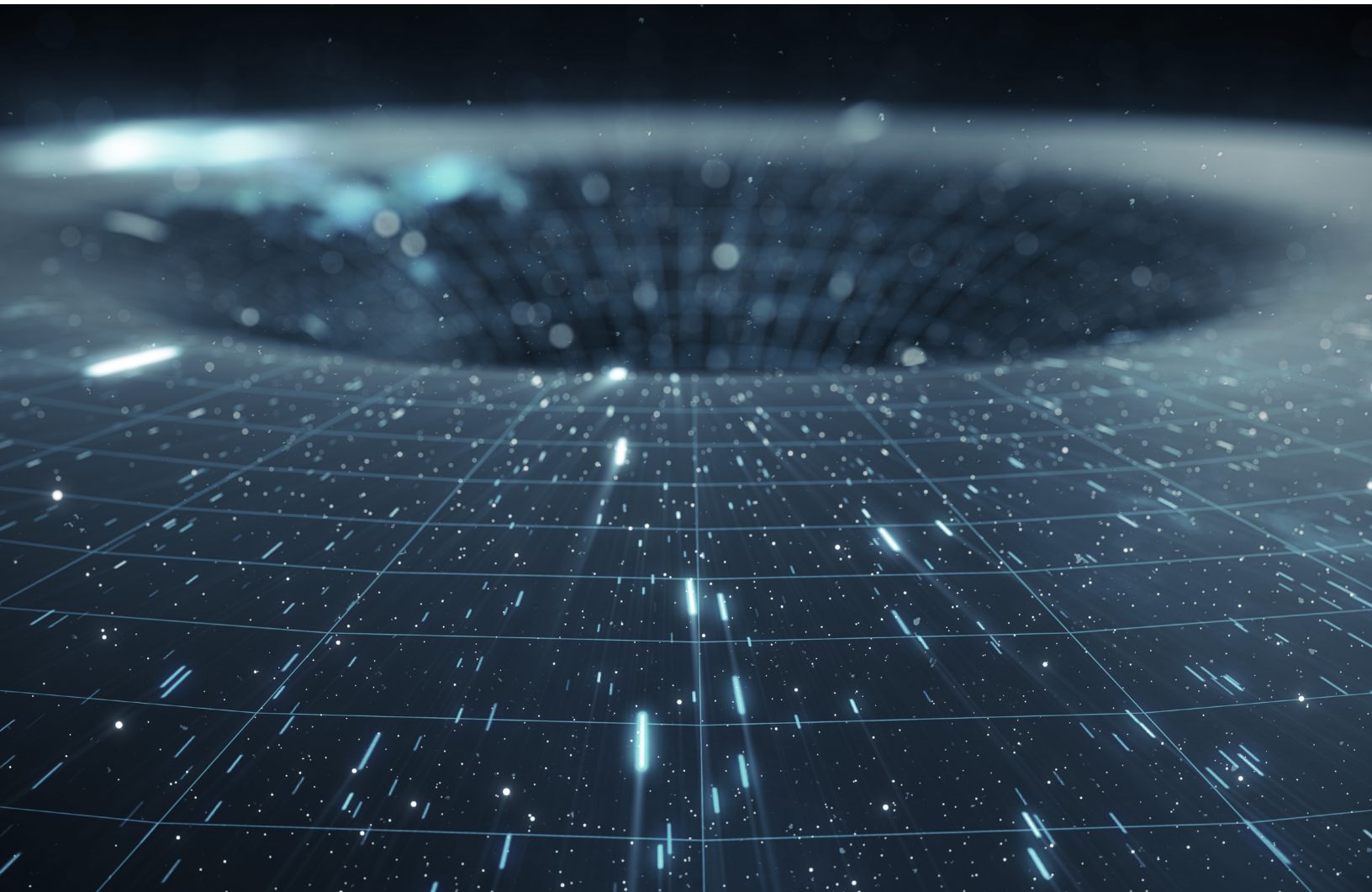
CAPCO

QUANTUM COMPUTING IN FINANCIAL SERVICES

WHAT YOU NEED TO KNOW



For non-physicists, Quantum Technology sounds like something out of a science fiction movie - sub-atomic particles that can operate in multiple states simultaneously. So, what would this have to do with financial services? Why should we care?

Kevin Marshall, Principal Consultant, Lead Data Scientist at Capco, and Ph.D. in Quantum Physics, works closely with our clients in Financial Services to solve business challenges and drive opportunities. Kevin will help us understand this technology and what leaders in financial services need to know.

