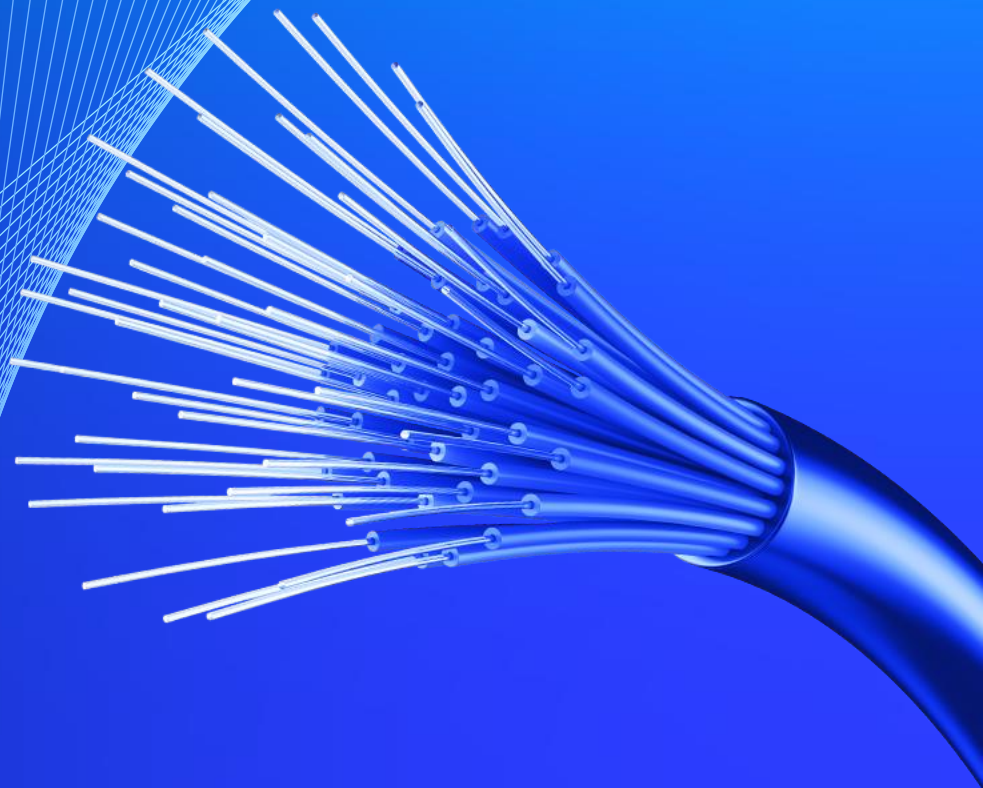
McKinsey Digital

Quantum communication: Trends and outlook

Market perspectives and impact of quantum technology for communications and computing

February 2025



Executive summary (1/2)

Quantum communication has attracted significant global attention because of its potential to revolutionize quantum security and secure networks across various sectors, including governments, research institutions, and telecommunications. This interest is fueled by several factors, including increased funding (eg, NATO initiatives), technical breakthroughs (eg, entanglement-based measurements), the importance of national security, and rising security demand (eg, China's recent developments in cybersecurity).

Product and industry landscape

- **The quantum communication landscape comprises three key categories**—security, networks, and services—and consists of six key verticals—quantum key distribution (QKD) solutions, post-quantum cryptography (PQC), modular interconnects, regional networks, quantum global internet, and quantum communication services. All of these are considered for quantum communication market sizing.
- **The highest level of maturity is currently seen for PQC, which has experienced the most commercialization.** This is primarily because of the lower implementation costs of PQC and early standardization by organizations such as NIST. This early momentum may experience a setback if breakthroughs in quantum algorithms, classical algorithms, or both show PQC to be vulnerable, especially given that the security of QKD is guaranteed by fundamental laws of physics.
- **The most fragmented vertical is expected to be PQC**, which will feature a mix of start-ups and established incumbents integrating and offering services, due to PQC's less complex hardware requirements compared with other verticals and the need to constantly remain "safe" in the face of evolving security needs.

Market sizing

- Leveraging product landscapes along with technological trends, we estimate the **total quantum communication market size to be $0.9 billion–$1.0 billion in 2023 and project it to reach $10.5 billion–$14.9 billion by 2035** with a CAGR of 23–25%. PQC is projected to hold the largest market share, with a market size of $2.4 billion–$3.4 billion by 2035.
- **While the government is expected to hold the largest customer share,** at 62–66% as of 2023, the private sector is projected to grow rapidly, with telecommunications and cybersecurity covering a 16–26% market share by 2035. This growth is driven by advancements in network infrastructure and data centers and by higher incumbent adoption by telecommunications companies, tech hyperscalers, and cybersecurity companies.
- **North America is forecast to capture the largest geographical share at 32% by 2035**, driven by substantial public funding and technological breakthroughs. However, Europe currently leads in quantum communication with QKD, supported by NATO prioritization and a vibrant start-up ecosystem.

Executive summary (2/2)

Market entry into quantum communication **leverages synergies shared with quantum computing** across the following:

- **Technology foundations** (eg, qubit modalities, system architecture)
- **Platform infrastructure** (eg, shared module and interconnect technologies)
- **Customer requirements** (eg, performance, ease of use as key purchasing factors)

The strongest synergies occur for applications and products that leverage entanglement as a resource (eg, regional quantum networks) or products that leverage modular photonic interconnects as part of their scaling strategy.

Q-Day, when cryptographically relevant quantum computers become capable of cracking classical encryption, could mark an inflection point for the commercial adoption of quantum computing and quantum communication, as the focus on security increases.

- 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 for quantum communication and competing classical solutions

While quantum communication poses unique security advantages, **classical solutions (eg, post-quantum cryptography) provide complementary alternatives that benefit from rapid adoption and lower cost of deployment**. Prevalent misconceptions (eg, regarding cost, performance) also surround quantum communication, which may be corrected by targeted messaging among key stakeholder groups.

Some quantum applications (eg, distributed or blind quantum computing) have no classical alternative and require quantum networks. But decelerators for wide adoption of quantum networks include low technology maturity and high development and deployment costs.

Key purchasing factors (eg, performance, ease of use) for quantum communication technologies vary depending on customer archetype, both for applications with alternative classical solutions and for new quantum applications.

Quantum communication developments affect core technologies for secure communications, quantum computing, and sensing.

Providing and driving secure communications

Developments in **post-quantum cryptography (PQC) and quantum key distribution (QKD)** are critical for mitigating growing threats to cybersecurity, including those posed by quantum computing (QC)

PQC and QKD have different advantages regarding performance, implementation, and cost, which affect the evolving market and deployment landscape for both technologies

Scaling and connecting quantum computers

Building scalable, fault-tolerant quantum computers requires interconnects in the form of short-scale quantum networking, which is experiencing dynamic technical development and commercial activity

Local quantum networks also provide **interfaces for QC resources with different modalities**, enabling users to leverage different qubit platforms together in one system

Enabling distributed computing and sensing

Large-scale quantum networks connecting QC resources enable distributed QC to enhance computing power and provide privacy

Quantum networks connecting quantum sensors improve sensitivity of the collective system, enhancing sensor performance and opening new potential applications

Overview: Quantum networks differ from classical networks and enable a range of quantum technologies.

Quantum vs classical networks

Quantum networks	**Networks that transmit quantum information** (eg, using single photons) **Enabling technologies** mostly at **low-maturity, R&D stages** Mostly **short-range, regional, low-bandwidth demonstrations**
Classical networks	**Networks that transmit classical information** (eg, using optical or RF[1] signals) **Widely adopted, commercially mature** across technology stack and service providers **Long-range, global, high-bandwidth** infrastructure across end users

Applications of quantum networks

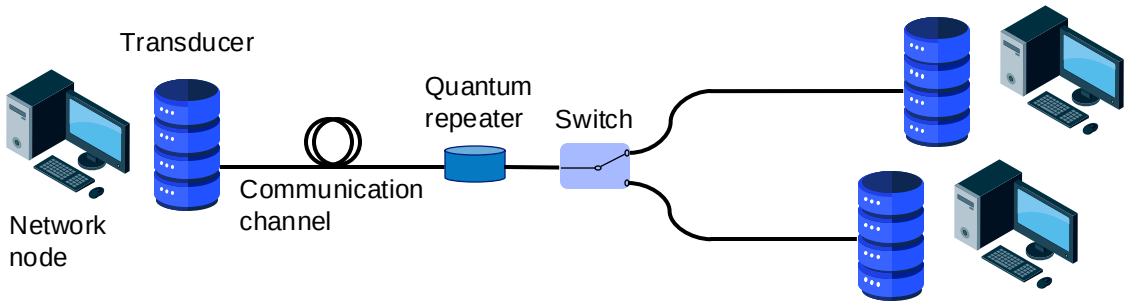
Distributed quantum computing	**Quantum networks provide efficient interconnects** between physically separated quantum computing hardware
Secure communications	**Enables provably secure communications** of classical information utilizing QKD[2] or by directly encoding messages as quantum information
Enhanced quantum sensing	**Improves sensitivity by leveraging entanglement-enhanced quantum sensing** through deploying arrays of sensors in tandem

1. Radio frequency (eg, cellular, Wi-Fi, Bluetooth). 2. Quantum key distribution.

Quantum networks differ in scale and application, and comprise multiple key technologies.

Deep dive to follow

Elements of quantum networks



Network node — **Sends or receives quantum information** on the network, including quantum computers, quantum sensors, single-photon sources and detectors

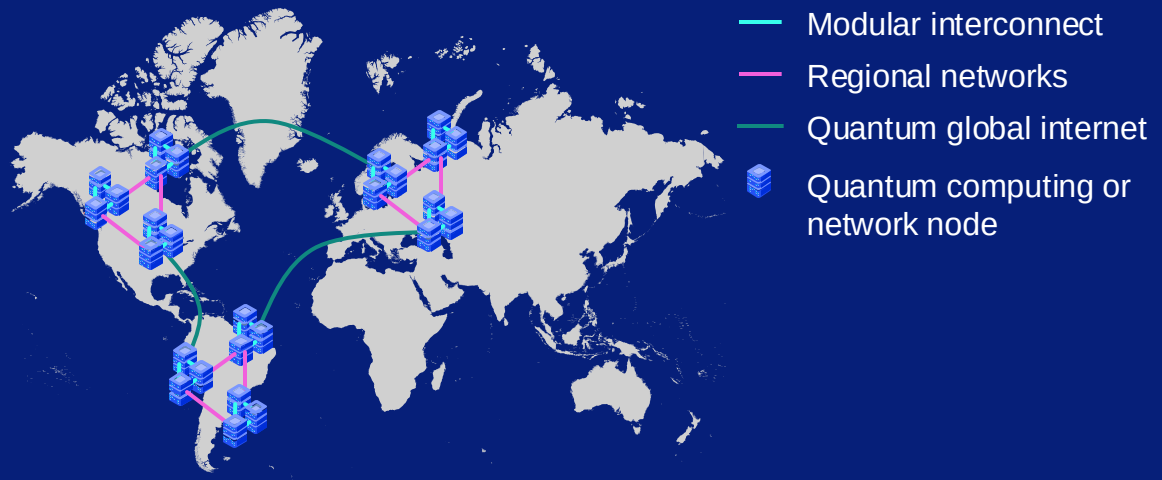
Transducer — **Converts one type of qubit[1] to another;** makes quantum information from one node compatible with the channels and other nodes in the network

