

Global Banking & Securities

# How quantum computing could change financial services

Fully scaled quantum technology is still a way off, but some banks are already thinking ahead to the potential value.

*by Miklos Dietz, Nico Henke, Jared Moon, Jens Backes, Lorenzo Pautasso, and Zaheen Sadeque*



© Getty Images

**Many financial services activities**, from securities pricing to portfolio optimization, require the ability to assess a range of potential outcomes. To do this, banks use algorithms and models that calculate statistical probabilities. These are fairly effective but are not infallible, as was shown during the financial crisis a decade ago, when apparently low-probability events occurred more frequently than expected.

In a data-heavy world, ever-more powerful computers are essential to calculating probabilities accurately. With that in mind, several banks are turning to a new generation of processors that leverage the principles of quantum physics to crunch vast amounts of data at superfast speed. Google, a leader in the field, said in 2019 that its Sycamore quantum processor took a little more than three minutes to perform a task that would occupy a supercomputer for thousands of years. The experiment was subject to caveats but effectively demonstrated quantum computing's potential, which in relative terms is off the scale.

Financial institutions that can harness quantum computing are likely to see significant benefits. In particular, they will be able to more effectively analyze large or unstructured data sets. Sharper insights into these domains could help banks make better decisions and improve customer service, for example through timelier or more relevant offers (perhaps a mortgage based on browsing history). There are equally powerful use cases in capital markets, corporate finance, portfolio management, and encryption-related activities. In an increasingly commoditized environment, this can be a route to real competitive advantage. Quantum computers are particularly promising where algorithms are powered by live data streams, such as real-time equity prices, which carry a high level of random noise.

The impact of the COVID-19 pandemic has shown that accurate and timely assessment of risk remains a serious challenge for financial institutions. Even before the events of 2020, the last two decades have seen financial and economic crises that led to rapid changes

in how banks and other market participants assessed and priced risk of different asset classes. This led to the introduction of increasingly complex and real-time risk models powered by artificial intelligence but still based on classical computing.

The arrival of quantum computing is potentially game changing, but there is a way to go before the technology can be rolled out at scale. Financial institutions are only just starting to get access to the necessary hardware and to develop the quantum algorithms they will need. Still, a rising number of initiatives suggest a tipping point is on the horizon. For banks yet to engage, and particularly those that rely on computing power to generate competitive edge, the time to act is now.

## Back to the future

A short theoretical diversion can show how quantum computing represents a step change in computational performance. Quantum computing is based on quantum physics, which reveals the slightly bemusing fact that specific properties of particles can be in two states, or any combination of the two states, at the same time. Whereas traditional computers operate dualistic processing systems, based on 1 and 0s, quantum systems can simultaneously be 1 and 0, or a mixture of 1 and 0. This so-called "superposition" releases processing from binary constraints and enables exploration of immense computational possibilities.

The answers produced by quantum calculations are also different from their binary cousins. Like quantum physics, they are *probabilistic* rather than *deterministic*, meaning they can vary even when the input is the same. In practice, this means that the same calculation must be run multiple times to ensure its outputs converge toward a mean.

To obtain a quantum state that can be brought into superposition, a quantum computer works not with bits but with quantum bits (*qubits*), which can be engineered as atomic nuclei, electrons, or photons (Exhibit 1). Through

superposition, an amount of  $N$  qubits can express the same amount of information as  $2^N$  classical bits, although this informational richness is not accessible to us because the  $N$  qubits will “collapse” back to behave like  $N$  classical bits when measured. But before that, while still in their (unobserved) state of quantum superposition, 2 qubits can be in the same amount of states as 4 classical bits, 4 qubits the same as 16 bits, 16 qubits the same as 65,536 bits, and so on. A system of 300 qubits can reflect more states than there are atoms in the universe. A computer based on bits could never process that amount of information, which is why quantum computing represents a true “quantum leap” in terms of capability.

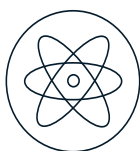
Another characteristic of quantum states is that qubits can become *entangled*, which means they are connected and that actions on one qubit impact the other, even if they are separated in

space—a phenomenon Albert Einstein described as “spooky action at a distance.” Quantum computers can entangle qubits by passing them through quantum logic gates. For example, a “CNOT” (conditional not) gate flips—or doesn’t flip—a qubit based on the state of another qubit.

Both superposition and entanglement are critical for the computational “speedup” associated with quantum computing. Without superposition, qubits would behave like classical bits, and would not be in the multiple states that allow quantum programmers to run the equivalent of many calculations at once. Without entanglement, the qubits would sit in superposition without generating additional insight by interacting. No calculation would take place because the state of each qubit would remain independent from the others. The key to creating business value from qubits is to manage superposition and entanglement effectively.

