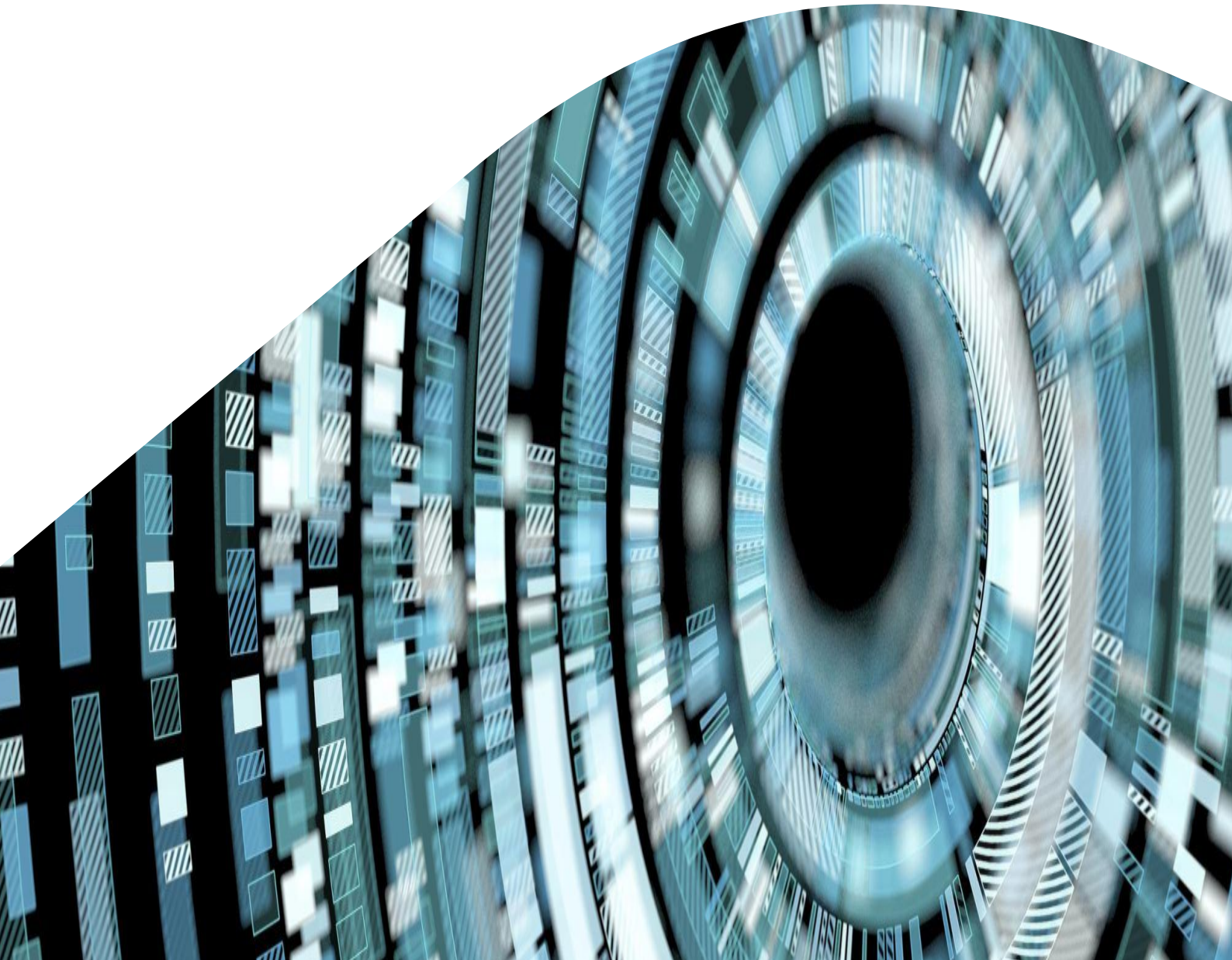
13 May 2026
ESMA50-481369926-33801

ESMA TRV Risk Analysis

Financial Innovation

Quantum computing in financial markets: applications, investments and prospects



ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis

European Securities and Markets Authority (ESMA)
Economics, Financial Stability and Risk Department
201-203 Rue de Bercy
FR-75012 Paris
France
risk.analysis@esma.europa.eu
ESMA – 201-203 rue de Bercy – CS 80910 – 75589 Paris Cedex 12 – France – www.esma.europa.eu
Cover photo: Image Microsoft 365

Financial Innovation

Quantum computing in financial markets: applications, investments and prospects

Contact: giulio.bagattini@esma.europa.eu[1]

Summary

Quantum technologies remain at an early stage of maturity, yet the associated ecosystem is expanding rapidly, particularly in the field of quantum computing. Quantum computing could enable substantial **speed and scalability gains for certain problems relevant to a range of industries, including financial services**. Its potential adoption by financial market participants could influence market efficiency, competitive dynamics, risk management practices and operational resilience, with possible implications for market integrity and financial stability.

First, this article examines the **funding and investment landscape of the global quantum ecosystem**. In 2025, global investment in quantum technologies reached record levels, reflecting elevated market expectations regarding their longer-term commercial prospects. In public markets, valuations of several quantum computing firms have increased markedly since late 2024, albeit amid pronounced volatility, underscoring the continuing uncertainty surrounding profitability pathways.

Second, the article assesses the **prospects for the application of quantum computing in financial market activities**. Potential use cases include optimisation algorithms (e.g. for portfolio management or trade settlement), stochastic modelling (e.g. for asset pricing or risk management), machine learning applications (e.g. for credit rating or fraud detection), and quantum-enabled blockchain technologies. While current quantum hardware capabilities remain limited, several financial institutions have developed quantum computing proofs of concept.

Alongside these opportunities, a sufficiently powerful quantum computer would pose a **significant threat to cybersecurity**, as it could undermine some of the cryptographic protocols currently used. Given the systemic and cross-sectoral nature of this challenge, initiatives are underway to support a transition to quantum-resistant encryption methods in the financial sector and across the wider economy.

As the technology evolves, the European Securities and Markets Authority (ESMA) will continue to monitor its implications and potential operational impacts on securities markets.

[1] This article was written by Giulio Bagattini.

I am grateful to Cyril Gruffat, Claudia Guagliano and Steffen Kern for comments and discussions. I also thank participants at the workshop on quantum computing in securities markets held at ESMA in September 2025.

