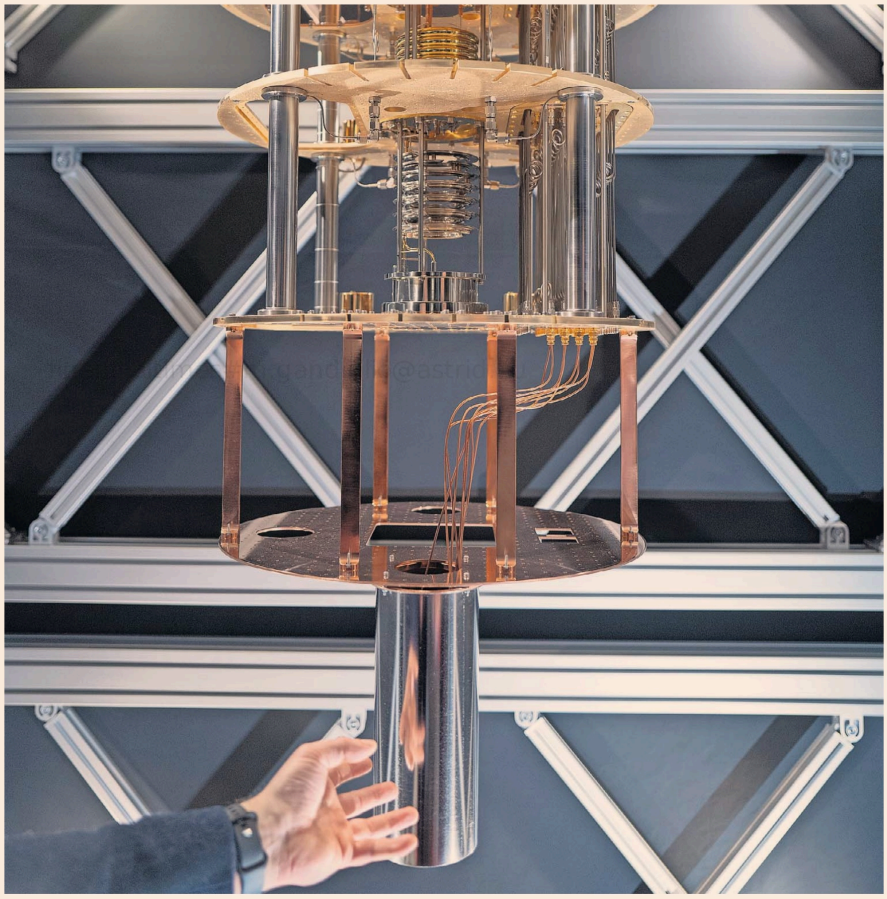
Companies are betting on the computing technology and its implications for sectors such as pharmaceuticals, finance and crypto. But sceptics worry about the hype.

By Michael Peel



The quantum revolution is closer than you think

Deep inside a data centre in Manhattan, a quantum computer is enshrined in an alcove like an idol. To reach it, visitors pass two sets of sliding doors and banks of the conventional machines it is predicted to surpass.

The computer's maker, UK-based company Oxford Quantum Circuits, has installed it for companies to use via cloud or fibre connections, giving them an opportunity to experiment with the technology first-hand. Nvidia AI hardware helps the column of copper and steel achieve extraordinary calculating powers, thanks to its ability to analyse and predict complex systems such as financial flows or chemical reactions.

After years of false dawns, many of the world's leading tech companies are now betting that quantum computers will start to outperform their conventional counterparts by 2030 — with a potentially huge impact on fields ranging from cryptocurrencies and financial services to drug discovery.

"It sounds really futuristic and I fully understand that," says Gerald Mullally, OQC's chief executive, pointing to his company's client base as a vote of faith in the technology's potential. "Essentially it's a bet that these companies are making that 'this is going to happen, it's going to matter and so the sooner we engage with it, the more practice we get.'"

But some scientists worry that the sheer power of the technology could endanger privacy and national security while others still doubt that useful machines can be made at all.

Today, quantum computers are no longer just found in research laboratories as companies explore the technology's commercial possibilities. Industry observers estimate there are scores of quantum computing systems in the world, a number forecast by the consultant McKinsey to rise to around 5,000 by 2030.

