Quantum Computing in Banking

How far are we from Day Zero?

Vijayalakshmi Muddu

Quantum computing as a theory has been around since 1981; however, it still reads like science fiction more than three decades later. Several movies in the sci-fi thriller genre revolved around quantum computers.

- **Sneakers (1992)** foretold a world in which a computer could decode all the computerised classified data in the world. (Two years after the movie came out, mathematician Peter Shor figured out the math that makes cryptography vulnerable to quantum computers.)
- **Minority Report (2002)** was creatively portrayed and accurately predictive of future technologies.
- **I, Robot (2004) and Eagle Eye (2008)** showed computers with near-human feelings and an ability to hack and control everything.
- **Matrix Trilogy (1999-2003)** and Transcendence (2014) created a sentient computer.

Paul Benioff proposed the first recognisable theoretical framework of quantum computing in 1982. Prof Richard Feynman lectured about 'Simulating Physics with Computers', also in 1982. In the last two decades, quantum computing is no longer in the realm of wild imagination but has become the hottest topic in both quantum physics and computer science.

So, what is quantum computing?

Quantum computing is a technology based on the principles of quantum theory. Quantum computing harnesses the laws of quantum mechanics to carry out complex data operations. Quantum mechanics pertains to the realm of sub-atomic particles where the laws of classical physics breakdown. It shows how particles and waves have a dual nature. Particles like electrons tend to behave like waves, whereas light waves also display particle nature.

A quantum processor has millions of qubits that explore all possible combinations to find the best answer. A qubit (or quantum bit) is the basic unit of quantum information (quantum version of the classical binary bit). Quantum entanglement (perfect correlation between quantum particles) allows qubits to communicate with each other even if they are miles (or even millions of miles) apart.

Today's quantum computers use physical qubits which are error-prone and can decay quickly. It is estimated that 1000 physical qubits would be required to make a single logical qubit to make it error-corrected, a goal yet to be realised. As of 2018, devices with up to 128 physical qubits have been announced. However, a commercially useful quantum computer is expected to be a 200 logical qubit machine (200,000 physical qubits).

Quantum computing changes the way information is stored and processed and greatly improves the efficiency of algorithms. Currently, the primary area of focus in quantum computing is optimisation problems – these are challenges where the goal is to find the best decision out of many possible decisions. The quantum ecosystem is fast evolving, enabling the 'fifth generation' of computers. While research on quantum computing is on, it is prompting interesting innovations in traditional computing, galvanising the classical computing industry into simulating quantum techniques.

Deloitte estimates that there are several industries where the time to start quantum-proofing has already passed.

Organisations in the automotive, military and defence, power and utilities, healthcare, and financial services sectors are today deploying long-lived systems that are not quantum-safe, exposing them to significant liability and financial overhead in the future. Quantum computing researchers have discovered improved ways of solving problems using conventional computers. Some researchers are seeking to bring 'quantum thinking' to classical problems, according to Natalie Wolchover, a science journalist for Qanta magazine.

Classical computers vs Quantum computers

- Classical computing involves binary values of 0 and 1; quantum computing also reads using 0 and 1, but it can hold much more complex information including negative values.

- Classical computing processes bits sequentially; in quantum computing, qubits are entangled such that altering the state of one qubit alters all other qubits, allowing quantum computers to converge on the right answer very quickly. Due to this property called superposition, quantum computers can do an extraordinary amount of calculations simultaneously.

- Classical computing specifically defines the desired outcomes, limiting the design of the algorithm; quantum computing enables simultaneous computations leading to several probabilistic outcomes, which increases confidence in the best answer.

'A Classical computation is like a solo voice – one line of pure tones succeeding each other. Quantum computation is like a symphony – many lines of tones interfering with one another,' says Seth Lloyd, an MIT Professor.

