovation clusters have a global footprint

Example clusters (nonexhaustive)

Boston	Harvard University	MIT	QuEra Computing	AWS	Nvidia
--------	--------------------	-----	-----------------	-----	--------

Chicago	University of Chicago	University of Illinois	EeroQ	IBM
---------	-----------------------	------------------------	-------	-----

Delft	TU Delft	Qblox	Intel
-------	----------	-------	-------

Oxford	University of Oxford	Oxford Quantum Circuits	Element Six
--------	----------------------	-------------------------	-------------

Tel Aviv	Tel Aviv University	Classiq
----------	---------------------	---------

Hefei	University of Science and Technology of China	CIQTEK	Tencent
-------	---	--------	---------

Seoul	Sungkyunkwan University	Yonsei University	Seoul National University	Norma
-------	-------------------------	-------------------	---------------------------	-------

Five key enablers support innovation clusters; start-ups are consolidating in quantum hubs.

 Deep dive to follow

Nonexhaustive

Accessibility and integration
Allow standardized platforms and easy quantum-classical integration

Industry or government partnerships
Support QT players through collaboration



Capital investments

Fund research, scale-up, and commercialization

Physical infrastructure and hardware

Provide advanced labs and quantum facilities

Academic institutions and research organizations, including talent
Develop critical know-how, nurture and motivate talent, incubate start-ups

Key insights

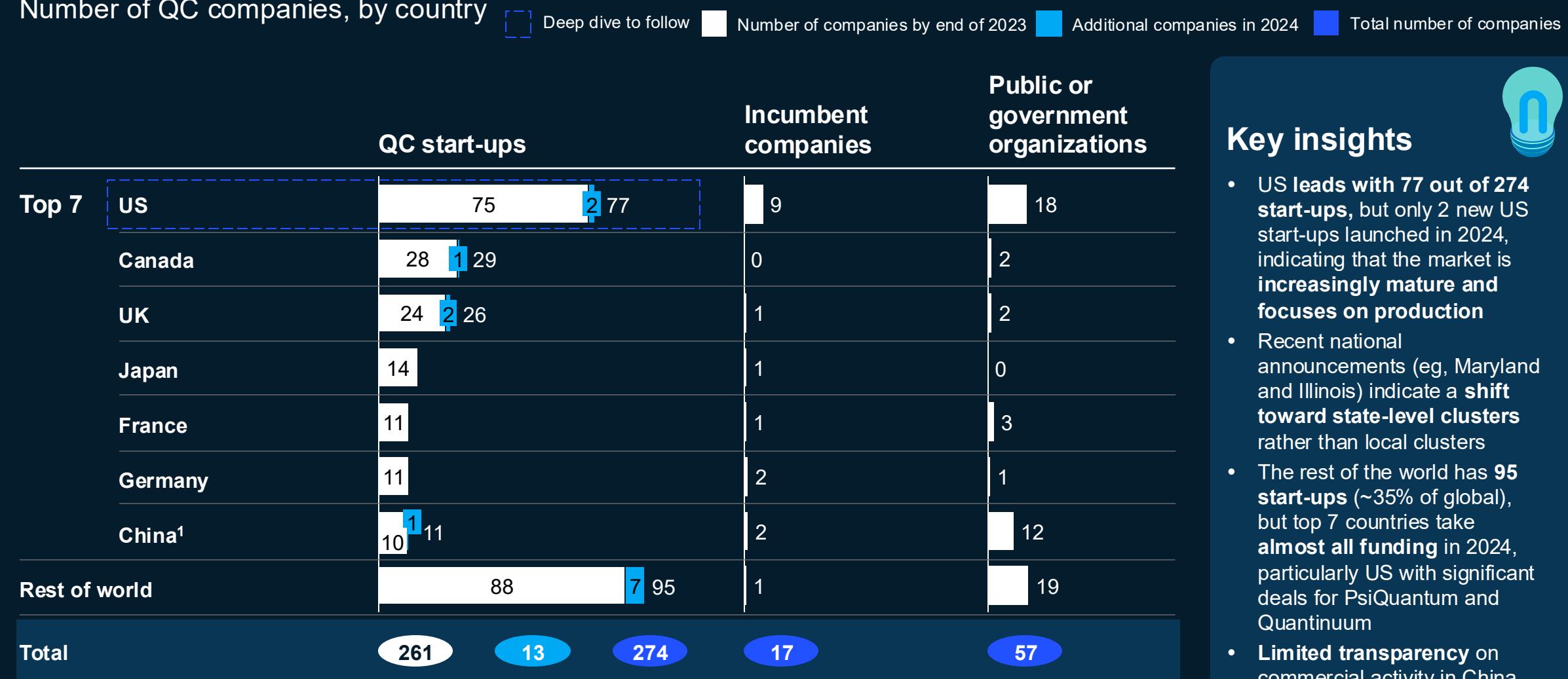
- **Healthy clusters require all five enablers in concert** to be self-sustaining over time
- **Significant investments are required** to sufficiently support all required enablers, especially for newly emerging clusters
- **Time is an essential factor**, as all elements cannot be built immediately by funding alone
- **Developing partnerships** (eg, with universities, industry players) helps accelerate the development of existing and emerging clusters

QC clusters consist of **QC start-ups, incumbent companies, and public or government organizations**; the trend is toward consolidation into quantum hubs across different regions



The most vibrant QC clusters are in the United States, evolving from newly founded start-ups toward a phase of consolidation into hubs.

Number of QC companies, by country



Key insights



- US leads with **77 out of 274 start-ups**, but only 2 new US start-ups launched in 2024, indicating that the market is **increasingly mature and focuses on production**
- Recent national announcements (eg, Maryland and Illinois) indicate a **shift toward state-level clusters** rather than local clusters
- The rest of the world has **95 start-ups** (~35% of global), but top 7 countries take **almost all funding** in 2024, particularly US with significant deals for PsiQuantum and Quantinuum
- **Limited transparency** on commercial activity in China

1. Commercial activity in China lacks transparency, with most QT efforts likely led by government-funded research institutions. Japan shows slightly more clarity but remains limited.

Deep dive: Both federal and state-level efforts are shaping the attractiveness of US QT clusters.

Federal efforts

Federal cybersecurity:

President Biden issued executive order to support US cybersecurity efforts

- Encourages transition to post-quantum cryptography (PQC)
- Strengthens security of US communication and identity management systems
- Promotes cutting-edge development and the use of QT for cybersecurity

Boosts focus on cybersecurity-related QT start-ups

Federal R&D funding:

Launched national quantum initiative reauthorization act to push quantum R&D

- Proposes \$2.7B for quantum R&D (2025–29)
- Aims to accelerate practical quantum applications
- Establishes 3 new NIST¹ quantum centers and 5 new NSF² centers, accelerating research within QT

Boosts government funding in QT clusters

Federal legislation:

Restricted investments in Chinese QC

- Blocks US investments in Chinese QC
- Aims to prevent improvement of China's military capabilities
- Requires US investors to notify government of relevant transactions

Pushes investors toward non-Chinese investments (and thus more US investments)

Benefit to US QT start-ups

State-level efforts

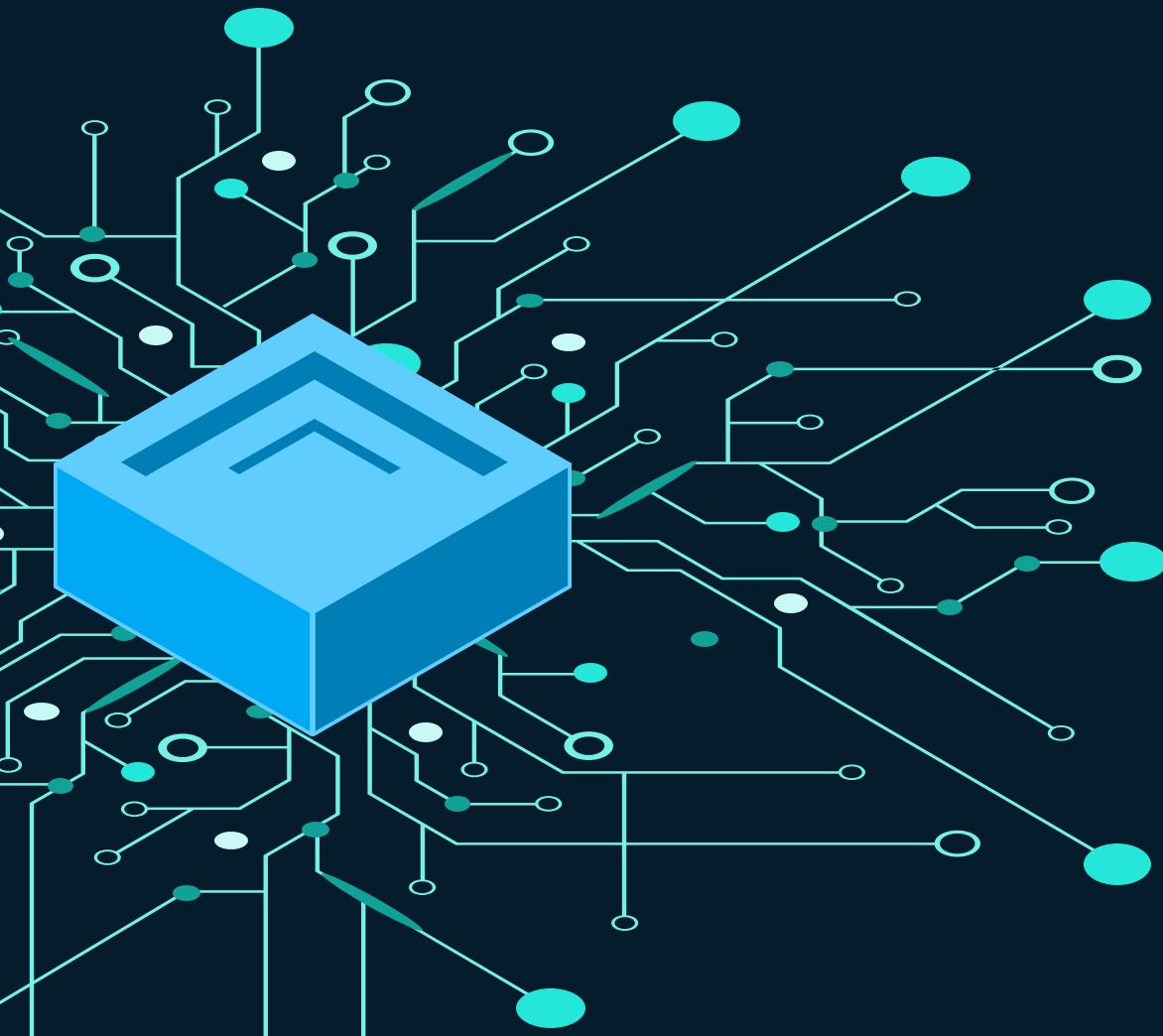
Multiple state-level efforts toward QT were published in 2024 and 2025, including the following:

- **Illinois announced a \$500M investment** to the development of a quantum park (including \$200M for cryogenic plant for PsiQuantum)
- **Maryland announced the Capital of Quantum initiative**, targeting \$1B in investments in partnership with IonQ and University of Maryland