Exhibit 1

## **Qubits are the fundamental units of information processing in quantum computers.**



The idea of quantum computing is to switch from classical bits as information processing units to quantum bits or “qubits.” Qubits are governed by quantum mechanics—effects like superposition and entanglement play a large role in determining the efficacy of quantum calculations.



There are many different ways to physically realize qubits— from using trapped calcium ions to superconducting structures. In each case, quantum states are being manipulated to perform calculations.



Quantum algorithms can effectively tackle certain problems that cannot be solved with conventional computers in a reasonable amount of time. Managing qubit capabilities (superposition, entanglement) is key to creating business value with quantum computers.

Source: McKinsey

## An intermediate step

At the leading edge of the quantum revolution, companies such as IBM, Microsoft, and Google are building quantum computers that aim to do things that classical computers cannot do or could only do in thousands of years. However, the notion of “quantum supremacy”—that is, proof of a quantum computer solving a problem that a classic computer could not tackle in a reasonable amount of time—is predicated on assembling a sufficient number of qubits in a single machine. The world’s leading developers have got up to around 60 qubits, which is enough to put the world’s most powerful computers to the test but arguably not to outperform them. That was, until Google reported having achieved quantum supremacy for the problem of random number generation, using just 53 qubits assembled in their Sycamore processor.<sup>1</sup>

In spite of this milestone, no one has yet managed to scale quantum computers for them to be useful for practical applications. Some of the calculations relevant to the financial industry would require hundreds or thousands of qubits to resolve. Given the pace of development, however, the timescale for obtaining sufficient capacity is likely to be relatively short—perhaps five to ten years.

However, capacity is only half the story. Qubits are notoriously fickle. Even a tiny change in the environment, such as a heat fluctuation or radio wave, can upset their quantum state and force them back into a classical state in which speed-up evaporates. The more qubits are present, the more unstable the system becomes. Qubits also suffer from correlation decay, known as “decoherence.”

One route to stability is to keep quantum chips at sub-zero temperatures (in some cases 250 times colder than deep space) and in an isolated environment. However, there is no avoiding the fact that the hardware challenge is significant.

The world is still waiting for the first quantum processor with more than a hundred qubits that can operate in a coherent manner, that is, with a fidelity in excess of 99 percent.<sup>2</sup> But there is a theoretical intermediate step, which is the so-called quantum annealer. Quantum annealers focus on a single class of tasks, known as discrete optimization problems, which are based on a limited number of independent variables.

Among other things, an annealer may be used to execute hill climbing algorithms: an optimization approach that is analogous to exploring a range of mountains. In seeking the highest peak (or lowest valley), a classic algorithm measures each in turn. A quantum annealer explores all at once by “flooding” the landscape and raising the water level until only the highest sticks out. The good news for the financial industry is that a high number of essential algorithmic tasks are optimization problems; portfolio optimization is an example.<sup>3</sup>

## Who stands to benefit and how?

In assessing where quantum computing will have most utility, it’s useful to consider four capital markets industry archetypes: sellers, buyers, matchmakers (including trading platforms and brokers), and rule setters. Generally, sellers and matchmakers invest in IT to build capacity rather than address complexity. Buyers and rule setters, on the other hand, often require more complex models. Quant-driven hedge funds, for example, aim to profit through analytical complexity. This would make them a natural constituency for ultra-powerful processing. Large banks, which take on multiple roles in financial markets, are also significant early experimenters.

Quick wins for quantum computing are most likely in areas where artificial intelligence techniques such as machine learning have already improved traditional classification and forecasting. These typically involve time

---

<sup>1</sup> John Martinis, and Sergio Boixo, “Quantum Supremacy Using a Programmable Superconducting Processor,” Google AI Blog, October 23, 2019.

<sup>2</sup> Fidelity is a measure of the quantum computer’s action in real life against the theoretical action produced in code.

<sup>3</sup> The benefits of quantum annealing now exist only in theory. Its future utility will likely depend on the pace of development of fully-fledged quantum processors. It may be that if advancement is speedy, the interim annealer step will quickly become redundant.

series problems, which are often focused on large, unstructured data sets and where problems require live data streams as opposed to batch processing or one-time insight generation.

One unique characteristic of the logic gates in quantum computers is that they are reversible, which means that, unlike classical logic gates, they come with an undo button. In practical terms, this means they never lose information up to the point of measurement, when qubits revert to behaving like classical bits. This benefit can be useful in the area of explainability. An algorithm used to predict a loan default may determine whether individuals are granted mortgages and on what terms. However, if a customer's loan application is rejected, they may reasonably wish to understand why. In addition, the law in some cases requires a degree of explainability. In the United States, credit scores and credit actions are subject to the Equal Credit Opportunity Act, which compels lenders to provide specific reasons to borrowers for negative decisions.

