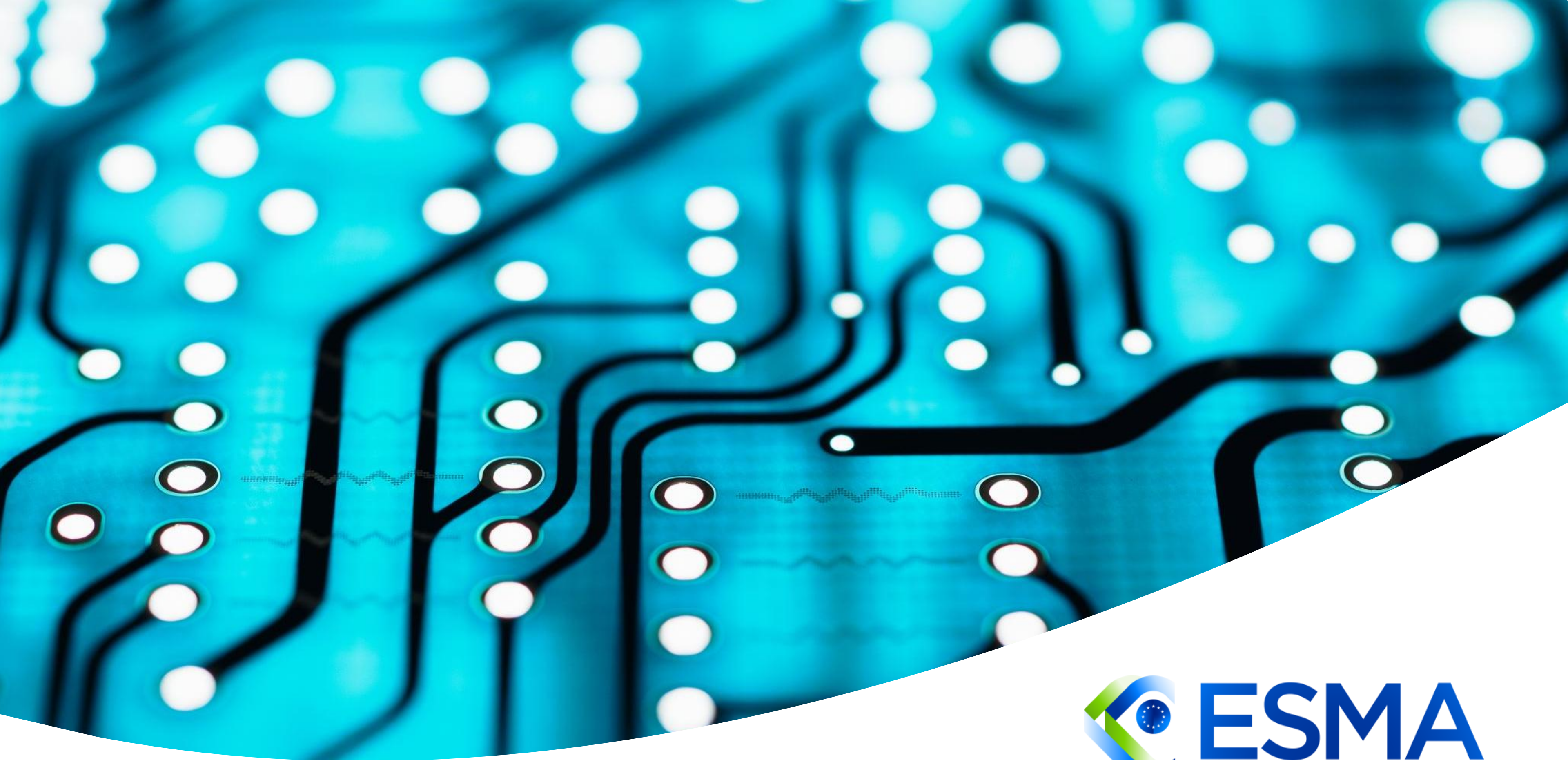


Quantum computing in financial markets: applications, investments and prospects

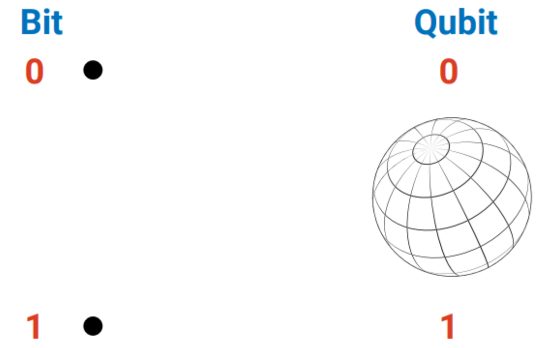
Webinar

2 June 2026

ESMA50-481369926-34328

Quantum computing: some key concepts

- Quantum computing (QC) leverages the principles of quantum mechanics to store and process information in a different way than "classical" computing
  - A qubit exists in a combination of the 0 and 1 states (superposition) until it is measured, resulting in a vastly higher information-encoding capacity of the system



- Quantum computing consists of three main parts:
  1. Encoding classical information in the qubits
  2. Modifying or computing this information, typically with quantum gates in quantum circuits
  3. Extracting classical information with a measurement process
- Quantum algorithms can reduce classical computing time on specific tasks ("quantum speedup"), solving problems at scales that are currently intractable

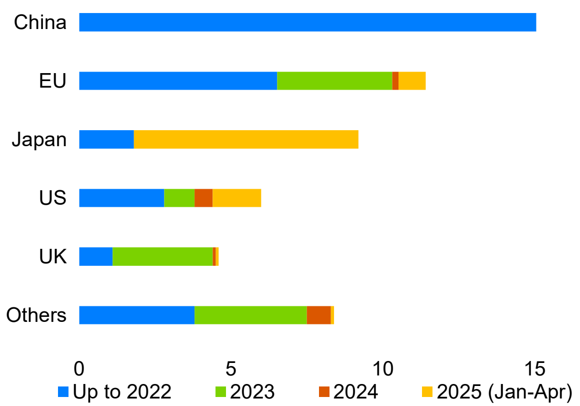
Quantum computing: technical advances raise interest

- Quantum computers have a long way to go before they become commercially available; yet steady advances in recent years have attracted attention
