Microsoft

Quantum impact: **Financial services**

http://microsoft.com/quantum

http://microsoft.com/en-us/research/project/post-quantum-cryptography/

Quantum impact: Financial services

Technology has always played an important role in the financial sector, beginning with the telegraph—which enabled rapid transmission of information—to credit cards, ATMs, and mobile payments. However, even with significant advancements in computing power, we are approaching the limits of what classical computing can predict or model. There are still many seemingly intractable problems that are waiting to be solved by mathematicians, programmers, and economists. Rapidly changing geopolitical situations, cyber security breaches, new and more stringent regulations, and the increase of data, all pose problems that are often unsolvable, even on today's most powerful supercomputers.

Quantum computing, with its ability to solve remarkably complex problems, is expected to answer some of the most challenging questions in the financial services industry. The financial sector is powered by data, with millions of decisions being made every day across all customer segments. Quantum computing is expected to be a strong driver for innovations, ultimately revolutionizing trading, credit scoring, underwriting, risk management and cybersecurity.

The promise of quantum

Quantum computing makes use of wave-like properties of nature to encode information in qubits that can process highly complex calculations more quickly. Where current computers would require billions of years to solve the world's most challenging problems, with the right algorithm, a scaled quantum computer could find a solution in weeks, days, or hours.

When designed to scale, quantum systems will have capabilities that exceed our most powerful supercomputers. As the global community of quantum researchers, scientists, engineers, and business leaders continue to collaborate to advance the quantum ecosystem, we expect to see quantum impact accelerate across every industry.

From bits to qubits

The quantum bit, or qubit, is the basic unit of quantum information. Whereas a classical bit holds a single binary value, 0 or 1, a qubit can be in a "superposition" of both values at the same time. This enables quantum mechanical effects such as interference, tunneling, and entanglement, which in turn empower quantum algorithms for faster searching, better optimization, and greater security. When multiple qubits are connected, these properties can deliver significantly more processing power than the same number of classical bits. For instance, four bits is enough for a classical computer to represent any number between 0 and 15. But four qubits is enough for a quantum computer to represent every number between 0 and 15 at the same time.

Quantum-inspired solutions

Emulating these quantum effects on classical computers has led to the development of new types of quantum solutions that run on classical hardware, also called quantum-inspired algorithms.[1] These algorithms allow us to exploit some of the advantages of quantum computing approaches today on classical hardware, providing a speedup over traditional approaches. Using quantum solutions on classical hardware also prepares us for the future of quantum optimization on actual quantum hardware.

Quantum use cases for financial services

Quantum computing promises faster and more accurate computations of more complex problems than today's classical computing. Quantum methods are well-suited for many use cases in the financial industry.

Portfolio management

Optimization scenarios are at the core of a multitude of financial problems. Portfolio managers, for instance, typically want to simulate all investment options to validate risk when estimating expected returns. Rebalancing an investment portfolio to keep pace with market movements is significantly constrained by computational limitations and transaction costs. Quantum technology may help cut through the complexity of today's trading environments and its combinatorial optimization capabilities may enable investment managers to improve portfolio diversification and rebalance portfolio investments in order to more quickly respond to market conditions.

Risk analysis—capital markets

Financial institutions must be able to accurately manage and compute risk for capital allocation, regulatory stress testing, and position hedging; protecting losses due to unforeseen events is something banks and insurance companies grapple with on a daily basis. Monte Carlo is the primary method for analyzing risk but is hampered by the increasing scale and complexity of models on classical computers. While financial institutions regularly model for 'Black Swan' events, like economic crashes, many organizations have had to completely redesign their models with the events of the COVID-19 pandemic. Quantum promises to provide a greater range of options in a shorter period of time, allowing institutions to better understand risk and prepare for unforeseen events.

Catastrophic risk modeling—insurance

Actuarial and risk modeling are resource-intensive calculations that insurance carriers run to help them identify risk, price insurance policies, and ensure that they have adequate levels of reserves. The reserving levels are especially important to the industry as they not only ensure the insurance carrier can meet its obligations or cover its liabilities, but financial services regulators set and monitor reserves on a regular basis to ensure companies are carrying adequate funds in case of an emergency. After the global financial crisis, regulators have made these reserving or liquidity requirements even more stringent. With initiatives such as Solvency II and new IFRS rules, insurers are being required to run ever-more complex and granular models at increased frequencies. As these exercises continue to move closer towards near-real time, quantum may be able to speed calculations and provide more accurate results.