1. National Institute of Science and Technology.

2. National Science Foundation.

Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

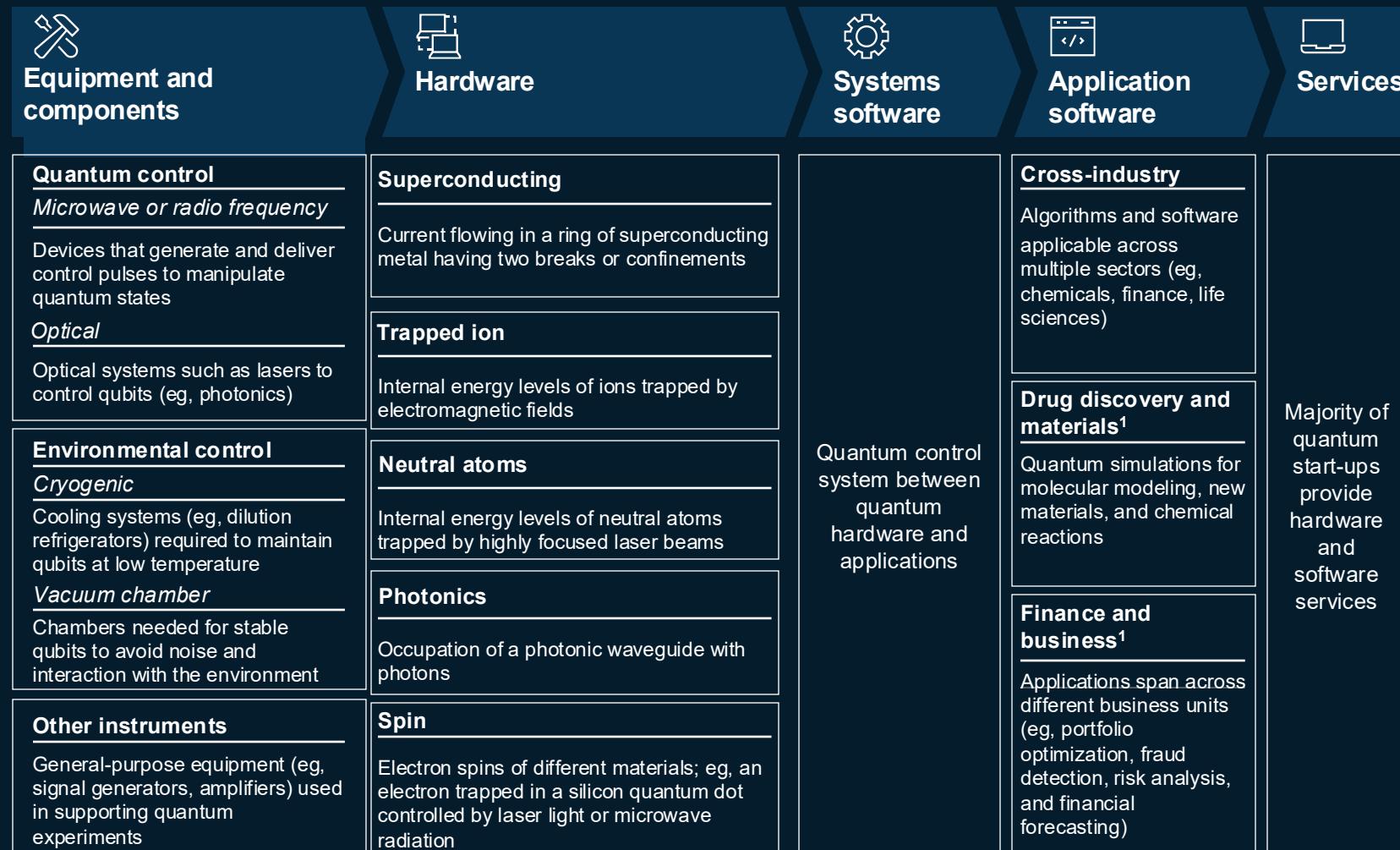
Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

Five major elements define the quantum value chain.

Nonexhaustive



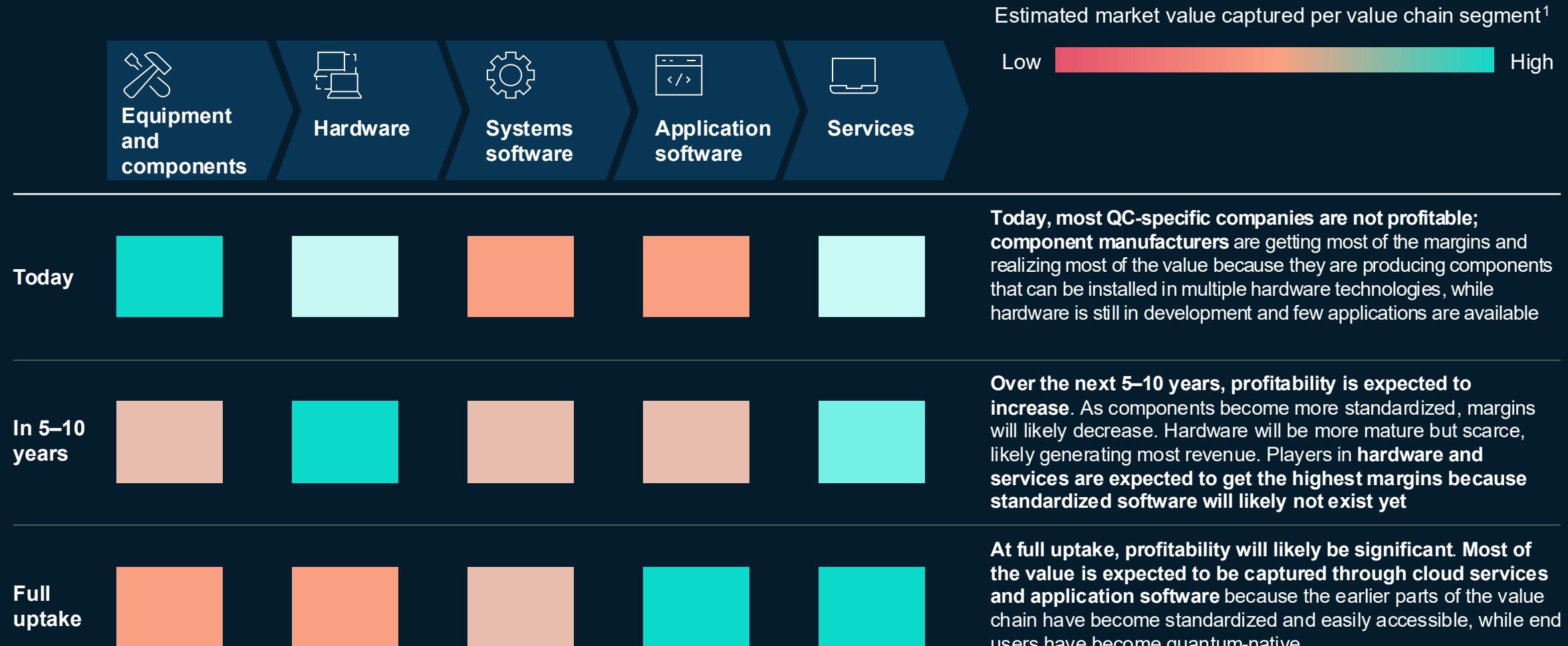
1. Example deep-dive sector with multiple specialized start-ups.

Additional insights



- **Equipment and component players can be divided into three categories** (quantum control, environmental control, and other instruments), and typically **provide products for multiple modalities** (eg, cryogenic equipment for both superconducting and spin qubits)
- **Majority of big tech players** (eg, Google, IBM) **specialize mostly in hardware development**, indicating the foundational importance of hardware and the significant investments required
- **Application software companies** mainly specialize in specific industries, driven by use case needs, in contrast to the remainder of categories, which are mainly industry-agnostic
- Majority of start-ups **provide some quantum services** because products are specialized in an early-stage technology

A value shift from equipment and components to application software and services is expected over the next five to ten years.

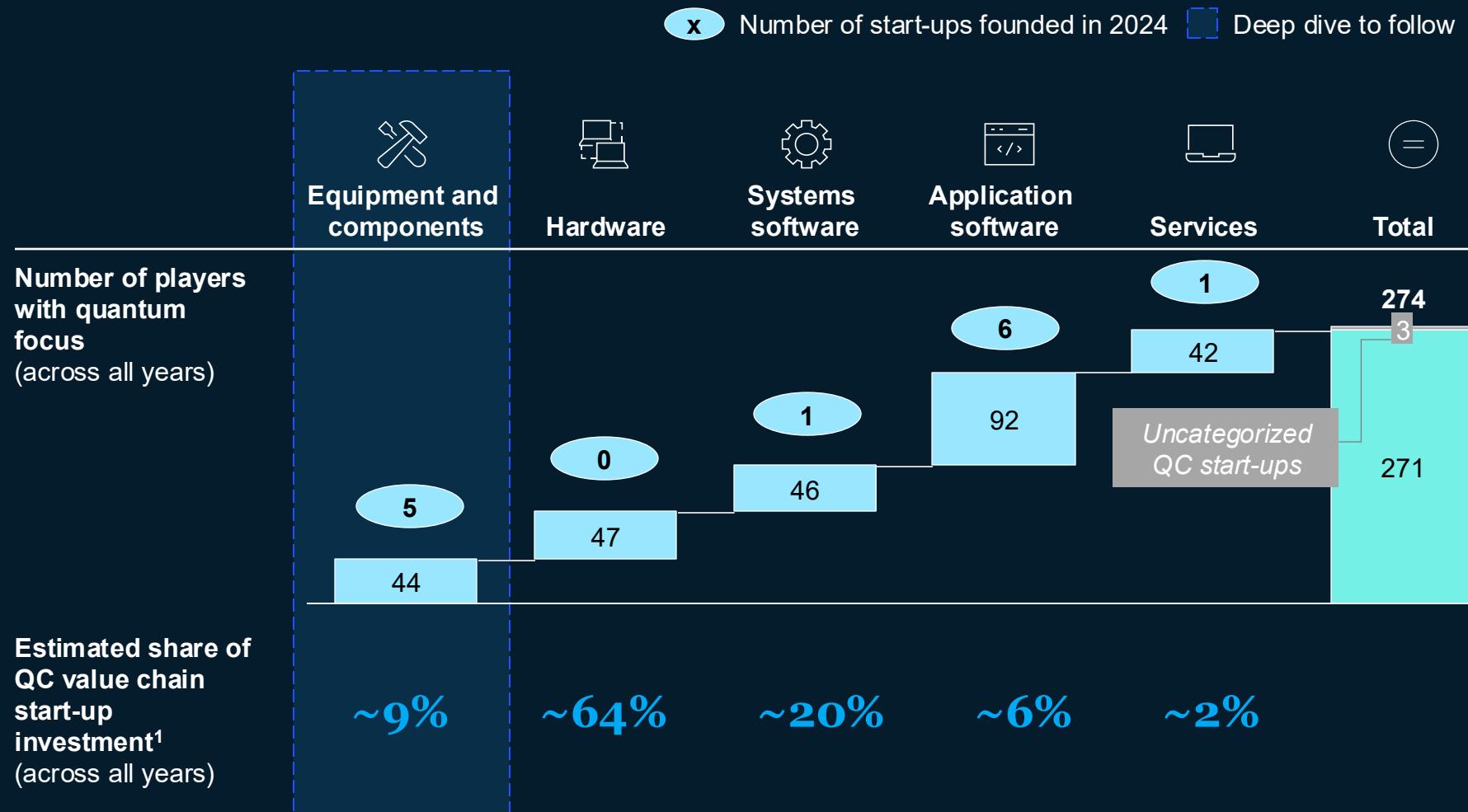


1. Total value captured per value chain segment will be a combination of total value captured by the QC industry and the relative share of total value captured per value chain segment.