Introduction

Quantum technologies – including quantum computing, quantum communication and quantum sensing – have the potential to exert a significant impact on the economy, science and security across a wide range of industries and applications. Although quantum technologies remain at an early stage of maturity, the associated ecosystem is expanding rapidly, marked by strong growth in firm creation and investment, particularly in the field of quantum computing.[2] Quantum computing could address certain classes of problems at a scale that is currently intractable even for the most powerful classical computers. While its global progress could be shaped by a small number of leading jurisdictions and firms, its potential applications are wide-ranging, spanning industries such as finance, chemistry, pharmaceuticals and logistics. Financial markets are often considered potential early adopters, as a range of finance-related tasks could – if quantum computers were to reach sufficient scale and robustness – be addressed by quantum algorithms capable of significantly accelerating certain computations and enabling new modelling approaches.

Against the backdrop of rapidly growing investment flows and heightened market interest, this article first examines the global and European funding and investment landscape for quantum technologies. In 2025, global investment in the sector reached record levels, reflecting expectations that quantum technologies could, over time, progress towards commercial viability. In public markets, valuations of several quantum computing firms rose sharply over the course of 2025, albeit with pronounced volatility, underscoring the continued uncertainty surrounding profitability prospects pending further technological breakthroughs, as well as the role of governments' strategic policy choices. As funding accelerates, the EU has introduced initiatives aimed at positioning the region as a global leader in quantum technologies by 2030.

The article then turns to the prospective applications of quantum computing in financial market activities. While current quantum hardware remains constrained, a number of financial market participants have begun to actively engage in quantum computing research, with several major banks, asset managers, and fintech start-ups announcing related initiatives in recent years. Potential use cases span optimisation problems (e.g. for portfolio management or trade settlement), stochastic modelling (e.g. for asset pricing or risk management), machine learning applications (e.g. for credit rating or fraud detection), and quantum-enabled blockchain technologies, with additional applications likely to emerge over time. Taken together, quantum computing could influence market efficiency, competitive dynamics, risk management practices and operational resilience, with potential implications for market integrity and financial stability.

At the same time, quantum computing poses a significant challenge for cybersecurity, as sufficiently powerful quantum computers could compromise some of the cryptographic protocols currently used to secure financial transactions, communications, and other critical digital processes. In response, initiatives are underway to facilitate a transition to quantum-resistant (or "post-quantum") encryption methods – new cryptographic algorithms designed to remain secure against attacks by quantum adversaries – both within the financial sector and across the wider economy. While global in nature, these developments are therefore likely to have far-reaching implications for the EU financial industry, in a manner similar to past waves of digital innovation.

TEXTBOX 1

Quantum computing: Fundamentals

Quantum computing is based on quantum mechanics, the fundamental physical theory describing the behaviour of matter at very small scales. Quantum computers use quantum bits, or *qubits*. Unlike classical bits, which encode information using one of two discrete values, a qubit can exist in a *superposition* of states – a quantum property whereby a particle occupies a probabilistic combination of multiple states (represented geometrically as a point on the surface of a sphere) until it is measured. When multiple qubits are combined, superposition gives rise to an exponential increase in the theoretical information-encoding capacity of the system. In addition, *entanglement* allows qubits to become interdependent: when qubits are entangled, measuring the state of one instantaneously reveals full or partial information about the state of another, irrespective of distance. Quantum computers exploit entanglement to generate complex correlations across their units of information.

As in classical computing, information in quantum computers (with the exception of quantum annealers, discussed below) is manipulated through *quantum gates*, which operate on individual qubits or on sets of qubits by acting on quantum properties such as superposition and entanglement. A quantum computation typically involves three main steps:

[2] See EPO/OECD (2025).

encoding classical information into qubits, processing this information via sequences of quantum gates, and extracting classical information through measurement.

Quantum gates are the building blocks of quantum circuits, which are used to implement quantum algorithms. These algorithms are specifically designed to exploit quantum effects in order to perform certain computations more efficiently than classical algorithms – a phenomenon known as *quantum speed-up*. Quantum algorithms are generally tailored to specific problem classes and must be executed on quantum hardware with sufficient capabilities to prevent practical overheads from offsetting theoretical performance gains. Despite notable progress in algorithm design, achieving *quantum advantage* – that is, a speed-up delivering tangible practical benefits – remains challenging for problems with commercially relevant specifications. In particular, further advances are needed to reduce resource requirements associated with tasks such as embedding classical data into quantum states, reading out quantum outputs, and performing classical pre- and post-processing.

The current phase of development is commonly referred to as *noisy intermediate-scale quantum* (NISQ) computing, reflecting the fact that existing devices are limited in size and affected by various sources of noise. Quantum computations require the control of extremely fragile quantum states, and qubits are subject to decoherence, a gradual loss of quantum information that leads to errors. *Quantum error-correction* techniques seek to address this challenge by encoding information redundantly across multiple physical qubits to form so-called *logical qubits*. Progress towards more powerful quantum computers therefore depends on increasing the number of physical qubits, reducing their error rates, and improving error-correction methods so as to lower the physical qubit overhead needed to create a logical qubit. *Fault-tolerant* quantum computers are theorised large-scale systems capable of performing reliable quantum computations over extended periods.

Quantum computers that operate using quantum gates are referred to as *universal quantum computers*, as they can, in principle, implement any quantum algorithm. Unlike classical computing, several competing hardware platforms exist for universal quantum computation, including superconducting circuits, photonic systems, neutral atoms, and trapped-ion technologies. *Quantum annealers* represent an alternative approach: they rely on physical interactions between qubits embedded in specific materials. While they can be scaled more readily, they are primarily suited to a narrow class of optimisation problems. With the exception of D-Wave's systems, most existing and planned quantum devices follow the universal, gate-based circuit model. Although current quantum hardware is highly energy-intensive – particularly due to cooling and control requirements – future large-scale systems could, for certain tasks, deliver computational efficiency gains that offset these costs. Nevertheless, the overall energy implications remain uncertain.

Despite the early stage of the technology, several firms – including major technology companies such as IBM, Microsoft and Amazon, as well as specialised quantum start-ups – already provide access to quantum computing hardware and software platforms, enabling experimentation and the development of potential quantum applications, including those relevant to financial services.

Investment landscape

Global funding environment

Over the past decade, **investment in quantum technologies** (including, alongside quantum computing, the fields of quantum communication and quantum sensing) **has expanded rapidly**, accompanied by rising innovation activity and firm entry worldwide. One source estimates total annual investment in quantum technologies at around USD 33bn globally in 2025, of which 38% was directed towards quantum computing.[3] While quantum communication plays an important role, quantum computing has emerged as the most dynamic segment, recording the fastest growth in both the number of firms and patenting activity.