Encryption and post-quantum cryptography

The same quantum computing power that will unlock solutions to complex challenges also threatens today's most sophisticated cryptography. Since Peter Shor of AT&T Bell Laboratories first published an efficient quantum algorithm for factoring in 1994, we have known that when a general-purpose quantum computer of sufficient size is built, then all our commonly-used public-key cryptographic algorithms will no longer be secure. A quantum computer with enough stable qubits to use Shor's algorithm to break today's public-key cryptography is still unavailable, but the risk is on the horizon. Working with industry and academic partners around the world, our goal is to develop new cryptographic algorithms that are resistant to attacks by quantum computers, and then to create new cryptographic standards for broad uses like online banking, secured communications, and mobile wallets.

Monte Carlo simulation

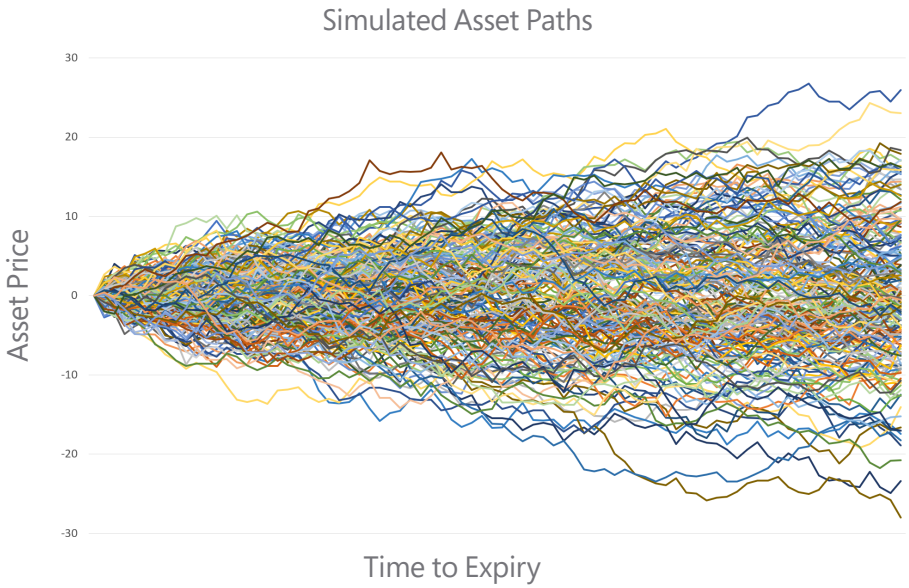
The Monte Carlo method—named after the famed casino in Monaco—is a forecast modeling technique, used to assess the likelihood of certain outcomes. Just as randomness is part of a game of chance like roulette or dice, Monte Carlo simulations account for uncertainty and randomness in complex systems.

Instead of estimating a single outcome, Monte Carlo simulations construct probability distributions over many possible outcomes, and where it really shines is in dealing with extremely large or complex systems.

In finance, the approach is typically used to simulate the effect of uncertainties affecting the financial object in question, which could be a stock, a portfolio, or an option. This makes Monte Carlo methods useful for portfolio evaluation, planning, risk evaluation, and derivatives pricing.

Monte Carlo techniques, being inherently random, are subject to error and in many financial scenarios, the number of simulations needed to achieve required confidence is very large. Quantum algorithms can improve these computations since quantum computers can run multiple scenarios simultaneously, and through quantum interference reduce the error in simulation.

By emulating these quantum effects on classical computers, we can take advantage of quantum computing approaches to design faster Monte Carlo sampling strategies, today.



Case study:

Quantifying risk with Willis Towers Watson

Willis Towers Watson

Willis Towers Watson, a leading global advisory, brokering and solutions company, has long used complex mathematical models to deliver great results for clients and turn risk into growth. However, some problems are still so challenging that they remain intractable with even the most advanced contemporary computational solutions.