Source: Contino; Crunchbase; Hyperion research 2020: SC20 HPC market results and new forecasts; interviews; PitchBook; QC players' technical road maps; *Quantum Computing Report*; S&P Capital IQ; Statista; McKinsey analysis

Most new start-ups in 2024 focus on application software or equipment and components.

Number of QC start-ups, by value chain segment



1. Approximate; based on PitchBook data.

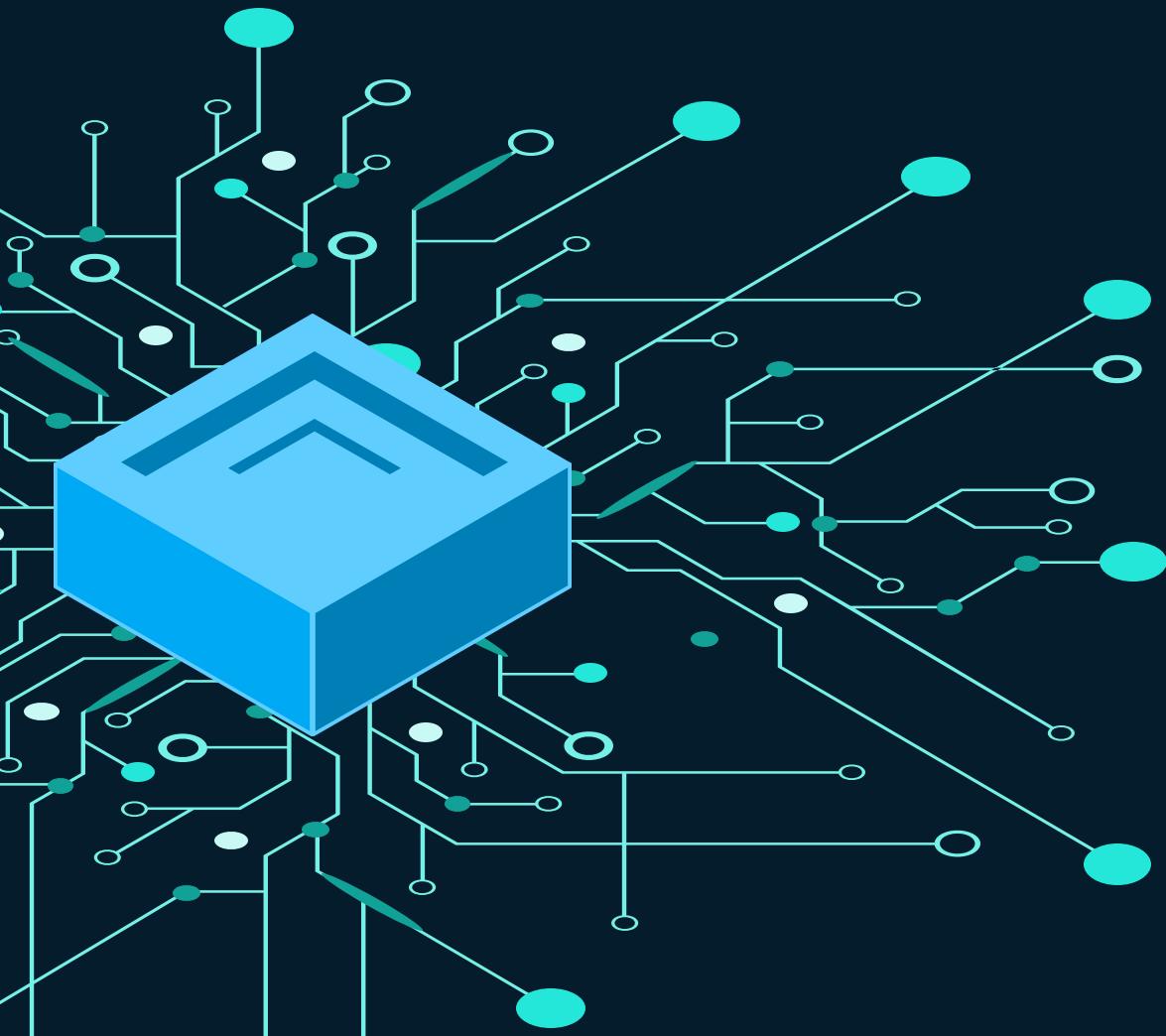
Source: Crunchbase; expert interviews; PitchBook; *Quantum Computing Report*; S&P Capital IQ



Key insights

- Equipment and components and application software segments are especially attractive for new start-ups (collectively accounting for 11 of 13 new start-ups)
- Equipment and components segment attracts investment attention because the hardware player-agnostic nature of the segment creates lower-risk opportunities
- Some players—particularly professional-services firms providing quantum services in addition to their main business—may fall outside the start-up category here because of their lack of specialization

Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

Four key messages describe the state of QComm.

1. Market sizing

Leveraging product landscapes along with technological trends, the total QComm market was an estimated ~\$1.0B in 2023, and it projects to reach \$11B–\$15B by 2035 with a CAGR of 22–25%. While governments hold the largest customer share (62–66% as of 2023), private sector involvement is projected to grow rapidly—eg, telecoms are expected to grow to 16–26% in 2035 from 2–6% in 2023

2. QComm landscape

The QComm landscape has three key categories (security, networks, and services) and six key verticals: quantum key distribution (QKD) solutions, post-quantum cryptography (PQC), modular interconnects, regional networks, quantum global internet, and QComm services. PQC, which has experienced the most commercialization, has the highest level of maturity

3. Value chain

The value chain includes components, hardware, application software, quantum network operators, and services. QComm hardware is still in development.

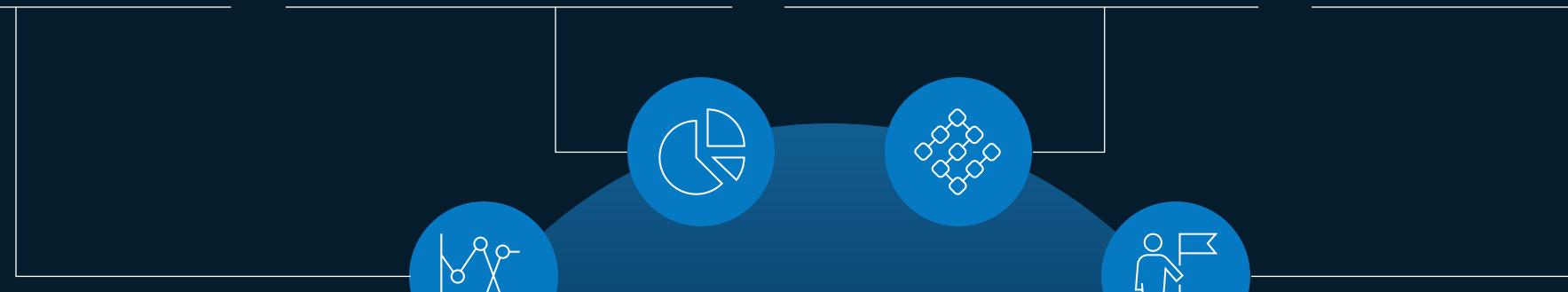
Long-distance communication requires the development of quantum repeaters, which amplify the signal. Start-ups and big players have entered the hardware market while the software market is still small

4. Q-Day implications

Q-Day could force a critical shift in security strategies, requiring potential partnerships between early movers in QKD, PQC, and networks to unlock long-term value

Many industries with sensitive data and high cryptographic requirements are facing large potential Q-Day impacts

Q-Day's exact timing will determine the demand profile and competitive landscape



Key messages in quantum communication

1. The QComm market is projected to reach \$11 billion to \$15 billion by 2035.

Market size, \$ billion Academia Government¹ Telecommunications² and cybersecurity Financial services Healthcare Other³

Market breakdown by customer type, 2023–35, %



1. Includes civil government and defense.

2. Includes public cloud providers.

3. Includes manufacturing, automotive, insurance, etc.

Source: McKinsey analysis; expert interviews; press search



Key insights

- The QComm market is expected to reach between **\$11B and \$15B** in 2035, with a CAGR of **22–25%**
- **Government (including defense)** is the largest player in the current market, with 62–66% estimated market share in 2023
- **Telecommunications** is estimated to have an **increasing market share** over the time horizon, increasing from 2–6% in 2023 to 16–26% in 2035, led by growth in networks markets
- **Financial services** is expected to be a major use case, with an estimated 14–24% market share in 2035, though there is significant uncertainty in the timing of its market growth

2. QComm applications span security, networking, and services.

Nonexhaustive

QComm



Quantum security

Description

Solutions such as QKD ensure provably secure encryption of quantum information, while PQC ensures safety against quantum attacks

Quantum networking

Transfer of quantum information between nodes uses principles such as entanglement to enable applications over longer distances (eg, quantum global internet)

QComm services

Services range from technical support for hardware devices to expert consulting for adoption

Example companies

- Toshiba
- Quantum Xchange
- QuantumCTek
- ID Quantique
- AWS
- Cisco
- IonQ
- Qunnect

- Toshiba
- NEC
- ID Quantique

Note: Several companies cover multiple areas; nonexhaustive

2. Six key verticals shape QComm.

	Quantum security		Quantum networks		Services	
Verticals	QKD (including QRNG¹)	PQC	Modular interconnect	Regional networks	Quantum global internet	QComm services
Description	Software and hardware products that enable detection of interception attempts (including hardware QRNG ¹ products). QKD consists of prepare-and-measure protocols and entanglement-based protocols	Classical algorithms (eg, hash-based, lattice-based, etc) designed to be secure against potential threats posed by quantum computers (but not quantum-secure)	Devices designed for connecting qubits, including switches and transducers (eg, for frequency conversion), to enable low-error and efficient computing and communication	Interconnected data center systems for QComm across municipalities and regions (<1,000-km networks), leveraging repeaters and critical components such as entanglement sources and quantum memories	Technologies enabling intercontinental transfer of quantum information using repeaters involving both free-space and fiber-based systems (>1,000 km)	Services ranging from technical support for hardware devices to expert consulting for adoption
Example industries (nonexhaustive)	Cybersecurity, finance, telecommunications, IoT, automotive	Cybersecurity, finance, telecommunications	Academia, finance, telecommunications, government, IoT	Finance, government, telecommunications	Finance, government, telecommunications	Finance, healthcare, telecommunications

1. Quantum random number generation.

Source: Expert interviews; press search; McKinsey analysis

2. PQC, QKD, and QComm services are already in (partial) production; modular interconnect and networks are less mature.

Nonexhaustive

 Deep dive to follow  Production  Partial production  Near production  In development