- Financial institutions may be early adopters of QC: some large US and EU banks are already studying use cases and developing proofs of concept
- The "ecosystem" for QC and other quantum technologies (QTs) – such as quantum communications and quantum sensing – has been expanding rapidly, with growth in investments and the creation of new firms
- But QC may break some common encryption techniques (e.g. RSA), which poses a systemic threat to the financial system (e.g. databases, online banking, payments)
- Thus, its relevance for the financial industry and for policymakers is two-fold:
    1. Growing value and financing needs of the quantum ecosystem
    2. Operational impact of quantum computing

Investment landscape

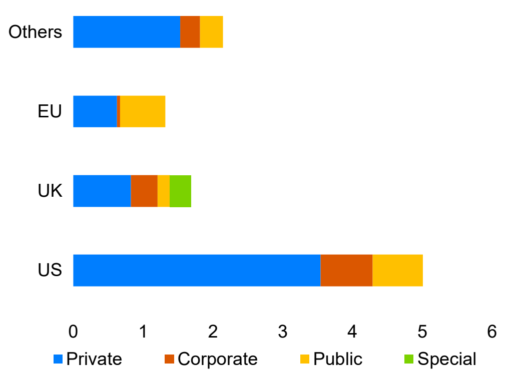
Global funding environment to quantum technologies

Public investments in quantum technology
China and EU committed the most funds



Note: Announced public investment in quantum technology research and development as of April 2025 (USD bn). "EU" is the sum of the EU27 countries and EU funding. "Others" include countries with less than USD 3bn in cumulative investment.
Sources: McKinsey & Company, ESMA