> 'Essentially it's a bet that these companies are making that "this is going to happen; it's going to matter"'

Scientists say that advances in performance and capability will be incremental.

But investors have been enthused by developments such as Microsoft's announcement last week of its next-generation Majorana 2 quantum chip and its expectations of a quantum computer that can solve "commercially viable, reasonable problems" by 2029.

When Honeywell-backed quantum computing company Quantinuum launched an initial public offering on Nasdaq this month its shares were valued at more than $15bn. The stock price of rival group IonQ has risen more than 700 per cent since September 2024.

Google and IBM are both targeting the delivery of useful machines by 2030. Sundar Pichai, Google's CEO, said in November that the technology was now "where maybe AI was five years ago".

Governments are also making strategic investments. The US announced plans last month to take equity stakes worth $2bn in nine quantum computing companies, including a start-up backed by a firm with links to the Trump family and one taken public by a Pentagon official.

Sceptics point to the significant technical hurdles that remain to making useful quantum computers. Existing machines are still far too error-prone. The "engineering challenges" that the devices' developers insist can be solved in the next few years are formidable.

But as the new machines begin to indicate they can outperform conventional computers in niche areas — what the industry dubs "quantum advantage" — the risk of dismissing the technology's importance is growing.

Organisations are readying themselves for the prospect of Q-Day — the predicted moment when quantum computers are capable of breaking the cryptographic methods on which modern societies rely.

Not just ones and zeros

Serious research into quantum computing began in the 1980s and has developed more slowly than advocates had hoped.

Originally researchers wanted to see if it was possible to enhance computers by exploiting unusual quantum effects exhibited by matter at the atomic and subatomic scales.

Quantum computers can transcend the limitations of the traditional binary computer bit, which can exist in two states, denoted by zero and one.

By contrast, quantum bits, or "qubits", can exist in both those states at once. This allows quantum machines to survey multiple potential solutions simultaneously, rather than dealing with them one by one like a conventional computer.

One analogy is a maze. Where a quantum computer can examine the whole map to find a way through, a traditional machine will keep exploring dead ends until it finds the route. Quantum computers' superior processing power should make them better able to generalise from small amounts of data and sift through multiple complex patterns.

The technology still has far to go to be fully developed.

A working quantum computer will require at least 1,000 logical qubits, according to research published by the California Institute of Technology in March. OQC's Genesis has 16.

But many companies are already experimenting with the technology because of its promised leap in capability, predicting early uses for the machines in areas such as chemistry and materials science.

The idea is that because of their own workings and structure the computers will be better able to analyse and predict chemical behaviour determined by atomic and subatomic interactions governed by quantum rules. In a sense, they will be speaking the same language.

As a result, a sufficiently powerful quantum machine should in theory be adept at predicting the interactions between drugs and living cells that determine whether a new pharmaceutical will work.

Such possibilities have already led tech companies to pair up with industrial groups. Google has collaborated with pharmaceuticals company Boehringer Ingelheim on drug discovery, Bosch on materials science and Mercedes-Benz on battery technology. It has also worked with the carmaker Volkswagen to research traffic flow and optimisation.

> '[It] may improve how firms manage risk, price investments, optimise portfolios and detect fraud'

Chevron Technology Ventures, the venture capital arm of the oil multinational, was a returning investor in a £260mn fundraising round concluded by OQC last week. Chevron says its investment reflects its interest in quantum technologies in areas such as cyber security, data processing and complex system optimisation.

Boosting financial services

Rob Otter, head of global technology applied research at JPMorgan Chase, says that the financial services industry also anticipates "early benefits from quantum computing, as it is able to efficiently process and analyse large, fast-arriving data sets, such as transaction records, market feeds or risk signals".

He adds that over time the technology "may improve how firms manage risk, price investments, optimise portfolios and detect fraud, leading to more efficient markets and better customer outcomes".

In experiments, quantum machines have also shown potential for improving fraud detection, overcoming drawbacks in existing AI-based methods. The relative scarcity of fraud cases means AI lacks a large dataset to learn from and criminals change their methods, meaning models need constant retraining.

The technology company Unisys has said it has seen promising results from partnerships with the online payments company Paysafe and the UK's National Quantum Computing Centre.