Quantum security



Quantum networks



Services



Verticals	QKD (including QRNG)	PQC	Modular interconnect	Regional networks	Quantum global internet	QComm services
Key use cases and drivers	Telecommunications players increase attention on QKD to improve communication security ¹ (eg, Toshiba and IDQ) Key enabler is quantum repeaters, allowing long-distance QComm	Tech companies prepare for a post-quantum world (eg, Apple has introduced PQC protocols for enhanced security in iMessage)	Research institutions, data centers, and quantum computer companies leverage entanglement-based quantum components (eg, switches, interconnects) to synchronize systems and connect qubit chips in quantum computers	Data centers and telecommunications players adopt regional quantum networks to securely transfer data (eg, EPB in Chattanooga, Tennessee, and BT and Toshiba network in London), while the military uses them for drone operations, driven by demand for efficient, confidential, and secure data exchange	Government deploys satellite or fiber-based QComm to secure global data transmission, driven by the necessity to provide encrypted connectivity over large distances	Various industries (eg, financial services, telecommunications) use scalable platforms offered by emerging start-ups to incorporate quantum solutions

Status of commercialization



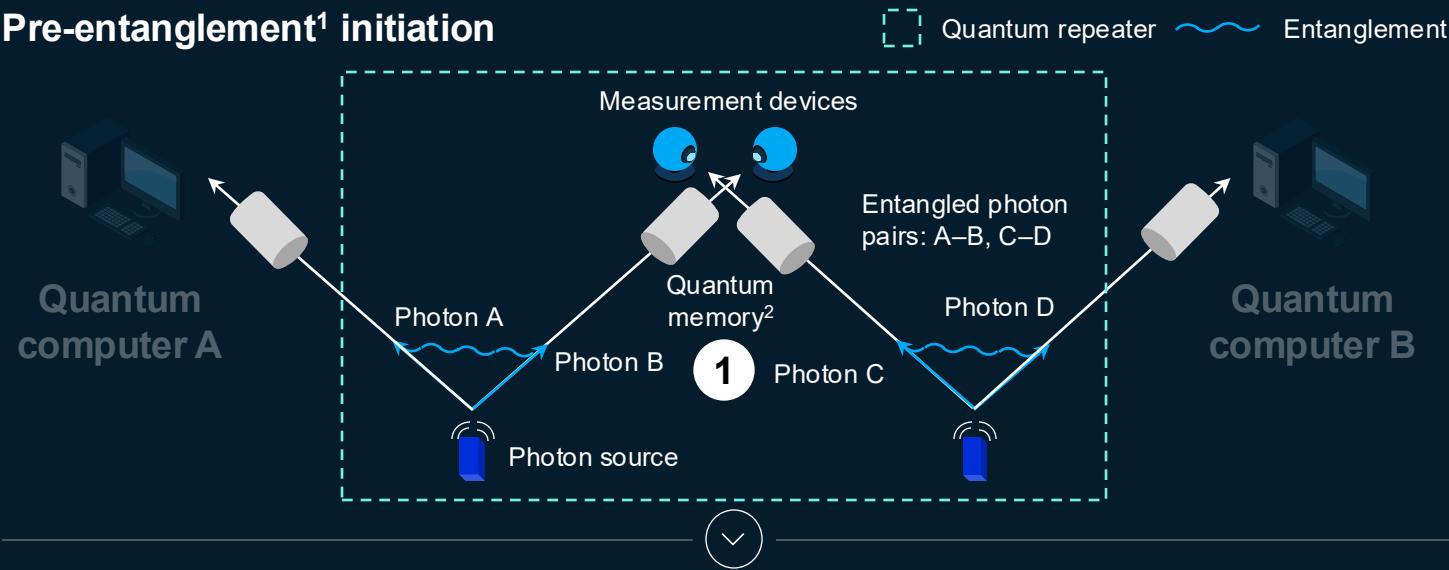
Quantum networks, while promising to revolutionize secure communication and quantum information, depend on the progress of entanglement-based hardware to connect quantum sensors, quantum computers, and data centers. With each technological breakthrough, major networking market growth can be expected

1. QKD development, which does not require repeater technology, is already in production, but commercialization of products that depend on repeater technology are still in development.

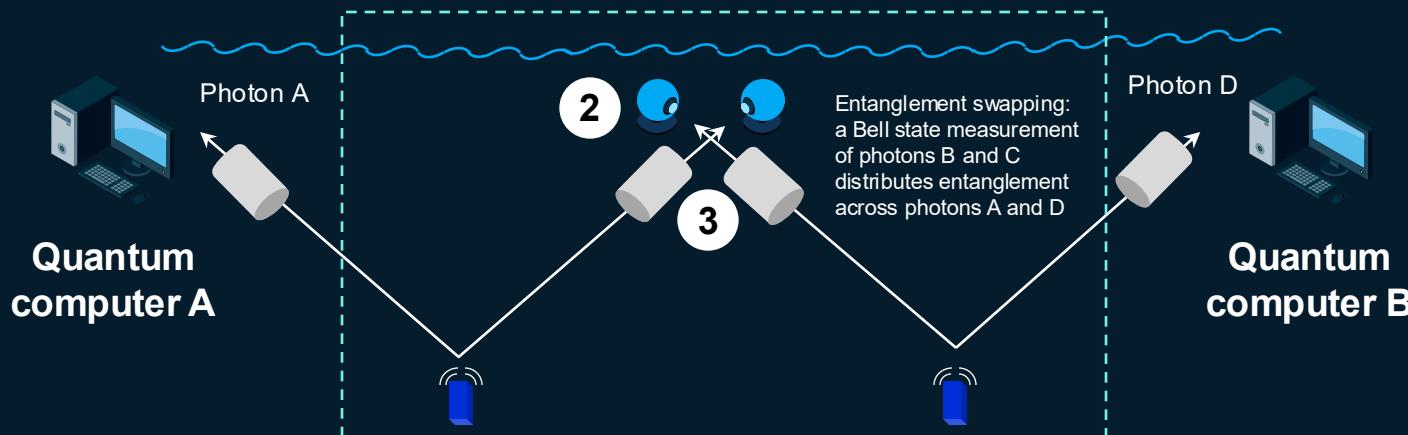
Source: Expert interviews; press search; McKinsey analysis

2A. Deep dive: Quantum repeaters are the building blocks of QComm, enabling quantum key distribution through entanglement.

Pre-entanglement¹ initiation



Post-entanglement¹ communication



1. Entanglement is a key feature of quantum mechanics, connecting (or “entangling”) two physically separated quantum systems.

2. Quantum memory stores the quantum state of a qubit (eg, encoded in a photon in the quantum network).

Source: Expert interviews; press search; Gabriel Popkin, “The internet goes quantum,” *Science*, 2021, Volume 372, Number 6546; McKinsey analysis

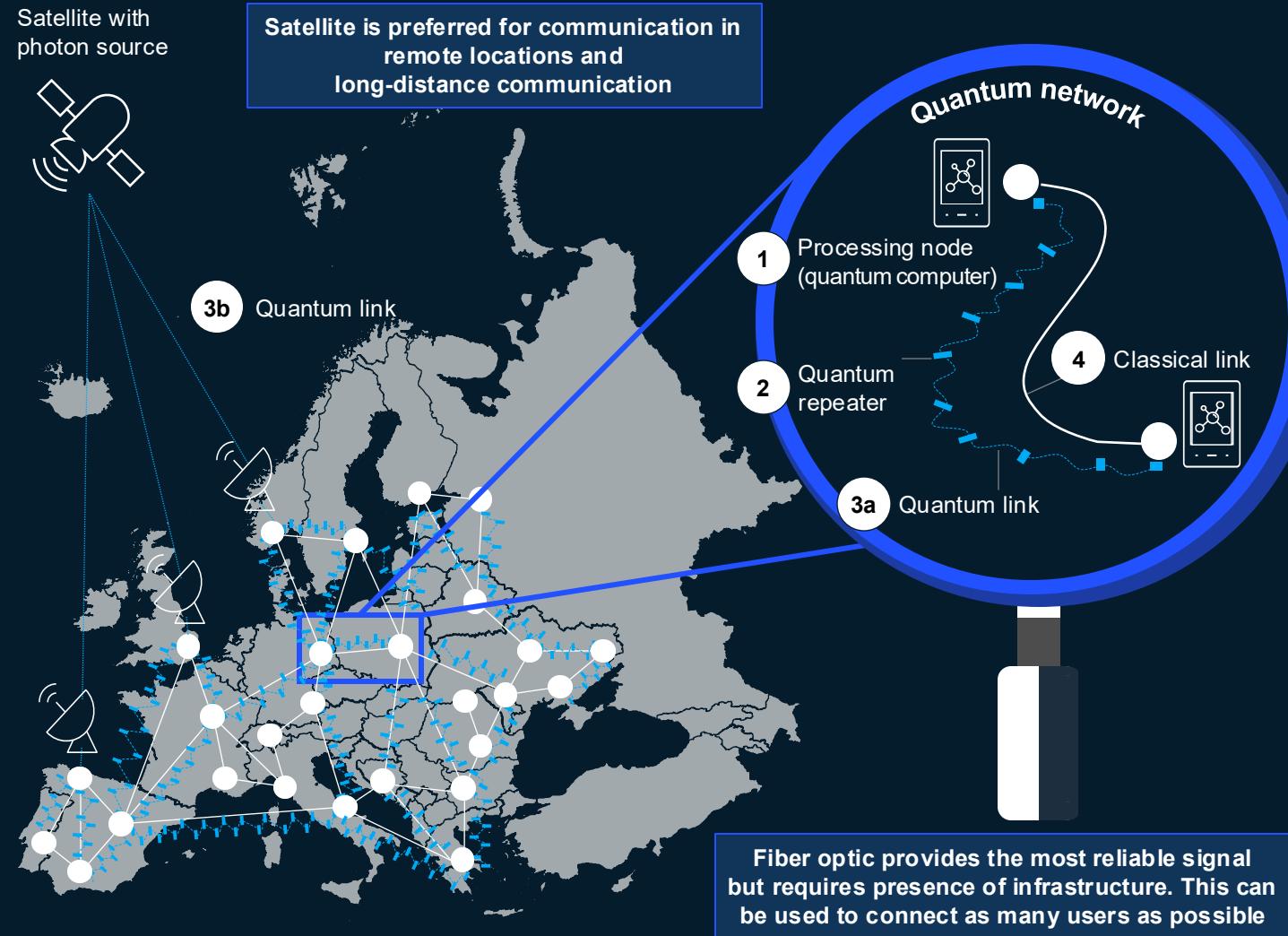
Key insights

- 1 **Quantum repeaters distribute entanglement beyond the distance that one entangled photon source can reach**
- 2 **Measurement devices at the repeater perform an entanglement swap, which distributes entanglement across the unmeasured pair of photons**
- 3 **Quantum memories assist in the entanglement swap so that photons do not need to arrive simultaneously for measurement**



2B. Deep dive: Quantum global internet can be achieved through satellite with photon source and quantum network infrastructure.