LET'S START WITH THE BASICS:

Key terms[1]:

- Quantum computing is essentially harnessing and exploiting the amazing laws of quantum mechanics to process information.
- A traditional computer uses long strings of 'bits,' which encode either a zero or a one. A quantum computer, on the other hand, uses quantum bits, or qubits
- A qubit is a quantum system that encodes the zero and the one into two distinguishable quantum states. But, because qubits behave quantumly, we can capitalize on the phenomena of 'superposition' and 'entanglement.'

Superposition is a qubit's ability to simultaneously operate in multiple states, while entanglement refers to a uniquely non-classical correlation between particles. These phenomena contribute to why Quantum Computers can compute the solutions to certain calculations much quicker than traditional computers. Alas, building a universal fault-tolerant quantum computer that is large enough to perform useful computations remains a difficult challenge. However, progress continues to be made, and the field has been pushed forward by academia and industry.

1. https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101

THE ASPIRATIONS OF QUANTUM COMPUTING

		CLASSICAL	QUANTUM
CHARACTERISTICS	Data	Information is encoded in 'bits' as sequences of 0's and 1's	Information is stored in qubits which can have states of 0's and 1's, or a combination of 0's and 1's governed by quantum physics
	Speed	Certain problems, with large human impact would take millions of years	Opens the door to solving these problems in minutes or even seconds
	Limitations	We are reaching the end of Moore's law and starting to run up against fundamental limitations	An entire new regime to explore that doesn't play by the same rules as classical computer
OUTCOMES	Improved Customer Experience	Machine learning models for fraud detection, relevant product recommendations and financial advice are limited by complexity	Ability to understand and model complex systems in a short amount of time enabling a more rapid innovation cycle
	Greater Effectiveness	Simplifying assumptions are made to solve problems ranging from derivative pricing to risk management	Improve effectiveness of decisions by capturing real-world complexity and allowing FIs to better utilize their resources
	Faster Response	Ability to understand complex systems (e.g., demand forecasting, pricing, etc.) is often limited to daily batch processing	Enable real-time updates by leveraging streaming data and faster quantum algorithms

NOW LET'S CONNECT THIS BACK TO FINANCIAL SERVICES.

Consistently on the top five list of priorities for financial services executives globally are data and data protection. Like most other enterprises that deal with large amounts of data, banks rely on technologies that encrypt and protect their data. Classic encryption methods leverage keys that are so large that traditional computers cannot decode them; most of these algorithms derive their security from the 'difficulty' of a particular mathematical problem. However, many encryption algorithms in-use today are susceptible to being broken by a quantum computer of sufficient size as efficient quantum algorithms exist for solving the underlying problems where there are no known efficient classical algorithms.

How real is this risk? NIST, the National Institute of Standards and Technology, from whom most financial institutions model their cyber risk frameworks, is taking this very seriously. With a view that sufficiently large quantum computers will be built to break essentially all public-key schemes currently in use within the next twenty or so years. NIST has published a series of reports and initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.[2]

IBM recently announced the marriage of their pioneering quantum capabilities with their cloud offering. IBM is now offering quantum-safe cryptography support for key management and application transactions in their cloud, providing a holistic quantum-safe cryptography approach to securing data available today.[3] While this may prove to be a differentiator as FI's make decisions on their cloud strategies, it will also require an enhanced understanding of the impacts of this technology for use today.

Future-Proofing with Quantum Resistant Algorithms

The implication of the advent of quantum computing on cryptography is not just that certain classical algorithms will not be safe anymore. Patient adversaries that can collect sensitive data today, encrypted with a susceptible algorithm, would be able to sit on the vault until they could acquire a large enough quantum computer, perhaps decades later, and then use it to break through the lock. This form of 'harvest and decrypt' scheme is why the industry needs to adequately prepare ahead of time.

How should FI's Leverage the NIST Outputs

NIST has a long-tenured history of providing guidance and standards on the adoption and use of cryptographic algorithms. It should not surprise that the industry will be watching closely as they look to provide transparent leadership in establishing quantum-resistant public-key cryptography schemes. The learnings from the process and standards developed to evaluate quantum-resistant public-key cryptographic algorithms will likely be leveraged to inform future frameworks.

2. https://csrc.nist.gov/projects/post-quantum-cryptography
3. IBM Cloud Delivers Quantum-Safe Cryptography and Hyper Protect Crypto Services to Help Protect Data in the Hybrid Era - Nov 30, 2020

OUTSIDE OF QUANTUM CRYPTOLOGY, WHAT ARE OTHER APPLICATIONS?