Communication channel — **The path quantum information travels** between nodes, including optical fiber, free-space transmission

Quantum repeater — **Exchanges entanglement between qubits** to enable long-range quantum communication

Switch — **Routes quantum information between paths** to enable communication between one node and multiple others

Quantum networks used for quantum communication



Modular interconnects — **Devices and networks designed to connect qubits** for low-error and efficient computing and communication, **primarily within data centers**

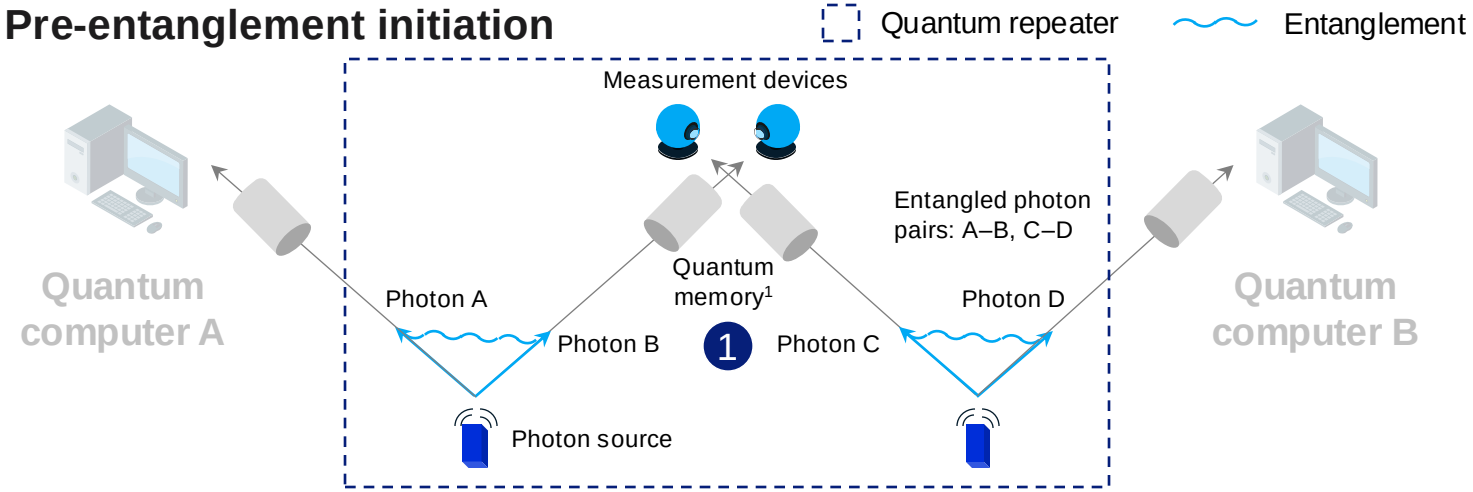
Regional networks — Fiber networks that **transmit quantum information across metropolitan and regional areas**

Global quantum internet — Fiber networks or satellites **enabling long-distance (eg, >1,000 km) transfer** of quantum information

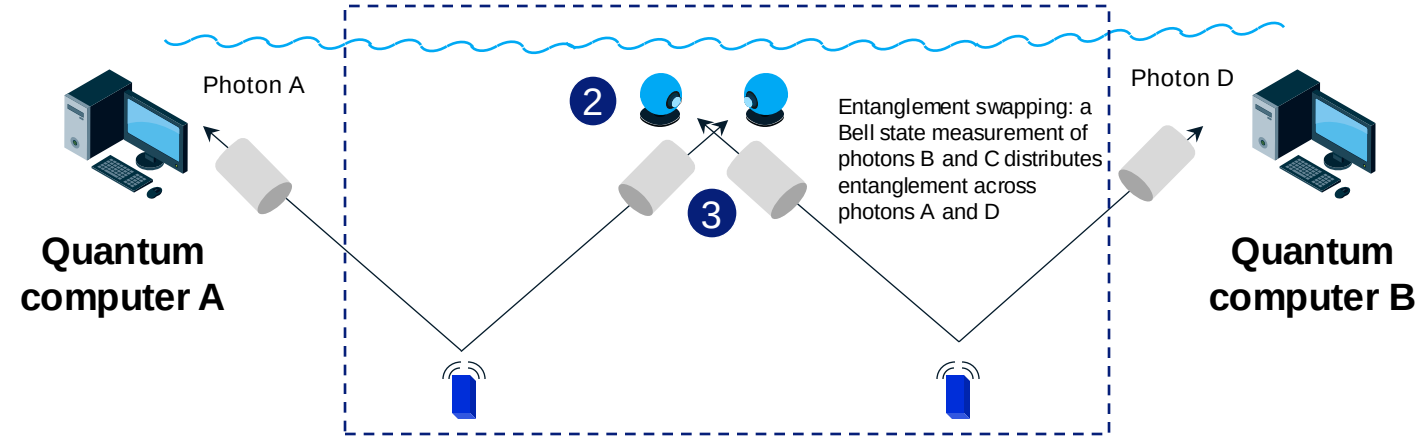
1. A qubit, or quantum bit, is the fundamental unit of quantum information in quantum computing and quantum communication.

Deep dive: Quantum repeaters enable entanglement distribution within quantum networks.

Pre-entanglement initiation



Post-entanglement communication



1. Quantum memory stores the quantum state of a qubit (eg, encoded in a photon in the quantum network).
Source: Gabriel Popkin, "The internet goes quantum," *Science*, 2021, Volume 372, Number 6546

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

? What is entanglement?

An essential feature of quantum mechanics, **entanglement occurs when the states of distinct quantum systems cannot be described independently**

Deep dive: QKD, which leverages quantum communication, provides stronger security guarantees than classical cryptography.

✕ Disadvantage ✓ Advantage

	Classical cryptography[1]	Quantum key distribution (QKD)
Operational principle	**Uses public keys**, which senders use for encryption, and **private keys**, which recipients use for decryption	**Leverages principles of quantum mechanics** to generate encryption keys
Security vulnerabilities	**Vulnerable to attacks on the security of the transmission channels and keys**, especially leveraging advances in quantum or classical computing, which enable decrypting private keys in practical time	**QKD is theoretically provably secure** and alerts communicating parties to the presence of an eavesdropper, but in practice, hardware vulnerabilities are possible in the implementations of certain protocols
Comparison	✕ **Vulnerable to advances** in cryptographically relevant quantum or classical computing ✓ **High bandwidth** and inexpensive due to mature technology stack ✕ **Potentially expensive upgrades** to hardware security modules to protect against quantum computing attacks	✓ Enables the **highest degree of security** ✕ **Relatively low bandwidth** and expensive (used only for secure key distribution) ✕ **Foundational components and integration** currently in R&D

1. Specifically describing an asymmetric encryption scheme (eg, RSA). While alternative classical encryption schemes exist, asymmetric encryption plays a key role in securing data today.

Section 1: Market assessment

Context

We assess the market landscape for quantum communication by identifying the respective verticals, assessing maturity, and analyzing key trends. We project market size by 2035 with a vertical breakdown, an industry view, and the geographic breakdown.

Topics

A Market drivers

- Accelerators and decelerators in the industry
- Status of commercialization
- Technological maturity and progress
- Barriers to entry in the market
- Fragmentation of the current market
- Geographical trends and geopolitics

B Market sizing

- Assessment
- Vertical breakdown
- Industry breakdown
- Geographic breakdown

Quantum communication applications span security and networking.

Non-exhaustive

Focus of this document

	Quantum communication (Qcomm)		Quantum computing (QC)	Quantum sensing
	Quantum security	Quantum networking		
Description	Solutions like quantum key distribution (QKD) ensure provably secure encryption of quantum information, while post-quantum cryptography (PQC) ensures safety against quantum attacks	Transfer of quantum information between nodes using principles such as entanglement to enable applications over longer distances (eg, quantum global internet)	Use of qubits to perform certain calculations at unprecedented speeds, enabling complex computational problem solving, simulations, and optimizations with minimal energy consumption	Enhanced measurement precision and sensitivity, with use cases in fields such as medical imaging and navigation systems potentially surpassing classical sensors in sensitivity and accuracy
Example companies[1]	ID Quantique QuantumCTek Quantum XChange Toshiba	AWS Cisco IonQ: Qubitekk Qunnect	IonQ IBM Quantinuum QuEra	AOSense Infleqtion Sandbox AQ

1. Non-exhaustive list of companies; QC companies listed based on estimated revenue.

Source: McKinsey analysis

Key factors driving market growth include increasing cybersecurity demand and technological breakthroughs.

	Accelerators	Decelerators
Technology	**Ongoing research and breakthroughs are addressing key challenges** (eg, the development of entanglement-based QKD modalities enabling longer distances and higher key rates)	**Technical hurdles exist** for maintaining quantum states over long distances and developing key components (eg, repeaters) for scalable quantum networks
Funding	**Growing recognition of quantum potential is attracting investment** from governments, multilateral organizations (eg, NATO), venture capital, and corporate R&D	**Securing consistent funding for quantum communication ventures can be difficult** given long development timelines and lack of serious market studies
Demand	**Increasing cyberthreats and data breaches are driving demand** for ultrasecure communication methods, and PQC may not be immune to quantum decryption in the long run	Some CIOs lack education on the **costs and benefits of quantum solutions**
Regulatory and policy	**Governments have started prioritizing national security** through the development of quantum strategies to maintain strategic independence	**An ongoing lack of standardized regulations**, including international standards, is creating uncertainty and slowing market growth
Infrastructure	**Major telecommunications companies can potentially leverage their existing network infrastructures** to implement and scale quantum solutions	**New or upgraded infrastructure** compatible with quantum networks could be required to transfer quantum information

Source: Expert interviews; McKinsey analysis

Market segmentation: Six key verticals shape quantum communication among security, networking, and services.

Verticals		Description	Example industries
Quantum security	QKD solution (including QRNG[1])	Software and hardware products that enable detection of interception attempts (incl largely hardware QRNG[1] products). QKD consists of prepare-and-measure protocols and entanglement-based protocols	Cybersecurity, finance, telecommunications, IoT, automotive
	PQC	Classical algorithms (eg, hash-based, lattice-based, etc) designed to be secure against the potential threats posed by quantum computers	Cybersecurity, finance, telecommunications
Quantum networks	Modular interconnect	Devices designed for connecting qubits, including switches and transducers (eg, for frequency conversion), to enable low-error and efficient computing and communication	Academia, finance, telecommunications, government, IoT
	Regional networks	Interconnected data center systems for quantum communication across municipalities and regions (<1,000 km networks), leveraging repeaters and critical components such as entanglement sources and quantum memories	Finance, government, telecommunications
	Quantum global internet	Technologies enabling intercontinental transfer of quantum information using repeaters involving both free-space and fiber-based systems (>1,000 km)	Finance, government, telecommunications
Services	Quantum communi-cation services	Services ranging from technical support for hardware devices to expert consulting for adoption	Finance, healthcare, telecommunications

1. Quantum random number generation.

Commercial adoption: PQC, QKD, and QComm services are already in (partial) production.