The **quantum "ecosystem"** comprises a combination of startups specialising in the development of quantum and quantum-enabling technologies ("quantum startups"), which typically rely heavily on early-stage private investment and public funding, alongside a broader set of established organisations. The latter include large technology firms and incumbents that invest substantially in quantum research and development (R&D), provide cloud-based quantum computing services, or supply key enabling components. These large corporates are regarded as a major source of global spending on quantum computing, reflecting the scale of their overall R&D budgets.[4]

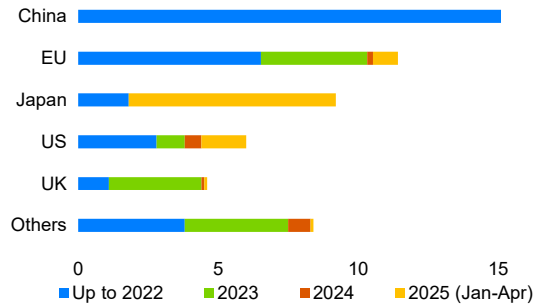
Governments have also increasingly signalled their intention to support the development of quantum ecosystems within their respective jurisdictions, reflecting the long development timelines, high capital intensity, and scientific uncertainty inherent in quantum technologies. Cumulative **public funding commitments** announced globally were estimated at around USD 55bn as of April 2025, with China accounting for the largest share, followed by the EU and Japan (Chart 1). Public funding has also played a material role in supporting higher-risk early-stage investments, thereby facilitating the

[3] See Research and Markets (2025). The total investment also includes USD 10.5bn in the field of quantum materials. It comprises public funding, venture capital and corporate R&D expenditure.

[4] While granular figures have not been disclosed, the share of corporate R&D directed towards quantum technologies is potentially comparable in scale to – or larger than – global investment in quantum startups (see Chart 2).

emergence and scaling-up of quantum-focused firms.[5]

Chart 1
Public investment in quantum technologies
China and EU committed the most funds



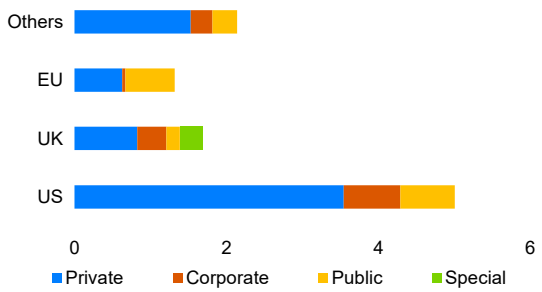
Note: Announced public investment in quantum technology research and development as of April 2025 (USD bn). "EU" is the sum of the EU27 countries and EU funding. "Others" includes countries with less than USD 3bn in cumulative investment.
Sources: McKinsey & Company, ESMA

Investment in **quantum technology startups** – more than 80% of which was directed towards quantum computing – has expanded markedly since 2020, driven initially by private investors, including venture capital funds, hedge funds, corporations, angel investors and accelerators. Investment flows have nevertheless been uneven, shaped by the global economic cycle and potential crowding-out effects associated with the recent surge in interest in artificial intelligence (AI). After exceeding USD 2bn in both 2021 and 2022, investment in quantum startups declined to USD 1.3bn in 2023 before rebounding to around USD 2bn in 2024. Public funding from governments, sovereign wealth funds and universities accounted for a growing share of this total, reaching one third of overall investment.[6]

While China has positioned itself as a global leader in terms of public funding, **the US has largely relied on a market-driven approach** that promotes collaboration between companies and universities. This model has fostered a dynamic venture capital environment in which private investment exceeds public spending (Chart 2). The US stands out as the leading player across quantum technologies, ranking first in terms of firm entry, innovation output, and total investment mobilised. Consistent with this pattern, the US hosts the largest number of quantum startups worldwide, with 77 out of 274 firms. However, only two new US-based companies were launched in 2024, which may point to a maturing domestic ecosystem. Companies focused on quantum computing have increasingly shifted towards **revenue generation**, earning an estimated USD 650-750mn in 2024, with revenues expected to exceed USD 1bn by the end of 2025, driven in part by the growing deployment of quantum hardware.[7]

By contrast, **the EU benefits from strong fundamental research capabilities and a solid base of quantum startups** translating scientific advances into technological developments. Nevertheless, EU-based companies have historically attracted lower levels of private investment than their US counterparts, leaving them more reliant on public funding programmes. Overall, the share of government funding in the quantum ecosystem is higher than that observed for startups in other sectors.[8]

Chart 2
Investment in quantum technology startups
US startups rely on private and corporate funding



Note: Total investment in quantum technology startups by location and primary investor type, 2001–2024 (USD bn). “Private” includes investments from venture capital funds, hedge funds, angel investors, and accelerators. "Corporate" includes investments from corporations and corporate venture capital in external startups. “Public” includes investments by governments, sovereign wealth funds, and universities. "Special" includes special-purpose acquisition companies and other special deal types.
Sources: McKinsey & Company, Pitchbook, ESMA

Large corporations with substantial quantum computing portfolios include IBM, Intel, Microsoft and Alphabet (see EPO/OECD, 2025).

5 In the EU, the European Commission recently published a quantum strategy which foresees research initiatives and new infrastructure to support quantum technologies, underscoring their key role for Europe’s competitiveness and strategic autonomy (see EC, 2025b).

6 See McKinsey & Company (2025). Ruane et al. (2025) report a similar trend but slightly higher figures for total venture funding to quantum technology companies, estimating that it reached approximately USD 2.6bn in 2024.

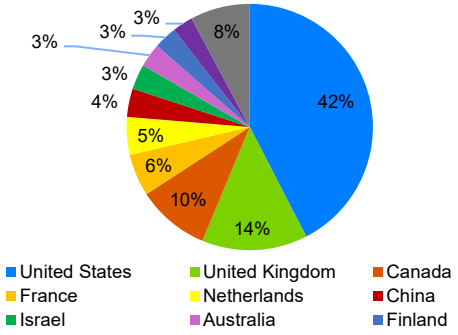
7 See McKinsey & Company (2025).