In terms of the current state of the art, we see four key drivers of demand for quantum computing:

**Scarcity of computational resources:** Companies relying on computationally heavy models (e.g., hedge fund WorldQuant, which has more than 65 million machine learning models) employ a Darwinian system to allocate virtual computing capacity; if model X performs better than model Y, then model X gets more resources and model Y gets less. The cost of classical processing power, which rises exponentially with model complexity, is a bottleneck in this business model. This could be unlocked by the exponential speed-up delivered by qubits over classical bits.

**High-dimensional optimization problems:** Banks and asset managers optimize portfolios based on computationally intense models that process large sets of variables. Quantum computing could allow faster and more accurate decision-making,

for example determining an optimal investment portfolio mix.

**Combinatorial optimization problems:**

Combinatorial optimization seeks to improve an algorithm by using mathematical methods either to reduce the number of possible solutions or to make the search faster. This can be useful in areas such as algorithmic trading, for example helping players select the highest bandwidth path across a network.

**Limitations in cryptography:** Current cryptographic protocols rely on the fact that conventional computers cannot factor large numbers into their underlying prime factors. This would not be the case for quantum computers. Using a sequence of steps known as Shor's algorithm, they could at some stage deliver an exponential increase in speed of prime factorization and thus be able to "guess" the prime factors used in the encryption. On the other hand, quantum encryption would be sufficiently powerful to prevent intrusion by even the most powerful classical or quantum computers.

## What business lines will benefit most?

In late 2019, a Bank of America strategist said quantum computing would be "as revolutionary in the 2020s as smartphones were in the 2010s."<sup>4</sup> However, from a business line perspective, the most promising use cases are likely to be those that require highly complex and/or exceptionally fast models. In valuation, for example, the ability to speedily identify an optimal risk-adjusted portfolio is likely to create significant competitive advantage. For loan and bond portfolios, more precise estimates of credit exposures should lead to better optimization decisions. More broadly, capital allocation across a range of corporate finance activities can be improved by insights into the size and materiality of risks, while payments and transfers can be protected through better encryption.

---

<sup>4</sup>Chris Matthews, "Quantum computing will be the smartphone of the 2020s, says Bank of America strategist," MarketWatch.com, December 12, 2019.

Equity and FX trading offer significant possibilities, amid demand for ever-more accurate market risk and scenario calculations, and growing appreciation of the utility of raw computing power in smart routing and trade matching. Some large banks already expend large amounts of computational resources optimizing private interbank trading, suggesting it makes sense to seek an edge in this area.

Finally, sales, marketing, and distribution can benefit from sharper decision making, for example in relation to resource allocation and tailored services. This holds true for most organizations with large and diverse customer bases but especially for banks, which still spend a large proportion of their operating expenditure on branches and call centers.

As of now, the major Wall Street banks are leading the charge in the quantum realm. A Goldman Sachs researcher in January 2020 said quantum has the potential to become a critical technology.<sup>5</sup> Still, Goldman's efforts are at an early stage. In its early experiments, the bank found that Monte Carlo simulations, which require significant amounts of conventional computing power, cannot yet be parallelized on a quantum system. It therefore refocused on developing approaches to decrease the depth of quantum circuits required to do these calculations.

JPMorgan and Citigroup, meanwhile, have set up quantum computing initiatives and even bought stakes in computing start-ups.<sup>6</sup> JPMorgan also experimented with Honeywell's quantum computer in an effort to ease mathematical operations that involve Fibonacci numbers.<sup>7</sup>

In late 2019, Wells Fargo joined the IBM Q program, a community of companies, startups, academic institutions, and research labs working to explore practical applications.<sup>8</sup>

European banks are also exploring quantum computing opportunities. BBVA has formed a partnership to explore portfolio optimization and more efficient Monte Carlo modelling.<sup>9</sup> Also in Spain, Caixa Bank is running a trial hybrid framework of quantum and conventional computing with the aim of better classifying credit risk profiles.<sup>10</sup> In mid-2020, UK's Standard Chartered revealed its exploration of quantum computing applications, such as portfolio simulation, in collaboration with US-based Universities Space Research Association.<sup>11</sup>

These initiatives make sense because they allow financial firms to test quantum algorithms on simulators or the cloud without acquiring full-scale quantum computers. This appears to be a sensible strategy as long as quantum computers remain subcritical for practical applications and there is no dominant design for scaling quantum capabilities.

