TIC Asset Management

Quantum Computing: Big Claims, Bigger Questions



By Miguel Jordão

On 2 June 2026, two announcements showed how much enthusiasm and money are flowing into quantum computing, well before the technology has shown that it can pay its way. Microsoft unveiled its new chip, Majorana 2, and claimed that its qubits were roughly a thousand times more reliable than its predecessor, adding that the company now expected to build a full-scale quantum computer by 2029, several years earlier than planned [1]. However, this claim came in an arXiv preprint that had not been peer-reviewed, and therefore many physicists remain unconvinced. Microsoft's previous chip had drawn the same doubts a year earlier [2]. On the same day, IBM committed more than $10 billion over five years to its own quantum programme, a quieter but far bigger commitment [3].

That combination of a contested promise and a very large bet defines quantum computing today. The money is substantial: investors placed $12.6 billion into quantum start-ups in 2025, more than six times the figure for the previous year, even though the companies building the machines earned only about $1 billion between them [4]. So is the enthusiasm. A few weeks before Majorana 2, Quantinuum sold shares to the public for the first time, at a valuation above $14 billion on roughly $31 million of revenue [5].

Therefore, the question is whether this is already an industry that an investor can analyse, or a venture bet that happens to be publicly traded. This article argues that the honest answer depends less on the number of qubits a company reports than on three questions.

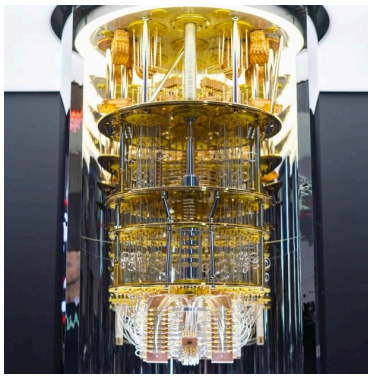


Figure 1: IBM´s Quantum Computer
Source: News EPFL

Can the machine perform difficult, reliable calculations? Does it solve a problem that someone is willing to pay to have solved? And can the company fund the long wait until it can?

How quantum changes the computation?

Consider the basic unit first. A conventional bit is always either a 0 or a 1. A qubit is different. Until it is measured, it occupies a mixture of both states, a property known as superposition. When several qubits are connected through entanglement, their outcomes become correlated in ways that ordinary bits cannot reproduce. The key is interference: a good quantum algorithm makes the wrong answers cancel out and the right ones reinforce, so the useful result is the most likely to appear when the system is measured. A quantum computer does not test every answer at once and then reveal the winner, even though that is a common misconception.

Two consequences follow. First, a large number of qubits does not by itself produce a better machine. What matters is whether the qubits are stable and accurate enough to complete a long calculation before errors accumulate.

Second, the hardware is difficult precisely because each qubit must be isolated from its surroundings. Superconducting chips operate just above absolute zero, while other designs hold single ions or atoms in a vacuum and control them with lasers.

None of this makes quantum computers faster in general. In fact, for almost every task performed today, conventional computers remain faster and cheaper.

A quantum machine has an advantage only for certain classes of problems. The standard examples are narrow. Shor's algorithm factors large numbers, which places current encryption at risk; Grover's algorithm accelerates searches through unsorted data; and quantum simulation models molecules and materials, the task for which the hardware is best suited.

Advantage also comes in degrees: some exist only on paper, others have been shown in a laboratory, but none has yet beaten the best conventional computer on a problem worth paying for. Google reached the laboratory stage in October 2025, when its Willow chip ran a verifiable algorithm about 13,000 times faster than a leading supercomputer on the same task [6].

That line keeps shifting as conventional computers improve, and researchers warn that many promised speed-ups shrink once the cost of moving data in and out and of correcting errors is counted. The clearest lasting advantage is likely in chemistry and materials [7]. For now the realistic approach is hybrid: a conventional computer runs the workflow and hands the hard part to the quantum processor.

Where the value is, and what blocks it

If quantum computing succeeds commercially, the first returns are most likely to come from simulating nature. Chemistry and drug discovery are the closest fit, because determining how molecules behave is precisely what the hardware does.

Materials and energy follow the same logic, with possible gains in batteries, catalysts and fertilisers. Finance is the most actively pursued case, and one of the most debated.