Because of that, Willis Towers Watson has partnered with Microsoft to explore ways that quantum computing might assist the firm with its work in the areas of insurance, financial services, and investing.

"Current modelling techniques to quantify risk require a huge amount of computing power, using thousands of computers over many hours," says Willis Towers Watson CEO John Haley. "Quantum computing offers us the chance to look at our clients' problems in a different way. By focusing on how we would model the problems on quantum computers when they become available at scale, we are able to work with Microsoft to redefine the problems and speed up our solutions on existing hardware."

Quantum-inspired solutions harness the power of quantum physics to solve hard computational problems on classical hardware, today. Using these techniques, Microsoft is already able to gain orders of magnitude of performance acceleration in Azure. Once quantum computers become available at scale, even greater acceleration is possible.

As the development of the quantum computer progresses, customers like Willis Towers Watson will have access to a diverse set of quantum solutions, software, and hardware in Azure Quantum for the most complete, end-to-end quantum programming.

While there is still much work to be done, Willis Towers Watson and Microsoft are excited to see just how the quantum solutions of today and tomorrow will help transform the way financial industries improve risk management.

Preparing for a post-quantum world

Even though a large-scale quantum computer capable of running Shor's algorithm is not expected in the near term, the future availability of quantum computers at that scale are a threat to information we wish to protect with encryption today. Whenever we encrypt and send sensitive information over a public network (like the internet), we must assume that adversaries are recording that encrypted traffic for future decryption when sufficiently large quantum computers are available. This attack—record now, exploit later—means that we have to take steps today to secure sensitive information against the future quantum threat.

In response, the US National Institute of Standards and Technology (NIST) has begun the process of standardizing new public-key cryptographic algorithms that cannot be attacked efficiently even with the aid of a quantum computer. With participants from around the globe, this project's goal is to identify new cryptographic algorithms that are resistant to attacks by quantum methods and then standardize them for broad use. NIST's initial call for proposals attracted sixty-nine total submissions from around the world for key exchange and digital signature algorithms, including four proposals co-submitted by Microsoft Research. In January 2019, NIST selected twenty-six of those proposals to move forward to Round 2 of the selection process,[2] and in July 2020 selected 7 finalists and 8 alternates, including three Microsoft Research co-submissions.

It will be several more years before NIST finishes its process of selecting and standardizing new post-quantum algorithms. In the meantime, we must get to work today to begin protecting our customers and their data from future breaches. We know it will take time to migrate all of today's existing services and applications to new postquantum public-key algorithms—replacing cryptographic algorithms in widely deployed systems can take years— and we are committed to search for a solution that can provide protection while that work is ongoing.

Case study:
Project Natick

Project Natick[3] is a full-scale, fully operational datacenter module, installed underwater in the North Sea, off the Scottish coast. Microsoft Research has taken some of the traffic traveling between the data center and Microsoft headquarters in Redmond, Washington, and secured that traffic with an encrypted network tunnel protected with postquantum cryptography. While tunneling can certainly be tested in dry environments, by putting this technology to the test under more difficult circumstances[4] we have a good representation of what an actual data center customer experience would look like, under stress.
The Natick pressure vessel contains several racks of servers, all connected via a network inside the vessel. This network is then connected to the Microsoft global network through a set of underwater fiberoptic cables that connect to the facility on shore.

One of the servers that we call our "router node" runs our modified version of OpenVPN.[5] The router node connects to another server in Redmond to establish a post-quantum crypto-encrypted tunnel between the two sites.

Each router node runs Microsoft Research's modified version of OpenVPN in a virtual machine, and the session key for the data encryption is negotiated using a hybrid key exchange: a classical key exchange algorithm combined with a post-quantum key exchange algorithm. This hybrid key exchange incorporates the time-tested security of the classical algorithm against conventional attackers with the quantum security of the post-quantum algorithm. With a configuration change, we can use any of the key exchange algorithms supported by OQS's OpenSSL.[6]

We have measured bandwidth results that are consistent with running an unmodified version of OpenVPN over the same link using only classical cryptography. During tunnel operation, latency over the tunnel is comparable to the latency of the underlying connection. Variance between round-trip ping times is consistently less than 1 millisecond over a link with a typical round-trip ping time of 180 milliseconds.

