ANALYSIS

Quantum computing is coming – Is the financial sector ready?

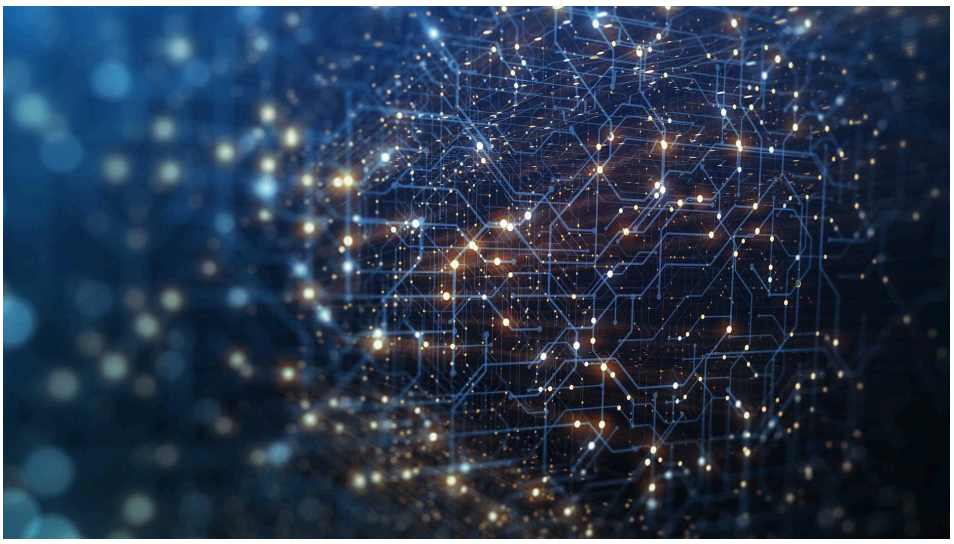
Yesterday – Analysis – Financial stability

Antti Hirvonen
Data Expert

Joonas Savolainen
Information Specialist

Heli Snellman
Senior Adviser

In early 2025, the Bank of Finland conducted a survey on the prospects, benefits and risks of quantum technology in the financial sector. Based on the survey responses, quantum technology has the potential to reshape business activities significantly in the long term. Only a few tests and practical trials have been conducted so far, however, as the technology is immature. As the opportunities of quantum technology, respondents cited the improvement of risk management and information security and the development of investment activities. Information security was also highlighted among the risks, however.



The opinions expressed in this article are those of the authors and do not necessarily reflect the views of the Bank of Finland.

Technological development and digitalisation have significantly shaped banking services over the past thirty years. While some of the technological advances are directly visible to customers, some are back-end systems working behind the scenes. One of the fields that is currently developing rapidly is quantum technology. It may have a profound impact on many sectors of society, including the financial sector.

Quantum computers differ fundamentally from conventional computers.[1] Quantum computers leverage the phenomena of quantum mechanics, such as superposition and entanglement, which makes them particularly efficient in certain tasks that require computational power.[2] Reaping the benefits of quantum computing requires an increase in the number of basic units of information used in quantum computers, i.e. quantum bits, or 'qubits'. It is equally important that qubits' sensitivity to disturbances be reduced. The third condition is the development of algorithms and software that utilise the special properties of quantum computing. Recent years have seen significant progress in all these fronts. There are, however, a number of problems that classical computers will remain better suited to tackle than quantum computers, so the different computing methods will be complementary.

In addition to benefits, digitalisation and new technologies also introduce new risks, and quantum technology is no exception. In the future, quantum computers will probably be able, among other things, to break current encryption algorithms.[3] Although this is not possible with the current quantum computers, it is already time to prepare for the information security risks posed by quantum computing. In fact, encrypted data can already be stolen and stored until quantum technology is sufficiently advanced to break encryption ('harvest now, decrypt later'). Digital signature forgery is another example of the risks.

To counter the information security risks posed by quantum computing, quantum-safe algorithms have been developed (post-quantum cryptography, PQC). A major step in their standardisation was taken in August 2024, when the US National Institute of Standards and Technology (NIST) released a set of post-quantum encryption standards. The Finnish Transport and Communications Agency (Traficom) has incorporated the NIST's standardised algorithms into the national criteria and recommends organisations to migrate to the post-quantum algorithms as soon as possible.