Quantum computers may tackle problems significantly faster, which address current challenges within Financial Services, by leveraging novel algorithms. Many banks have stood up Quantum POC teams exploring various ways Quantum Computing can be applied to Financial Services. For example,

- **Quantum Monte Carlo:** Canadian FIs, BMO and Scotiabank have partnered with a quantum computing company, Xanadu, to conduct a POC that applies this technology to the algorithms typically used for derivatives pricing. As part of the proof-of-concept project, Xanadu built a software suite to simulate quantum Monte Carlo on various trading products. This allows for benchmarking of the quantum speedup using conventional high-performance computers.[4]

- **Investment Portfolio Optimization:** Spanish Bank BBVA, working with their partner Multiverse, assess if the use of quantum technologies could help with defining the optimal path when configuring portfolios dynamically. The idea was to determine the optimal trading path for an investment portfolio consisting of 52 assets, using actual market price data corresponding with an eight-year timeframe. Processing this amount of data would have taken a normal computer using conventional algorithms about two days but using quantum algorithms cut this to seconds.[5]

- **Settlement Efficiency:** Barclays has been investing in quantum technology in collaboration with IBM, for the past three years with one of their earliest POCs related to the settlement of batches of securities transactions.[6]

- **Data Traffic Security:** European bank ABN Amro is collaborating with partners to prove that the circle of optimally secured data traffic can be encrypted using an advanced Quantum Key Distribution system that works via fiber optics and air. The goal is to guarantee the security of online and mobile banking, now and in the future.[7]

- **Customer Credit Risk:** Spain's CaixaBank has developed a hybrid computing framework — which combines quantum computing and conventional computing in different phases of the calculation process — to classify credit risk profiles. With this project, the institution is making improvements in risk scenario simulations and machine learning, underpinning increasingly complex algorithms that require large quantities of data to learn while also progressing its analysis of quantum computing applications.[8]

4. https://www.newswire.ca/news-releases/bmo-financial-group-and-scotiabank-partner-with-xanadu-on-quantum-computing-speedups-for-trading-products-866739711.html
5. https://www.finextra.com/newsarticle/36468/bbva-trials-quantum-computing-to-optimise-investment-portfolio-management
6. https://home.barclays/who-we-are/innovation/quantum-computing/
7. https://www.abnamro.com/en/newsroom/newsarticles/2019/abn-amro-investing-in-quantum-technology.html
8. https://www.caixabank.com/comunicacion/noticia/caixabank-becomes-the-first-spanish-bank-to-develop-risk-classification-model-using-quantum-computing_en.html?id=42234

How do Financial Institutions Get Started with their Quantum Strategy

Be Proactive: Although full-scale quantum computers are still years away, the industry should remain proactive in preparing for the implications of this paradigm-shifting technology. Closely following NIST and other trusted cryptography authorities' advice will aid to ensure that sensitive data remains protected even many years later.

Platforms for Exploration: Increasingly, there are opportunities to explore this space without building your own lab. For example, AWS has partnered with several hardware providers to enable experimentation with quantum computing through AWS Braket.[9] Similar to how the cloud has enabled Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), Quantum is expected to become accessible similarly and has not been so creatively dubbed, Quantum as a Service (QaaS).

Learn from the Implementation of AI: As we have learned through the adoption of Machine Learning and AI, the use case and access to data are key. FIs wasted capital investing in AI for use cases that could have as easily been solved through simpler approaches or lacked sufficient value because of the draw towards "shiny objects." While the use cases for Quantum are only starting to be imagined for financial services, keeping this pragmatic lesson in mind is important to avoid expectations exceeding value and operational pitfalls.

IS THIS WORTH THE FOCUS AND ATTENTION NOW?

While it is still widely believed that experts will need 10-20 or more years to solve for the engineering challenges associated with quantum computing and take the technology mainstream, many FIs are investing in technologies now that will have a ten or more year lifespan that is likely to overlap with the implementation of quantum standards and technology.[10] As noted in IBM's recent announcement, quantum innovation is already impacting the cloud technologies used today. Developing a quantum strategy will be key for all FI's over the next three years in order to future proof their investments, data security and maintain pace with innovative players in the industry.

For more information, please reach out to Kevin Marshall and Joanna Lewis at Capco.

9. https://aws.amazon.com/braket/
10. https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

AUTHORS

Joanna Lewis,
Partner, Capco

Kevin Marshall,
Ph.D. (Quantum Optics, Quantum Information),
Principal Consultant/Lead Data Scientist, Capco

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO

JN_2750