More than a dozen banks, among them JPMorgan Chase and Goldman Sachs, run quantum programmes, and pilots have reported large speed-ups for Monte Carlo risk and pricing in controlled tests. The proven speed-up there is, however, quadratic rather than exponential.

Article written in June

It needs fault-tolerant hardware (able to keep correcting its own errors during a long calculation) that does not yet exist, and it depends on loading large volumes of market data into the machine, a serious bottleneck. No bank yet runs quantum in production. BCG's own $2–5 billion estimate for the sector includes quantum-inspired methods that run on conventional computers, so part of the prize may never need a quantum machine at all [8].

Today's demand is real but limited: McKinsey counts more than 300 companies, including Airbus and Boehringer Ingelheim, working with quantum vendors, mostly on trials rather than production [4]. The headline forecasts (up to $2.7 trillion by 2035 from McKinsey, $450–850 billion by 2040 from BCG) are large but come from interested parties, and are best read as direction, not prediction [4][8].

The reason the payoff remains uncertain is error. Qubits lose their state to noise, and small mistakes accumulate over a long calculation. The solution is quantum error correction, which stores one reliable logical qubit across many physical qubits. That cost is the central difficulty: a useful machine may require hundreds or thousands of physical qubits for each logical qubit.

The encouraging development is that error correction has begun to work. In December 2024, Google's Willow chip crossed a barrier that had stood for nearly thirty years. Because every extra qubit carries noise of its own, adding qubits had always made error correction worse. Willow was the first chip clean enough for the reverse to hold, with more physical qubits driving the logical error rate down [9]. The fair way to compare companies is therefore not the raw qubit count but the number of logical qubits and their error rates. By that measure, 2024 and 2025 brought real progress: Microsoft and Atom Computing linked 24 logical qubits [10]; Quantinuum's Helios system reported 48; and a QuEra collaboration with Harvard and MIT reached 96 logical qubits [11]. IBM, using a more efficient error-correcting code, states that it can reduce the overhead by about 90 per cent and deliver a fault-tolerant machine with 200 logical qubits by 2029 [12]. The count is only part of the picture, however.

Qubit quality matters just as much, and this is where Microsoft's Majorana 2 was directed in June 2026, claiming qubits that retain their state for seconds, far longer than the microseconds typical of today's machines, although the result remains unreviewed and disputed [1].

The rest are the ordinary difficulties of hard engineering: cooling, lasers, vacuum systems and control electronics, scarce and costly talent, heavy capital needs and long timelines, and making a lab prototype behave identically every day. For drug discovery, McKinsey's optimists expect practical use in five to ten years, while sceptics put fully error-corrected machines ten to twenty years away [13]. The bottleneck is not more qubits, but enough reliable logical qubits to run long, useful calculations at a sensible cost.

Who could capture the value?

Even before the hardware matures, one consequence is already forcing decisions: encryption. Shor's algorithm would break the codes, RSA and elliptic-curve methods, that protect most online communications. In a sense the threat exists today, because data intercepted now can be stored and decrypted later. How distant is the machine that could do this? In May 2025 a Google researcher, Craig Gidney, estimated that breaking RSA-2048 might require fewer than a million noisy qubits and less than a week, twenty times fewer qubits than he had estimated in 2019 [14]. That figure is still far beyond any existing machine, but the threshold is falling. Governments have not waited. In August 2024 the United States standards body, NIST, published its first post-quantum encryption standards and advised organisations to begin the transition immediately [15]. That transition is itself a business, one that generates revenue well before any large quantum computer exists.

Bitcoin is the clearest illustration. Ownership is protected by ECDSA signatures, which Shor's algorithm would break, and about a quarter of all bitcoin is held in addresses whose public keys are already visible [16]. The risk is concrete enough that in 2025 BlackRock added quantum computing as a formal risk factor to its Bitcoin exchange-traded fund [17], while Bitcoin developers debate a quantum-safe upgrade that would eventually freeze coins left in exposed addresses [18].

The other major factor is national. Europe operates a €1 billion Quantum Flagship programme built around the goal of technological independence [19], and Germany and France have each committed billions more [20]. The United States has gone even further: on 22 June 2026 the Trump administration signed executive orders creating a federal programme to build a powerful quantum computer, which the administration says it can achieve by 2028, and requiring government systems to move to post-quantum cryptography by the early 2030s [21].

