# ESMA article on quantum computing in financial markets: applications, investments and prospects

**June 2026**

On 13 May 2026, ESMA published the article **"Quantum computing in financial markets: applications, investments and prospects"** as part of its Trends, Risks and Vulnerabilities Report. It examines the funding and investment landscape relating to the quantum technology ecosystem, its main applications in financial markets, and the risks associated with its development and adoption.

Quantum computing, like other quantum technologies applicable to communication and sensing, has the potential to have a significant impact on multiple economic, scientific and security-related sectors. Although these technologies are still at an early stage of development, the associated ecosystem is undergoing rapid expansion, driven by growth in investment and business activity, particularly in the field of quantum computing.

Based on the principles of quantum mechanics, quantum computing could tackle problems that are currently difficult for classical computers to solve, opening the door to significant advances in various sectors, including the financial sector. In particular, financial markets are seen as potential early adopters, given that various tasks could benefit from quantum algorithms capable of significantly speeding up calculations and enabling new analytical approaches, the following potential use cases stand out: (a) optimisation algorithms for asset management or trade settlement, (b) stochastic modelling for risk management or asset valuation, (c) machine learning applications for credit ratings or fraud detection, and (d) the development of blockchain technologies based on quantum computing.

Although these applications are still in their early stages, research in this field has already begun, and various entities — including major banks, asset managers and fintech start-ups — have started to develop initiatives related to quantum computing. At the same time, growing market interest has led to a significant increase in investment and the development of public and private initiatives aimed at promoting this technology, against a backdrop of significant uncertainties regarding its commercial viability and future development. In the public sphere, the European Commission's (EC) Quantum Europe Strategy[1], presented in 2025, stands out; its aim is to position the European Union (EU) as a world leader in these technologies by 2030.

Alongside its potential benefits, quantum computing also poses significant challenges. In particular, advances in the development of quantum computers could compromise the cryptographic protocols currently used to secure financial transactions, communications and other critical digital processes, which has prompted the launch of initiatives to facilitate the transition to quantum-resistant encryption methods.

[1] The European Commission's Quantum Europe Strategy.

It is worth noting that the EU was one of the jurisdictions where investment in quantum technologies grew the most in 2025; this, together with indicators such as patent registrations and scientific output, puts it on a path to progress, provided that sufficient capital can be mobilised to drive investment in these technologies.

Pregunta

### How is the development of quantum computing being funded?

Respuesta

Globally, investment in quantum technologies is estimated to have reached approximately $33 billion in 2025, of which 38% was specifically allocated to quantum computing, establishing it as the most dynamic segment of the ecosystem.

The role of the public sector, given its strategic importance, is particularly significant: cumulative public funding commitments exceeded $55 billion in April 2025, with China, the EU and Japan as the main drivers, respectively. These investments reflect the high capital requirements, long development horizons and technological uncertainty associated with these technologies, which necessitate the development of quantum ecosystems; consequently, the public sector is playing a significant role in supporting higher-risk investments in the early stages.

For its part, private investment — primarily through venture capital funds, hedge funds, angel investors, accelerators and large corporations — has been key to the development of the ecosystem. After exceeding $2 billion in 2021 and 2022, investment in quantum startups moderated in 2023 and recovered in 2024, against a backdrop of increased competition for capital with other emerging technologies such as artificial intelligence.

From a geographical perspective, the United States leads the global ecosystem in terms of total investment, innovation and number of companies, supported by a market-driven model that promotes collaboration between companies and universities. In contrast, the EU has a solid scientific base, but its companies tend to rely more heavily on public funding due to lower levels of private investment.

Overall, the funding pattern reflects a rapidly expanding sector that is still in its early stages, with high volatility in valuations and a significant reliance on public support, against a backdrop of uncertainty regarding its adoption timeline and cost-reduction potential. Against this backdrop, specialised investment vehicles are beginning to emerge, including some EU-domiciled exchange-traded funds (ETFs) — launched by managers such as iShares, VanEck and WisdomTree — as well as venture capital initiatives such as the fund backed by the Danish firm 55 North.

In line with this trend, venture capital funding has reached high levels globally by 2025. In Europe, there has been a notable increase in such funding, although it remains concentrated in a small number of companies: eight start-ups[2] have secured investments exceeding €100 million, a further 52 have collectively raised around €1 billion, and one of them has surpassed a valuation of $1 billion. The sector's significant funding needs highlight the necessity to make progress on the integration of European capital markets, as well as to promote initiatives such as the Savings and Investments Union.

[2] Four based in the UK, two in France, one in Finland and one in Spain.

Pregunta

## What are the applications of quantum computing in finance?

Respuesta

Quantum computing has the potential to transform the financial sector by offering processing and analytical capabilities that far exceed those of classical computing for certain complex problems. Specifically, quantum algorithms enable calculations to be performed with greater efficiency and speed than classical methods — a phenomenon known as *quantum* speedup —.