Quantum technology is seen to have lots of potential benefits

In February 2025, the Bank of Finland conducted a survey on the prospects, benefits and

1. See the VTT Technical Research Centre of Finland: Quantum computing: Practical guide to navigating the future, chapters 2–3.
2. Kvanttilaskenta uusien innovaatioiden lähteenä finanssimarkkinoilla – Euro ja talous ('Quantum computing as a source of new innovations in the financial markets'; in Finnish).
3. By applying Shor's algorithm, for example. See the VTT Technical Research Centre of Finland: Quantum computing: Practical guide to navigating the future, chapter 7.

risks of quantum technology in the financial sector. A total of approximately 30 financial sector companies operating in Finland responded to the voluntary survey. The respondents included banks, insurance companies, fund management companies and investment firms.

Respondents were requested to assess the opportunities offered by quantum technology in their own words. It was generally considered that, on the one hand, quantum computing could enhance the speed, efficiency and precision of present-day calculations and modelling, and, on the other hand, help solve entirely new kinds of problems. Respondents saw that the greatest potential of quantum computing lies in its ability to improve risk management and information security and develop investment activities. A fifth of respondents, however, did not see any benefits of quantum technology for their own business, at least at the moment.

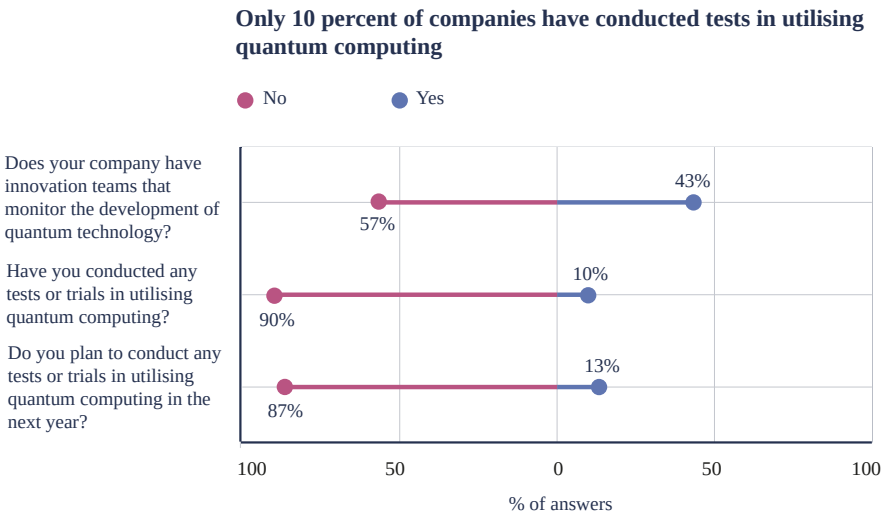
Nearly half of respondents found that quantum technology will bring benefits to risk management. The examples mentioned included the prevention of money laundering and fraud, and modelling of various risks in general. Quantum technology was also seen to enable more diverse and complex risk simulations, stress tests and scenario analyses. In investment activities, benefits were expected in the optimisation of investment portfolios, pricing of derivatives and in market analyses. These potential areas of application are well in line with the study by the Bank for International Settlements (BIS), which lists the potential advantages of quantum technology in the financial sector.[4]

Only a few cases of practical implementation as yet

Nearly half of the financial sector respondents have innovation teams that monitor the development of quantum technology (Chart 1). The average time spent on this monitoring in innovation teams is less than one person-year. It is also likely that companies monitor progress in quantum computing as part of regular work, even if they have not set up a specific innovation team. Every tenth respondent organisation had conducted tests or trials in utilising quantum computing, and over 10% were planning to do so in the next year.

4. Quantum computing and the financial system: opportunities and risks. Use cases in the financial sector are also assessed and described in the report Embracing the Quantum Economy: A Pathway for Business Leaders by the World Economic Forum and Accenture (pp. 29–31 and 49–50).

Chart 1.



Source: Bank of Finland.