8 See EPO/OECD (2025).

Venture capital

The largest share of funding for quantum startups has been provided through venture capital. Venture capital plays a critical role in supporting the growth of innovative firms, enabling them to scale more rapidly and expand into new markets. US-based quantum technology companies have led fundraising activity, accounting for 42% of global venture funding raised between 2018 and 2024 (Chart 3). EU-based firms attracted around 20% of global venture capital over the same period, while UK companies accounted for a further 14%.[9]

Chart 3
Venture funding to quantum technology startups
US startups attract largest venture funding share

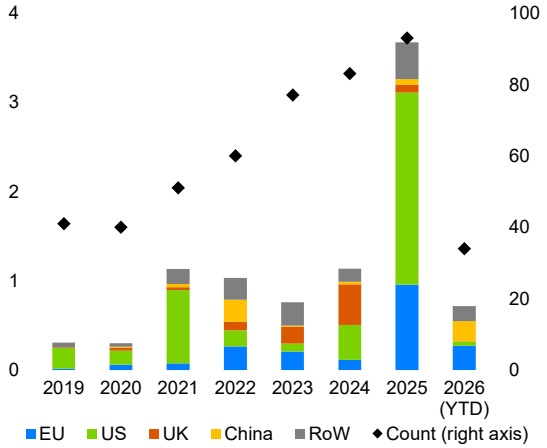


Note: Venture funding to quantum technology companies by domicile, out of a total of USD 10.7bn raised between 2018 and 2024. Quantum technologies include computing, communications & security, sensing & imaging, hardware and software.
Sources: Massachusetts Institute of Technology, ESMA

Focusing specifically on quantum computing, **venture funding reached record levels globally in 2025**, including outside the traditional North American centres of development (Chart 4). Notably, venture capital raised by EU-based quantum computing startups surged in 2025 to approximately EUR 950mn across 25 deals, representing a five-fold increase compared with the average annual funding observed over the previous three years.[10] Investment in US companies also soared, surpassing EUR 2bn, driven by a few large deals.[11]

The recent spike in investment activity was supported in part by the launch of some EU-based **pure-play quantum technology funds**.[12] More broadly, while US-based investors accounted for 52% of global investment in quantum companies over the period 2016-2024, funds based in European countries (particularly France, Germany, the Netherlands and the UK) have significantly increased their share of investment in quantum computing over time. This growing regional diversification points to the emergence of a more competitive global investment landscape.[13]

Chart 4
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). RoW = rest of the world, YTD = year to date. Data as of 7 April 2026.
Sources: Preqin, ESMA

Accounting for around 2% of total venture capital raised by European startups in 2025, quantum computing represents a **small, but growing share of the venture funding landscape**.[14]

[9] While private investment in Chinese quantum technology companies appears to be limited, commercial activity in China lacks transparency, with most quantum technology efforts likely led by government-funded research institutions and a strong emphasis on state-led development. See Groenewegen-Lau and Hmaidi (2024).

[10] This figure excludes the September 2025 acquisition of Oxford Ionics by US-based IonQ, which represented the largest exit in the sector.

[11] In particular, US-based companies PsiQuantum and Quantinuum raised respectively EUR 910mn and EUR 762mn.

[12] In 2025, Danish investor 55 North launched a venture capital fund dedicated to investments across quantum technology companies, with a fundraising target of EUR 300mn. In February 2026, Paris-based firm Quantonation closed a EUR 220mn early-stage fund focused on quantum technologies. In the US, Quantum Coast Capital has emerged as one of the few venture capital firms exclusively dedicated to investments in quantum technologies.

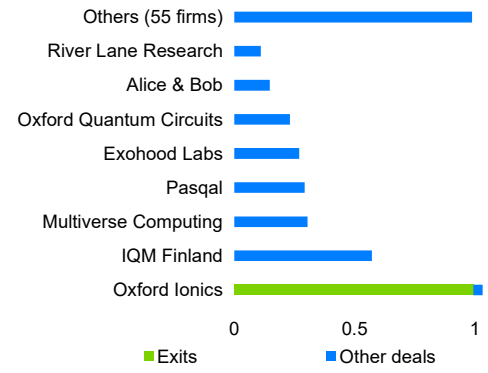
[13] See EPO/OECD (2025).

[14] Investment in quantum technology startups was thought to account for less than 1% of worldwide venture funding in 2024. See Ruane et al. (2025).

Global venture funding for quantum startups remains well below that directed towards more mature technologies, most notably AI. Generative AI startups alone raised approximately USD 25bn in 2024 and USD 35bn in 2025 – about 20 and 8 times the amount invested in quantum computing startups, respectively – underscoring the greater investor appetite for AI-related applications, but also the strong growth rate of quantum computing startup funding. [15] Overall, both technology sectors recorded robust funding growth in 2025, even as the broader venture capital environment remained subdued following a peak in 2021.

Venture investment in quantum computing startups has been **significantly concentrated**. In Europe, eight companies – four based in the UK, two in France, one in Finland, and one in Spain – each raised more than EUR 100mn, while a further 52 startups collectively attracted around EUR 1bn in funding (Chart 5). In 2025, Finland-based IQM raised USD 320mn, becoming Europe's first quantum computing "unicorn", defined as an unlisted startup with a valuation exceeding USD 1 bn. High-profile transactions have also strengthened investor interest, with IonQ's acquisition of UK-based Oxford Ionics for more than USD 1bn delivering substantial returns to the company's venture capital backers.

Chart 5
Venture funding to quantum computing startups
Eight companies dominate European landscape

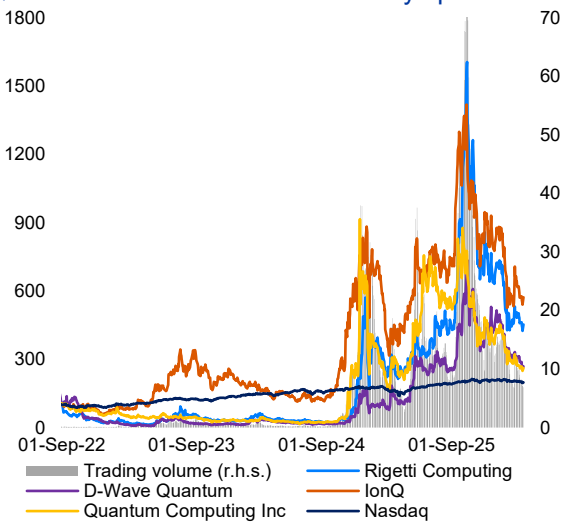


Note: Volume of venture capital deals involving European quantum computing companies (EUR bn) from 1st January 2018 to 7 April 2026.
Sources: Preqin, ESMA

Securities markets

Three quantum computing firms and one quantum photonics company went public in the US between 2021 and 2022. [16] Since late 2024, their shares have been characterised by repeated **valuation surges followed by corrections**, with the combined market capitalisation of the four companies temporarily exceeding USD 65bn and weekly trading volumes surpassing USD 70bn in late 2025 (Chart 6).