Potential applications of quantum computing that have been explored in the financial sector include:

1. **Optimisation.** Quantum algorithms can improve the resolution of complex optimisation problems, such as those related to portfolio optimisation, risk mitigation and hedging. They can also be useful in index replication or tracking[3] and trade settlement[4]. Furthermore, they can be applied to economic and financial modelling, including the prediction of financial contagion in networks of interconnected institutions during periods of stress and the identification of foreign exchange arbitrage opportunities. Finally, it is worth highlighting the possibility of adopting hybrid approaches in which quantum computing is used to identify asset combinations, whilst classical methods carry out the precise allocation within the portfolio.
2. **Stochastic modelling.** Stochastic modelling uses random processes and Monte Carlo simulations[5] to model financial variables such as share prices, interest rates and volatility. The use of quantum computing enables these simulation methods to be accelerated in the valuation of financial instruments — including European and exotic options and collateralised debt obligations (CDOs) —. These tools can also improve the calculation of risk metrics, such as value at risk (VaR) and credit risk analysis. Despite the theoretical advantage offered by quantum modelling, numerous challenges remain, such as the encoding of classical probability distributions into quantum states or hardware limitations — such as the low number of qubits and lack of fault tolerance —.
3. **Machine learning (ML).** The use of quantum ML (QML) algorithms can aid in the detection of complex patterns in large volumes of data, with applications in credit risk assessment, fraud detection and other classification and prediction tasks — such as credit rating downgrades —. QMLs fall into two

main categories: (1) methods that accelerate classical ML techniques, whose task is to search for patterns in conventional data by encoding them into quantum states and processing them with basic quantum linear algebra subroutines (QBLAS); and (2) native quantum ML algorithms that operate directly on quantum data generated within a quantum system. Although their applicability and practical relevance need to be reviewed, native approaches are considered more promising, although it is unclear whether they can offer a significant advantage in the financial sector.

4. **Decentralised ledger technologies** (DLT). Firstly, quantum computing may have a significant impact on DLT-based platforms, such as *blockchain*, as it could compromise the public-key cryptography used in them, as will be explained in more detail in the following section. Consequently, one of the alternatives being explored is the incorporation of advanced cryptographic techniques, based on quantum computing, in order to enhance their security. Another possible application involves using quantum computers to speed up the mining of bitcoins and other crypto-assets (CA) when performing calculations related to the so-called proof-of-work (PoW) and even to enable quantum PoW mechanisms, which would significantly reduce electricity consumption.
   Furthermore, quantum technology could improve the scalability and speed of decentralised consensus mechanisms, whilst also facilitating interoperability between different blockchains. In turn, it could be applied to the tokenisation of assets and to shared *know-your-customer* (*KYC*) processes between different financial institutions.

Although these applications offer significant advantages in terms of computational efficiency and processing, integration with traditional systems and the development of specific algorithms are still at an early experimental stage.

[3] In particular, in the selection of assets to replicate a broader market index.

[4] For example, when a clearing house determines the maximum number of transactions that can be settled between multiple participants without exceeding their credit limits, resolving the complex interdependencies between the parties involved.

[5] This consists of a numerical simulation technique used to estimate the expected value of a quantity that depends on one or more random variables, involving the generation of a large number of sampling trajectories based on underlying stochastic (random) factors. It is used, above all, for asset and risk valuation, but may require significant computational effort (for example, if the scale of the problem increases), so the use of quantum algorithms would facilitate the calculations.

Pregunta

## What are the risks associated with quantum computing?

Respuesta

Despite the numerous opportunities offered by quantum computing in the financial sector, its development poses significant risks that could affect its operation and security.

In particular, the main concern lies in its potential to compromise current cryptographic mechanisms, by solving certain mathematical problems — on which their security is based and which classical computers are unable to solve — much more quickly. The financial system — including banking, payment services, securities markets and asset management — relies heavily on public-key cryptography to perform key functions, such as digital signatures or ensuring the security of transactions, data integrity and the confidentiality of communications. In particular, in the field of DLT, the development of sufficiently advanced quantum computers could enable the breaking of some of these cryptographic systems and facilitate access to the private key from the public key, with a view to subsequently using it without the holder’s consent. Furthermore, the threat has a significant temporal dimension, as information encrypted today could be stored and decrypted in the future, once quantum technology reaches sufficient maturity.

Another risk to be considered is that of concentration within the sector, as the quantum computing market could become concentrated amongst a small number of suppliers. Such centralisation would create critical operational and supply dependencies for financial institutions, industries and public administrations.

Given the systemic and cross-sectoral nature of this challenge, initiatives aimed at facilitating the transition to encryption methods resistant to both classical attacks and those arising from quantum computing (*post-quantum cryptography*) are being stepped up.

Its gradual adoption is also emerging as a key element in preserving the stability and resilience of the financial system in the long term. Specifically, the EC has established a specific roadmap for the transition to post-quantum cryptography. The main milestones of this plan are to begin planning the transition and launching pilot projects in

2026, to complete the transition for use cases considered high-risk by 2030, and for medium-risk use cases by 2035.

For its part, the Digital Operational Resilience Regulation (DORA)[6] incorporates preparations for quantum computing into the EU regulatory framework by imposing obligations on financial institutions to implement cybersecurity risk management measures that address cryptographic vulnerabilities arising from technological advances, explicitly mentioning quantum computing.

[6] Regulation (EU) 2022/2554 of the European Parliament and of the Council, of 14 December 2022, on digital operational resilience in the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

**Links of interest:**

Quantum computing in financial markets: applications, investments and prospects - TRV article

This document is an unofficial summary of a document published by ESMA. It does not necessarily reflect CNMV's official position, its managers and directors' or the rest of its staff's on the matters addressed.

This document has been drafted using material downloaded from ESMA's website. ESMA does not endorse this publication and in no way is liable for copyright or other intellectual property rights infringements nor for any damages caused to third parties through this publication.