Washington has also begun acquiring equity stakes in the companies themselves, with the Commerce Department reported to be taking about $2 billion in stakes across nine quantum firms [22]. China is spending heavily as well, though in amounts that are difficult to confirm [20]. For an investor, this support has two sides. It can keep these companies alive through years of losses, but it can also push their share prices above what their results justify.

No single hardware design has prevailed, and that is the defining fact of the competition. To invest in a quantum company is to bet both on the team and on its chosen physics.

Architecture	Main trade-off	Status
Superconducting *(e.g. IBM, Google, Amazon)*	Fast gates, but weak connectivity and cryogenic cooling	Leading
Trapped ion *(e.g. IonQ, Quantinuum)*	Best accuracy, but slow, costly gates	Maturing
Neutral atom *(e.g. QuEra)*	Scales well, but slower and less mature	Fast rising
Photonic *(e.g. PsiQuantum)*	Room-temperature, but hard two-qubit gates	Early
Annealing *(e.g. D-Wave)*	Good for optimisation, but not general-purpose	Niche
Topological *(e.g. Microsoft)*	Error-resistant in theory, but unproven	Contested

Table 1: The main quantum hardware approaches: a simplified snapshot of their key trade-off and how developed each is today.

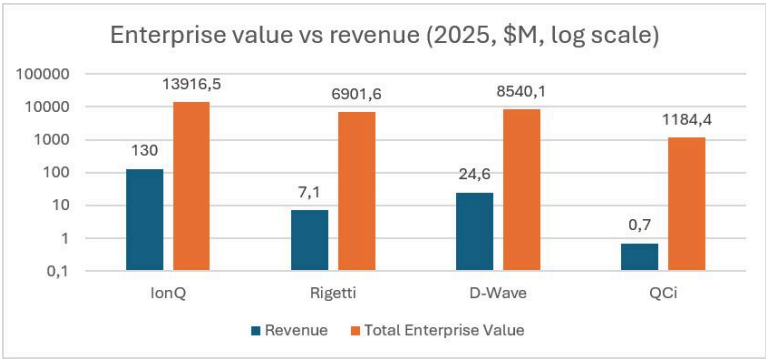


Figure 2: Enterprise value vs 2025 revenue (log scale: each gridline is 10× the one below). Source: Fiscal.ai.

Microsoft's topological approach, the Majorana line, stands apart: if the underlying physics holds, the qubits would resist errors by design, but as the table indicates the evidence remains disputed. Even within superconducting hardware the approaches diverge: Amazon's Ocelot chip uses cat qubits to suppress errors in the hardware itself, a different path from IBM's and Google's [23]. With no design clearly ahead, even Nvidia is hedging, having backed QuEra, Quantinuum and PsiQuantum in 2025 to cover the neutral-atom, trapped-ion and photonic approaches at once [24]. The lesson for an investor is plain: the field has not settled, and a poor choice of design can strand an otherwise capable company.

The investment case

The bull case is brief. If quantum computing becomes a core technology, its uses would reach across several large industries, and the first companies to get there could build leads that are hard to overturn as customers and software cluster around them. An effort this long can be sustained for years by well-funded governments and technology giants, as IBM's $10 billion commitment and Nvidia's investments across the field make clear [3][24]. Scarce expertise and strong patents could then keep competitors at a distance.

The bear case is equally brief and, at present, better supported by figures. Useful error-corrected machines may be a decade or two away [13]. The market forecasts are wide and originate with interested parties. Outside investors cannot easily verify a company's technical claims, as the dispute over Majorana shows [2]. And conventional computers may capture some of the expected applications first [7].

The valuations make the risk plain: as the chart shows, Rigetti's enterprise value was close to a thousand times its 2025 sales and D-Wave's around 350, against the thirty to fifty times that marked the peak of the dot-com leaders [25]. The shares are also extraordinarily fragile: in January 2025 they fell by up to 40% in a single day after Nvidia's chief executive said that genuinely useful quantum computers were 15 to 30 years away [26].

The disciplined response is to apply those three questions rather than react to the headlines: is progress measured in independently verified milestones or in press releases; are customers paying for a repeatable service or merely running trials; and can the company fund its plan without the repeated share issuance that erodes existing holders? One should then weigh how much success is already in the price, and whether the time horizon suits an investor who can tolerate high volatility.