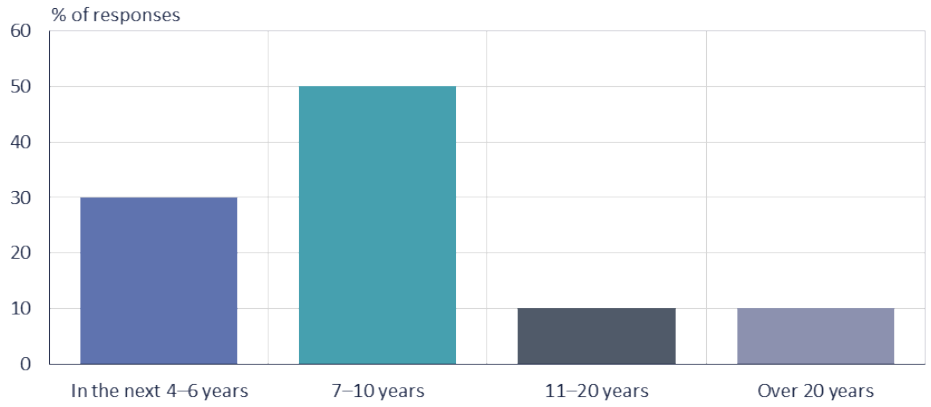
Quantum technology may change business considerably in the long term

Two out of three respondents saw quantum technology as an important or somewhat important competitive factor for the future. Insufficient investment in new technologies leads to a risk that a company will lag behind its competitors and lose its competitive position. Almost 40% of respondents felt that their readiness to utilise quantum technology was currently at or above the average level relative to domestic competitors. Readiness relative to foreign competitors was considered to be slightly weaker but, on the other hand, over half of respondents were unable to rate their readiness relative to competitors.

Four out of five financial sector companies surveyed believe that quantum technology will be part of their business process within the next 10 years (Chart 2). 40% of respondents felt that information about quantum technology was moderately well available for their own activities, and only just over 10% considered that they could find information well or very well (Chart 3).

Chart 2.

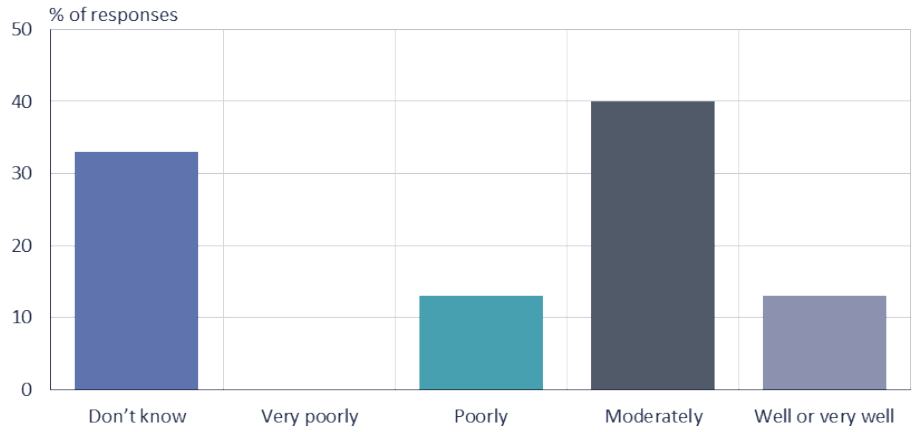
In what timeframe do you expect quantum technology to be part of your business processes?



Source: Bank of Finland.

Chart 3.

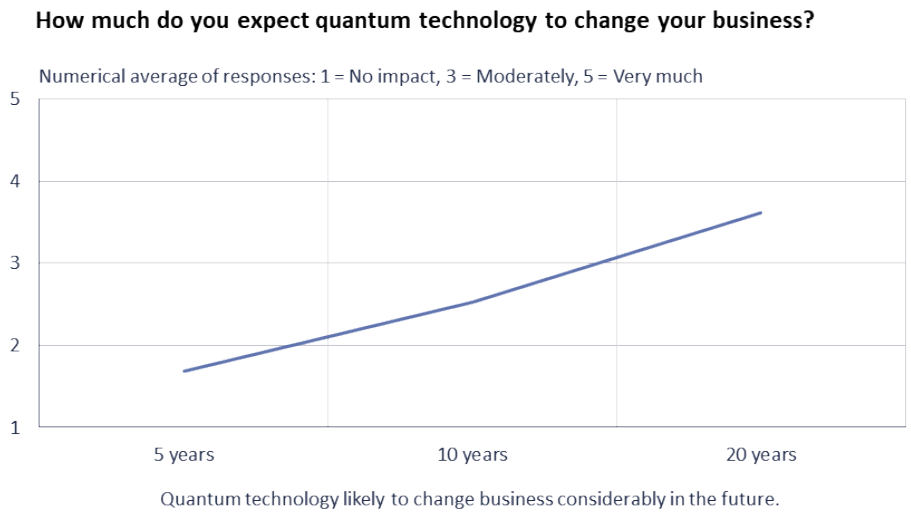
How well can you find information about the development of quantum technology in a form that is relevant to your operations?