Investments in quantum technology startups
US startups led on private and corporate funding



Note: Total investment in quantum technology startups by location and primary investor type, 2001–2024 (USD bn). "Corporate" includes investments from corporations and corporate venture capital in external startups. "Special" Includes SPACs and other special deal types.
Sources: McKinsey & Company, Pitchbook, ESMA

QT investment grew rapidly over past decade

- Investments in quantum technologies (incl. computing, communications and sensing) have increased substantially in last 5-10 years; about 80% goes to QC
- Quantum ecosystem includes established organisations (IBM, Google, MS) and focused startups which rely on venture investment and public funding
- Public funding to QT reached USD 55bn cumulatively as of 2025, led by China, with EU, UK, US and Japan pledging funds in recent years

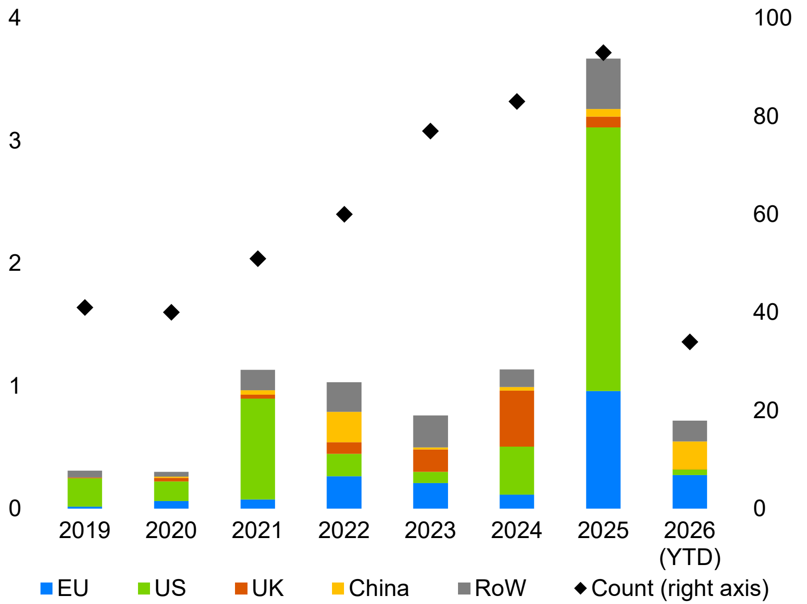
US leads on quantum startup financing

- The US is home to a dynamic startup environment for QTs. As of 2024, US startups raised 42% of global venture funding, led by private investment
- The EU has a solid base of quantum startups, but they attracted less funding, with a larger public share
- US and UK startups also receive investments from corporations
- Limited information on commercial activity in China

Venture capital investment in quantum computing

Venture funding to quantum computing startups

Quantum startups financing surged in 2025



Note: Volume of venture capital deals (EUR bn) involving quantum computing companies (excluding exits) by company domicile and total number of deals (right axis). Data as of 7 April 2026. RoW = rest of the world.
Sources: Preqin, ESMA

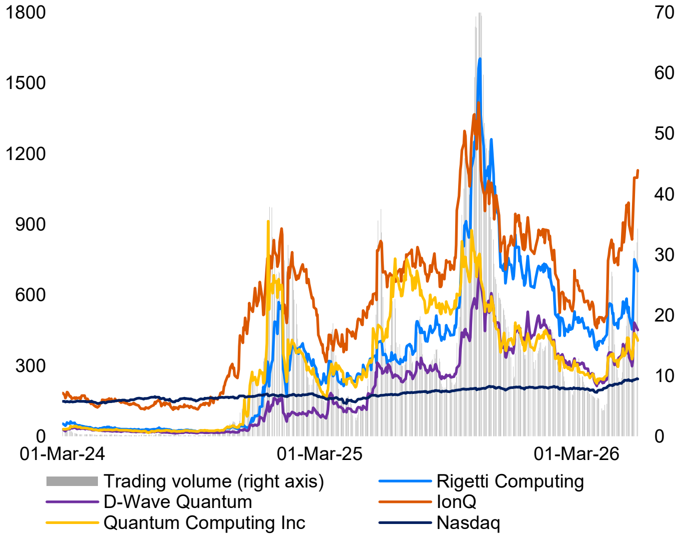
Quantum computing startups: recent fundraising boost