Non-exhaustive

Production · Partial production · Near production · In development

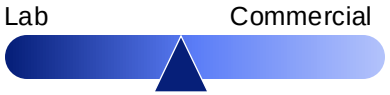
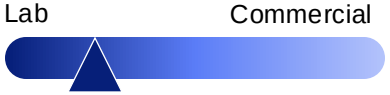
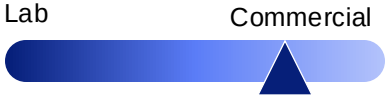
Verticals		Key use cases and drivers	Status of commercialization
Quantum security	QKD solution (including QRNG)	Telecommunications players increase attention on QKD to improve communications security[1] (eg, Toshiba and IDQ)	Partial production
	PQC	Tech companies prepare for a post-quantum world (eg, Apple has introduced PQC protocols for enhanced security in iMessage)	Production
Quantum networks	Modular interconnect	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	Near production
	Regional networks	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	Near production
	Quantum global internet	Government deploys satellite or fiber-based quantum communication to secure global data transmission, driven by the necessity to provide encrypted connectivity over large distances	In development
Services	Quantum communication services	Various industries (eg, financial services, telecommunications) use scalable platforms offered by emerging start-ups to incorporate quantum solutions	Production

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 do depend on repeater technology are still in development.

Source: Expert interviews; McKinsey analysis

Technology maturity: PQC leads in technological maturity among verticals, driving adoption and market growth.

Verticals	Technical target state for commercialization	Technology maturity	Required milestones and breakthroughs
QKD solution (including QRNG)	Integrate QKD hardware and management layer into existing infrastructure and advancing technologies (eg, repeaters) for long-range secure communication. Prepare-and-measure QKD is relatively more mature than entanglement-based QKD[1]		Technologies to extend range and key rate, enable error correction, and improve implementation of entanglement-based protocols
PQC	Implement the standardized PQC algorithm across organizations in a crypto-agile manner, allowing for updates with new algorithms if weaknesses are discovered (eg, NIST has standardized the PQC protocol, and the EU is expected to follow this trend)		Demonstration of error-corrected QC could increase demand and adoption for PQC
Modular interconnect	Connect qubits to expand their computational power, evolving from initial experimental configurations to deployable, commercial applications		Scalable, low-loss, fast-switching interconnects between modules
Regional networks	Focus on QComm links among regional data centers, developing quantum repeaters for secure, long-distance transmission and entanglement sources		Repeaters with high key rate, entanglement generation, and capacity for error correction
Quantum global internet	Deploy satellite-based QComm and develop a full-scale quantum internet to connect distant quantum computing resources		High-fidelity quantum channels (eg, satellite and fiber), mature repeaters, scalable quantum computers
Quantum communication services	Create user-friendly solutions for customer success, incl programming interfaces and protocols, leveraging implementation that is efficient and automated where possible		QComm and network infrastructure

1. On the technological maturity scale, entanglement-based QKD corresponds to the left arrow, and prepare-and-measure QKD corresponds to the right arrow.

Source: Expert interviews; McKinsey analysis

Ease of deployment: PQC is highly implementable in existing software, while QKD faces greater complexity.

High Low

Verticals	Key barriers to entry	Vulnerabilities	Ease of deployment
QKD solution (including QRNG)	Compatibility with existing network infrastructure and protocols is crucial High costs, deployment complexity, and incumbent intellectual property protection	**Fast followers:** Other players could adopt similar technologies over time due to less technical complexity in non-entanglement-based systems	Medium
PQC	Efficient implementation into the current code base Highly specialized talent in algorithms and crypto Lack of certainty over future protection	**Substitute technologies:** Emerging innovations in QC (eg, quantum cryptography) could disrupt PQC algorithms or render them obsolete	High
Modular interconnect	Existing patents on design and architecture Highly specialized talent	**Fast followers:** Potential for products to be standardized after the patents expire (similar to classical data center optical transceivers)	Low/Medium
Regional networks	Capital requirements and high cost attributed to the hardware in long distance Operational costs for maintenance and upgrades	N/A	Low
Quantum global internet	Geographical accessibility and deploying the secure satellite technology specific to geography High costs for global infrastructure Certification processes from governments	N/A	Low
Quantum communication services	Partnership to offer turnkey solutions for customers Lack of standardization	**Substitute technologies and fast followers:** Hardware providers might gain maturity in software and consultancy and diminish the market for services	High

Source: Expert interviews; McKinsey analysis

Market concentration: PQC is highly fragmented among tech incumbents and start-ups, while QKD comprises fewer players.

High Low

Verticals	Fragmentation level	
QKD solution (including QRNG)	Low	Incumbents (eg, ID Quantique, Toshiba) have significant presence, driven by hardware challenges and high R&D and capital requirements, which limit entry for smaller players
PQC	High	Growing presence of incumbents and start-ups reflects evolving maturity of the field as well as a mix of in-house research and strategic partnerships in finance and telecommunications
Modular interconnect	Medium	Academic research remains fragmented, with QC players driving most advancements in hardware (eg, transducers, switches)
Regional networks	Low	Governments, alongside telecommunications companies, prioritize QComm infrastructure, particularly for long-distance applications (eg, Chattanooga, Berlin, Chicago)
Quantum global internet	Low	Government-led projects are the biggest for quantum satellites (eg, China) and the quantum internet with some investments from telecommunications companies and start-ups (eg, SpeQtral)
Quantum communication services	Medium	Companies (eg, IBM Quantum Safe) are increasingly positioning themselves as platform service providers, partnering with established companies

Source: Expert interviews; McKinsey analysis

Global activity: Europe is active in developing quantum networking, while the United States is leading efforts in PQC.

Geographic area	Trends	Announced government investments in quantum technology ($ billion, by end of 2023)
Europe	**NATO prioritizes quantum technologies**, **with Europe playing a significant role in network** development as well as national security interests from European governments; eg, the European Quantum Communication Infrastructure (EuroQCI) initiative, a Quantum Technologies Flagship initiative, backed by €1 billion. Additionally, **Berlin is emerging as a quantum hub:** TU Berlin is developing a quantum-secured network, and Deutsche Telekom is investing in opening a quantum lab	**12.7**[1]
United States	**The US shows increased activity in PQC as well as quantum networks.** NIST is leading efforts on post-quantum encryption standards, which include standardized instructions and algorithms for incorporating into products and encryption systems against future quantum computer threats. In quantum networks, Chattanooga and Qubitekk have partnered to launch the first commercially available, industry-led effort in the United States, while Cisco has also launched a quantum testbed in Los Angeles	**3.8**
China	**China shows early advantage in satellite-based quantum communication** and quantum networks with plans to launch new quantum satellites over the next few years. China is also actively advancing QKD, having built a system that spans thousands of kilometers, connecting four major cities	**15.3**
Asia–Pacific (excluding China)	**Japan has made progress in QKD and PQC solutions** and prioritizes quantum secure networks (eg, Toshiba, SoftBank). **Korea is also driving progress** with breakthroughs in quantum repeaters and announced plans to develop a 100 km regional quantum network	**5.9**[2]

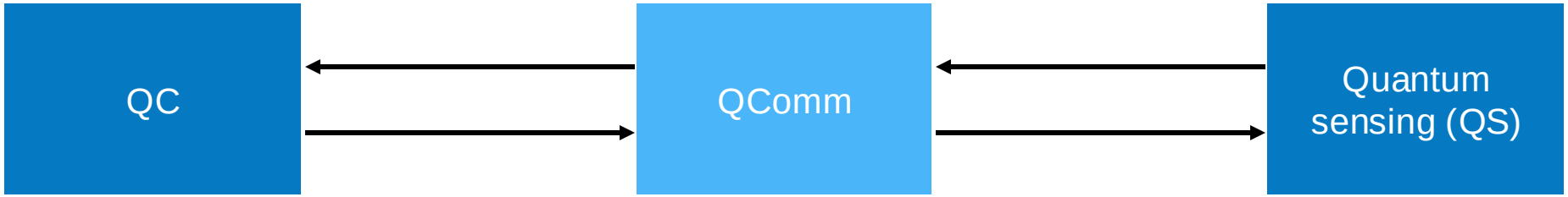
1. Includes Germany, the United Kingdom, France, and the Netherlands.
2. Includes South Korea, Japan, and India.

Source: Expert interviews; McKinsey analysis

The quantum communication market could reach $10.5 billion to $14.9 billion by 2035.

Quantum technology total addressable markets (TAMs) in 2035, $ billion

The TAM is the theoretical potential for the core market assuming full market penetration



TAM

28.0–72.0[1] | **10.5–14.9**[1] | **0.5–2.7**[1]

Interdependencies

Progress in QC could drive growth in the QComm market

Commercial progress in QC also leads to more demand for networking and communication