Chart 6
Publicly traded quantum computing companies
Quantum stocks saw recent volatility spikes



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

These dynamics were driven by several catalysts, including expectations of substantial external funding (including from the US government), announcements of technical milestones, and ambitious projections regarding the potential economic impact of quantum computing. Notwithstanding heightened investor interest, these pure-play quantum firms remained at an early stage of commercialisation and continued to operate at significant losses.

[15] Venture capital raised by EU AI startups was growing but it was more contained, having reached USD 16bn in 2025, including USD 2.7bn directed towards generative AI companies. See https://oecd.ai/en/data.

[16] IonQ and D-Wave Quantum are listed on the New York Stock Exchange, while Rigetti Computing and Quantum Computing Inc. (a quantum photonics company) are listed on Nasdaq. Outside of the US, there are very few publicly traded companies whose primary focus is adjacent to quantum computing, such as Archer Materials (listed on the Australian Securities Exchange) and Quantum eMotion (listed on Canada's TSX Venture Exchange).

Reflecting growing market attention, 2025 also saw the launch of the first three EU-domiciled **exchange-traded funds (ETFs) with a specific focus on quantum computing**.[17] These equity ETFs – which collectively held USD 0.6bn in assets under management (AUM) as of the end of March 2026 – typically invest in a mix of pure-play quantum computing firms, large technology companies developing quantum hardware or software, and suppliers of quantum-enabling technologies. In the US, comparable products include a quantum-computing- and machine-learning-themed ETF and a recently launched pure-play quantum computing fund, managing USD 3.3bn and USD 0.03bn in AUM, respectively.

Despite these developments, investment vehicles providing exposure to quantum computing remain relatively scarce in public securities markets. A textual analysis of regulatory and marketing documents of investment funds indicates that only five additional EU-based funds – two ETFs and three actively managed funds – out of more than 35,000 analysed explicitly identify quantum computing as an investment theme.[18]

Applications in financial markets

The financial sector may be a particularly relevant beneficiary of quantum computing, as it is characterised by a range of computationally demanding problems for which a growing set of quantum algorithms has already been developed. Quantum algorithms have the potential to outperform classical algorithms for certain problem classes, a phenomenon known as *quantum speedup* (see Textbox 1).[19] In some cases, researchers have demonstrated proofs of concept for *quantum advantage* – that is, a speedup yielding a practical benefit – and, more rarely, for *quantum supremacy*, defined as the ability to solve a problem that is infeasible for classical computers within a reasonable timeframe. Nevertheless, current quantum hardware remains insufficient to solve real-world, industry-scale financial problems more efficiently or more accurately than established classical approaches.

Within financial markets, prominent domains in which quantum computing approaches have been explored include **optimisation** (e.g. portfolio optimisation and transaction settlement), **stochastic modelling** (e.g. Monte Carlo simulations), and **machine learning** applications (e.g. fraud detection and credit scoring). In addition, quantum-based **blockchain** architectures have been proposed as a potential avenue for improving processing speed and security relative to existing models.

Optimisation

Quantum computing offers a range of heuristics and algorithms for addressing optimisation problems, a domain that currently appears among the most promising for commercially relevant applications on noisy intermediate-scale quantum (NISQ) hardware. In particular, many computationally demanding financial optimisation problems can be formulated as *combinatorial optimisation* tasks, in which solutions are drawn from a finite set of discrete values. Problems belonging to the *quadratic unconstrained binary optimisation* (QUBO) class – characterised by quadratic objective functions – are especially well suited to quantum optimisation techniques.[20]

In finance, **mean-variance portfolio optimisation, risk minimisation** and **hedging** problems typically involve a quadratic risk term derived from the variance–covariance matrix of asset returns. These problems can therefore be expressed in QUBO form and addressed using

[17] The eponymous "quantum computing" UCITS ETFs were launched by asset managers iShares, VanEck and WisdomTree.

[18] The text analysis was conducted on approximately 525,000 PRIIPS key information documents, 269,000 key investor information documents and 450,000 factsheets issued by 35,189 EU-domiciled investment funds (primarily UCITS) until January 2026 and accessed through Morningstar.

[19] Such speedups are confined to specific types of problems for which quantum effects can be effectively exploited, including the factorisation of large numbers, searches over unstructured datasets, the solution of complex optimisation problems through the simultaneous exploration of large solution spaces, and the simulation of quantum systems such as molecules and materials.

[20] Quantum approaches applicable to combinatorial optimisation include quantum annealing, gate-based variational algorithms, and methods based on quantum unstructured search. See Herman et al. (2023).

combinatorial quantum optimisation algorithms. Such algorithms exploit quantum superposition to explore many possible portfolio configurations simultaneously, while quantum entanglement can be used to capture interdependencies across assets.

A closely related application is **index tracking**, where a subset of assets must be selected to replicate a broader market index, for example by providers of index-tracking ETFs. Cardinality constraints – limiting the number of assets included – render the optimisation problem non-convex, making it computationally intensive for standard classical methods. These features make index tracking amenable to quantum annealing and other quantum optimisation approaches.[21]

Another potential application of quantum optimisation arises in **transaction settlement**, where a clearing house must determine the maximum set of transactions that can be settled among multiple participants without any party breaching its credit limits. Because a participant's outgoing payments may depend on incoming transactions, the problem involves complex interdependencies across counterparties. Identifying the largest feasible settlement set – and thereby reducing settlement failures – can become computationally challenging, particularly if transaction volumes handled by central counterparties increase, for instance due to market expansion or the growing issuance of digital tokens. Huber et al. (2024) show that this problem can be formulated as a QUBO and assess several quantum approaches using synthetic transaction datasets.

Additional examples of economic and financial modelling tasks that can be mapped to a QUBO formulation include **predicting financial contagion** in networks of interconnected institutions with mutual exposures during periods of stress, as well as identifying **currency arbitrage opportunities** – that is, trading cycles that yield positive returns without assuming directional risk.

Quantum algorithms can also be applied to **continuous or convex optimisation problems**, such as determining optimal asset weights in a portfolio. However, these problems are already efficiently addressed using classical computing techniques. As a result, it remains an open question whether quantum approaches can deliver a practical speedup in such settings. Proposed applications therefore tend to rely on hybrid workflows, in which quantum algorithms are used to identify promising combinations of assets, while classical methods are employed to refine their precise allocation.[22]

More broadly, the **hybridisation of quantum and classical computing** through decomposition-based approaches represents a pragmatic response to the limited number of qubits available on near-term (NISQ-based) quantum devices – an important constraint on large-scale financial applications. In such frameworks, a classical computer decomposes a complex problem into smaller sub-tasks, which are solved individually on a quantum processor. The classical system then aggregates the partial solutions into a global result.