One piece of Unisys fraud detection research found that the quantum approach achieved zero false negatives while minimising false positives. This is notable because false negatives mean frauds are missed, while false positives frustrate customers because it means legitimate transactions are blocked.

Quantum computing "sits at the intersection of AI, data and security", says Ken Moore, Mastercard's chief innovation officer. Future quantum applications could extend to areas such as risk modelling and next-generation cryptography, he adds.

As soon as the first experimental quantum computers were released in the 1990s, scientists began to make predictions about Q-Day, the supposed date when quantum computers will be able to crack commonly used cryptography systems. Such a development would put at risk a swath of confidential data ranging from national security secrets to health records and personal financial information.

Common existing cryptographic methods are founded on the multiplication of very large prime numbers. These can only be broken if the computer can work out the identity of the numbers, which would take existing machines so long it is impractical.

By contrast, a quantum computer of sufficient size could tackle the problem on a timescale that criminals could take advantage of, since the technology can perform complex calculations much more quickly than conventional machines.

The menace is the greater because hackers can steal data today to break open after Q-Day: a strategy known as "harvest now, decrypt later".

The prospect has spooked cryptocurrency companies. They are especially vulnerable because crypto theft can be carried out anonymously and they have fewer safeguards than traditional banks. Ayo Akinyele, head of engineering at RippleX, the blockchain development arm of crypto group Ripple, told the FT last month that the quantum threat "has moved from theoretical to credible".

Across industries and governments, institutions are preparing for the possibility of Q-Day by introducing so-called post-quantum cryptography. These are new "quantum-safe" algorithms, including three developed in 2024 under the supervision of the US National Institute of Standards and Technology. This year the institute announced nine more candidate algorithms, as the battle to protect the world's data intensifies.

The limits of the technology

Almost no one in the industry sees quantum computers as a replacement for conventional machines because the technology will be best suited for a relatively narrow range of highly complex tasks.

The history of computing suggests that quantum devices are likely to boost demand for the conventional machines needed to support them, says Timothy Costa, Nvidia's vice-president and general manager of quantum. "What computing does is it grows the pie," Costa says. "Quantum will do that too." He adds that the same logic suggests quantum computers and AI will not duel for supremacy but rather fuel each other.

As the quantum processing units at the heart of the machines become more capable, they will require more adept AI to calibrate them and to perform error correction. Some quantum computer experts think the devices could play a role in generating new synthetic data for AI models to learn from.

The semiconductor industry could also use AI to create useful quantum devices, which in turn could find better materials for semiconductor design, Costa says.

All this is still years away at least. Some scientists warn against hyping a sector whose ambitious timelines they question. Others express scepticism about whether useful machines can be made at all.

One big problem that causes operational faults is "noise" — random variations and distractions that can lead to errors in qubit calculations. Quantum phenomena are vulnerable to environmental disturbances such as heat or magnetic fields that can affect results.

Developers use error correction techniques to mitigate such problems, but researchers such as Gil Kalai, a mathematician at the Hebrew University of Jerusalem, have argued that it may be impossible to make such workarounds sufficiently robust.

The sector faces other technical obstacles. Work is needed on areas such as the hardware and software interfaces between the devices and conventional machines, and on developing algorithms to run on the quantum devices.

But proponents of the technology, such as OQC's Mullally, who argues that quantum computers may be much more energy efficient than their conventional counterparts, hold out the prospect of a series of major breakthroughs. His group predicts that by the middle of the next decade, its Genesis model will be superseded by new generations named Titan, Athena and Atlas.

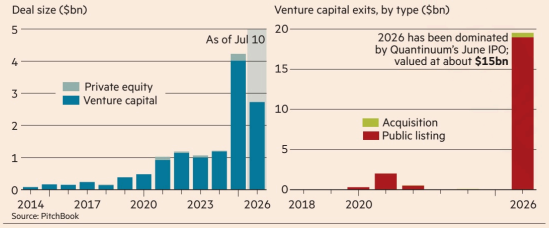
Mullally says such mythic language should not obscure the seriousness of the progress the technology is making.

"The industry does lean . . . into this kind of fictional scientific dream world overall," he says. "But it is now much more real."

Oxford Quantum Circuits' quantum computer at the OQC data centre in New York

Pascal Perich/FT

Investment in quantum computing has soared and a wave of listings has hit the market



Source: PitchBook