Technological advancements in QS could accelerate QComm market development

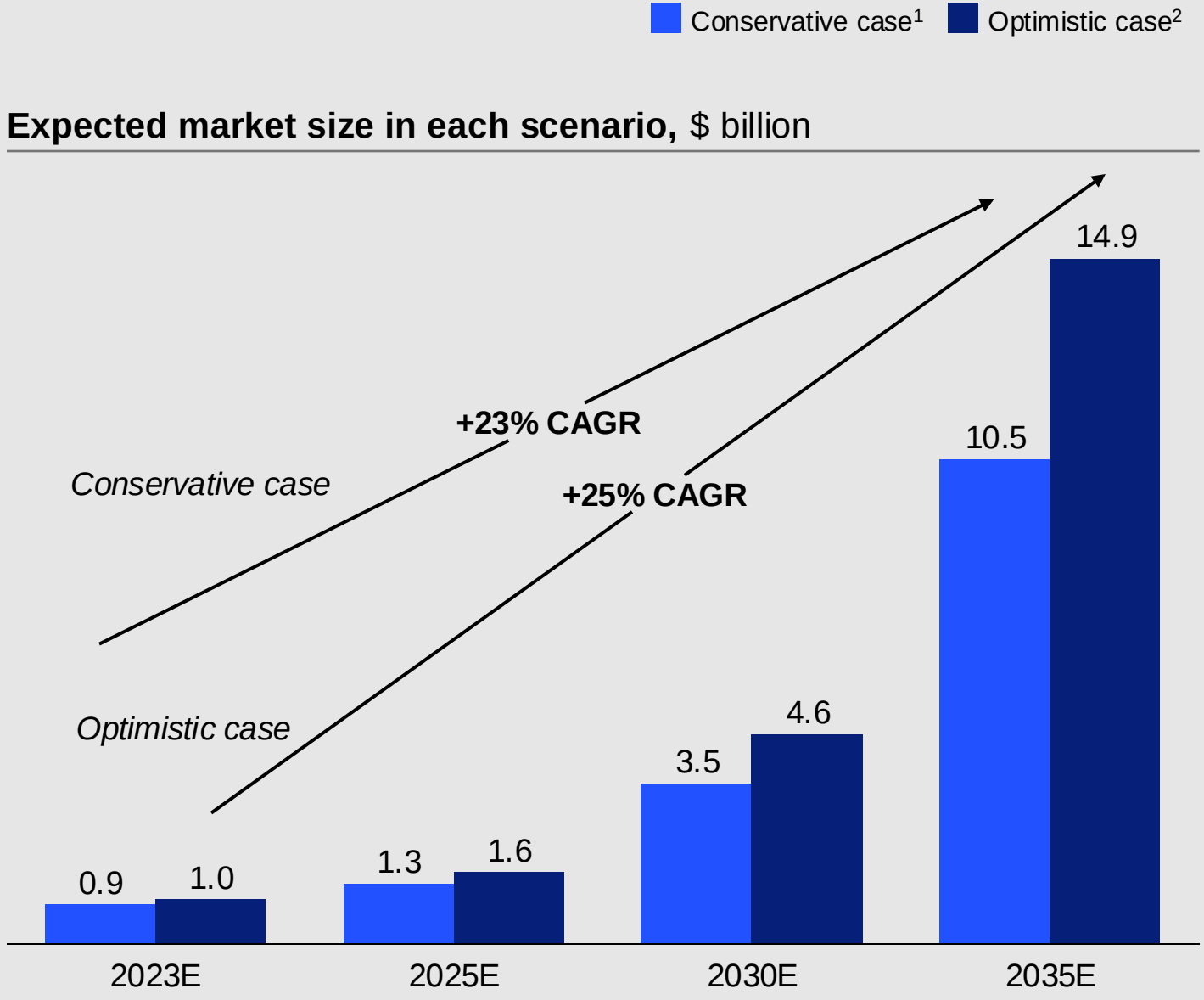
Large-scale adoption of QS coupled with technological progress (eg, coherence time) could enable the development of entanglement-based QS networks

The QC TAM is broadly estimated across conservative and optimistic scenarios given a large variance in potential technological progress, adoption rates, and scaling opportunities

1. Range shows conservative and optimistic scenario market sizes.

The quantum communication market is expected to reach $10.5 billion to $14.9 billion in 2035 with a CAGR of 23 to 25 percent.

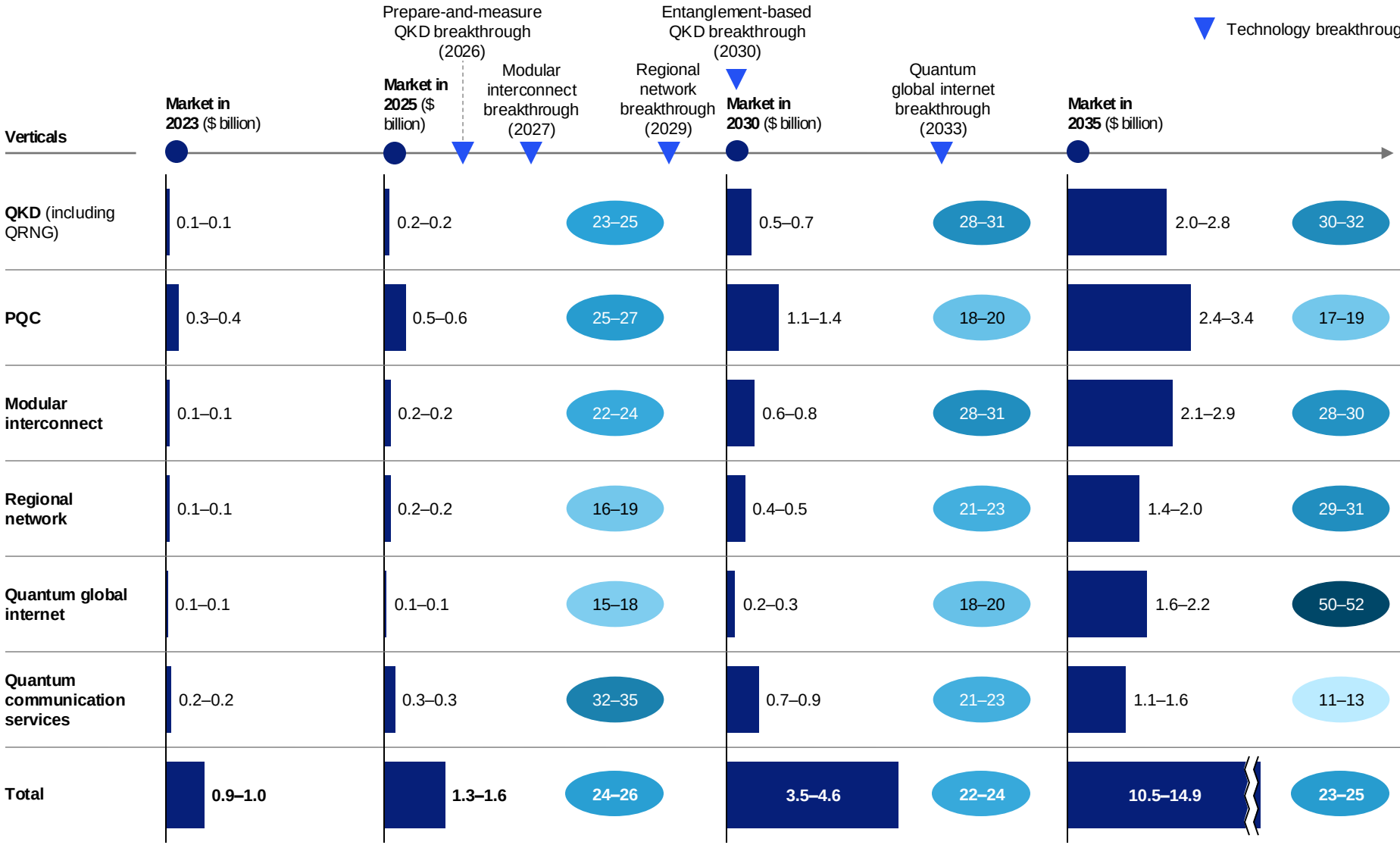
Expected market size in each scenario, $ billion



1. Assumes slower rates of adoption of quantum technologies and lower growth rates of the market.
2. Assumes faster rates of adoption of quantum technologies and higher growth rates of the market.

Source: Expert interviews; McKinsey analysis

PQC and modular interconnects are forecast to have the largest market size across verticals in 2035.

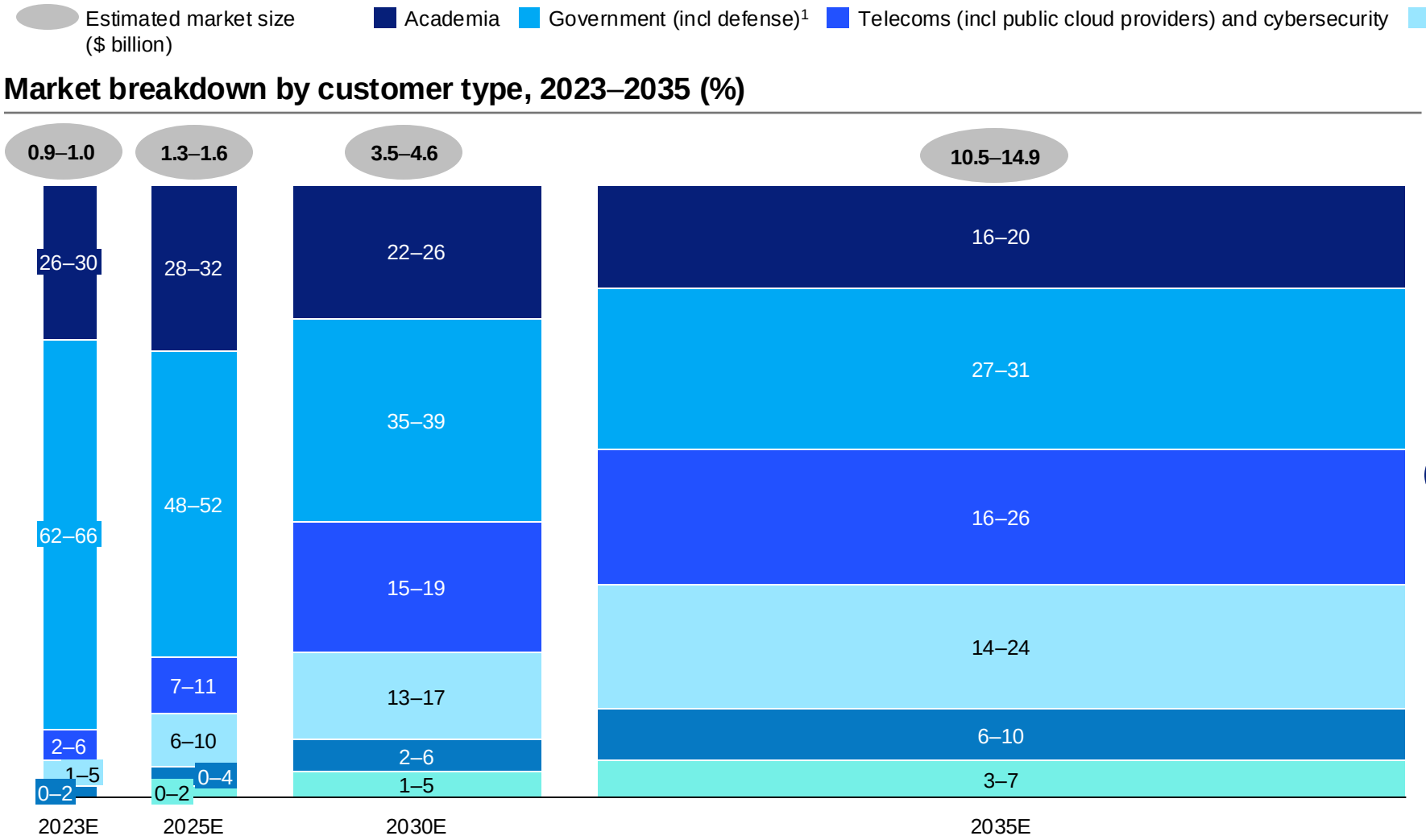


Rationale for forecast growth

- Growth will be driven by increasing technological progress and adoption, and will make QKD the third-largest vertical market by 2035
- Market will become increasingly standardized and grow more slowly, from 25–27% CAGR in 2023–25 to just 17–19% CAGR in 2030–35
- Assumed potential technological breakthrough in 2027 will drive growth with a CAGR of 28–31% in 2025–30
- Assumed potential technological breakthrough in 2029 will expand market potential, driving growth to 29–31% CAGR in 2030–35
- Assumed potential technological breakthrough in 2033 will lead to a surge in market growth to 50–52% CAGR in 2030–35
- Stand-alone services growth will slow over time to 11–13% CAGR in 2030–35 as other verticals integrate services into their offerings

Source: Expert interviews; McKinsey analysis

Telecoms and financial services are expected to form an increasing share of the quantum communication market.