As Karen Easterbrook, Senior Principal PM Manager at Microsoft Research says, "If we can get this to work underwater, then we can get this to work anywhere. We want post-quantum cryptography to be running on every link between every Microsoft datacenter and ultimately between every Microsoft datacenter and every Microsoft customer. And this is a necessary first step toward being able to make that happen."

Azure Quantum

Quantum computing applies the properties of quantum physics to process information. Where current computers would require billions of years to solve some of the world's most challenging problems, a scaled quantum computer may find a solution in weeks, days, or hours. Azure Quantum is an open ecosystem of quantum partners and technologies. Building on decades of quantum research and scalable enterprise cloud offerings, it is a complete solution that gives you the freedom to create your own path to scalable quantum computing.

Azure Quantum is also your entry point to integrate quantum inspired optimization running on classical Azure hardware for immediate results. Through a familiar Azure environment, you'll have access to all the tools and resources you need to quickly ramp up on your journey to a quantum future and have an impact with quantum technology today.

An open ecosystem, enabling you to access diverse quantum software, hardware, and solutions from Microsoft and our partners.

A trusted, scalable, and secure platform that will continue to adapt to our rapidly evolving quantum future.

Quantum impact today, with pre-built solutions that run on classical and accelerated compute resources (also referred to as optimization solutions).

Get ready for your Azure Quantum experience with the Quantum Development Kit

The Quantum development kit is an open-source development kit to develop quantum applications and solve optimization problems. It includes the high-level quantum programming language Q#, a set of libraries, simulators, support for Q# in environments like Visual Studio Code and Jupyter Notebooks, and interoperability with Python or .NET languages.

As quantum systems evolve, your code endures.

Learn more at https://azure.com/quantum

Prepare your organization

Tackling the world's toughest challenges requires computational power that exceeds that of today's most powerful computers. Where classical computing may take a billion years to address some of these challenging problems, quantum computing has the power to solve these problems in weeks, days, or even hours.

1. Find relevant use cases for your business

See how organizations like yours are using quantum solutions. The Microsoft Quantum website has case studies that show how companies are using quantum technology for their businesses, today.

2. Build a quantum workforce

Ensure your organization is ready for quantum computing by assembling a quantum task force comprised of C-suite sponsors, business unit managers, and developers. Augment over time with quantum specialists and mathematicians that are familiar with applications and algorithms that are most relevant for your business.

3. Join the Microsoft Quantum Enterprise Acceleration Program

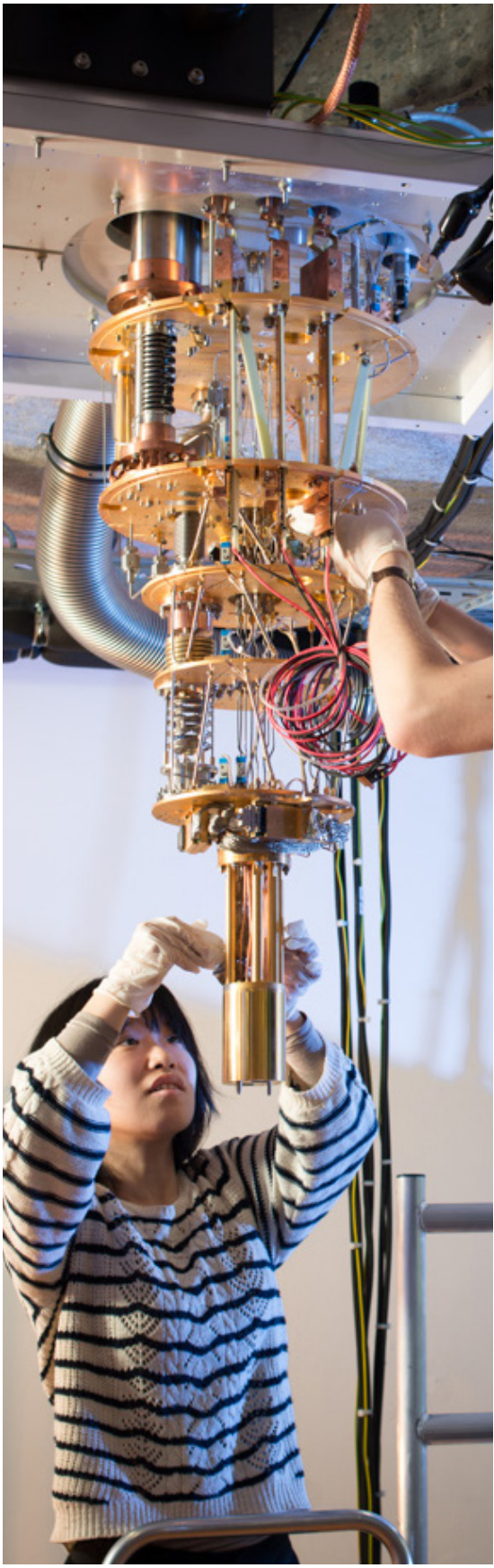
Microsoft offers the Enterprise Acceleration Program to develop high-value, custom quantum solutions alongside the world's best quantum talent. This is a paid offering for Microsoft's most advanced enterprise customers to accelerate quantum adoption through direct collaboration with the Quantum team. Contact us to get started.