Stochastic modelling

Stochastic processes form the basis for modelling a wide range of financial variables, including stock prices, interest rates, and volatility. The stochastic differential equations underlying these processes are typically solved using numerical techniques such as *Monte Carlo simulations* – a class of computational methods based on repeated random sampling. Quantum systems are well suited to the modelling of stochastic processes, as probability distributions can be encoded directly into quantum states.

One widely used simulation technique that can be adapted to quantum algorithms is *Monte Carlo integration* (MCI). MCI is commonly employed to estimate the expected value of a quantity that depends on one or more random variables – for example, the payoff of a derivative contract – by generating a large number of sample paths based on the underlying stochastic drivers. In finance, MCI plays a central role in asset pricing and risk estimation, but it can rapidly become computationally intensive as the dimensionality of the problem increases. **Quantum Monte Carlo integration** (QMCI) is a quantum algorithm that offers a theoretical quadratic speedup over

[21] See Palmer et al. (2022).

[22] See Markham and Grassie (2025).

classical MCI, meaning that it requires quadratically fewer simulated paths to achieve a given level of accuracy in estimating an expectation.

Quantum Monte Carlo methods are relevant to two broad areas of financial modelling. First, they can be applied to the **pricing of derivative instruments**, including European and exotic options as well as collateralised debt obligations. [23] Second, they can support **risk modelling** applications, such as the calculation of value-at-risk (VaR) and credit risk metrics, where Monte Carlo simulations enable the incorporation of high levels of uncertainty and correlated shocks. Beyond these applications, QMCI-based approaches have also been proposed for sensitivity analysis (e.g. the computation of option "Greeks"), credit valuation adjustment, and the valuation of portfolios of derivative instruments.

Despite the theoretical quadratic speedup associated with QMCI, several implementation challenges introduce substantial **computational overheads** that currently prevent the realisation of quantum advantage, such as encoding classical probability distributions into quantum states – a prerequisite for quantum Monte Carlo methods. [24] In addition, current **hardware constraints**, including limited qubit counts, restricted circuit depth, and the absence of full fault tolerance, would need to be overcome before QMCI can be applied to real-world financial problems. As a result, while QMCI represents a promising avenue for the application of quantum computing in finance, its prospects for commercial deployment remain uncertain.

Beyond QMCI-based methods, a range of other quantum algorithms relevant to financial modelling is under active study. These include approaches designed to improve upon classical numerical techniques for solving **partial differential equations** (PDEs), which can become computationally intractable in high-dimensional and complex settings. However, quantum alternatives to PDE-based methods are generally less mature than QMCI-based approaches, and their potential computational advantage over established classical methods has yet to be clearly demonstrated.

Machine learning

Machine learning (ML) has become an integral component of a wide range of applications in the financial industry. In parallel, a growing body of quantum machine learning (QML) algorithms has been developed, relying on either fault tolerant quantum computing, near term approaches, or hybrid combinations of the two.

Broadly, QML algorithms can be grouped into methods that aim to **accelerate classical ML techniques** and quantum-native approaches. The former seek to identify patterns in classical data by encoding the data into quantum states and subsequently manipulating these states using quantum linear-algebra primitives, often referred to as *quantum basic linear algebra subroutines* (QBLAS). A number of such algorithms have been proposed that may, in principle, offer quadratic or even exponential speedups over classical counterparts, including quantum principal component analysis (PCA), quantum support vector machines (SVMs), and quantum reinforcement learning. [25] However, efficiently encoding large classical datasets into quantum states stored in quantum registers or QRAM remains a significant challenge. These constraints, together with additional sources of overhead, generally imply a reliance on error-corrected or fully fault-tolerant quantum hardware.

By contrast, **quantum-native ML algorithms** operate directly on quantum data generated within a quantum system. As they avoid the demanding step of encoding classical data into quantum states, such approaches may be deployable on the relatively small and noisy quantum devices potentially available in the near term. For this reason, quantum-native algorithms are often viewed as a more promising avenue for early QML applications. Nevertheless, it remains unclear whether these methods can deliver a

[23] See Rebentrost et al. (2018).

[24] The preparation of an arbitrary quantum state can be computationally demanding to the extent that it fully offsets the theoretical speedup offered by a quantum algorithm. The development of so-called quantum memory (QRAM), which remains at a nascent stage, could help overcome this challenge.

[25] See Biamonte et al. (2017).

meaningful advantage in practical financial use cases.

Quantum variants of supervised learning algorithms, such as SVMs and nearest-neighbour classifiers, have been proposed for pattern recognition and classification tasks, including **credit assessment** and **fraud detection**. These may take the form of quantum subroutines designed to accelerate existing classical workflows, or fully quantum versions of established algorithms. For example, quantum-enhanced classification methods analogous to QUBO problems have been applied to the **prediction of credit rating downgrades**. Experimental implementations on current quantum hardware have achieved classification accuracy comparable to classical benchmarks, while offering greater interpretability.[26] Likewise, several quantum formulations of PCA have been developed, in which principal components are represented in quantum superposition. As with many QBLAS-based techniques, however, extracting useful classical information from the quantum output remains a substantial challenge.

Overall, while QML holds the promise of substantial computational speedups for specific problem classes, further work is required to refine algorithmic designs and assess their feasibility in real-world applications. In particular, although exponential quantum speedups are theoretically possible for certain tasks, their **practical relevance remains uncertain** – especially in settings dominated by purely classical data, where achieving such advantages may ultimately prove impractical.[27]

Distributed ledger technologies

Quantum computing may affect distributed ledger technologies (DLTs), such as blockchain platforms, and the crypto-assets that rely on them in several respects. Existing platforms depend on digital signatures, public-key cryptography, zero-knowledge proofs, and hash functions, making them **vulnerable to sufficiently powerful quantum computers** (see Textbox 2).[28] At the same time, ongoing theoretical research is exploring the incorporation of advanced **cryptographic techniques grounded in quantum information theory** – including quantum key distribution, quantum random number generation, and quantum communication channels – into blockchain architectures, with the aim of enhancing network security and mitigating malicious attacks.