Key takeaways

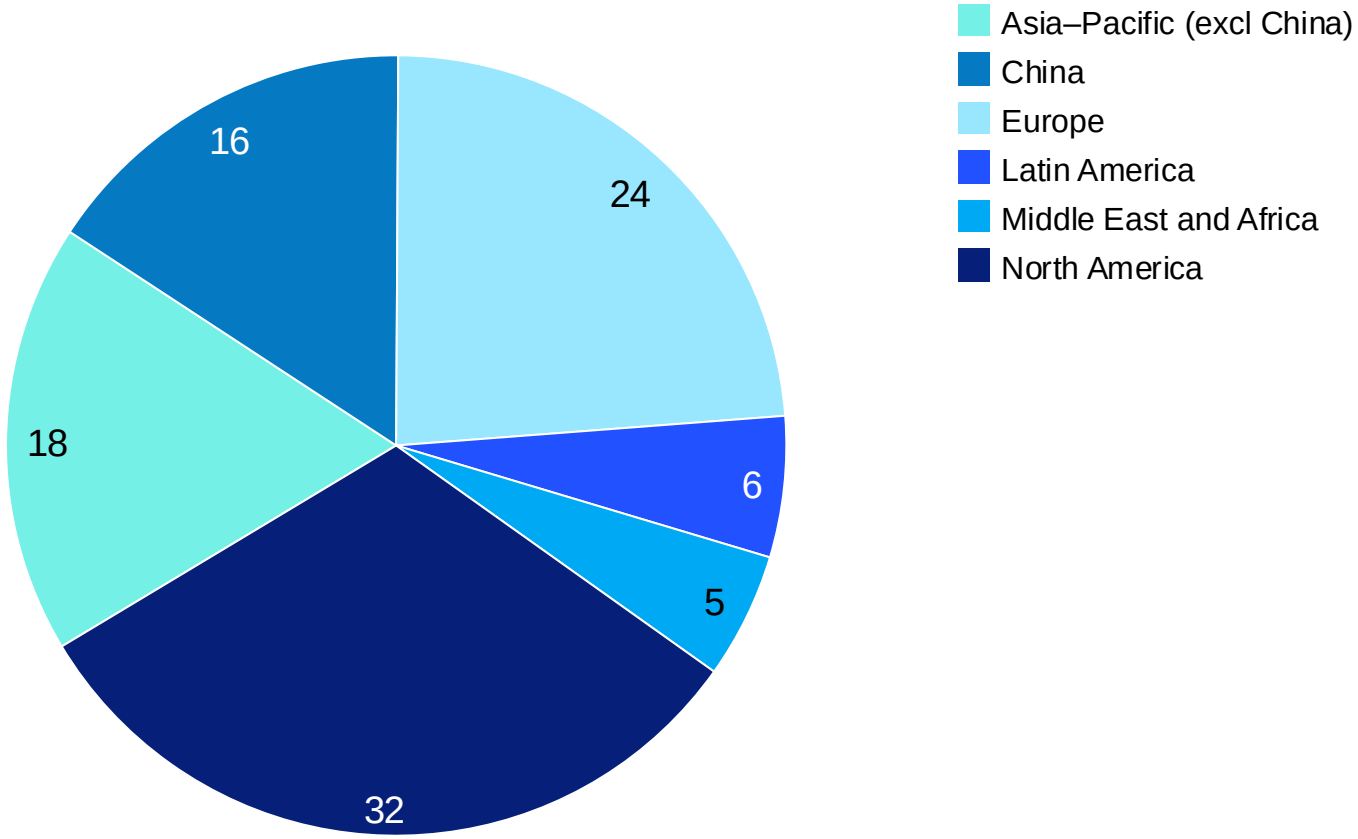
- **Government (including defense) is the largest player** in the current market, with 62–66% estimated market share in 2023
- **Telecoms are estimated to have an increasing market share** over the time horizon, increasing from 2–6% in 2023 to 16–26% in 2035, led by growth in networks markets
- **Financial 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

1. Includes civil government and defense.
2. Includes manufacturing, automative, insurance, etc.

Source: Expert interviews; McKinsey analysis

North America is forecast to have the largest market share (about 32 percent), driven by increased investment and start-up activity.

Geographic breakdown of the quantum communication market, 2035 (%)



Note: Figures do not sum to 100%, because of rounding.
Source: Expert interviews; McKinsey analysis

Key observations and takeaways

- **North America's public funding and increased competition among US states** will drive start-up activity, with an expected 32% market share
- **Europe is expected to retain a strong presence in the market** (24% market share), driven by NATO prioritization of quantum initiatives and funding and a strong start-up presence
- **China is forecast to remain a key player in 2035 (16% market share),** driven by public investment and strong performance in the networks market

Section 2: Technology and ecosystem

Context

We assess the quantum communication (QComm) technology landscape and ecosystem, including synergies with quantum computing (QC), the implications of Q-Day,[1] and other accelerators and challenges that drive development and adoption of QComm technologies

Topics

A Broad trends affecting QComm growth

- Technology synergies with QC
- Q-Day signals, opportunities, and impacts
- QComm advantages versus existing solutions

B Drivers for adoption of each technology

- Factors affecting relative adoption of QKD[2] and PQC[3]
- Common misconceptions about QKD and PQC
- Key buying factors for QComm solutions
- State-of-the-art performance today and outlook

1. When cryptographically relevant quantum computers successfully crack classical encryption. 2. Quantum key distribution. 3. Post-quantum cryptography.

QComm market leverages strong synergies with QC for technology, customer requirements, and partners.

✓ Common to QC and QComm — Differences between QC and QComm

	Synergies and key differences	Quantum computing	Quantum communication
Technology requirements	✓ Leverage quantum control and algorithms ✓ Require scalability and efficient interfaces ✓ Use long-coherence quantum memories — QC requires greater local connectivity, while QComm requires longer-distance connectivity — QComm requires transporting entangled flying qubits over longer distances	• Quantum control (eg, for error correction or mitigation) • Efficient interfaces for control and readout • Highly connected qubits in local register • Scalable architecture for modules • Efficient algorithms for desired problems	• Some quantum control (eg, for error correction at repeater and readout) • Efficient interfaces for readout, scaling • Efficient entanglement generation and distribution • Ability to span long distances and enable high key rates
Customer requirements	✓ Prioritize performance and production readiness as key differentiator ✓ Require suitable algorithms and protocols for specific applications and use cases — QC may require less integration with existing classical networking infrastructure than QComm	• High compute performance (beyond classical when possible) • Easy-to-use software stack • High system availability • Support in building and deploying algorithms to solve specific problems	• Provably secure cryptography systems • Compatibility with other components in communication infrastructure • High reliability and low error rates across required ranges with high key rates • Deployment and ongoing support
Partners	✓ Can provide improved algorithms or architectures (eg, academic researchers) ✓ May enable access to essential equipment or infrastructure (eg, R&D, manufacturing) ✓ Provide access to talent (eg, academic or industry experts via strategic partnerships)	• Strong collaboration with academic and government institutions for R&D • Partnerships with end users (including academic and industry) to develop algorithms and use cases	• Partnerships with industry players to develop and refine technology capabilities • Strong collaboration with organizations establishing regional / global standards

Source: Expert interviews; McKinsey analysis

QComm's strongest synergies with QC technology are in interconnects and regional quantum network components.

High Medium Low

Verticals	Examples	Synergies with QC	Synergy level
QKD solutions	• Prepare-and-measure protocols (eg, BB84) • Entanglement-based protocols (eg, E91)	• Requires scalability, connectivity for qubit networks • Leverages long-coherence quantum memories • Ideally compatible with classical data center, networking infrastructure	Medium
PQC	• Key establishment via ML-KEM[1] • Digital signature authentication schemes ML-DSA[2] and SLH-DSA[3]	• No direct synergies with QC, but PQC can be co-deployed with QKD	Low
Modular interconnects	• Interconnects between QC modules within data center	• Interconnects required for scaling QC qubits • Enables entanglement distribution and qubit connectivity over short distances	High
Regional quantum networks	• Metropolitan-scale quantum link connecting Delft and the Hague	• Qubits for QC (including error correction) can be integrated within quantum repeaters	High
Global quantum internet	• Components primarily in R&D stage	• Connecting global networks of QC resources (for distributed or blind quantum computing) requires quantum networking capabilities	Medium

1. ML-KEM: Module-lattice-based key-encapsulation mechanism. 2. ML-DSA: Module-lattice-based digital signature algorithm. 3. SLH-DSA: Stateless hash-based digital signature standard.
Source: Expert interviews; McKinsey analysis

Different qubit modalities vary in compatibility with modular interconnects and synergies with quantum network applications.

Illustrative Non-exhaustive

Low High

Qubit modality	Example companies	Maturity[1]	Synergies with QComm	Challenges for use in QComm
Trapped ions	AQT IonQ Quantinuum		Small registers of ions with long coherence times enable error-corrected quantum repeaters Ability to operate at room temperature eases deployment of quantum communication infrastructure	Low ion-photon coupling efficiency (may be improved using optical cavities and multiplexing) Long gate times (may require multiplexing)
Superconducting circuits	Alice & Bob, AWS, Google, IBM, IQM, Rigetti, SEEQC		Strong coupling to microwave photons enables transferring entanglement to and from qubits	Optical communications requires transduction of microwave photons from qubits (currently in R&D stage) Operation at cryogenic temperatures (~mK) can create challenges for deployment
Neutral atoms	Atom Computing Pasqal QuEra Computing		Reconfigurable arrays of atoms with long coherence times enable error-corrected quantum repeaters Ability for operation at room temperature convenient for deployment within communications infrastructure	Low atom-photon coupling efficiency (cavities and multiplexing can improve) Array blocks are reconfigurable and support the use of optical cavities but may have shorter lifetimes and require reloading
Photonic qubits	PsiQuantum, Xanadu Quandela		Native photonic platforms ease integration effort High-performance integrated photonics components can be reused for QComm	Requirements for low-loss, fast-switching photonic components Need cryogenic (~K) single-photon detectors
Spin qubits	Intel[2] Photonic		Long coherence times makes spin qubits good candidates for quantum memories Solid-state matrix enables stronger coupling using integrated photonic cavities for entanglement transfer	Optical communications may require transduction of microwave photons from qubits (currently in R&D stage) Operation at cryogenic temperatures (~K) can create challenges for deployment