Schematic overview, illustrative



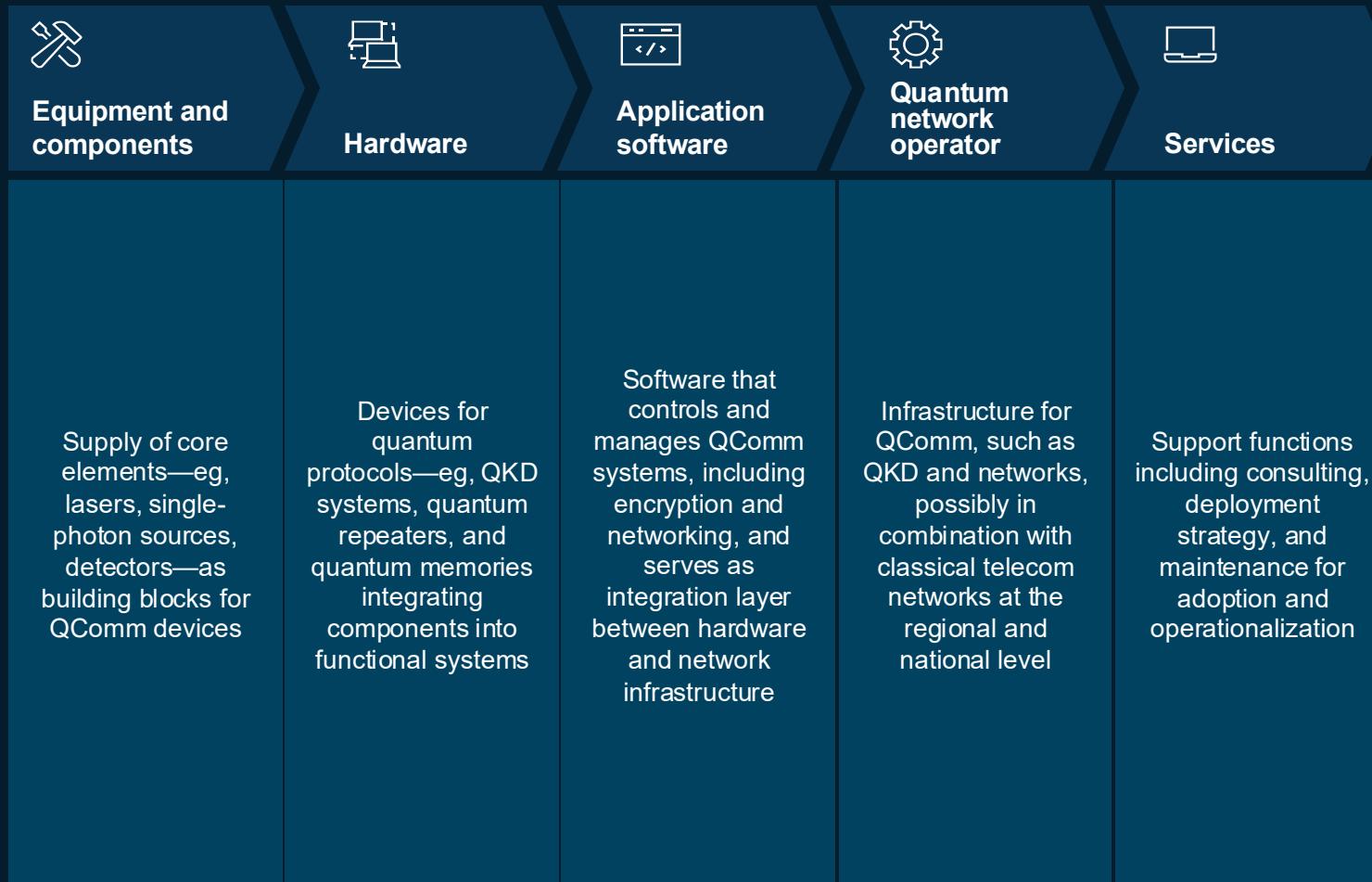
Key insights

- 1 **Processing nodes** can be future quantum computers (processors) connected through the network; these require sufficient storage time to enable communication
- 2 **Quantum repeaters** amplify the signal and reduce error rates to enable communication over long distances
- 3 **Quantum links** provide the infrastructure for the quantum information transfer. This is done through:
 - 3a **Fiber optic cables**, connected with quantum repeaters—enabling mainly regional quantum networks
 - 3b **Free-space communication systems**, based on satellite communication with a detector—enabling mainly global quantum networks
- 4 Classical links enable classical information transfer secured by quantum encryption protocols using quantum links



3. The QComm value chain is dominated by large, established technology players.

Nonexhaustive



Key insights

- QComm hardware is still in the development stage. Secure communication across short distances has been realized, yet (inter)continental connections require the development of quantum repeaters, which are expected in the next ~10 years
- Big global players have entered the hardware segment of the QComm market, yet medium-size start-ups are more advanced in terms of technology. Therefore, big players are starting collaborations or even incubations
- The software market is relatively immature; various start-ups are scaling up
- Various telecommunications providers have started to invest in QComm; these are likely to fulfill the role of quantum network operators in the future

4. Quantum computers could break classical encryption, causing an inflection point for technology (known as Q-Day).

Illustrative

Q-Day definition

The point at which quantum computers can break classical encryption, exposing sensitive data and creating an urgent need for quantum-safe security measures

Impact post Q-Day¹

- Sensitive data using legacy encryption (including critical private information) becomes vulnerable, leading to potentially large economic and societal disruption
- Organizations and governments face immediate need to implement PQC and QKD to safeguard future operations
- Substantial investments may be made in PQC and QKD to enhance security and prevent data loss



Q-Day drivers

- Breakthrough quantum algorithms that crack classical encryption standards
- Advances in error-correction techniques that drastically reduce the number of physical qubits needed to create a reliable logical qubit, making large-scale, fault-tolerant quantum computing practical
- Rapid hardware advances delivering stable, high-fidelity quantum systems

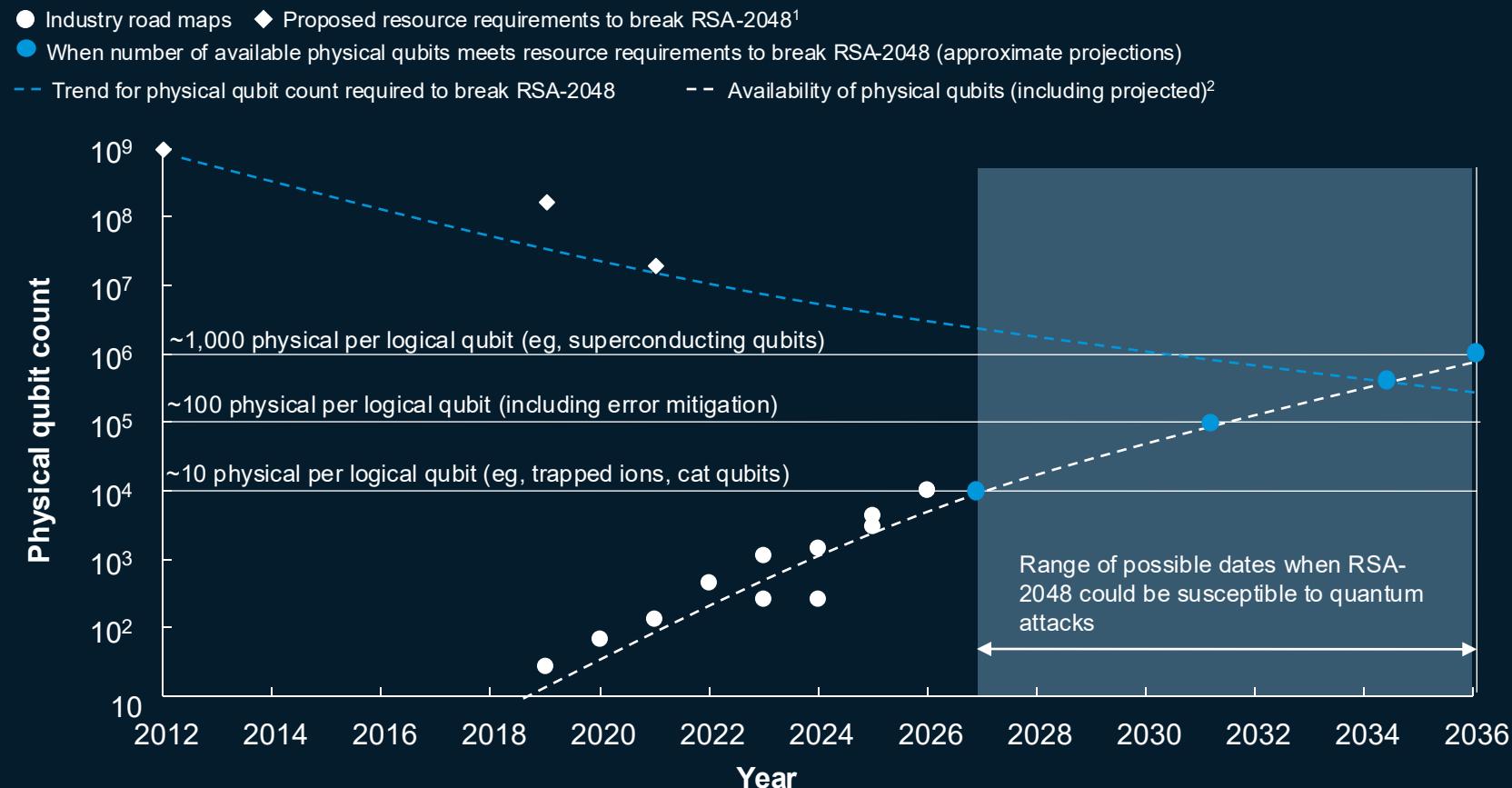
1. Vulnerability extends to years preceding Q-Day for store-now, decrypt-later attacks depending on data lifetime.

Source: Alice & Bob; Google; IBM; Microsoft; Quantinuum; QuEra; McKinsey analysis

4. Classical security protocols could be susceptible to quantum attacks; business leaders may need to prepare for Q-Day.

Illustrative

Quantum resource availability and requirements by year (illustrative), 2012–36



1. Craig Gidney and Martin Ekerå, "How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, April 2021.

2. Historical for pre-2024, projected for post-2024.

Source: Alice & Bob; Google; IBM; Microsoft; Quantinuum; QuEra; McKinsey analysis

Key insights

- Once RSA-2048 is susceptible to quantum attacks (which could happen once ~1,000 logical qubits are reached), the first signs of Q-Day may show
- However, timelines depend not only on number of qubits but also on the algorithms developed (ie, proposed resource requirement to break RSA-2048¹)
- Business leaders may need to prepare for Q-Day before RSA-2048 is susceptible to quantum attacks, eg, through PQC



4. Q-Day is expected to have a strong impact on verticals that are highly reliant on cryptography but have lower crypto-agility (1/2).

