# QUANTUM COMPUTING: FUTURE-PROOFING FINANCIAL SERVICES

Financial institutions are increasingly under pressure to make high-stakes decisions in real time while taking on the least possible risk. As financial products become increasingly complex, the requirement for more powerful computing arises. Quantum computers are finally on the verge of taking up the challenge.

Infosys | Knowledge Institute

The financial services industry has used mathematical models and classical computing algorithms to manage business risks for decades. However, those systems weren't always fail-safe and have inaccurately predicted business risks several times, most notably during the 2008 subprime mortgage crisis.[1] Many financial services problems are not completely solvable by traditional computers in a realistic time frame. These are called NP* problems, which include problems like portfolio optimization, risk estimation, and financial market predictions. All these problems have a high number of variables, and a traditional computer cannot factor in all variables in the forecasting model at the same time.

Growth in data volumes, business risks, security threats, and regulations will soon make today's computers insufficient. Moore's law — which says the number of transistors in an integrated circuit doubles every two years — is expected to falter within the decade. The growth of computing power will have to come from other technological advances.[2] Quantum computing has long been seen as a solution — and several banks are already experimenting with it.

## Table 1. Differences between classical and quantum computing

| Basis of difference | Classical computing | Quantum computing |
|---|---|---|
| Operating foundation | Uses bits that can be either 0 or 1 at a time | Uses qubits that can be both 0 and 1 at the same time |
| Temperature requirements | Can operate at room temperature | Needs an extremely low (superconducting) temperature to operate |
| Error rate | Low | High |
| Growth in computational power | Linear | Exponential |
| Optimal use cases | Day-to-day computational needs | Optimization problems, data analysis, simulations, cryptography, and secure communication |

Source: Infosys

# Overcoming the quantum leap

Though quantum computing has some potential business applications, it comes with several technical challenges that make commercial adoption difficult. Despite being over three decades old, quantum computers haven't matured enough to be widely used for day-to-day business requirements. And the ones that are available are expensive. Typically, these computers are extremely difficult to build, engineer, and program.

First, most commercially available quantum computers today require a highly controlled environment to operate, including an extremely low temperature and minimal to zero interference from the surrounding environment. Second, due to the fundamental differences between traditional and quantum computing, businesses find it difficult to develop algorithms to solve business problems.

Last, the majority of quantum computing programming languages are hardware specific and need users with highly specialized skills to implement quantum algorithms.

Yet, solutions to these issues are emerging. For instance, to tackle the challenge of erroneous outputs, one solution is to guess the error-free results based on a bunch of outputs at various noise levels. Another method uses a hybrid system of quantum-classical algorithms where highly critical tasks are managed by quantum computers and the bulk of programs run on a powerful traditional computer. An increasing number of companies are offering quantum computing in the cloud, which can rapidly democratize access and boost adoption. These methods have started proving quantum computers useful in today's context. And as researchers continue to overcome the challenges, financial institutions have started exploring the technology.

# Early adoption in financial services

Despite the challenges and roadblocks, quantum computing has a wide range of current applications across the financial services industry (Figure 1).