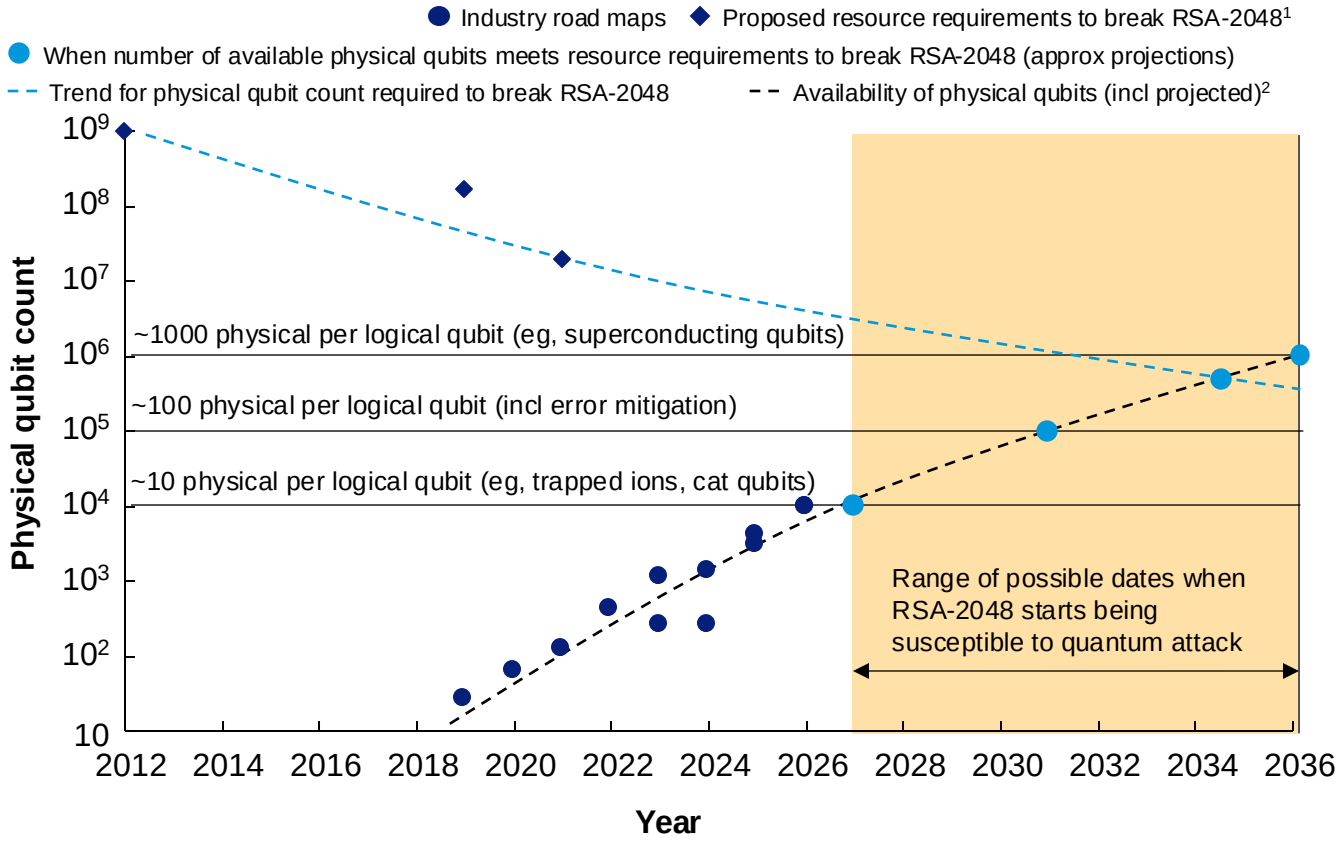
1. Technology maturity measured according to availability of qubit platform at product level for commercial availability vs for only R&D availability.
2. "Intel's new chip to advance silicon spin qubit research for quantum computing," Intel, June 15, 2023.

Source: Expert interviews; McKinsey analysis

Q-Day could mark an inflection point in the quantum computing, quantum communication, and technology ecosystem.

Illustrative

Quantum resource availability and requirements by year, 2012–36



Impacts post Q-Day[3]

- Sensitive data using legacy encryption (including critical private information) becomes vulnerable, leading to potentially large economic and societal disruption
- Organizations may adopt quantum-safe cryptography at accelerated rate to prevent loss of sensitive data
- Substantial investments may be made in PQC and QKD to enhance security and prevent data loss

Q-Day drivers

- Innovation and investment in QC improves system performance (including hardware and algorithms) enabling greater capabilities and efficiency
- Developments in quantum error correction and mitigation reduce the number of physical qubits per logical qubit needed for useful computation
- Innovations in quantum algorithms enable successful cyberattacks against classical algorithms (which include PQC) previously thought to be secure

1. Craig Gidney and Martin Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, 2021, Volume 433.
2. Historical for pre-2024, projected for post-2024.
3. 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

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

Illustrative

Type	Signal	Description	Examples
Acceleration	**Changes in investment patterns**	Shifts in public or private investments could indicate imminent or achieved breakthroughs in quantum technology	Increases in government funding for quantum technology 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 quantum technology
	Increasing adoption of competing technologies	Greater adoption of competing solutions may indicate challenges with competing in competitive markets	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 quantum computing to AI, QKD company refocusing on PQC
	Slowing innovation	Technical obstacles prevent major breakthroughs in scaling quantum computers	Quantum computing players missing milestones for logical qubits

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

+ Low ++ Medium +++ High

Preliminary

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 help provide crypto-agility, high Q-Day impact due to diverse, highly distributed infrastructure	+++
Global energy and materials	Oil and gas	++	+	+	Limited secure communication requirements, low IT maturity, limited Q-Day impact	+
	Sustainable energy	++	+	++	Critical infrastructure has high security requirements, other parts of segment have lower security requirements	++
	Chemicals	+	+	+	Limited secure communication requirements, lower IT maturity, limited Q-Day impact	+
Travel, transport, and logistics	Travel, transport, and logistics	++	++	++	Medium demand for secure communication and storage, digitalization efforts to enhance IT modernization improve crypto agility, medium Q-Day impact due to highly distributed infrastructure	++
Pharma and medical products	Pharmaceuticals	++	++	+++	IP and health records require secure communication and storage, some crypto agility from digital technology influx, high Q-Day impact	++

Likely QKD adopters include industries with high Q-Day impact and low 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—when commonly used cryptosystems (eg, RSA, ECC) are susceptible to quantum attack—will affect operations.

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

+ Low ++ Medium +++ High

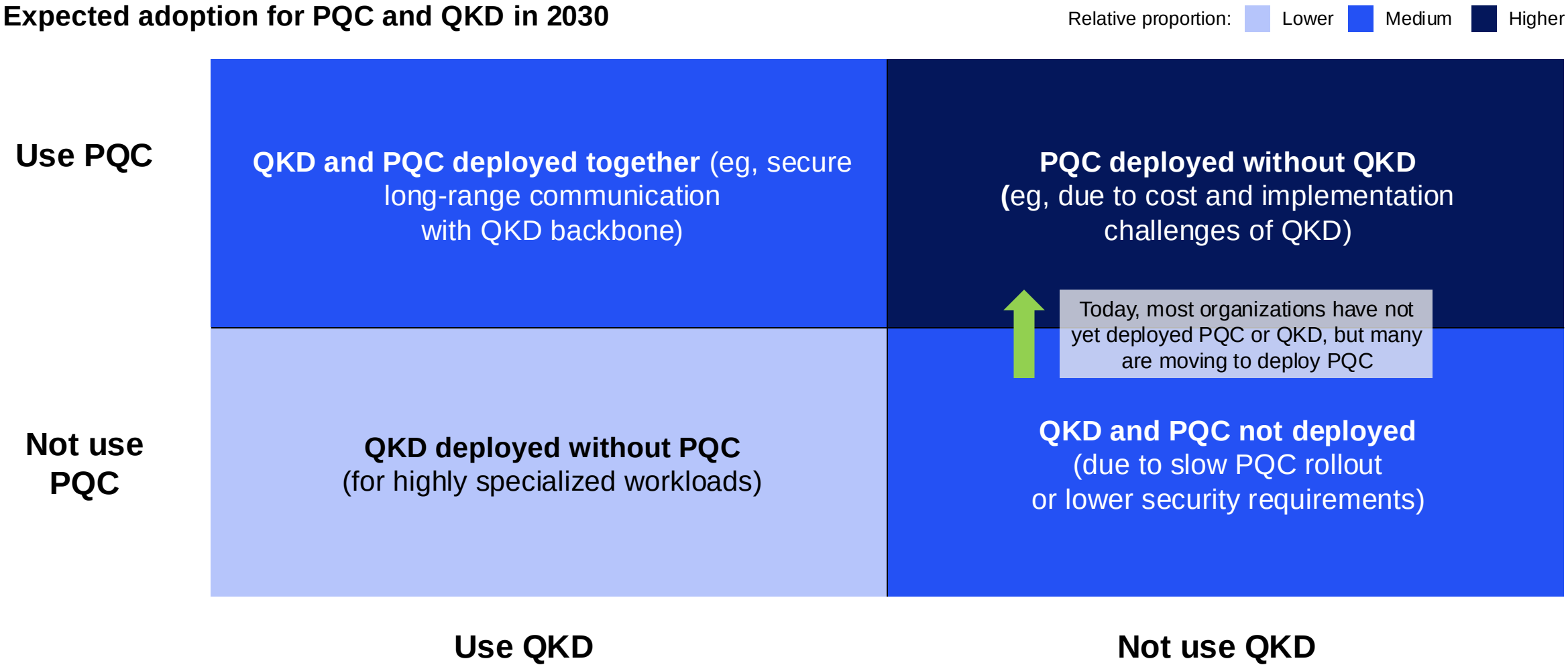
Preliminary

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	+++
	Media	++	+++	++	Limited security and privacy requirements with high crypto-agility due to technology focus	++
Government	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—when commonly used cryptosystems (eg, RSA, ECC) are susceptible to quantum attack—will affect operations.

PQC and QKD may be deployed separately or together, with PQC adoption expected to lead in the next five years.

Expected adoption for PQC and QKD in 2030



Source: Expert interviews; McKinsey analysis

Quantum networking enables security proofs and scalable QC, while PQC provides quantum-safe classical algorithms.

Preliminary

Uses, or can use, quantum entanglement

Applications of quantum networks	Quantum technology	Classical counterparts	Technological adoption drivers	Demand drivers
Quantum-secure communications	QKD[1] Entanglement-based quantum networks	PQC Trusted nodes[2]	Industries with high security requirements (eg, defense, finance)	Security guarantees Total cost of ownership
Connecting quantum computing resources	Scalable quantum computing Distributed quantum computing	High-performance computing (eg, supercomputers)	Hyperscalers with specific quantum offerings in mind Other players requiring quantum solutions (eg, pharma company pursuing drug discovery)	Computing requirements (eg, quantum vs classical algorithms)
Data privacy	Blind quantum computing	Homomorphic encryption	Industries with strict data privacy requirements (eg, finance, pharma)	Privacy requirements

1. Prepare-and-measure QKD protocols do not require entanglement, while entanglement-based QKD protocols do.
2. Can be integrated with quantum technologies to classically enable QKD over long distances. However, security guarantee of QKD is lost.

While QKD can be provably secure, PQC has shorter time to deployment and lower infrastructure requirements.