Source: Bank of Finland.

Companies considered that quantum computing would change their own business greatly in the long term. Although no major changes were expected in the next five years, the impact would be considerable during the next 20 years (Chart 4).

Chart 4.

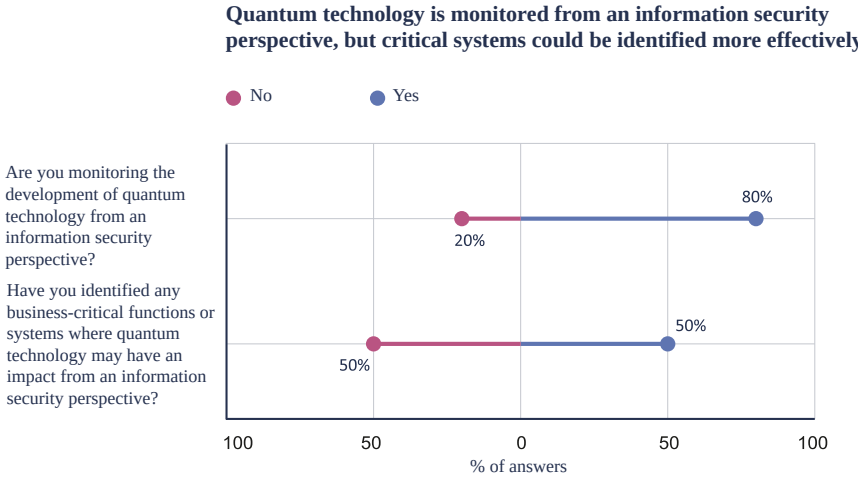


Source: Bank of Finland.

Information security and particularly decryption highlighted among the risks

The biggest risks identified in quantum computing were security-related issues and, in particular, decryption of present data. 80% of respondents stated that they were monitoring the development of quantum technology from an information security perspective (Chart 5). Half of respondents had identified business-critical functions or systems where the development of quantum technology could have an impact, particularly from the perspective of information security.

Chart 5.



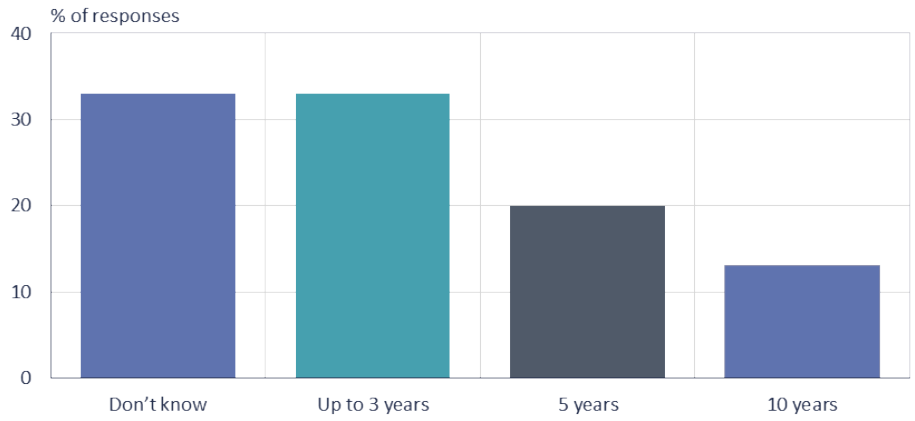
Source: Bank of Finland.

One third of respondents believed the potential information security threats posed by quantum technology must be addressed now. It is often recommended that companies start transitioning to post-quantum cryptography by mapping out the cryptographic solutions they use, i.e. by implementing a cryptographic inventory.[5] Just under half of respondents had planned to implement such an inventory but had not yet done so.

Four out of five respondents found that 'harvest now, decrypt later' attacks are a relevant risk. More than half of respondents were of the opinion that the most critical information should remain confidential for at least 20 years. One sixth considered that the time frame should be at least 10 years, and 10% felt that 5 years was sufficient. One third of respondents stated that it would take up to 3 years for their organisation to transition to post-quantum cryptography (Chart 6). One tool for assessing the quantum threat is Mosca's theorem[6], which indicates the year when a company should start migrating to post-quantum algorithms. If the time required to change algorithms and the time that data must remain confidential is greater than the time before a cryptographically relevant quantum computer becomes available, there is a risk that data will be compromised while it is still to be kept secure.

Chart 6.