## Preparing for a quantum future: Three principles

Many financial industry participants rely on computing power to improve decision making and serve customers better. Over the next few years, quantum computing is likely to supercharge these activities. To be sure, this will be a long road, and most banks are taking their first steps. However, there are three actions for banks to consider now as they begin the journey:

- **Build research partnerships and IP.** There are opportunities to partner with quantum developers—Amazon, D-Wave, IBM, Google, Microsoft, Rigetti, and Xanadu are among the companies in the arena. These specialists have the hardware and expertise to help organizations develop their capabilities.
- **Create a small team focused on quantum computing.** Partnerships are not one-way streets,

<sup>5</sup>Richard Waters, "Wall Street banks ramp up research into quantum finance," *Financial Times*, January 6, 2020.

<sup>6</sup>Sophia Chen, "Banks are betting that quantum computing can find them an investment edge," *Protocol.com*, May, 4, 2020.

<sup>7</sup>Matt Swayne, "JP Morgan Chase Unleashes Honeywell's Quantum Computer on Tough Fintech Problems," *thequantumdaily.com*, July 2, 2020.

<sup>8</sup>Penny Crossman, "Behind Wells Fargo's foray into quantum computing," *americanbanker.com*, November 25, 2020.

<sup>9</sup>"BBVA and Multiverse showcase how quantum computing could help optimize investment portfolio management," *bbva.com*, August 26, 2020.

<sup>10</sup>"CaixaBank becomes the first Spanish bank to develop risk classification model using quantum computing," *caixabank.com*, April 16, 2020.

<sup>11</sup>Karl Flinders, "Standard Chartered latest bank to explore quantum computing," *July 14, 2020*.

## Expert view: An interview with Visweswaran Vish R, founder and CEO of CogniFrame

**McKinsey:** What kinds of financial industry problems can quantum computing solve?

**Visweswaran Vish R:** Quantum computing is excellent for solving intractable and/or computationally intensive non-convex and stochastic optimization problems. Non-convexity essentially manifests itself when you start to peel away the constraints of an optimization problem. Sources of non-convexity could include combinatorial/discrete optimization, the choice of models (risk metrics, utility functions, objective functions such as VaR, and trading trajectory), the market cost and irrationality embedded in data, and nonlinear/inequality constraints.

**McKinsey:** Are there specific use cases you can highlight?

**Visweswaran Vish R:** Pure classical optimization methods have started to hit a ceiling, which means that optimizing for higher return on assets using quantum is an imperative, in our view. Typical use cases include asset-liability management (active balance-sheet management), collateral optimization, calculations relating to Solvency II, capital adequacy and Basel IV, portfolio optimization, and government bond and forex management. Insurers, central banks, pension funds, and asset managers can benefit.

**McKinsey:** How do you integrate classical computing with quantum technologies?

**Visweswaran Vish R:** Not everything is “quantumizable.” Essentially, you should pick problems that you can handle at scale using current quantum technology, which can also deliver the greatest impact value. The quantum hardware focuses on the “hard” optimization part of the workflow while classical computers take care of the “easier” parts including data manipulation, modeling, simulation, and analysis.

**McKinsey:** What is the range of finance industry R&D budgets typically allocated to quantum computing?

**Visweswaran Vish R:** The very large institutions have started to look at this closely. A few have hired quantum specialists to start understanding the space and applications, and they are beginning to make investments in R&D. I expect the big jump will be over the next 12 to 18 months.

and quantum providers are also keen to learn from financial industry players about their algorithms and requirements. Ensure you bring something to the party.

- *Scout for potential investments/joint ventures.* The challenges of building quantum systems mean that joint ventures are likely to be common. These may take the form of working

with a cloud offering, or combining hard optimization problem-solving via quantum solutions with classical computing for data manipulation, simulation, and analysis. The latter might be achieved through a vendor platform that can smooth the adoption process and assist in running proofs of concept.



Early movers are likely to have an advantage. However, in all cases, a practical first step is to rewrite internal algorithms in quantum language, which will lay the groundwork for meaningful investment.



Some in the banking industry believe that quantum computing is more science fiction than fact, and that computational power isn't

a key differentiator for the business model. And there is, of course, more to serving clients than computational speed and agility. Still, quantum computing increasingly appears to be a game changer in tackling complex or intractable problems, particularly in the optimization area. It is only a matter of time before quantum solutions enter the mainstream, which means the window for getting up to speed and gaining competitive advantage will not be open for long.

**Jens Backes** is a senior solution leader and associate partner in McKinsey's Barcelona office, **Miklos Dietz** is a senior partner in the Vancouver office, **Nicolaus Henke** and **Jared Moon** are senior partners in the London office, **Lorenzo Pautasso** is a consultant in the Munich office, and **Zaheen Sadeque** is an associate in the Toronto office.

Copyright © 2020 McKinsey & Company. All rights reserved.