No data · Lower · Medium · Higher

Tech-nology	Security guarantee	Performance[2]	Time to deployment	Total cost of ownership (TCO)	Infrastructure requirements[3]	Technology maturity	Example companies[4]
QKD	Provably secure[1] (eg, with entanglement-based QKD)	Key rates on order of kb/s to Mb/s Repeaterless network lengths on order of 100 km	Longer due to required installation (eg, hardware for quantum technology infrastructure)	Large initial investments for infrastructure (including hardware), with additional infrastructure maintenance costs	Requires hardware for key distribution and potentially quantum repeaters May require dedicated networking infrastructure	Commercially available but some advanced technologies under development	ID Quantique QuantumCTek Toshiba
PQC	Heuristically secure (may be vulnerable against future attack leveraging quantum or classical algorithms unknown today)	Key rates on order of Gb/s Can be distributed over existing global networks	Shorter due to implementation (eg, software update on existing hardware; hardware upgrades sometimes required)	Lower TCO when only software updates required Higher TCO if new hardware required to replace legacy systems	Lower infrastructure requirements if only software updates required May require replacement of legacy hardware	Relatively new technology (eg, with recent NIST standardization)	IBM PQShield SandboxAQ
Quantum networks	Provably secure[1]	Testbed networks under development	Commercial data not available	Large initial investments for infrastructure (including specialized hardware), with additional infrastructure maintenance costs	Requires quantum transmitters, receivers, and potentially repeaters May require dedicated networking infrastructure	Technology under development	Aliro Quantum IonQ/Qubitekk Qunnect

1. Theoretically provably secure, but vulnerabilities exist for some hardware implementations.
2. Measured by key rates and maximum deployment distances.
3. Includes the specialized hardware required to implement new technologies and the classical infrastructure that must be replaced.
4. Includes companies with research or products in QKD, PQC, or quantum networks.

Source: McKinsey analysis

Major players in government and the private sector have begun to adopt PQC ahead of Q-Day.

Preliminary

Sector	Organization	PQC adoption
Private	**Apple**	Introduced PQ3 protocol (based on PQC standard ML-KEM) for iMessage in March 2024
	IBM	Provides access to quantum-safe algorithms based on finalists for NIST PQC standards in IBM z16 mainframe and supports quantum-safe encryption on IBM Cloud
	Google	Began using PQC for internal communications in 2022. Chrome enabled PQC standard ML-KEM by default for TLS 1.3 and QUIC on desktop in May 2024
	Cloudflare	Reported that >16% of human-generated HTTPS requests to Cloudflare services in mid-August 2024 were protected by PQC
Public	**NSA**	Outlined timeline to completely transition to PQC standards by 2033
	NIST	Initiated search for PQC algorithms to define standards in December 2016 and published 3 standards in August 2024
	CISA	Launched PQC Initiative to support adoption of PQC standards in critical infrastructure across government agencies
	European Commission	Published recommendation in April 2024 to develop Post-Quantum Cryptography Coordinated Implementation Roadmap within 2 years
Inter-governmental	**NATO**	Announced strategic initiative to transition to PQC and committed to allowing member states to support one another in developing PQC and QKD

Implications

- Increase in web traffic protected by PQC supports notion that PQC is **present in quantum-safe cryptography**
- NSA transition timeline points to substantial **cost of replacing legacy hardware** for PQC
- International commitment to adopt PQC may **drive increased demand**
- Growing adoption of PQC and awareness of threat posed by Q-Day could **fuel investment in both PQC and QKD**

Source: Apple; CISA; Cloudflare; Google; IBM; NIST; NSA

Evolving security needs, technology maturity, and cost determine adoption of QKD, PQC, and quantum networks.

Preliminary

✓ Driver of adoption — Little effect on adoption — ✗ Obstacle to adoption

	Security	Performance	Total cost of ownership
QKD	✓ **Provable security may drive demand** as QC matures, particularly if existing PQC algorithms prove vulnerable	✗ **Low key rates and limited key distribution range may limit demand** until technology matures ✓ **Combining QKD and PQC** could achieve long-range communication while retaining security of QKD	✗ **Requires deployment of expensive quantum hardware** and potentially a dedicated quantum channel ✗ **Possible cost of updating hardware** as technology matures could dissuade early adopters
PQC	✗ **Heuristic PQC algorithms are vulnerable** against quantum attacks, which could erode consumer confidence in PQC ✓ **Mathematically proven PQC algorithms** provide direct competition to QKD security	✓ Reliance on **mature technologies with high performance will drive demand** for PQC while QKD technology matures	✓ **Cost of PQC software may be low** in many instances ✗ **High costs of replacing legacy equipment**[1] may slow adoption or drive adoption of QKD
Quantum networks	— Provable **security only drives demand if information can be sent more efficiently with a quantum network** than with QKD and a classical network	✓ **QC performance could fuel adoption of quantum networks** because there is no classical alternative to transmit quantum information ✗ **Without QCs, quantum networks may only see adoption** if performance can exceed that of high-performing classical communication networks	✓ **Cost of module interconnects important** in determining whether QC players buy solution or seek to develop solution in-house — **Cost of regional and global networks likely has little effect on adoption** if few large providers build and sell access to network

1. US government projects spending $7.1 billion to transition to PQC.

Key misconceptions prevalent in the QComm market include the role of repeaters in QKD and the cost of implementing PQC.

Non-exhaustive

Misconceptions	Drivers of misconceptions	Situation in industry	Implications for the industry
PQC is unconditionally secure against future quantum attack	Standardization of PQC algorithms, adoption in big tech	Developments in quantum or classical algorithms could break PQC encryption	Future attacks that demonstrate vulnerability of PQC could drive greater adoption of QKD
Upgrading to PQC only requires a software update	Perception as a pure software solution, ease of adoption in cloud-hosted solutions	Large costs required to transition legacy systems with hardware encryption to PQC	Companies must evaluate whether large cost of adopting QKD justifies adopting PQC instead for certain use cases
All QKD schemes are impervious to eavesdropping	QKD protocols are theoretically impervious to eavesdropping under ideal conditions	Some QKD systems are susceptible to hardware attacks while, eg, entanglement-based DI-QKD[1] systems are not susceptible	Developing low-cost QKD that meets rigorous security requirements important for capturing market share
Quantum repeaters are the only solution to enable long-range QKD	Transmitting quantum information with quantum repeaters retains security guarantee of QKD	Substantial portion of QKD market views trusted nodes as satisfactory solutions, and satellites can distribute keys globally	Quantum repeater technology not required for QKD market to capture meaningful market share
Fiber networks are key cost drivers for QKD deployments	Perceived costs of establishing dedicated optical fiber communications between parties	Other hardware costs for QKD are a substantial portion of implementation cost	Reducing hardware costs for QKD is key to reducing deployment costs
PQC adoption removes the need for QKD for secure communications	Both address security needs for communications and have dynamic factors driving adoption (eg, quantum computing capability)	Solutions can coexist, including hybrid solutions that combine benefits of both technologies	Customers may choose to adopt both PQC and QKD depending on security needs

Key takeaway: Developing low-cost, deployable solutions for maximally secure QKD implementations is key to long-term success in the market

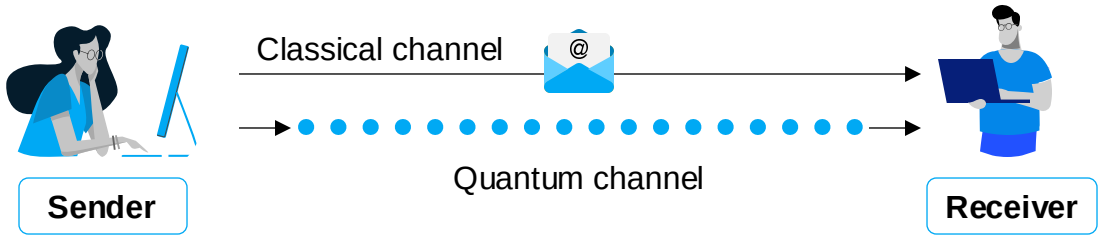
1. Device-independent QKD.

Source: Expert interviews; McKinsey analysis

While prepare-and-measure QKD is gaining traction in the market, entanglement-based QKD has some practical security advantages.

Illustrative

Prepare-and-measure QKD



Basic procedure

1. Sender prepares photon in select basis and transmits state to receiver
2. Receiver measures photon in random basis and communicates basis to sender
3. If bases agree, photon measurement used to generate key

Benefits

Utilizes simpler implementation not requiring source of entangled photons

Enables higher key generation than entanglement-based QKD

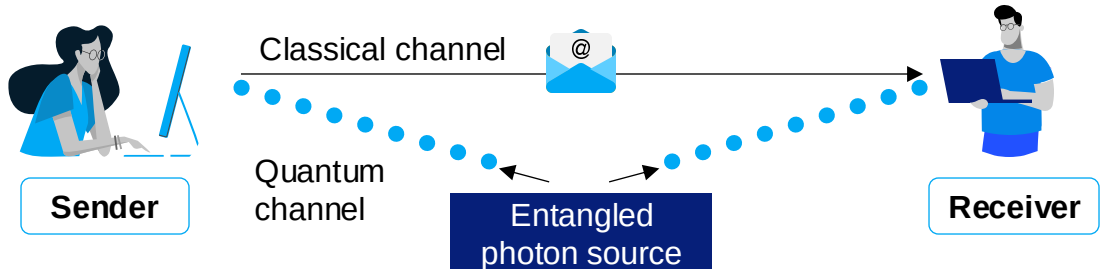
Lower cost to implement due to less sophisticated technology involved

Drawbacks

Provides lower security guarantees in practical implementations

Not compatible with quantum repeater technology

Entanglement-based QKD



Basic procedure

1. Entangled photon source sends one photon to sender and one to receiver
2. Both parties measure photons in independently selected random bases
3. Both parties classically communicate measurement bases
4. Correlations between photons measured in same bases used for key

Benefits

Enables stronger security guarantees in practical implementations

Can be combined with quantum repeaters for long-range QKD

Drawbacks

More complex setup required to generate and measure entangled photons

Slow key generation rates relative to prepare-and-measure QKD

Higher cost to implement due to more sophisticated technology required

Key buying factors for broad adoption of QComm technologies include performance, cost, and reliability.

Non-exhaustive

Vertical	Key buying factors	Metrics and features
QKD	Performance	Key rate, max channel length, maximum allowable loss, security parameter
	Cost	Hardware costs, costs of any dedicated channels, maintenance, training
	Reliability[1]	Channel uptime, hardware life cycle, maintenance requirements
	Ease of use	Ease of deployment (including integration with existing infrastructure), support services and tools
Quantum networks[2]	Performance	Throughput, bandwidth, latency, error rate, max channel length, maximum allowable loss
	Reliability	Network uptime, hardware life cycle, maintenance requirements
	System compatibility	Integrability with existing systems (eg, for different quantum modalities), tools for test and control

Implications

- Customers' trust in QKD provider plays key role in driving demand
- Key rate and channel length must increase for QKD to compete with PQC in the near term
- Performance and reliability are key buying factors as consumers make initial transition to QKD
- Cost is relatively small factor for customers (eg, multinationals) with high security requirements
- Cost is important for enabling broader adoption of QKD in long run

- Technological development is required to achieve performance and reliability for commercialization
- Integrability with variety of quantum modalities is key to achieving widespread interconnectivity
- Cost is relatively unimportant for regional and global networks due to market concentration

1. Includes reputation (eg, brand, track record).
2. Includes local (eg, modular interconnects), regional, and global quantum networks.