- Venture capital raised by quantum computing startups reached record levels globally in 2025, with surges both in the US (EUR 2bn) and the EU (EUR 950mn)
- Two EU pure-play quantum technology venture capital funds were launched in late 2025, on track to raise EUR 520mn
- Quantum computing startups accounted for about 2% of EU venture capital; 1% globally (GenAI: 20x in 2024, 8x in 2025)

Publicly-traded companies and investment funds

Stock prices and capitalisation of quantum companies

Heightened volatility for quantum stocks in 2025



Note: Stock prices of selected quantum computing companies, their total traded volume (USD bn), and Nasdaq index values. Prices and index values are rebased at 100 on 1/9/2022. The trading volume is calculated on a 5-day rolling window.
Sources: Refinitiv Eikon, ESMA

CIO JOURNAL

Quantum Computing Companies Are in a Race to Go Public

The number of publicly traded pure-play quantum firms could triple this year as companies race to capitalize on investor enthusiasm

By Isabelle Bousquette Follow

April 27, 2026 7:00 am ET

Quantum computing stocks in boom-and-bust cycles

- Four QC companies went public in the US between 2021 and 2022; their valuations boomed in 2025, with their combined market capitalisation temporarily surpassing USD 65bn, but remain highly volatile (down to USD 45bn as of 27 May 2026)
- Three more QC companies went public between February and March 2026; five (three of which European) are expected to follow as soon as this year

Several quantum computing ETFs launched

- The first three EU quantum computing exchange-traded funds (ETFs) were launched in 2025 (combined assets of EUR 0.6bn as of March 2026); two US ETFs (USD 3.3bn)
- Other quantum investment vehicles are still rare in public markets: only a few tech-oriented UCITS funds (2 ETFs, 3 active funds) promote quantum computing as one of their investment themes

Various potential applications, but risk for cryptography

Computational advantage offered, with implementation hurdles

- Quantum algorithms have the potential to **outperform classical algorithms** for specific problems ("quantum speedup") in the financial industry
- Current capabilities are limited; various **hurdles** persist (limited scale and stability of quantum hardware, data encoding into quantum states)

Quantum cyberthreats and quantum-safe cryptography

- **Breaking current encryption** is the single most significant risk from capable quantum computers
- Attackers could **decrypt protocols** used in financial services, blockchains, and databases, including by **harvesting data now to decrypt them in the future**
- This global, cross-sectoral concern demands a coordinated transition to **quantum-safe cryptography** in the financial sector and beyond
- The EU Member States and the European Commission envisage **high-risk use cases** to be made quantum-safe **by 2030**

Optimisation and stochastic modelling

Optimisation

- Quantum algorithms can tackle **computationally intensive financial optimisation problems** such as portfolio optimisation, financial index tracking, transaction settlement, predicting financial contagion in a network, finding currency arbitrage opportunities
- This domain presents potential “near-term” applications, where some **quantum speedup** may be achieved on faulty and limited-scale hardware

Stochastic modelling

- Modelling and simulating stochastic processes is key for **derivatives pricing** and **risk predictions**, but it can quickly become **computationally intensive**
- The quantum Monte Carlo integration (QMCI) algorithm yields a **quadratic speedup** relative to its classical counterpart by encoding probability distributions in the quantum states
- A number of hurdles (e.g. data encoding, qubit decoherence) impose **computational overheads** that render practical usefulness difficult to realise