Leading financial firms are already testing the waters. While most are in nascent stages, the outlook is promising. Below are some of the most immediate use cases.
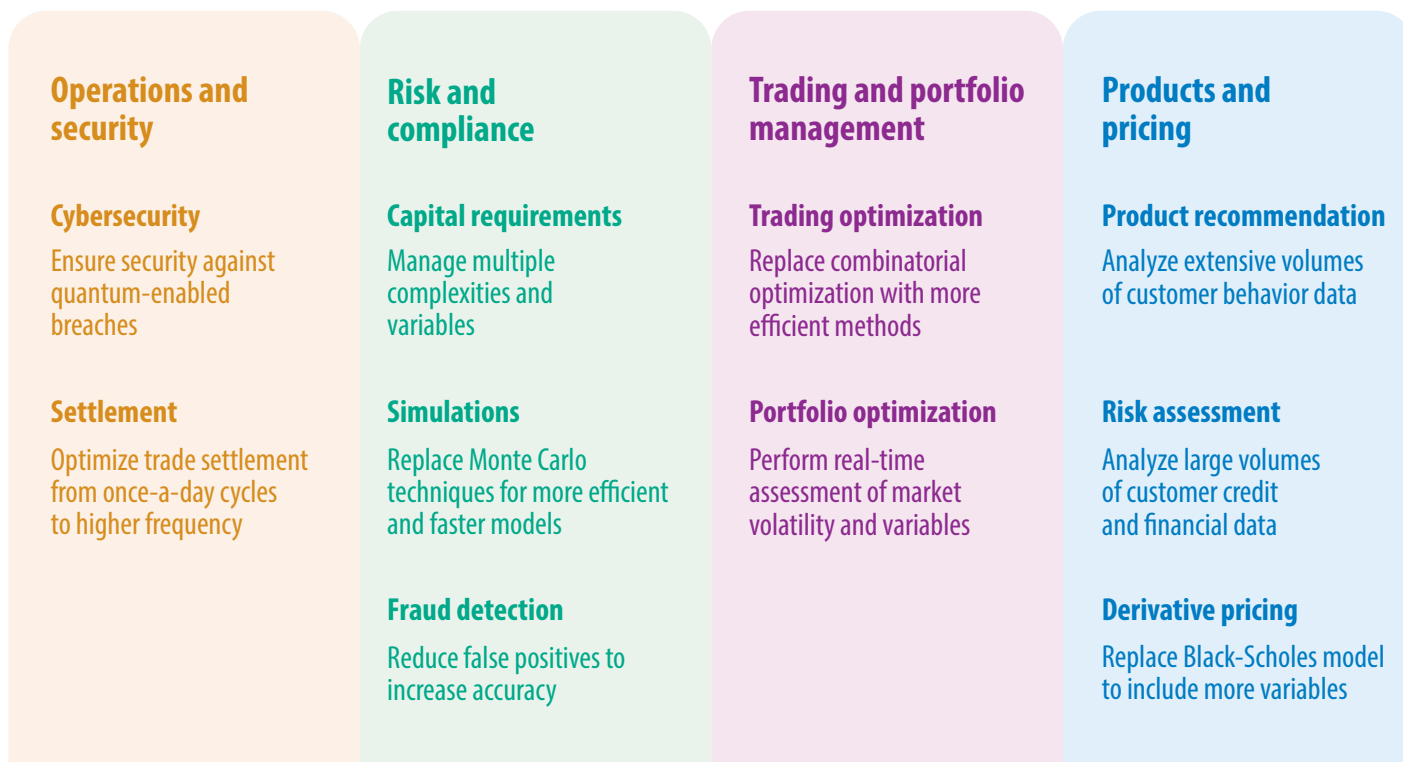
## Predict customer needs :

Companies have vast opportunities to engage their growing number of digital customers with targeted offerings. Banking customers today expect hyper-personalized services, which can be achieved by using data to generate real-time insights and offering products and services accordingly.

However, it is extremely difficult to create analytical models that can

* NP (nondeterministic polynomial time) is a class of computational problems that can be solved in polynomial time by a "nondeterministic" algorithm. A nondeterministic algorithm is one that can "guess" the correct answer rather than have to perform an exhaustive search.

## Figure 1. Quantum computing applications for financial services

| Operations and security | Risk and compliance | Trading and portfolio management | Products and pricing |
| --- | --- | --- | --- |
| **Cybersecurity**<br>Ensure security against quantum-enabled breaches | **Capital requirements**<br>Manage multiple complexities and variables | **Trading optimization**<br>Replace combinatorial optimization with more efficient methods | **Product recommendation**<br>Analyze extensive volumes of customer behavior data |
| **Settlement**<br>Optimize trade settlement from once-a-day cycles to higher frequency | **Simulations**<br>Replace Monte Carlo techniques for more efficient and faster models | **Portfolio optimization**<br>Perform real-time assessment of market volatility and variables | **Risk assessment**<br>Analyze large volumes of customer credit and financial data |
| | **Fraud detection**<br>Reduce false positives to increase accuracy | | **Derivative pricing**<br>Replace Black-Scholes model to include more variables |

Source: Infosys

churn the mountains of behavioral data needed to target customers. Financial institutions that can't offer relevant and timely recommendations will surrender their share of the wallet from existing customers and fail to reach new ones. In fact, financial institutions lose up to $10 billion in revenue annually due to poor data management practices.[3]

> As banking customers expect hyper-personalized services, quantum computers can churn mounts of behavioral data and generate real-time insights to develop personalized offerings

Quantum computing can more accurately simulate customer purchasing preferences based on demographic data, whether it's a new insurance policy, mortgage, or credit card. The customer's personal information, meanwhile, can be protected more effectively through quantum encryption.