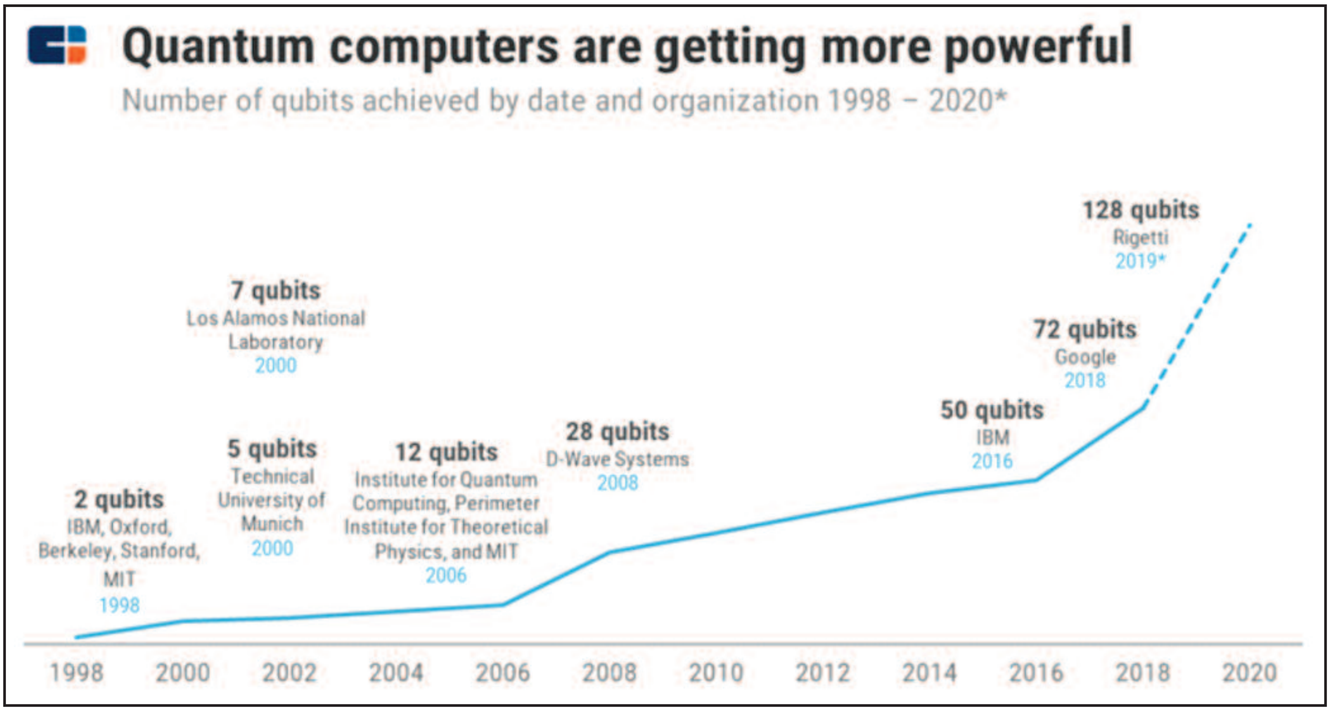
Quantum computing and the rest of the world

Large companies like Intel, Google, Lockheed Martin etc, are collaborating with universities to foster research. IBM has announced a series of partnerships with corporations and academic institutions to explore the practical aspects of this technology. Massachusetts Institute of Technology, Princeton University and the University of Waterloo are all working on quantum computer prototypes.

Many countries, including China, are investing heavily in research and development into quantum computing. Even governments around the world (USA, Australia, European Commission) are forging ahead with quantum computing initiatives.

Satya Nadella, CEO of Microsoft, articulated that Quantum Computing, Mixed Reality and Artificial Intelligence (AI) would be the three path-breaking technologies to shape the world in the coming years.

Microsoft today runs several labs around the world that specialise in the fabrication of quantum devices. *'At Microsoft, we're on the cusp of empowering a quantum revolution with our unique, topological approach,'* Nadella says, hoping that *'quantum computing will make AI even more intelligent.'*



*(Source: MIT, Qubit Counter. *Rigetti quantum computer expected by late 2019)*

Quantum computing for financial services

Quantum computing is gaining the interest of the financial services industry which is looking to increase manifold, the speed of trades, transactions and data processing.

One of the biggest potential uses of quantum computing is simulation. Quantum computing helps identify a better way to manage risk in financial portfolios. The processing time and cost for high-quality solutions can increase exponentially if a classical computer is used whereas a quantum computer can do it speedily with increased optimisation capabilities, driving new cost savings and opportunities for revenue generation.

The potential benefits of quantum computing for financial services could be:

- Solving increasing problems in critical areas like cybersecurity to safeguard customer financial data using next-gen cryptography; financial data encoded with quantum cryptography is far more secure than current levels of digital security.
- Detection of fraudulent activities by recognising patterns of behaviour much faster, leading to proactive fraud risk management.
- Optimising Portfolio management for assets with interdependencies.
- Predictive analytics in customer behaviour by combining quantum computing with AI.
- A combination of quantum computing and blockchain technology could be the most hack-proof technology in the Internet of Things (IoT) era.
- Automated decisions using sets of pre-programmed rules like seamless approval of loans and mortgages.
- Significantly increase transaction speed and reduce processing costs
- Downtime on infrastructure using quantum computing would be non-existent.