Machine learning and blockchain

Machine learning

- Quantum algorithms for ML **find patterns in classical data** by mapping the data to quantum mechanical states and manipulating those states using quantum mechanical properties
- Various quantum ML algorithms useful in the financial sector have been developed, such as for **credit rating** and **fraud detection**
- While their feasibility remains uncertain, some methods potentially offer **exponential speedups**

Blockchain and distributed ledger technologies

- Quantum devices could yield a speedup in **performing proof-of-work**, meaning they could be used for mining Bitcoin and other cryptocurrencies
- Quantum computing offers avenues for entirely new **quantum blockchains** with more efficient, faster and more secure protocols for distributed ledgers
- Quantum blockchains could be used for **tokenisation** and other financial sector applications

Conclusions and outlook

- Quantum technologies are growing in a dynamic ecosystem, with **investments and commercial interest likely to keep increasing** over the next few years
- While it lags behind the US, the EU can still develop an **internationally competitive quantum ecosystem**, including through more **efficient and integrated capital markets** that better support technological innovation
- Potential **financial applications are diverse**, with some large financial institutions positioning themselves at the forefront of quantum computing research
- Timing and trajectory of impact on markets and financial institutions remain **uncertain and dependent on multiple variables**: technical breakthroughs, governments' strategic decisions, ability to sustain commercial interest, etc.
- Regardless of the timeline, **transition to quantum-safe cryptography** requires forward-looking planning and action