In 2017, Commonwealth Bank of Australia joined forces with Telstra, the federal government, the New South Wales government, and the University of New South Wales to develop Australia's first quantum computing company. This venture aims to generate real-time analysis of customer data by understanding patterns and interactions and, as a result, provide highly tailored products, insights, and advice.[4]

## Optimize trading :

Financial market complexity has increased exponentially due to higher trading volumes, the evolution of financial instruments, and stringent regulations. For example, derivatives trading is increasingly complex due to the introduction of concepts like the valuation adjustments model.[5]

With such complications, investment managers often struggle to account for real-life variables, such as market volatility and customer life event changes, when optimizing portfolios. An automated response would require the simulation of a large number of scenarios and investment options, a difficult task for traditional computing. Quantum computing can help manage that trading complexity. Its optimization capabilities can help portfolio diversification, rebalance portfolio investments and investor goals, and streamline trading settlement processes.

The Bank of Montreal and Scotiabank partnered with quantum computing startup Xanadu to apply quantum technology to derivatives pricing algorithms. As part of that proof of concept, Xanadu built a software suite to run quantum Monte Carlo simulations — the go-to technique for risk impact and uncertainty analysis — on various trading products.

The objective was to speed up trading portfolio pricing, which is especially time consuming with existing systems.[6]

In another example, BBVA collaborated with Multiverse Computing to find out whether quantum technology could help define the best path for dynamic portfolio configuration. The bank aimed to identify optimal trading paths for an investment portfolio of 52 assets, with actual market price data from an eight-year time frame. Processing such complex data would take a traditional computer two days, whereas a quantum computer could do it in a few seconds.[7]

Along similar lines, Japanese bank Nomura joined with Tohoku University to explore quantum computing applications that could optimize portfolios and predict stock returns. The bank currently uses a quantum computer from Canadian firm D-Wave Systems to develop and test several models. The bank reported that it

can simultaneously generate about 800,000 samples. Conventional systems, however, could only create one at a time.[8]

## Actively manage and minimize financial risks :

Financial institutions must constantly consider risk management, effective hedging, and regulatory compliance. So far, traditional computers have helped minimize risk reasonably well. But liquidity management, derivatives pricing, and risk measurement require complex calculations. This makes it difficult to manage the risk costs on trades, and Monte Carlo simulations are limited by the scaling of estimation errors. In the future, even larger sets of stress test scenarios will be needed to satisfy regulations, directives, and standards.

The volume, value, and complexities of financial instruments are only going to increase, and traditional

computing methods that are currently applied will not be able to keep up for long. Quantum computing can help financial institutions build sophisticated economic models with more variables and deviations that create better risk profiles. Further, the quantum annealing technique offers methods that identify better portfolio optimization. And quantum machine learning can eliminate data blind spots and prevent financial assumptions about the markets that might not hold true in the real world.

Quantum computers can build models with high number of variables and deviations to create comprehensive risk profiles and facilitate better decision making for financial institutions

Spain's CaixaBank developed a hybrid computing model — where quantum and traditional computers work together at different calculation stages to classify credit risk profiles. The bank uses this model to improve its risk simulations and machine learning algorithms, which require vast amounts of data. This application helped the bank significantly reduce the time needed to complete risk analyses.[9]

## Create quantum-safe encryptions :

Conventional computers cannot factor large numbers into their underlying prime factors in reasonable time. This has been the basis of all existing cryptographic standards. However, it won't be the case for quantum computers. They can deliver an exponential increase in the speed of prime factorization and allow for the identification of prime factors used in encryption. Random number generation mechanisms today are not truly random, i.e., they appear to be random, but those numbers follow an underlying pattern, and this pattern can be decoded by powerful computers. The inherent nature of quantum particles to exhibit "randomness" helps in obtaining true random numbers, which is helpful in financial applications — ranging from financial security to Monte Carlo simulations.

Current encryption standards will be particularly vulnerable to quantum attacks, which makes cybersecurity a critical aspect of quantum computing. Nearly all financial services companies have two known vulnerabilities in common: a reliance on legacy hardware and an inability to quickly change encryption standards. Waiting for cybercriminals to have quantum computers will create massive risk for the industry. Financial institutions need to prepare for a post-quantum cryptography era by developing the right skill sets, algorithms, cybersecurity standards, and encryption solutions.

Quantum encryption can prevent data breaches and thefts by even the most powerful classical or quantum computers. Quantum key distribution (QKD) uses quantum mechanics principles to encrypt and transmit data. With this approach, quantum cryptography encrypts data in a way that is believed to be unhackable.