+ Low ++ Medium +++ High

Industry	Key segment	Cryptographic requirements ¹	Crypto-agility ²	Q-Day impact ³	Rationale	QKD adoption likelihood
Finance	Financial services	+++	+++	+++	High demand for secure communication and long-term storage; IT modernization efforts to help provide crypto-agility; high Q-Day impact due to diverse, highly distributed infrastructure	+++
	Oil and gas	++	+	+	Limited secure communication requirements; low IT maturity; limited Q-Day impact	+
Global energy and materials	Sustainable energy	++	+	++	High security requirements for critical infrastructure; lower security requirements for other areas of segment	++
	Chemicals	+	+	+	Limited secure communication requirements; lower IT maturity; limited Q-Day impact	+
	Travel, transport, and logistics	++	++	++	Medium demand for secure communication and storage; digitalization efforts to enhance IT modernization to improve crypto-agility; medium Q-Day impact due to highly distributed infrastructure	++
Pharma and medical products	Healthcare	++	++	+++	IP and health records requiring secure communication and storage; some crypto-agility from digital technology influx; high Q-Day impact	++

1. "Cryptographic requirements" refers to degree of need for strict cryptographic standards.

2. High crypto-agility if software and hardware infrastructure are amenable to rapid updates of cryptographic systems.

3. Estimated degree to which Q-Day will affect operations.

Source: Expert interviews; press search; McKinsey analysis

Likely QKD adopters include industries with high Q-Day impact and low crypto-agility

4. Q-Day is expected to have a strong impact on verticals that are highly reliant on cryptography but have lower crypto-agility (2/2).

+ Low ++ Medium +++ High

Industry	Key segment	Cryptographic requirements ¹	Crypto-agility ²	Q-Day impact ³	Rationale	QKD adoption likelihood
Advanced industries	Automotive	++	++	++	Requires secure communication over long product lifetimes but limited compute	++
	Aerospace and defense	+++	+++	+++	Strongly requires secure communication and storage, often with high crypto-agility	+++
	Advanced electronics	++	++	++	Some security requirements (by customer) with digitalization; medium crypto-agility	++
	Semiconductors	++	+	++	Some security requirements with complex value chain, some with low crypto-agility	++
Insurance	Insurance	+++	+++	+++	Strong requirements for security and privacy over long durations; growing digital presence helps enhance crypto-agility	+++
Telecom, media, and technology	Telecom	+++	++	+++	Strong security requirements with complex value chain, some with low crypto-agility	+++
Government	Media	++	+++	++	Limited security and privacy requirements with high crypto-agility due to technology focus	++
	Defense	+++	+++	+++	Strong requirements for secure communication and storage; high crypto-agility	+++
	Security	+++	+++	+++	Strongest requirements for secure communication and storage; high crypto-agility	+++

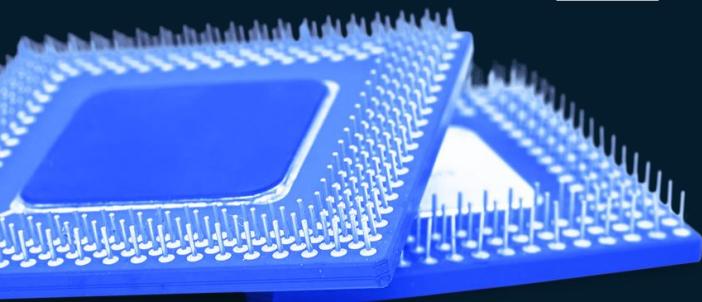
1. "Cryptographic requirements" refers to degree of need for strict cryptographic standards.

2. High crypto-agility if software and hardware infrastructure are amenable to rapid updates of cryptographic systems.

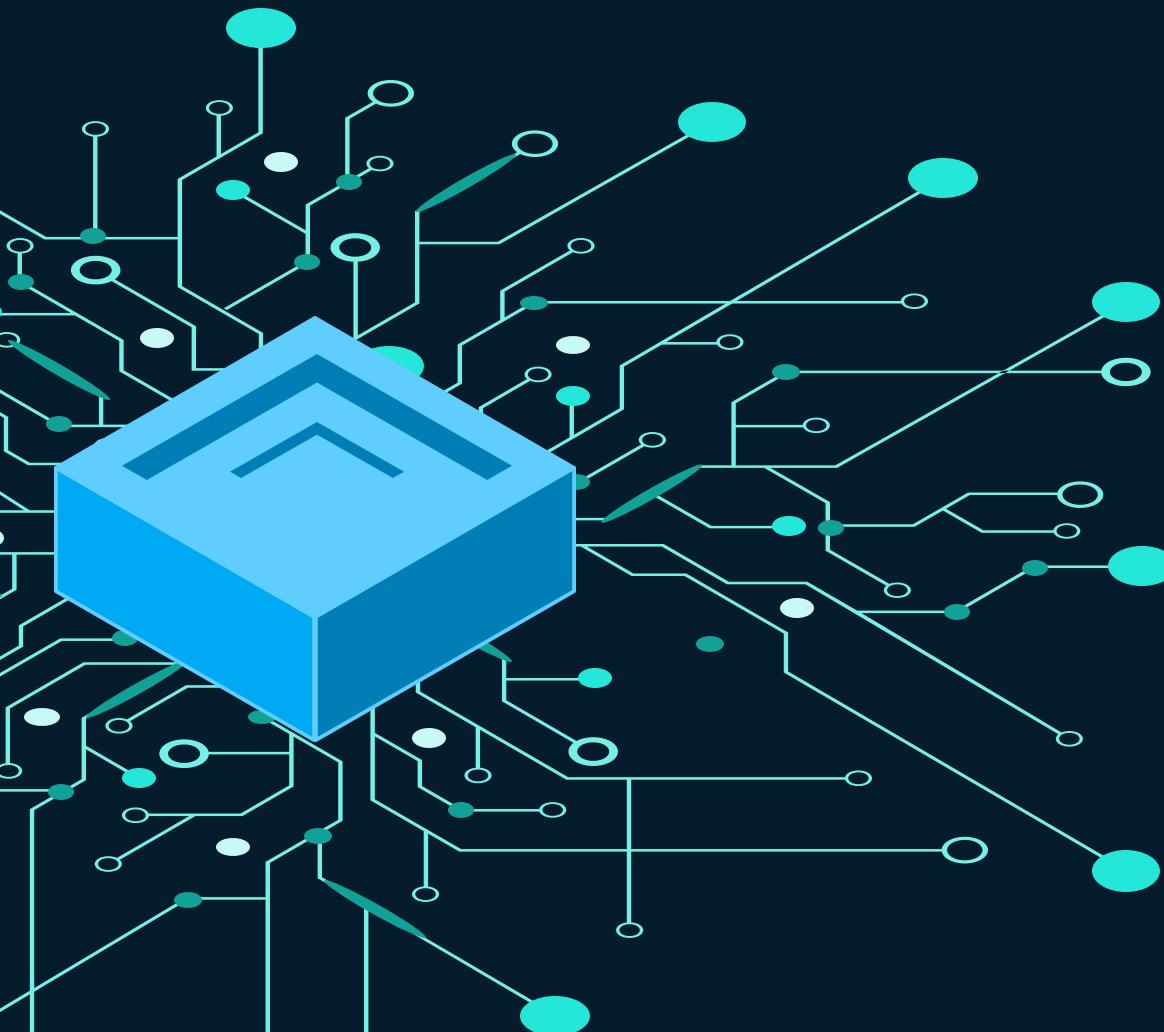
3. Estimated degree to which Q-Day will affect operations.

4. Signals that indicate acceleration or deceleration toward Q-Day can inform strategic decision-making.

Type	Signal	Description	Examples
Acceleration 	Changes in investment patterns	Shifts in public or private investments could indicate imminent or achieved breakthroughs in QT	Increases in government funding for QT research
	Major technological breakthroughs	Technological breakthroughs critical to the technology road map are announced, ideally by multiple players, indicating successful R&D	Scaling of qubits, quantum repeaters
	Adherence to announced timelines	Commitment and ability to remain on schedule indicate that major issues in R&D and production are likely resolved	Achieving milestones for logical qubits (eg, gate fidelity)
	Increased partnerships	Depending on partnership profiles, partnerships may indicate strong desire to grow quickly beyond local networks	Announcement of use case breakthroughs through partnership
	Changes in publication, patent activity	Significant increase or abrupt decrease in publication or patent activity provides insights into maturity of emerging technologies	Published research showing improved fidelity, acceleration in patents awarded
Deceleration 	Reduced investment	Reduced investment discourages new companies (especially those with large capital expenditure requirements) and may slow tech development	Fewer deals, leading to less investment in QT
	Increasing adoption of competing technologies	Emergence of competing solutions may indicate the challenges of a competitive market	Widespread adoption of PQC, reducing demand for QKD
	Redirected resources	Companies pivoting away from technologies such as fault-tolerant quantum computing may indicate that technology development has stalled or there are other commercially suitable alternatives	Pivoting from QC to AI; QKD companies refocusing on PQC
	Slowing innovation	Technical obstacles prevent major breakthroughs in scaling quantum computers	QC players missing milestones for logical qubits



Contents



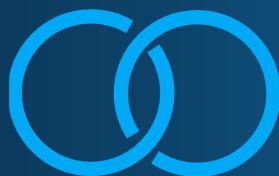
- Introduction
- Innovations and breakthroughs
- Market size and value at stake
- Investment landscape
 - Private funding
 - Public announcements
- Clusters and start-ups
- Value chain
- Deep dive into QComm
- QT impact on cutting-edge technologies**
- Methodology and acknowledgments

QT has significant synergies and mutual impact with selected cutting-edge technologies.

Technologies selected from *McKinsey Technology Trends Outlook*

Nonexhaustive

Mutual impact between QT and cutting-edge technologies



A

AI and machine learning

Play a central role in **accelerating quantum software**; benefit significantly from the **computational power quantum computers** could offer

B

Robotics

Drives automation in quantum manufacturing and potentially benefits from QT through enhanced computing power, optimized software applications, secure communication and authentication, and improved navigation and sensing precision

C

Sustainability and climate tech

Demand energy-efficient, high-impact solutions, making them both beneficiaries and drivers of innovation in quantum technologies—with significant benefits from boosted computing power, algorithm optimization, and molecular simulation

D

Cryptography and cybersecurity

Face both existential risks and transformative opportunities from quantum capabilities; potentially a critical area of impact

QT is an essential catalyst—enabling and accelerating breakthroughs in a wide array of cutting-edge technologies.

Impact of QT on cutting-edge technologies, selected high-impact topics

Nonexhaustive



Deep dives to follow



QC

A AI and machine learning

- QC improves **AI algorithm efficiency** through quantum algorithms
- QC increases **memory size** through quantum hardware
- QC speeds up **memory loading time** through quantum hardware
- QC enhances **AI training** through increased computing power

A. QC could potentially speed up AI training constraints, while AI could potentially speed up QC development.

QC could potentially solve multiple AI training constraints, while AI could potentially speed up QC development.

Importance: Moderate

Impact: Moderate

Assessment: Moderate

Example: Google's Quantum Computing Research Group is working on developing quantum algorithms for AI training, which could potentially speed up the process. QC could also potentially solve multiple AI training constraints by providing faster computation times.

B. Major players are pursuing synergies between AI and quantum computing.

Example: Google and IBM are both working on developing quantum algorithms for AI training, which could potentially speed up the process. QC could also potentially solve multiple AI training constraints by providing faster computation times.

Importance: Moderate

Impact: Moderate

Assessment: Moderate

Example: Google's Quantum Computing Research Group is working on developing quantum algorithms for AI training, which could potentially speed up the process. QC could also potentially solve multiple AI training constraints by providing faster computation times.