Source: Expert interviews; McKinsey analysis

Improving upon the performance specifications of leading QKD and quantum network players is key to broadening adoption.

Illustrative

QKD systems

QComm technologies	Industry examples			Requirements for broad adoption
Company[1]	**Toshiba**	**Q*Bird**	**ID Quantique**	Improved deployment methods, including satellites, trusted nodes, and mobile ground stations, are needed to deploy QKD with existing performance metrics
QKD protocol	BB84 with decoy states and phase encoding	MDI[2] with decoy states	BB84 with decoy state	Certain high-security customers might prefer repeaters over trusted nodes to extend key distribution range for fiber QKD deployments
Key rate	3000 bps at 10 dB channel loss	≥500 bps at 125 km (0.2 dB/km)	Typically ~1,000 bps at 24 dB channel loss	Improved integrability with existing telecom infrastructure could broaden addressable market
Max channel length	150+ km (30 dB max channel loss)	200 km (40 dB channel loss)	150 km (30 dB channel loss)	
Security guarantee	$<10^{-10}$ key failure probability	Not available	$\sim10^{-12}$ probability of eavesdropper knowing 1 bit of 256 AES key	

Quantum networks

Qunnect	AWS	
99.84% network uptime realized over 15 days; **entanglement fidelity at 99%** with 20,000 entangled photon pairs per second[3]; system includes automatic polarization compensation	**Entanglement storage >1 s** realized in a 35 km fiber network, demonstrating use of **quantum memory** to store information in network and **transduction from optical to telecom qubits**	High-fidelity quantum transduction is needed to enable interconnections between quantum modalities[4] Repeater technology must develop to enable long-haul quantum communication

1. Metrics listed for Long-Distance QKD System LD from Toshiba, MQ4000 Line from Q*bird, and Clavis XG QKD System from ID Quantique. Units converted to enable direct comparison between products.
2. MDI: measurement device independent. 3. Note fiber losses may be high (~17 dB). 4. Need for transduction relevant to quantum interconnects, regional quantum networks, and global quantum internet.

Source: Expert interviews; McKinsey analysis

Meet the team behind this report

Key contacts

Lareina Yee
Senior Partner
Bay Area

Rodney Zemmel
Senior Partner
New York

Henning Soller
Partner
Frankfurt

Michael Bogobowicz
Partner
New York

Martina Gschwendtner
Engagement Manager
Munich

Alex Zhang
Associate
San Francisco

Sara Shabani
Associate
New York

Christian Leefmans
Associate
Boston

Shabbir Merali
Associate
London

Appendix

Methodology: Market sizing

Market assessment methodology

A triangulated methodology combining a top-down approach, a bottom-up overlay, and expert insights, is used to estimate the market size for quantum communication:

- **The top-down approach** assesses the classical communication market size, the forecast growth rate, and the quantum market share
- **The bottom-up overlay** uses industry-wide data to estimate the breakdown of verticals
- **Expert insights** and market reports are integrated to validate assumptions and refine estimates

Assumptions

Key assumptions to ensure a stable and predictable projection include the following:

- No single player will capture the market significantly, leading to a competitive and diverse landscape
- There will be technological breakthroughs in networks, which will result in higher adoption and growth
- No major disruptions from emerging technologies, and an increasing quantum share of the classical market

Identified gaps

Despite the comprehensive approach employed in market sizing for quantum communication and networks, **certain gaps remain:**

- Limited availability of historical data for quantum, which can constrain the accuracy of growth projections
- Inherent uncertainty in predicting technological advancements and market adoption rates, which can vary widely based on unforeseen regulatory changes and other factors
- Expert interviews may sometimes reflect biases

Methodology: Market sizing approach and inputs

Overview

A triangulated approach is used for estimating market sizing:

- A top-down analysis of the overall market
- Bottom-up vertical splits and trends
- Expert insights to establish solid assumptions

Inputs

For each vertical, the following assessments influence the shape of future market growth:

- **Accelerators and decelerators** in the industry
- **Status of commercialization**
- **Technological maturity** and progress
- **Barriers to entry** in the market
- **Fragmentation** of the current market
- **Geographical trends** and geopolitics

Methodology: Market sizing scenarios

Overview of the methodology

Description

1. The **QComm market size was estimated** by identifying the quantum market share capture by year, the overall classical market size in 2023, and the forecast growth of the classical market across the time horizon

2. The **breakdown of the vertical share of the overall market size** was estimated by calculating the relative proportion of each vertical's corresponding classical market size for 2023

3. The **vertical growth rates were refined through expert insights on vertical market trends**, and an additional growth boost was added for the network component of QComm once the "trigger" of technological breakthrough was met

Key assumptions

The QComm market is defined as including both revenue and funding (from venture capitalists, governments, and corporate R&D)

Increasing quantum share of the classical market over time, and an increasing funding landscape for QComm

Trigger points for technological breakthroughs are estimated to be 2027 for modular interconnects, 2029 for regional networks, and 2033 for the global quantum internet, where it is assumed that a breakthrough in quantum tech will lead to a significant jump in growth rate (with a growth boost of 9%, 10%, and 60% respectively)

Analysis

The market size is estimated to be ~$0.9 billion–$1.0 billion in 2023 and ~$10.5 billion–$14.9 billion in 2035 with a CAGR of 23–25%

Scenarios

We have developed 2 scenarios:

1. **Conservative scenario with slower adoption of QComm** technologies due to technological challenges and adoption hurdles, which **could lower the revenue and the funding growth rate**
2. **Optimistic scenario with faster commercial adoption and higher growth rate** of QComm technologies, characterized by rapid advancements in technology and swift adoption by industry

Methodology: Market sizing assumptions deep dive

Preliminary

Verticals	Assumptions
QKD solution (including QRNG)	QKD will have a limited share of the current quantum communication market, currently made up of data security, data privacy, and application security components, but will exhibit strong growth to become the largest vertical by 2035
PQC	PQC will have the largest vertical share of the current quantum communication market, composed of cloud security, integrated risk management, and identity access management components
Modular interconnect	Trigger for technological breakthrough in 2027 resulting in a 9 p.p.[1] permanent increase in growth rate per annum relative to baseline
Regional networks	Trigger for technological breakthrough in 2029 resulting in a 10 p.p. permanent increase in growth rate per annum relative to baseline
Quantum global internet	Trigger for technological breakthrough in 2033 resulting in a 60 p.p. permanent increase in growth rate per annum relative to baseline
Quantum communication services	Quantum communication services will increasingly be integrated with products within verticals, resulting in a decline in the stand-alone quantum communication services market

General assumptions

- **Overall classical market forecast to grow over time**, with an increasing quantum share
- **Market size across all verticals to grow over time,** following technological breakthroughs
- **Steady increase in funding and investment** from venture capitalists, governments, and corporate R&D across the time horizon

1. Percentage point.

Source: Expert interviews; McKinsey analysis

Glossary of key terms (1/2)

Term	Definition
Blind quantum computing	A type of quantum computing in which a user's computation is not interpretable by the operators of the quantum computer
Crypto-agility	A property that describes the ability of an organization to update its security infrastructure in response to novel threats
Entanglement	A quantum mechanical phenomenon in which the states of distinct quantum elements cannot be described independently
Entanglement distribution	The act of entangling physically separate quantum systems by coupling a qubit entangled to the first system to a qubit coupled to the second system
Entanglement swapping	A key feature of quantum communication schemes in which entanglement is distributed over pairs of entangled qubits
Entanglement-based QKD	Quantum key distribution protocols that use entanglement to generate cryptographic keys
Fault-tolerant quantum computing	A quantum computer in which the logical error rate (the rate at which qubits end up in an unintended state) can be made sufficiently low to perform intended operations
Homomorphic encryption	A type of encryption in which the encrypted data can be operated on as if it were in its decrypted form, thus allowing a user to conceal data from an eavesdropper who might have access to the computational hardware
Hyperscaler	Large-scale cloud service providers (eg, AWS, Google Cloud, Microsoft Azure)
Post-quantum cryptography	Classical encryption algorithms designed to withstand attacks from cryptographically relevant quantum computers
Prepare-and-measure QKD	QKD protocols that rely on the preparation and measurement of quantum states to distribute cryptographic keys
Q-Day	The date on which quantum computers become sufficiently powerful to attack classical cryptography (eg, RSA)

Glossary of key terms (2/2)

Term	Definition
Quantum coherence	A property of quantum systems that describes how long the system maintains its quantum information before unwanted noise makes the quantum information irretrievable
Quantum communication (QComm)	Transmission of quantum information—eg, to enable quantum computing (eg, distributed QC) and other applications (eg, secure communications). Quantum communication systems include quantum networks
Quantum computing (QC)	Computation that leverages properties of quantum systems
Quantum control	Controllably manipulating the state of individual qubits and systems of qubits
Quantum key distribution (QKD)	Communication protocols that leverage fundamental properties of quantum physics to enable provably secure communications
Quantum memory	A device or system that enables the storage and retrieval of a quantum state
Quantum sensing (QS)	Sensing protocols that leverage quantum systems to achieve greater sensitivity
Qubit	The fundamental unit of quantum information in quantum computing and quantum communication
Spin	Quantized, intrinsic angular momentum possessed by fundamental particles
Trusted node	In QKD, a method to distribute keys over long distances that involves measuring, regenerating, and then relaying the quantum information. Because measuring the quantum information introduces a security vulnerability, the trusted node must be operated by trusted operators

Deep dive: Example players developing solutions for the entanglement-based QKD technology stack

Example companies	Products available or under development	Key considerations
Quantum Optics Jena	Sells ELVIS QKD systems that rely on an entanglement-based QKD protocol based on the BBM92 protocol. QKD systems are offered at both 800nm (short-distance and free-space) and 1300nm/1500nm (fiber)	Quantum Optics Jena appears to have a product on the market for entanglement-based QKD
Q*Bird	Sells QKD modules with a measurement device-independent QKD protocol that can perform multipoint-to-multipoint QKD	Q*Bird appears to have a product for entanglement-based QKD already on the market
LQUOM	Advertises the LQ-PS-100 cavity-enhanced two-photon source on the company website and highlights its application to quantum repeater technology	While website advertises equipment that can be used for entanglement-based QKD, the company does not appear to be selling any full QKD solutions
levelQuantum	Filed patent for a new, device-independent QKD (DI-QKD) protocol	Company does not appear to be selling products currently
IonQ/Qubitekk	Sells hardware, including an entangled photon source and the Bohr-IV Quantum Network. Collaborated with EPB to build a commercial quantum network that could enable building entanglement-based QKD	IonQ/Qubitekk has developed and deployed all components for a quantum network, which could be used to implement entanglement-based QKD
Aliro Quantum	Sells software for emulating and deploying entanglement-based quantum networks. Aliro technology is used in the EPB quantum network	Aliro's software solutions can be combined with other companies' hardware to facilitate designing and building quantum networks

McKinsey Digital