Singapore must look beyond AI and build its quantum tech talent now
By By Paul Griffin

The Business Times, BT Weekend, Page 27, Section: THE BROAD VIEW
Saturday 5 September 2026
963 words, 750cm² in size
42,600 circulation

Singapore must look beyond AI and build its quantum tech talent now

Financial institutions should nurture professionals today for tomorrow's threats

By Paul Griffin

AS ARTIFICIAL intelligence reduces the number of traditional entry-level tasks through which young technologists once learnt their professions, quantum computing seems to be an even less obvious career choice because of its perceived high barriers to entry.

I would argue the opposite. Quantum computing is still at a sufficiently early stage – there is a window to train people before the field matures.

The technology's power lies in its ability to solve problems in ways that classical computers cannot. It speeds up simulations, optimisations and complex tasks dramatically.

Using quantum computers to solve business problems is increasingly accessible.

However, this capability also poses a cybersecurity threat. Quantum computers could potentially break longstanding cryptographic systems protecting our business transactions, an ability that current AI models do not have.

But just as you do not need to be a physicist to be a data scientist, you do not need to be a quantum physicist to work with quantum technology for business.

To maintain Singapore's edge as a financial hub, we need professionals familiar with the technology to protect our systems against future quantum computers.

"Harvest now, decrypt later"

In banking and financial services, quantum approaches are already being explored to tackle computationally demanding problems, including the Monte Carlo simulation, a widely used technique in financial derivative pricing, and rare-event and tail-risk estimation.

More urgently, our financial institutions need quantum-safe cybersecurity, which is essentially the science of protecting against attacks from quantum computers.

They need to secure data for its entire lifetime, to protect the confidentiality of long-lived financial information, digital identities, payment infrastructure and communication.

A quantum team would need to know where vulnerable cryptography exists within an organisation, and guard against "harvest now, decrypt later" threats.

This is a phenomenon in which adversaries collect and store encrypted information even though they are currently unable to decrypt it.

In such a scenario, an attack can begin years before a cryptographically relevant quantum computer exists.

When such a technology becomes available, algorithms could break widely used public-key cryptography, potentially allowing previously captured sensitive data to be decrypted retrospectively.

To maintain Singapore's edge as a financial hub, the Republic needs professionals familiar with quantum computing to protect its systems against future quantum computers. PHOTO: BT FILE

Hence, it is especially important for banks to transition to quantum-safe cryptography today.

Building a talent pipeline

The quantum professionals we need must know how to use quantum algorithms, what data to provide, how to interpret their outputs, and when a particular type of quantum processor is appropriate for a problem.

I see two parallel roles developing for these professionals in our financial sector: people who can explore where quantum computing may create advantages, and others who can help organisations migrate towards post-quantum cryptography and broader quantum-safe architectures.

Singapore's computing schools have an opportunity to develop what might be called quantum application and quantum safe engineers. These new practitioners sit at the intersections of quantum computing, cybersecurity and industry.

They would understand quantum principles and be equally comfortable with data science, cybersecurity and cryptography, along with cloud computing and conventional high-performance computing.

And even without owning hardware, our students can access quantum processors through the cloud for hands-on experimentation through a "learning by doing" strategy.

This approach would let students get familiar with behaviours that are difficult to glean from equations alone, such as sampling variation, hardware connectivity, scalability constraints, and the gap between theoretical complexity advantages and practical performance.

They can also experiment with post-quantum cryptographic libraries, benchmark migration approaches and study how quantum-safe systems integrate with existing applications.

When it comes to quantum security, students should understand which systems are affected, which are not, how post-quantum algorithms differ from classical ones operationally, and how a bank might migrate a complex technology estate without disrupting existing services.

They also need to know how different quantum hardware technologies are suitable for different workloads.

To enable this pedagogical operation, computing schools need to collaborate with industry to provide students with real problems, realistic data sets, existing technology architectures, security constraints and meaningful performance benchmarks.

A case in point is the Young Talent Programme for AI in Finance, announced by Deputy Prime Minister Gan Kim Yong in May, with participation from key financial institutions and technology partners.

It gives students structured real-life work exposure through formal coursework, internships and capstone projects with industry players.

While the programme focuses on building AI capabilities for finance among students, it serves as a good framework for a similar one focusing on quantum technology.

Organisations should begin developing internal capability now, as migration across complex banking infrastructure takes years. Staff need time to understand their cryptographic dependencies early on.

Because of the ties between Singapore's financial sector, universities, technology ecosystem and national investment in quantum technologies, the Republic is well positioned to nurture the quantum professionals who can keep us safe when the technology matures.

As physicist Richard Feynman said, if you cannot build something, you do not fully understand it. I would add: If you cannot use it, you do not yet understand its value; if you cannot secure it, you may not understand its risk.

Quantum computing's power lies in its ability to solve problems in ways that classical computers cannot. It speeds up simulations, optimisations and complex tasks dramatically.

The writer is an associate professor of information systems (practice) at Singapore Management University, where he teaches and researches on quantum computing in financial services.

The commentary is based on the writer's own experiences, observations and argument. AI tools were used for drafting and editing. The writer remains fully accountable for the commentary's accuracy, originality and final form.