B Robotics

- QC boosts **computing power** and **optimizes software applications**
- QComm secures **communication between robots** and enables **quantum authenticated access**
- QS enhances **navigation** and **sensing precision**

B. Robotics could be significantly affected across all three quantum technology pillars.

Importance: High

Impact: High

Assessment: High

Example: In the field of robotics, QC could potentially boost computing power and optimize software applications, leading to more efficient and accurate robot navigation and sensing. QComm could secure communication between robots and enable quantum authenticated access, ensuring the safety and security of robotic operations. QS could enhance navigation and sensing precision, allowing robots to operate more effectively in complex environments.

C Sustainability and climate tech

- QC improves computing power to **accelerate material discovery**
- QC improves **simulation of complex systems**, specifically systems with quantum behavior
- QC enhances **optimization in production** through quality and speed of optimization problems

C. QC will have a high impact on several areas in sustainability and climate tech.

Importance: High

Impact: High

Assessment: High

Example: In the field of sustainability and climate tech, QC could potentially accelerate material discovery by improving computing power. QC could also improve simulation of complex systems, specifically those with quantum behavior, such as climate models. QC could enhance optimization in production through quality and speed of optimization problems, leading to more efficient and sustainable manufacturing processes.

Relevance for QT pillars



QComm



QS

D Cryptography and cybersecurity

- QC threatens **classical cryptography** and provides new **cybersecurity solutions**
- QComm enables new security protocols (eg, from classical to **quantum-based QKD**), and improves security standards through **quantum random number generation**

Deep dive in
QComm section

D. Cryptography and cybersecurity

Importance: High

Impact: High

Assessment: High

Example: QC threatens classical cryptography by providing new cybersecurity solutions. QComm enables new security protocols, such as quantum-based QKD, and improves security standards through quantum random number generation.

D. Organizations may need to prioritize the protection of critical data assets as QT capabilities advance.

Importance: Moderate

Impact: Moderate

Assessment: Moderate

Example: Organizations may need to prioritize the protection of critical data assets as QT capabilities advance. QC could potentially threaten classical cryptography, while QComm could enable new security protocols and improve security standards.

Key data types at risk:

- Data stored with service agencies
- Customer data
- Financial data
- Healthcare data
- Intellectual property
- Operational data
- Personal data
- Product data
- Risk data
- Social and economic data
- Supply chain data
- User data

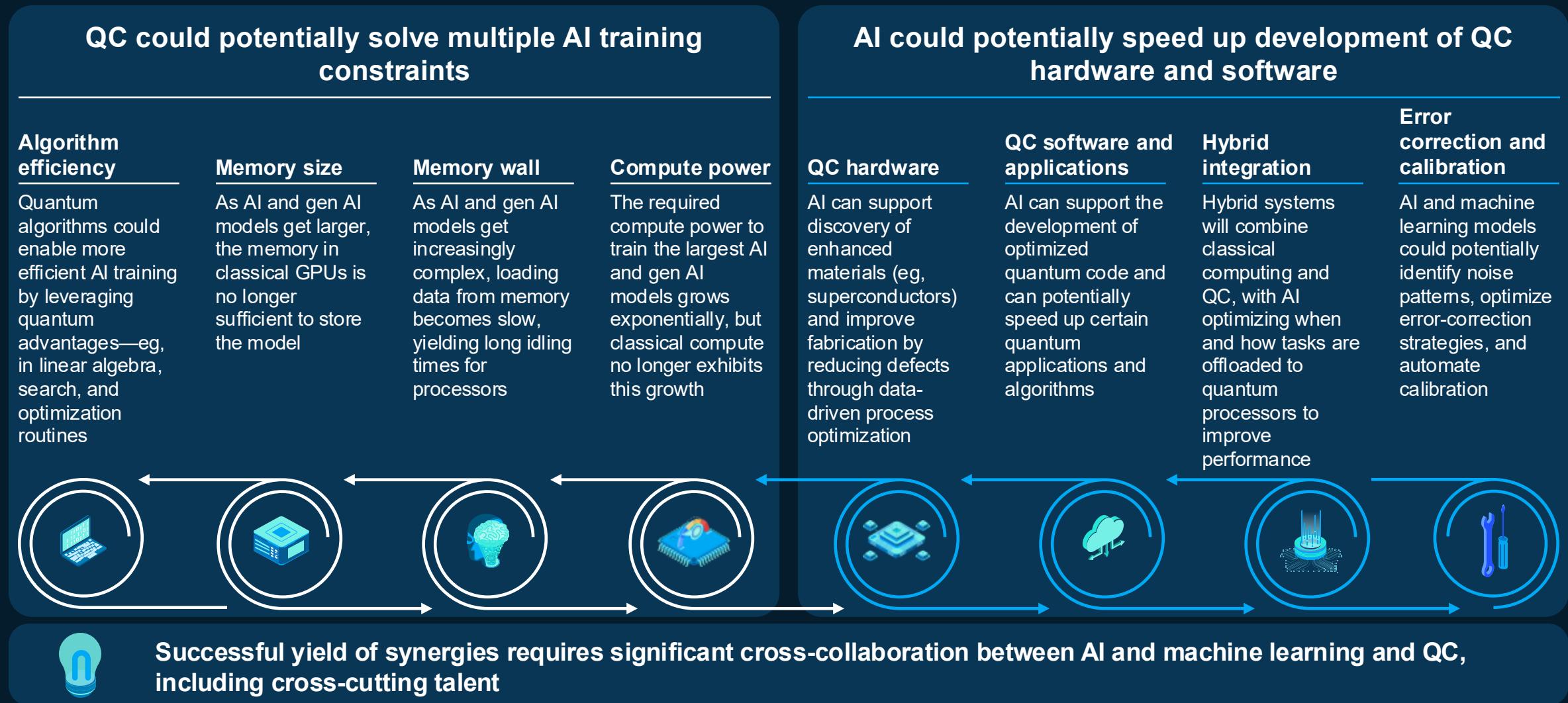
Considerations:

- Most organizations have information they regularly collect and store, such as customer data, financial data, and operational data. QC could potentially threaten classical cryptography, while QComm could enable new security protocols and improve security standards.
- Organizations must prioritize the protection of critical data assets as QT capabilities advance. QC could potentially threaten classical cryptography, while QComm could enable new security protocols and improve security standards.

A. QC could potentially solve multiple AI training constraints, while AI could potentially speed up QC development.

Selected top synergies between AI and machine learning and QC

Nonexhaustive



A. Major players are pursuing synergies between AI and quantum computing.

Example AI and machine learning and QC announcements

	Announcement	Impact
Japan's AIST	IonQ and QuEra each signed memorandum of understanding with Japan's AIST (IonQ, April 2025; QuEra, April 2024) to advance national quantum computing capabilities with a focus on quantum and AI applications ¹	The ABCI-Q system is meant to be a platform for the advancement and development of several areas: <ul style="list-style-type: none">• Quantum circuit simulation• Quantum machine learning• Classical-quantum hybrid systems• New algorithms inspired by quantum technology
IonQ		
QuEra	IonQ will provide cloud access to its Forte-class systems, while QuEra will deliver a neutral-atom quantum computer to integrate with AIST's Nvidia-powered ABCI-Q supercomputer with the goal of creating a hybrid platform for simulations and quantum-AI applications ¹	
Nvidia	Nvidia announced its Accelerated Quantum Research Center (NVAQC) in Boston (March 2025) ² The center will integrate quantum hardware with AI supercomputing infrastructure ²	NVAQC creates a hub for hybrid innovation, blending quantum capabilities with large-scale AI computing The center pushes a shift from research to real-world scaling, with dedicated facilities and industrial partnerships
SoftBank		
Quantinuum	SoftBank and Quantinuum announced a strategic partnership to integrate quantum computing and AI for practical applications (January 2025) ³ The collaboration aims to unlock innovative QC solutions that will overcome limitations of classical AI while realizing next-generation technologies ³	The collaboration combines SoftBank's scale with Quantinuum's quantum capabilities. Partnership aims to achieve breakthroughs by developing QC solutions that surpass current limitations of AI
Quantinuum	Quantinuum unveiled Generative Quantum AI (Gen QAI) in February 2025 ⁴ The framework integrates quantum-generated data into AI workflows to enhance performance in applications such as drug discovery, financial modeling, and logistics optimization ⁴	Gen QAI demonstrates a path to hybrid AI–quantum applications, showing how quantum systems can complement traditional AI The launch signals growing commercial readiness, moving beyond theory toward scalable, real-world AI solutions enhanced by quantum capabilities

1. IonQ and QuEra websites. 2. Nvidia website. 3. SoftBank and Quantinuum websites. 4. Quantinuum website.

Source: Expert interviews; press search; Lareina Yee, Michael Chui, Roger Roberts, and Mena Issler, "McKinsey Technology Trends Outlook 2024," McKinsey, July 16, 2024; ; McKinsey analysis

B. Robotics could be significantly affected across all three quantum technology pillars.

Selected top synergies between robotics and QT

Impact mainly related to:  Innovation  Speed  Accuracy  Quality



Potential synergies between QT and robotics	Impact description	Example use case
Hardware: Boost computing power	 Enhance computing power from QC hardware, potentially enabling better autonomous control from decision-making algorithms	Allowing autonomous cars to make better and faster decisions
	 Increase computing resources to speed up simulations, prototyping, and testing of robotics	Accelerating development of general-purpose robots
Software: Optimize software applications	 Enhance robotics planning, learning, and coordination through quantum algorithms	Enabling warehouse robotics to optimize pick-and-place tasks
Secure robot communication	 Enhance protection of robotic data from interception and manipulation	Safeguarding communication of ground units in defense missions
Enable authenticated robotics access	 Guarantee access control through QKD	Preventing hijacking of delivery robots in urban settings
Improve robot navigation and awareness	 Enhance robot navigation using highly precise quantum inertial sensors (eg, gyroscopes)	Guiding underground or underwater robots without GPS access
Improve precision and sensitivity of sensors	 Enable detection of ultrafine physical changes for precision tasks	Enhancing surgical robotics with more accurate touch detection

C. QC will have a high impact on several areas in sustainability and climate tech.

Selected top synergies between sustainability and climate tech and QC

Impact mainly related to:  Innovation  Speed  Accuracy  Quality

Potential synergies ¹ with QC	Impact description	Example use case
Improve computing power	 Accelerate material discovery and other computation-heavy areas by reducing the time needed for computation and by increasing accuracy of computations	Enabling discovery of more effective carbon capture materials Enhancing biological nitrogen fixation for green ammonia production Speeding up research toward longer-lasting, faster-charging, and more powerful batteries
Improve simulation of complex systems	 Improve ability to model complex systems, such as molecular interactions or climate models, for more accurate simulations	Enabling simulation of complex biological systems with molecular interactions Supporting climate modeling and scenario-based simulation with high complexity Enabling molecular simulation for carbon capture and catalyst design
Enhance optimization in production	 Improve accuracy and speed of optimization problems through quantum algorithms—relevant for production optimization across industries, power efficiency, and emission reductions across the value chain	Improving load balancing in electrical grids for efficient integration of renewables Enhancing supply chain optimization to reduce carbon footprint of renewable technologies Improving vehicle routing and transportation space usage to reduce emissions from the transport sector Optimizing production processes for a wide array of industries, reducing contribution to global pollution