Customer Relationship Management will improve from the automation of targeted services. Customer purchasing preferences based on demographic data can be predicted with greater accuracy using quantum computing.

However, customer personal information needs to be protected more effectively through simultaneous automation and analytics by proactive anticipation and prescriptive response. J P Morgan Chase and Barclays Bank have been giving serious consideration to quantum computing and have begun experimentation in 2017. JP Morgan entered into a partnership with IBM to explore the use of this technology in financial services with direct access to cloud-based IBM Q systems to perform corporate experiments. The current areas of interest for JP Morgan Chase are trading strategies, portfolio optimisation, asset pricing and risk analysis, by leveraging on quantum computing, which requires the use of complex algorithmic models.

Japanese banks MUFG and Mizuho have tied up with IBM Q Hub at Keio University to experiment with future applications for quantum computing in the financial sector. Japan's Nomura has launched a joint research project on using quantum computing in asset management with Tohoku University in Sendai.

CBA has joined telco firm Telstra, the Federal Government, the New South Wales Government and the University of New South Wales (UNSW) in an $83 million venture to found Australia's first quantum computing company.

Retail bank NatWest has partnered with Fujitsu on a proof-of-concept project that aims to optimise its mix of high-quality liquid assets, including bonds, cash and government securities. NatWest's quantum technology team has completed highly complex calculations on the bank's £120bn-value High-Quality Liquid Assets portfolio at 300 times the speed of conventional cloud-based compute resources, and with a higher degree of accuracy, says NatWest's director of innovation Kevin Hanley.

Expert insights from an IBM Report *'Getting Your Financial Institution ready for the Quantum Computing Revolution'* opine that FIs are exploring quantum computing, both to dramatically speed up immensely complicated calculations and to improve their accuracy. Engaging now is important, as use cases are being identified, and proprietary ecosystems are being formed.

The 28 largest banks worldwide manage more than USD 54 trillion combined. The US stock and bond markets alone are capitalised at more than USD 70 trillion. In markets these large, creating new algorithms to optimise portfolios, price derivatives, analyse risk, or calculate more accurate default probabilities, can have a massive and widespread impact on the long-term success of global FIs and their customers.

Although fully fault-tolerant universal quantum computers are years away, it is essential that organisations engage now as important and promising use cases are being identified, tools and algorithms are in development, and proprietary ecosystems are being formed. Such efforts will coalesce over time, providing first movers with quantum advantage.

New risks from quantum computing

Quantum computing is a giant leap forward in computing power, theoretically. However, it is used in business applications is still in an exploratory stage. *'Commercialising the technology is a complex task in part because qubits cannot yet maintain their quantum mechanical state for very long and they are delicate and easily disrupted by changes in temperature, noise and frequency'* - The Wall Street Journal.

It is also widely believed that when bad actors get access to quantum computers, they'll use them to crack existing encryption algorithms.

According to Deloitte, *'One frightening aspect of QC development is the certainty—not merely the potential—that QCs will be used to crack previously undecipherable codes and breach earlier un-hackable systems.'*

Lack of quantum-safe public key encryption could result in a systemic failure of the current banking and financial sector approach to information security while exposing large volumes of high-value data to be breached. The Global Banking and Finance Journal argues that the significance of the problem for the financial sector cannot be overestimated. Today, fraud linked to online banking as well as e-commerce transaction is an ever-growing issue in the classical computing world.

In the future, quantum computers, with their ability to break current public-key cryptography, may push online fraud from what is currently a manageable problem to subjecting the financial sector to systemic breach scenarios.

It goes on to argue further that recent fintech innovations are also at risk. Many blockchain-based technologies rely on the Elliptic Curve Digital Signature Algorithm (ECDSA): an algorithm that is not currently 'quantum-safe'. This places the burgeoning cryptocurrency markets at risk, as quantum computers will probably break the underlying cryptography at the core of these technologies, leading to cyber bank robberies of a previously unseen magnitude.

Elisabetta Zaccaria, a cybersecurity expert, recommends that 'One method of developing quantum-safe public-key cryptography is the deployment of a new set of public-key cryptosystems for classic computers capable of resisting quantum computer attack.

These cryptosystems are called 'quantum-safe' or 'post-quantum cryptography'. The principle behind them is the use of mathematical problems of complexity beyond

GUIDELINES FOR AUTHORS

Articles should be submitted using only Arial font in MS Word. Text of the article should be in **font size 12**, with headings in **font size 14 in bold**. Subheadings should be made **italic and bold in font size 12**.

Authors sending their articles for publication in 'The Indian Banker' should submit a certificate in the following format along with the material for publication. They should also send their brief biodata, scanned photo and email address. **Articles should be invariably between 2400 and 6000 words.**

The editorial committee has decided to consider ***only those articles*** which are following the above standard and are accompanied by the prescribed certificate.