4. Experience impact today through Azure Quantum

Microsoft is building a full-stack quantum ecosystem, delivered through the power and scale of Azure's global cloud services platform. Apply to become an early adopter for preview access to Azure Quantum.

5. Plan for post-quantum cryptography

The best way to start preparing is to ensure that all current and future systems have cryptographic agility – the ability to be easily reconfigured to add quantum-resistant algorithms. As you begin to plan for this transition, plan pilots of post-quantum cryptography to better understand implications for your IT infrastructure. Please download, pilot, and provide feedback on Microsoft Research's libraries and protocol integrations.[7] You can talk to us at msrsc@microsoft.com.



Authors

Dr. Brad Lackey

Senior Principal Researcher, Microsoft

Brad Lackey is a Quantum Solutions Architect, specializing in creating quantum and quantum-inspired algorithms to solve real-world industrial problems. He also does foundational research in quantum information theory and quantum programming languages.

Daragh Morrissey

Senior Principal Researcher, Microsoft

Daragh Morrissey is a Director for Artificial Intelligence in the Microsoft Worldwide Financial Services team. His areas of focus are driving successful adoption of Artificial Intelligence and enabling Microsoft customers to innovate in partnership with the Microsoft Fintech ecosystem.

He has presented at Industry events such as FinDEVr, Americas FinTech Conference, SIBOS, FinTech Montreal, and global Microsoft events (Inspire, Ready, and Envision). He is a Certified IT Architect Professional the International Association of Software Architects (IASA).

Karen Easterbrook

Senior Principal PM Manager at Microsoft

Karen Easterbrook is a Senior Principal PM Manager in the Security and Cryptography team in Microsoft Research. She has worked on applied research teams at Microsoft for over twelve years, first on the "Venice" Mesh Networking incubation, a hardware project and then on a variety of security and cryptography projects including searchable encryption, homomorphic encryption, various ECC projects, and most recently post-quantum cryptography.

References

1. S. Mandrà, Z. Zhu, W. Wang, A. Perdomo-Ortiz, and H. G. Katzgraber, "Strengths and weaknesses of weak-strong cluster problems: A detailed overview of state-of-the-art classical heuristics versus quantum approaches," Phys. Rev. A, vol. 94, p. 22337, 2016

2. NIST's Post-Quantum Cryptography Program Enters 'Selection Round:' https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

3. Project Natick: https://natick.research.microsoft.com

4. Post-Quantum Crypto Tunnel to the Underwater Datacenter: https://www.microsoft.com/en-us/research/project/post-quantum-crypto-tunnel-to-the-underwater-datacenter/

5. Post-quantum Crypto and VPNs: https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn/

6. Open-quantum-safe/openssl, supported algorithms: https://github.com/open-quantum-safe/openssl#supported-algorithms

7. Cryptography in the era of quantum computers: https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/