Working along these lines, European bank ABN Amro is collaborating with QuTech, a quantum technology research joint venture between Delft University of Technology and the Netherlands Organisation for Applied Scientific Research, to prove that a QKD system can encrypt data traffic transmitted via both fiber optics and air. The goal is to guarantee the security of online and mobile banking, now and in the future.[10]

Quantum encryption can safeguard financial data from breaches and thefts by the most powerful classical or quantum computers

DGB Daegu Bank of South Korea is working with SK Telecom to improve its mobile app's security using 5G quantum cryptography. This will enable Samsung Galaxy A Quantum smartphone owners to use the handset's quantum random number generator for security. The chipset in the smartphone generates true random numbers that cannot be predicted by hackers.[11]

And Nomura is working with Toshiba Corp., the National Institute of Information and Communications Technology, and NEC Corp. to test quantum cryptography in real-world financial data transmissions. In this joint venture, Nomura provided access to financial systems with sample data to test how a QKD system works in the wild.[12]

## Getting quantum ready

Financial institutions have already started testing quantum computing to solve business problems, but there is a lot more to be explored. The earlier a financial institution invests in exploring quantum computing, the higher are its chances of getting ahead of the competition.

The adoption of quantum computing in the financial services sector depends on three primary pillars:

- Identifying business-specific use cases — While there are several applications of quantum computing in financial services, most businesses won't need all. Business leaders will have to identify use cases based on strategic goals and prioritize investment in exploring the technology.

- **Developing a quantum workforce** — To make an organization quantum ready, financial institutions will have to build a team that understands the technology, including its capabilities and limitations. This requires bringing together C-suite sponsors, business unit managers, developers, quantum specialists, and mathematicians who can collectively develop quantum solutions for prioritized use cases.

- **Picking the right expertise** — Quantum computing requires highly specialized knowledge that is specific to the use case. For instance, when looking to optimize an investment portfolio, a bank should consider partnering with a company that provides a hybrid system to identify optimal investment scenarios. However, if the priority is boosting cybersecurity, the financial institution should choose a partner that provides quantum-safe encryptions.

As quantum hardware and software evolve, it is crucial for financial institutions and governing systems to seize the benefits and brace for threats. Even if the start is small with only a few test areas, it is important to get started. For many financial services firms, quantum computing is still considered optional — but it won't be for much longer.

## References

1. Quantum computers could be the ultimate defence against the next global financial crisis, Katia Moskvitch, March 1, 2019, Wired.

2. The chips are down for Moore's law, M. Mitchell Waldrop, Feb. 9, 2016, Nature.

3. The Future of Client Onboarding for Financial Institutions, Feb. 6, 2019, Fenergo.

4. Commonwealth Bank rooting for Australia's foray into quantum computing, Antony Peyton, Aug. 25, 2017, Fintech Futures.

5. Exploring quantum computing use cases for financial services, Dr. Elena Yndurain, Dr. Stefan Woerner, Dr. Daniel J. Egger, 2019, IBM.

6. Xanadu, BMO, Scotiabank joint project uses quantum for trading products, Jessica Galang, Aug. 21, 2019, Betakit.

7. BBVA and Multiverse showcase how quantum computing could help optimize investment portfolio management, Aug. 26, 2020, BBVA.

8. Quantum Computer Research of Nomura Asset Management, Masaya Abe, Yuto Tadokoro, Takayuki Takigawa, November 2019, Nomura.

9. CaixaBank becomes the first Spanish bank to develop risk classification model using quantum computing, April 20, 2020, CaixaBank.

10. ABN Amro explores the security applications of quantum technology, June 27, 2019, Finextra.

11. DGB Daegu Bank uses quantum cryptography to protect app users, Aug. 20, 2020, Finextra.

12. Beginning Joint Verification Tests on Quantum Cryptography Technology to Enhance Cybersecurity in the Financial Sector, Dec. 21, 2020, Toshiba.

## Authors

### Vijayaraghavan Varadharajan

*Principal Reaearch Scientist – Infosys*
vijayaraghavan_v01@infosys.com

### Mohammed Aamir Qudsi

*Senior System Engineer – Infosys*
mohammedaamir.qudsi@infosys.com

### Akshay Pachbudhe

*Senior System Engineer – Infosys*
akshay.pachbudhe@infosys.com

### Abhinav Shrivastava

*Consultant – Infosys Knowledge Institute*
abhinav.s08@infosys.com

Infosys® | Knowledge Institute

## About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

**Infosys**®
Navigate your next

For more information, contact askus@infosys.com