These questions point to a range of options rather than a single decision. A large, diversified company such as IBM, Google, Microsoft or Amazon offers quantum computing as a small component within a profitable business. The pure plays, namely IonQ, Rigetti, D-Wave, Quantum Computing Inc. and now Quantinuum, offer concentrated exposure, with real potential and a real risk of failure: IonQ ended 2025 with billions in cash but modest revenue relative to its valuation, while Rigetti's full-year sales amounted to only a few million dollars [27]. Quantum can also be played across the value chain: cloud access, software and algorithms, enabling hardware such as lasers and cryogenics, and post-quantum security. Because quantum is still unproven, the lower-risk bet is on these layers, especially the suppliers of enabling hardware, who sell to the whole industry and earn even if no single machine ever works out.

Is quantum computing investable yet? The science is credible and the engineering is advancing, but the industry is not mature: no design has prevailed, no business model is proven, and steady revenue is rare. How closely it resembles a venture investment depends on the route chosen, not on the field as a whole. The signs to watch are clear: real progress in logical qubits towards machines such as IBM's planned 2029 system, a useful result that surpasses conventional computers on a problem that generates revenue, repeat commercial work rather than trials, and pure plays whose finances begin to resemble a business. Until then, the question is not how many qubits a company has, but what those qubits can do, how reliably, who will pay for the result, and how much capital the company will consume before it arrives.

Sources:

[1] https://news.microsoft.com/source/features/innovation/majorana-2-microsoft-discovery-agentic-ai/ [2] https://www.nature.com/articles/d41586-026-01788-y [3] https://newsroom.ibm.com/2026-06-02-ibm-commits-more-than-10-billion-to-quantum-computing,-funding-its-roadmap-from-todays-leading-systems-to-the-worlds-first-fault-tolerant-quantum-computers [4] https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026-a-commercial-tipping-point [5] https://thequantuminsider.com/2026/06/02/quantinuum-expands-ipo-as-valuation-climbs-above-14-billion/ [6] https://blog.google/innovation-and-ai/technology/research/quantum-echoes-willow-verifiable-quantum-advantage/ [7] https://arxiv.org/abs/2307.00523 [8] https://www.bcg.com/press/18july2024-quantum-computing-create-up-to-850-billion-of-economic-value-2040 [9] https://www.nature.com/articles/s41586-024-08449-y [10] https://azure.microsoft.com/en-us/blog/quantum/2024/11/19/microsoft-and-atom-computing-offer-a-commercial-quantum-machine-with-the-largest-number-of-entangled-logical-qubits-on-record/ [11] https://www.quera.com/press-releases/quera-computing-marks-record-2025-as-the-year-of-fault-tolerance-and-over-230m-of-new-capital-to-accelerate-industrial-deployment [12] https://www.ibm.com/quantum/blog/large-scale-ftqc [13] https://pubs.acs.org/doi/10.1021/acs.jctc.2c00574 [14] https://arxiv.org/abs/2505.15917 [15] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards [16] https://www.deloitte.com/nl/en/services/consulting-risk/perspectives/quantum-computers-and-the-bitcoin-blockchain.html [17] https://www.sec.gov/Archives/edgar/data/0001980994/000143774926006058/bit20251231_10k.htm [18] https://github.com/bitcoin/bips/blob/master/bip-0361.mediawiki [19] https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship [20] https://thequantuminsider.com/2026/03/26/leading-quantum-computing-countries/ [21] https://www.whitehouse.gov/fact-sheets/2026/06/fact-sheet-president-donald-j-trump-ushers-in-the-next-frontier-of-quantum-innovation/ [22] https://www.nbcnews.com/business/economy/trump-order-quantum-computer-rcna351237 [23] https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip [24] https://thequantuminsider.com/2025/09/13/how-is-nvidia-betting-on-quantum-a-look-at-nventures-quantum-investment-playbook-from-skepticism-to-strategic-stakes/ [25] Fiscal.ai (enterprise value ÷ FY2025 revenue) [26] https://www.cnbc.com/2025/01/08/quantum-stocks-like-rigetti-plunge-after-nvidias-huang-says-the-computers-are-15-to-30-years-away.html [27] https://www.datacenterdynamics.com/en/news/quantum-computing-earnings-q4-and-fy25-ionq-d-wave-rigetti-results/