1. Early-state quantum computing will likely be energy consumption intensive (due to inefficient cryogenics, etc). As the technology matures and scales, advancements in engineering are expected to drive improvements in energy efficiency.
Source: Expert interviews; press search; Lareina Yee, Michael Chui, Roger Roberts, and Mena Issler, "McKinsey Technology Trends Outlook 2024," McKinsey, July 16, 2024; McKinsey analysis

D. Cybersecurity could be significantly affected by QT—for example, through quantum algorithms.

Selected top cybersecurity areas affected by QT

Cybersecurity <i>Protecting systems, networks, and data from attacks and disruptions</i>	Top areas	Definition	Classical approach	Potential impact of QT
	Incident management (including outlier detection)	Detects, analyzes, and mitigates suspicious or harmful activity	Uses heuristics or machine learning to flag abnormal patterns	Quantum algorithms could potentially detect subtle anomalies in large data sets more efficiently
	Continuity management	Maintains essential functions during cyberattacks or system failures	Relies on scenario planning and manual contingency plans	Quantum optimization may improve real-time decision-making during disruptions
	Recovery management	Restores systems, services, and data after a cyber-incident	Follows predefined recovery playbooks with static priorities	Quantum algorithms could potentially optimize recovery order for faster full restoration
	Threat detection	Identifies unauthorized access, malware, or malicious behavior	Uses pattern matching and machine learning models to flag known or suspected threats	Quantum algorithms may increase detection accuracy and reduce false positives
	Random number generation <i>Cross-cutting (ie, present in both QC and QComm)</i>	Produces unpredictable numbers for secure encryption and system behavior	Uses pseudo-random number generators (eg, hardware noise)	Quantum-based generators can produce truly random values, strengthening both symmetric and asymmetric cryptographic schemes

D. Cryptography faces significant changes with the rise of QT; many cryptography protocols could potentially be broken.

Selected top cryptography areas affected by QT

 Deep dive to follow

Cryptography
Securing information through confidentiality, integrity, authentication, and non-repudiation

Top areas	Definition	Classical approach	Potential impact of QC
Key exchange	Enables two parties to securely agree on a shared secret key for communication	Uses asymmetric encryption based on computationally hard mathematical problems (eg, RSA)	
Digital signatures	Confirms the authenticity of digital messages or documents and secures connections (eg, TLS ¹)	Built on asymmetric encryption (eg, RSA, ECDSA); widely used in software updates and certificates	Quantum algorithms (eg, Shor's ² and Grover's ³) can potentially break or weaken current cryptography (eg, AES ⁴), thus requiring quantum-safe alternatives
Encryption and decryption	Analyzes and attempts to break cryptographic systems to uncover hidden data or vulnerabilities	Requires vast time or computing power to attack strong encryption; may not be feasible to break without quantum computing	

1. Transport layer security. 2. Shor's algorithm is a quantum algorithm that can factor large numbers exponentially faster than classical methods. 3. Grover's algorithm is a quantum search algorithm that speeds up attacks by searching unsorted databases. 4. See S. Mandal et al., "Implementing Grover's on AES-based AEAD schemes," Sci Rep, in *Nature*, Sept 10, 2024.
Source: Expert interviews; press search Lareina Yee, Michael Chui, Roger Roberts, and Mena Issler, "McKinsey Technology Trends Outlook 2024," McKinsey, July 16, 2024; McKinsey analysis

D. Organizations may need to prioritize the protection of critical data assets as QT capabilities advance.

Nonexhaustive

Quantum algorithms (eg, Shor's and Grover's) pose threats to classical encryption, while technologies such as QKD and QRNG offer quantum-secure methods for protecting data

Quantum security deep dive in QComm section

Consideration



Most short-term information (eg, daily transactions or temporary contracts) typically becomes irrelevant within 50 years and is less of a concern for long-term quantum-era breaches



Key data types at risk

Data stored with secret agencies

Sensitive records and data held by intelligence or national security agencies



Long-term personal records, including biometric data

Data tied to lifelong commitments (eg, insurance contracts, bank accounts, housing contracts, work contracts) and any biometric data records (eg, fingerprints or facial features used for face ID)



Social and health records

Health histories, family details, welfare information, and critical data managed by social security system



Organizational affiliations

Membership data from political parties, unions, and similar entities with long-term significance

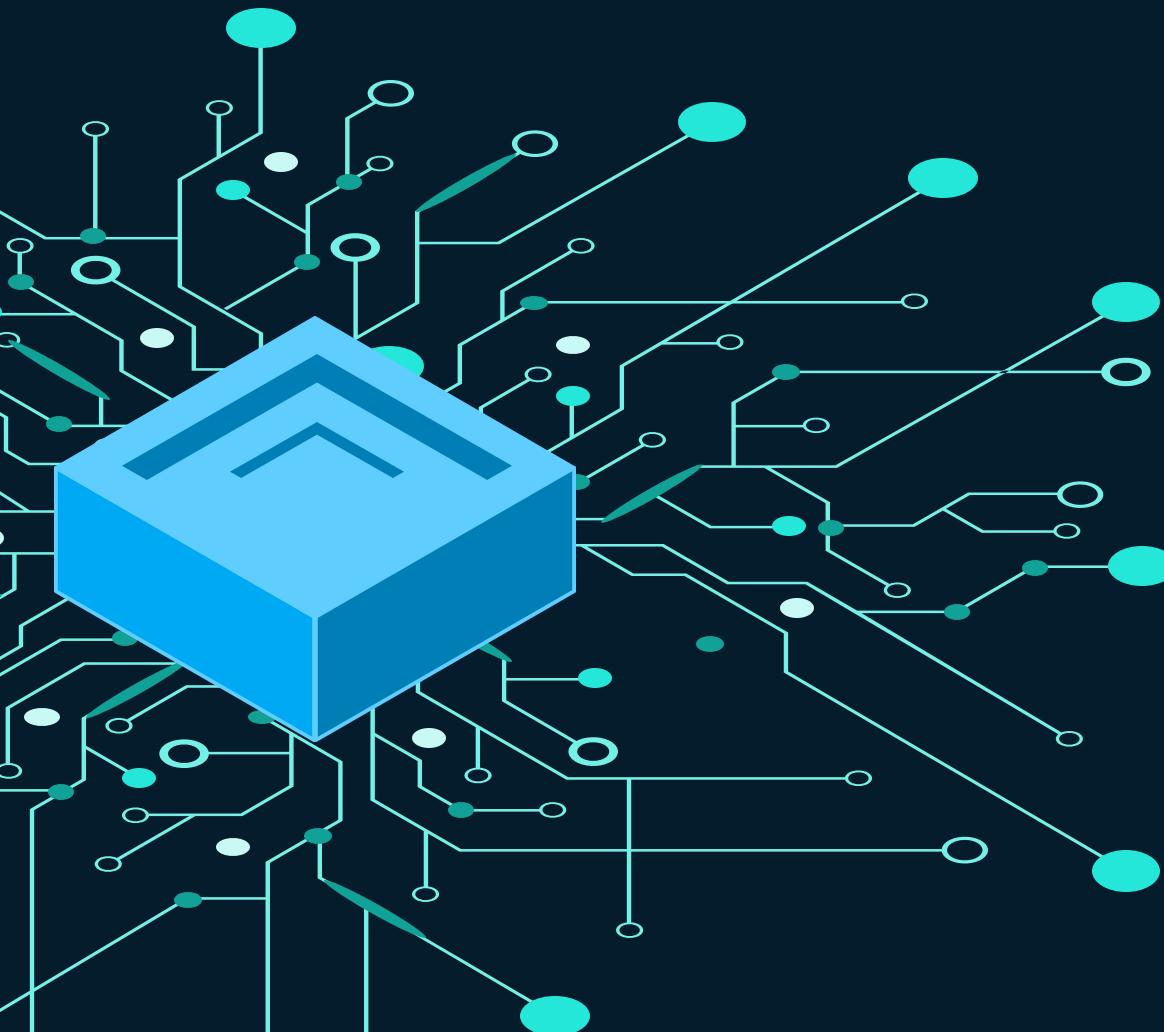


Digital profiles

Intellectual property of organizations (eg, recipes, blueprints)
User profiles stored by online retailers and social platforms; persistent digital identities vulnerable over time



Contents



Introduction

Innovations and breakthroughs

Market size and value at stake

Investment landscape

- Private funding
- Public announcements

Clusters and start-ups

Value chain

Deep dive into QComm

QT impact on cutting-edge technologies

Methodology and acknowledgments

Methodology

QT investments, patents, publications, revenue, market sizing, and player landscape



Investment analysis

Start-up investment data was sourced from PitchBook and subsequently analyzed by the McKinsey team. This analysis includes deal size, stage, HQ location, and investor type to provide insight into capital flows within the QT landscape

Public funding assessment

Public funding data was compiled through comprehensive press research and supplemented by PitchBook records, capturing government and institutional investments into quantum technologies

Patent landscape evaluation

Patent data was extracted from PatSnap, filtered by QT and analyzed by the McKinsey team to assess the innovation pipeline across QC, QComm, and QS

Scientific publications

Publication data was extracted from Nature Index, filtering for publications in physical sciences. Share per country is based on share of publications (ie, fractional measure that splits credit among coauthoring institutions), while total count is based on count (ie, total count of publications). 2024 data includes data from Jan 1, 2024, to Dec 31, 2024, while 2023 data includes data from Sept 1, 2022, to Aug 31, 2023

Revenue

Revenues are estimated based on the publicly announced revenues of QC start-ups and assume 30–40% of total revenue is distributed among private companies with less than \$1M in revenue according to market reports

Market sizing approach

Market sizes were estimated across two scenarios based on growth rate, each reflecting different adoption trajectories of QC, QComm, and QS. These scenarios account for varying assumptions about both the pace of technological breakthroughs and the rate of commercial uptake

QT player landscape

To map the QT ecosystem, the following definitions were applied:

- **Start-ups:** Companies founded within the past 25 years with estimated revenues below \$200M
- **Incumbents:** Established companies generating revenues exceeding \$200M
- **Component manufacturers:** Included only if they produce components specifically designed for QT applications; suppliers of general-purpose components were excluded
- **Hardware developers:** Included if they have either demonstrated a quantum computer or publicly committed to building one
- **Telecommunications providers:** Included if they are actively investing in QComm with the ambition to serve as quantum network operators

Meet the team behind the Quantum Technology Monitor

This research was conducted in collaboration with the McKinsey Technology Council, which brings together a global group of scientists, entrepreneurs, researchers, and business leaders. Together, they research, debate, inform, and advise, helping executives from all sectors navigate the fast-changing technology landscape.

Key contacts



Henning Soller

Partner
Frankfurt



Martina Gschwendtner
Engagement manager

Munich



Sara Shabani

Associate
New York



Waldemar Svejstrup
Associate

Copenhagen

Collaborators



Michael Bogobowicz

Partner
New York



Anna Heid
Associate partner

Zurich



Scarlett Gao

Engagement manager
London



Linshu Li

Engagement manager
Stamford