How much time do you estimate your organisation will need to transition to post quantum/quantum-safe cryptography?



Source: Bank of Finland.

Immaturity of technology, lack of expertise and costs cited as challenges

Respondents felt that the biggest challenges during the next five years were the immaturity of quantum technology, lack of expertise and the lack of useful use cases (Chart 7). High costs were also seen as a problem. Assessing the impacts of quantum technology in the long term (in the next 20 years) was considered to be very challenging,

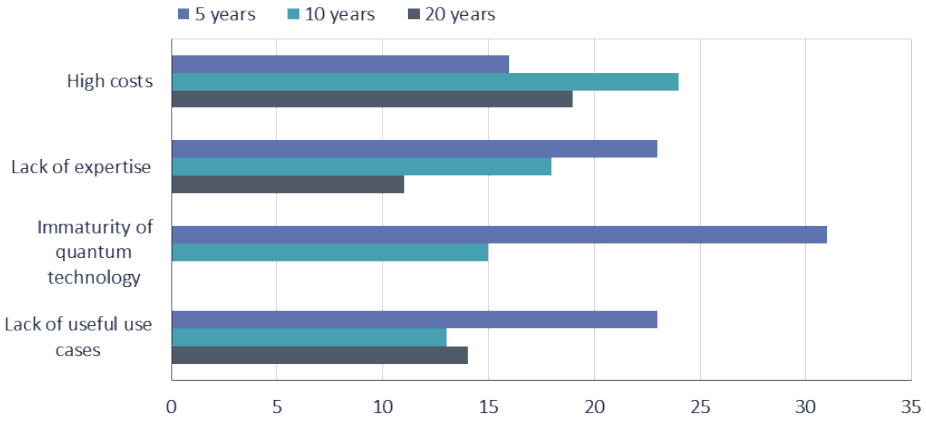
5. See e.g. the National Emergency Supply Agency: Data Security Impacts of Quantum Computing – Preparedness recommended, pp. 16–19.
6. See ibid., p.4.

and nearly half of respondents felt that it was impossible. Costs were seen as a problem in the long term, too, even though it was assumed that skills would improve, technology would become more mature and use cases would be found.

Chart 7.

Where do you see the biggest challenges to the implementation of quantum technology?

Challenges to implementation of quantum technology by time horizon



Source: Bank of Finland.

One of the questions was whether current legislation imposes restrictions on the utilisation of quantum technology. 80% of respondents felt that this was not the case. However, one fifth stated that there were restrictions through, for example, the EU's artificial intelligence legislation, the General Data Protection Regulation (GDPR) and other regulations affecting banks' activities.

Companies should prepare for the coming of quantum technology

Based on the survey, financial sector companies operating in Finland are monitoring the development of quantum technology. While potential benefits have been identified, quantum technology is still immature, so its utilisation has not yet been tested to a great extent. In the long term, quantum technology may significantly reshape financial sector activities. Companies have assessed the risks posed by the new technology, and the responses highlighted the concern that quantum computers could break current data encryption methods.

As quantum computing continues to advance, it has the potential to revolutionise current IT solutions. All financial sector participants should therefore monitor progress in the field and evaluate what quantum computing could mean for their own business and how they should prepare for its arrival. Each participant must be ready to act and transition to post-quantum cryptography. Confidence is of the utmost importance for financial stability. Therefore, if new threats materialise, this would weaken customers' confidence in digital services. Updating existing systems will take time and, on the other hand, participants must also be ready to upgrade post-quantum cryptographic solutions as the

field advances.

In Finland, quantum computing has been explored in, for example, the FutureQ research project, which has brought together representatives from a number of different industries and also from the Bank of Finland. It is important that collaboration between different actors continues, both in Finland[7] and internationally.

It is important for Finland and Europe to be able to reap the benefits of quantum computing and other new technologies. Finland's Quantum Technology Strategy 2025–2035 was published in April 2025.[8] The European Commission, in turn, has also published its Quantum Europe Strategy in July 2025.

Our common goal should be to ensure that Finland and Europe stay at the forefront of quantum computing. The power of quantum computing should be harnessed to support our competitiveness and resilience.

Tags

quantum computing, information security, quantum technology, financial sector

7. An example of collaboration in Finland is the Finnish Quantum Institute (InstituteQ): https://instituteq.fi/.
8. Finland's Quantum Technology Strategy 2025–2035: A new engine of growth and builder for a sustainable future – Ministry of Economic Affairs and Employment.