Some researchers have argued that quantum computers could exploit Grover's algorithm to achieve a quadratic speedup relative to classical systems when **performing proof-of-work** calculations, potentially enabling their use in the mining of Bitcoin and other crypto-assets.[29]

A growing body of research investigates the potential **integration of quantum computing into blockchain** systems. Amin et al. (2025), for example, propose and test a blockchain architecture based on a *proof-of-quantum-work* consensus mechanism, under which quantum computers are required to validate transactions. Such a quantum-based approach could significantly reduce the substantial electricity consumption associated with classical proof-of-work mining – by up to three orders of magnitude in the tested framework.

DLTs – particularly public blockchains – also face inherent scalability constraints, as transaction block sizes are limited and it is generally recognised that network size, consensus speed and security cannot be expanded simultaneously. In theory, quantum-enabled blockchains could **enhance the scalability and speed** of distributed consensus mechanisms, improve security, and facilitate interoperability across different blockchains.[30] Quantum entanglement could be leveraged to ensure the integrity of communicated information in a distributed system, as any tampering with one part of an entangled state would be immediately detectable (see Textbox 1). Moreover, quantum entanglement could enable a reduction of verification times in distributed consensus protocols, overcoming the need for the request-response communication pattern characteristic of classical systems, which entails multiple

[26] See Leclerc et al. (2023).
[27] See Doosti et al. (2024).
[28] See Wu (2025) for a detailed discussion of the threat posed by quantum computing to digital signature schemes in blockchains.
[29] See Bard et al. (2022).
[30] See Seet and Griffin (2019).

back-and-forth message exchanges between network participants. Quantum-enabled distributed ledgers could be leveraged for financial applications such as tokenisation and know-your-customer processes involving data shared across institutions.

Overall, while quantum blockchains require new algorithms capable of effectively exploiting quantum capabilities, such systems may offer significant advantages, including enhanced computational efficiency, improved security, faster transaction processing, and more efficient consensus formation. At the same time, integrating quantum-enabled blockchains with existing classical systems poses significant challenges, particularly with respect to secure communication and seamless data exchange between quantum and classical systems. [31] Against this backdrop, practical experimentation with quantum blockchains and distributed ledgers remains at an early stage.

Prospects for deployment in finance

The prospects for the practical application of quantum computing in financial markets remain **heterogeneous across use cases**. Conditional on continued incremental technological progress, certain applications – such as portfolio optimisation and QML – may gradually approach practical relevance, given that some related methods are compatible with NISQ devices. By contrast, most real-world applications of quantum Monte Carlo methods require a large number of error-free qubits, placing the theoretical benefits associated with quadratic speedups beyond the capabilities of NISQ technology. Quantum-enabled blockchain approaches, meanwhile, remain largely experimental, with seemingly less advanced testing activity. More generally, many proposed quantum approaches rely on **heuristics** expected to deliver practical benefits based on empirical performance, rather than on general-purpose algorithms with formally established optimality guarantees.

While it is unknown whether quantum computing will ultimately deliver material advantages for financial applications, some major financial institutions are already investing in quantum research and capability-building. Looking ahead, a key objective of proof-of-concept initiatives will be to **assess commercial viability** by identifying those computational processes and sub-routines where the performance gap between existing methods and prospective quantum approaches is greatest, such that the expected gains offset implementation costs and operational complexity.

Ultimately, the feasibility of translating these approaches into end-to-end advantage for practical applications will depend on the evolution of quantum hardware and system architectures. Should commercial deployment become viable, adoption in the financial sector might rely on a limited number of third-party quantum hardware providers. Early indications suggest that the quantum hardware market could develop around a relatively **concentrated supplier base**, reflecting the technical complexity of quantum systems and the need for highly specialised components.

TEXTBOX 2

Quantum computing threats to cryptography

Quantum computing poses a serious threat to digital security due to its potential to undermine some widely used cryptographic techniques. A sufficiently advanced quantum computer could implement *Shor's algorithm*, which enables the factorisation of large numbers exponentially faster than any known classical algorithm. This capability would allow quantum computers to break public-key cryptographic schemes such as Rivest–Shamir–Adleman (RSA), elliptic-curve cryptography (ECC), and other systems based on large-number factorisation or related mathematical problems. The financial system, including banking, payment services, securities markets and asset management, relies extensively on RSA and ECC for core functions such as secure communications, digital signatures, transaction integrity and confidentiality of records. At present, however, such attacks remain well beyond the reach of existing NISQ devices.

Post-quantum cryptography (PQC) refers to a new generation of cryptographic algorithms designed to remain secure against attacks by large-scale, fault-tolerant quantum computers. The US National Institute of Standards and Technology (NIST) led a public process to evaluate candidate PQC algorithms, resulting in the release of the first PQC standards in 2024.

Although quantum computers capable of threatening current cryptographic systems are not expected to materialise in the near term, cybersecurity authorities already recommend initiating the transition to quantum-resistant solutions, in light of the lengthy cryptographic migration processes and the large number of stakeholders involved. In addition, sensitive data faces heightened retroactive risks once quantum attacks become feasible, as information harvested today may be decrypted in the future ("harvest now, decrypt later").

[31] See Naik et al. (2025).

Against this backdrop, global regulatory bodies view PQC migration as an urgent, coordinated, multi-year endeavour essential to safeguarding digital security and trust in the financial system and across the broader economy. The European Commission's roadmap for the transition to PQC, for example, sets out a series of milestones, including initiating transition planning and pilot projects by 2026 and completing the transition for high-risk use cases by 2030 and for medium-risk use cases by 2035 (see EC, 2025a). In parallel, the Quantum Safe Financial Forum, a multi-stakeholder initiative established by Europol, seeks to support PQC transition efforts in the financial sector. It outlined a methodology for assessing PQC migration priority as a function of risk and migration time (see Europol, 2026).

Quantum-related preparedness measures fall within the EU regulatory perimeter mainly through technology-neutral requirements embedded in cybersecurity and ICT-risk frameworks. The Digital Operational Resilience Act (DORA) obliges in-scope financial entities to implement cybersecurity risk-management measures covering cryptographic vulnerabilities arising from technological developments, including quantum computing.[32] In addition, the NIS 2 Directive significantly strengthens cybersecurity obligations for essential and important entities, encompassing many actors that are directly or indirectly connected to the financial system.[33]

Conclusion

Quantum technologies are at an early stage of development, yet public- and private-sector investment in quantum computing R&D has been gathering momentum. In particular, 2025 was marked by a notable **increase in venture capital** raised globally, including by EU-based startups. Reflecting recent technological progress, investor optimism drove surges in the valuations of several quantum computing firms, although these gains were partly reversed amid pronounced volatility. Such **boom-and-bust dynamics** are not uncommon for emerging technologies and often reflect fluctuating expectations about adoption and cost reductions. In the case of quantum computing, the substantial gap between long-term potential and near-term commercial applicability creates fertile ground for **market volatility**, with further valuation swings possible.