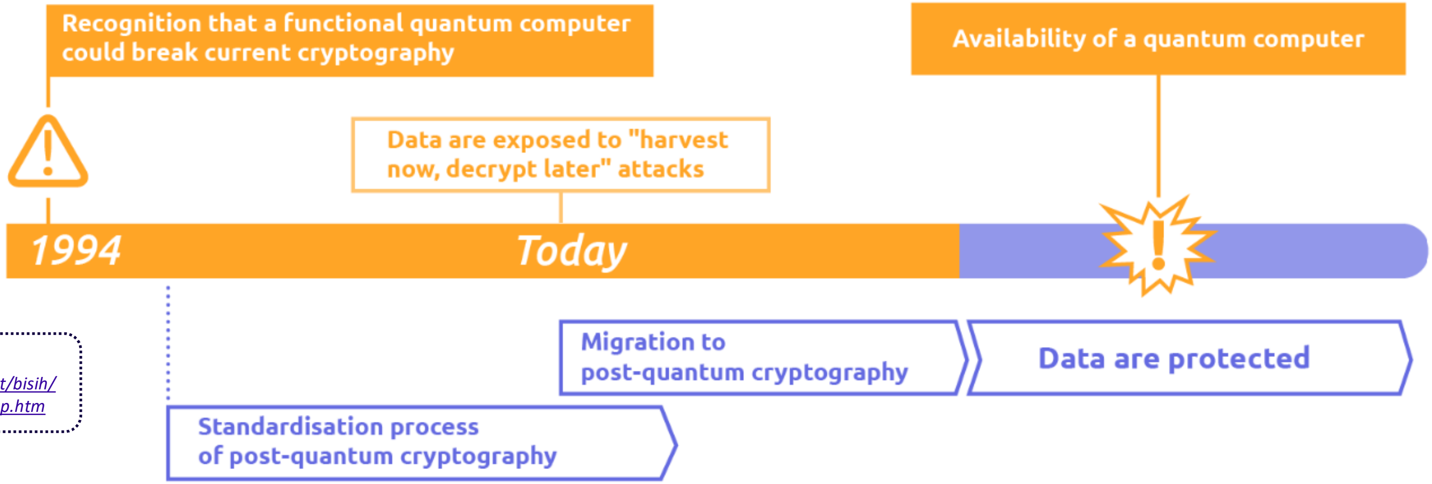
Discussion

EC Strategy

- The Draghi report on European competitiveness published in September 2024 flagged quantum computing as one of the critical technologies where the EU lags behind.
- The European Commission put forward a cross-sectoral Quantum Strategy in July 2025, to work closely with Member States and the European quantum community, including industrial actors:
  - The Strategy mainly aims to **foster a quantum ecosystem** for companies and researchers, and this also encompasses the objective to address QC-related vulnerabilities.
  - For the financial sector, the Strategy builds on the Savings and Investments Union project's goal to enable a **better financing ecosystem and removing obstacles to cross-border investment in the EU**. For instance, venture capital is instrumental to the development of quantum technologies.
- The European Commission work programme 2026 refers to the release of a **Quantum Act** by mid-2026. It may focus on three dimensions at least:
  - coordinating the relevant research and innovation investments across the Member States,
  - improving the EU industrial capacity in designing and producing quantum technologies,
  - ensuring the security and resilience of quantum supply chain.

The cybersecurity dimension (1/3)

- In terms of cybersecurity threat, quantum computers, should they reach sufficient size and power, will be able to break the encryption schemes widely used today to secure financial transactions, communication and data. In the meantime: "*harvest now, decrypt later*" scenario, where malicious actors store encrypted data for decryption once PQC solutions are available.
- April 2024: EC recommendation (EU) 2024/1101 to recommend the Member States to implement a coordinated roadmap for the transition to post-quantum cryptography
- November 2024: the US National Institute of Standards and Technology (NIST) has defined PQC algorithm standards: it states that traditional public-key cryptographic mechanisms will be disallowed from 2035.



Graph from BCBS: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

The cybersecurity dimension (2/3)

- June 2025: the NIS Cooperation Group workstream on PQC published its « roadmap for the transition to PQC », stressing that the transition from quantum-vulnerable cryptography towards PQC will take well over five years so should be properly anticipated:
  - By 2030 (max): « High-risk » use cases to be transitioned to PQC, i.e. quantum-safe software and firmware upgrades should be enabled by default.
  - By 2035 (max): Quantum-safe upgrades should be enabled by default for any kind of use cases.
  - Intermediary steps are crucial:

    (i) to create and to maintain current inventories of assets that perform cryptographic / that have cryptographic operations performed on them;

    (ii) to map (both internal and third-party) dependencies for applications, services, platforms, operations (important to consider the supply chain);

    (iii) to perform quantum risk assessment (i.e. quantum threat to cryptography);

    (iv) to invest progressively into PQC solutions (the implementation of the relevant solutions can be done by steps, e.g. as part of other IT investments).

The cybersecurity dimension (3/3)

- **NIS 2 Directive** and the **Digital Operational Resilience Act (DORA)** require (financial) entities in scope to adopt cybersecurity risk-management measures, including on the use of state-of-the-art cryptography.

  ➔ DORA RTS ICT RMF, recital (9) about cryptographic controls: "*Financial entities should follow a flexible approach, based on risk mitigation and monitoring, to deal with the dynamic landscape of cryptographic threats, **including threats from quantum advancements**.*"

- The **Cybersecurity Act 2** requests ENISA to contribute to the development and evaluation of cryptographic algorithms, in particular in the area of post-quantum cryptography, then to establish a process to solicit and evaluate cryptographic algorithms.
- Some other EU regulations may also be relevant, though less specific about quantum computing (e.g. the Cyber Resilience Act (CRA) which lays out horizontal cybersecurity requirements for all products with digital elements placed on the EU market).

ESMA, as a regulator and supervisor, will continue monitoring that financial regulations applicable to the EU financial entities are up-to-date, are applied effectively and promote supervisory convergence.

Q&A

Giulio Bagattini
Consumer, Sustainability and Innovation Analysis Unit
Economics, Financial Stability and Risk Department

Cyril Gruffat
Digital Finance and Innovation Unit
Markets and Digital Innovation Department

ESMA
European Securities and Markets Authority

www.esma.europa.eu

@ESMAComms

European Securities and Markets Authority (ESMA)