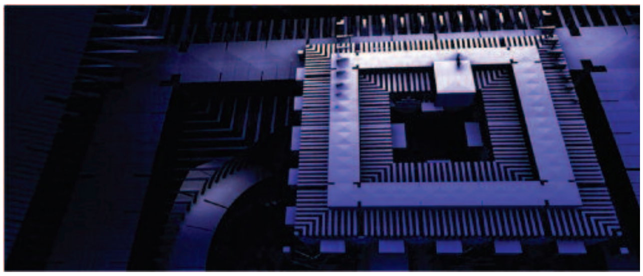
The Editor
'The Indian Banker'

I/We hereby declare that the article titled ______________________________ submitted by me/us is the original article to the best of my/our knowledge. I/we also declare that this article has neither been published elsewhere nor has it been submitted to any other publication, and that I/we have not reproduced material from any published source except as permitted by the Copyright Act.

I/We undertake to indemnify IBA against any action for any violation of Copyright Act resulting from publication of this article in 'The Indian Banker'.

Signature(s) ____________ ______________ ____________________

Name(s) ______________ ______________ ____________________



(Photo Credit: Pixabay)

quantum computing's ability to solve them. The information security industry currently recognises five types of cryptosystems as promising replacement candidates for current cryptography. These are hash-based, code-based, lattice-based, multivariate-based and super-singular isogeny-based.

International standards bodies, including the National Institute of Standards and Technology (NIST) USA, are currently in the process of conducting more analysis and research before they can go forward on determining which of these to adopt.

Quantum computing and India

In the global race to build quantum computers, India has so far been present only in theory compared to the US, China and the handful of other European countries that were spending large amounts of money. India has several theorists, but only a few have been trying to build a quantum computing device.

Department of Science and Technology (DST), Indian Institute of Science (IISc), Tata Institute of Fundamental Research (TIFR) and Indian Institute of Science, Education and Research (IISER) are currently engaged in quantum computing research.

In 2018, Microsoft India launched the Microsoft Garage – an experimentation resource for its employees, to encourage problem-solving in new and innovative ways. Microsoft Garage is collaborating with Indian engineering students by leveraging on its strength in quantum programming and algorithms, to grow the worldwide tribe of scientists, experimentalists and programmers working on quantum computing.

The DST has set up a programme called Quantum-Enabled Science & Technology (QuEST). As a part of the programme, it will invest a sum of INR 80 crore in a span of three years to facilitate research in this field. During January 2019, a road-map that would help in laying the groundwork for building quantum computers in India was discussed in the first meeting of QuEST connoting Phase I of India's quantum computing programme. After three years, the Indian Space Research Organisation (ISRO), Defence Research and Development Organisation (DRDO), and Department of Atomic Energy (DAE) are expected to jointly pool in a sum of INR 300 crores to push QuEST to Phase 2 that would ensure that India's quantum computing programme matches international standards.

Quo Vadis

Quantum computing is real, even if it is in its infancy. It is widely believed that quantum computing will solve the increased computing needs of financial firms using far less energy than traditional computers.

According to an IBM report, Quantum computing is nearing a phase of commercialisation that may change our world. Visionary organisations are already aligning with the emerging quantum computing ecosystem to become 'quantum ready' – exploring use cases and associated algorithms that address complex problems and help enable new business models. Quantum supremacy is not there yet as quantum-ready algorithms may take a few more years to arrive.

To sum up in the words of Lee Braine, the Chief Technology Officer of Barclays, *'Combined with Artificial Intelligence, quantum computing will be the most disruptive technology since the invention of the wheel. Those who do not embrace this new paradigm today will be left behind.'*

About the Author

Vijayalakshmi Muddu is currently working as DGM and Senior Faculty at the State Bank Institute for Consumer Banking. Prior to this, she was deputed as CEO, Chicago and Vice President & Head (Syndications) at US Operations, New York.

She holds a Master's in Economics and was awarded a Gold Medal in Public Administration for Bachelor's in Arts. She also holds additional certifications like Diploma in Business Finance, Marketing, Management, International Banking, Trade Finance etc.

She had joined as a Probationary Officer in State Bank of India in 1990. Her experience spans nearly three decades in Credit, Retail, Forex and International Banking including assignments of Relationship Manager, Team Leader, Forex Dealer, Head of IB Division and Branch Management.
An avid reader, enjoys writing, classical music and movies, gardening, painting and is an enthusiastic homemaker.

She can be reached at srfaculty2.sbicb@sbi.co.in