Quantum computing is expected to have its greatest impact in addressing narrowly defined, highly complex computational problems, suggesting a role in specialised applications rather than broad, general-purpose deployment. **The financial sector might be an early beneficiary**, given its exposure to computationally intensive tasks for which promising quantum algorithms have been proposed, notably in optimisation, simulation, and selected ML applications. At the same time, sufficiently powerful quantum computers could pose a significant **threat to cybersecurity** by undermining some of the cryptographic protocols currently used to secure transactions, communications and blockchains – an emerging risk that has prompted policymakers to call for the timely adoption of quantum-resistant alternatives.

Depending on the trajectory of technological progress, the quantum computing market may evolve around a restricted base of providers. Such concentration could give rise to **operational and supply-chain dependencies** should financial institutions – as well as other industrial users and state actors – come to rely on a small group of quantum hardware vendors.

While the US and China lead in several critical quantum computing components and materials, the EU closed 2025 as one of the world's fastest-growing jurisdictions in terms of quantum-related investment. Indicators such as patenting activity and scientific publication output suggest that the region is well positioned to sustain further progress. Maintaining this trajectory, however, will depend on the EU's ability to mobilise sufficiently large investment flows. In this respect, ongoing initiatives to advance the Savings and Investments Union and deepen the integration of European capital markets may play an important role in **reinforcing the global competitiveness of the EU's quantum computing ecosystem**. As the technology evolves, ESMA will continue to monitor its implications and potential operational impacts on financial markets.

[32] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA) and Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework.

[33] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).

References

Bard, D. A. and Kearney, J. J. and Perez-Delgado, C. A. (2022), *Quantum advantage on proof of work*, Array, Vol. 15. https://doi.org/10.1016/j.array.2022.100225.

Biamonte, J. and Wittek, P. and Pancotti, N. *et al.* (2017), *Quantum machine learning*, Nature, 549, pp. 195–202. https://doi.org/10.1038/nature23474.

Doosti, M. and Wallden, P. and Hamill, C. B. and Hankache, R. and Brown, O. T. and Heunen, C. (2024), *A Brief Review of Quantum Machine Learning for Financial Services*. https://doi.org/10.48550/arXiv.2407.12618.

EC (European Commission) (2025a), *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, Part 1, Version: 1.1, EU PQC Workstream, NIS Cooperation Group. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

EC (European Commission) (2025b), *Quantum Europe Strategy: Quantum Europe in a Changing World*, Communication from the Commission to the European Parliament and the Council. https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy.

EPO/OECD (European Patent Office and Organisation for Economic Co-operation and Development) (2025), *Mapping the global quantum ecosystem: A comprehensive analysis based on innovation, firm, investment, skills, trade and policy data*, EPO, Munich/OECD Publishing, Paris. https://doi.org/10.65216/20251217-0001.

Europol (2026), *Prioritising post-quantum cryptography migration activities in financial services*, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf

Groenewegen-Lau, J. and Hmaidi, A. (2024), *China's long view on quantum tech has the US and EU playing catch-up*, MERICS Report, Mercator Institute for China Studies. https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf.

Herman, D. and Googin, C. and Liu, X. *et al.* (2023), *Quantum computing for finance*, Nature Reviews Physics, 5, pp. 450–465. https://doi.org/10.1038/s42254-023-00603-1.

Huber, E. X. and Tan, B. Y. L. and Griffin, P. R. and Angelakis, D. G. (2024), *Exponential qubit reduction in optimization for financial transaction settlement*, EPJ Quantum Technology, Vol. 11, no. 52. https://doi.org/10.1140/epjqt/s40507-024-00262-w.

Leclerc, L. and Ortiz-Gutiérrez, L. and Grijalva, S. and Albrecht, B. and Cline, J. R. K. and Elfving, V. E. and Signoles, A. and Henriet, L. and Del Bimbo, G. *et al.* (2023), *Financial risk management on a neutral atom quantum processor*, Physical Review Research, 5. https://doi.org/10.1103/PhysRevResearch.5.043117.

Markham, C. and Grassie, R. (2025), *Quantum Computing Applications in Financial Services*, Research Note, Financial Conduct Authority. https://www.fca.org.uk/publication/research-notes/quantum-computing-applications-financial-services.pdf.

McKinsey & Company (2025), *The Year of Quantum: From concept to reality in 2025*, Report. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025.

Naik, A. S. and Yeniaras, E. and Hellstern, G. *et al.* (2025), *From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance*, Financial Innovation, Vol. 11, no. 88. https://doi.org/10.1186/s40854-025-00751-6.

Orus, R. and Mugel, S. and Lizaso, E. (2019), *Quantum computing for finance: Overview and prospects*, Reviews in Physics, Vol. 4. https://doi.org/10.1016/j.revip.2019.100028.

Palmer, S. and Karagiannis, K. and Florence, A. and Rodriguez, A. and Orus, R. and Naik, H. and Mugel, S. (2022), *Financial Index Tracking via Quantum Computing with Cardinality Constraints*. https://doi.org/10.48550/arXiv.2208.11380.

Rebentrost, P. and Gupt, B. and Bromley, T. R. (2018), *Quantum computational finance: Monte Carlo pricing of financial derivatives*. https://doi.org/10.48550/arXiv.1805.00109.

Research and Markets (2025), *Public and Private Investment in Quantum Technologies in Leading Countries by Quantum Computing, Quantum Sensing, Quantum Communication, Quantum AI, Quantum Life, and Quantum Materials 2025*, Report. https://www.researchandmarkets.com/reports/6202527/public-private-investment-in-quantum.

Ruane, J. and Kiesow, E. and Galatsanos, J. and Dukatz, C. and Blomquist, E. and Shukla, P. (2025), *The Quantum Index Report 2025*, MIT Initiative on the Digital Economy, Massachusetts Institute of Technology, Cambridge, MA, May 2025. qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf.

Seet, J. and Griffin, P. R. (2019), *Quantum consensus*, 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Proceedings, pp. 1–8. https://ink.library.smu.edu.sg/sis_research/6016.

Wu, W. (2025), *Why quantum matters now for blockchain*, Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School. https://www.jbs.cam.ac.uk/2025/why-quantum-matters-now-for-blockchain.