Quantum Computing

What you need to know about this rapidly
emerging field that can solve problems faster
than a supercomputer

Quantum computing is quietly moving from an interesting physics challenge to potentially a strategic solution in boardrooms worldwide. The global market for quantum technology is expected to reach up to US$97 billion by 2035. Canada sits close to that shift, with a deep research base and a small set of firms trying to translate scientific advantage into industrial capability.

What is quantum computing?

Quantum computers aren't replacing classical machines. They're a specialist tool for problems that even today's best supercomputers can't handle. In 2024, Google's Willow chip completed a benchmark calculation in under five minutes that would take a leading supercomputer an estimated 10 septillion years, vastly exceeding the age of the universe.

A classical computer tries possibilities one by one, through binary bits (0 or 1). Whereas a quantum computer uses qubits, which keep many possibilities alive at once (superposition), links parts of the problem so they move together (entanglement) and uses cancellation/reinforcement to make wrong answers fade and right answers stand out (interference).

Why does quantum computing matter?

It can solve problems classical computers can't handle. Bain estimates quantum computing could unlock up to $250 billion in value across pharmaceuticals, finance, logistics, and materials science. Consider drug discovery: bringing a drug to market could cost up to $4 billion and can take more than a decade. Add to that, the fact that about 90% of drug trials fail. Quantum computers can simulate molecular interactions at the atomic level: something classical machines can only approximate, heavily compressing timelines.

The security clock is already ticking. The most immediate business risk is "harvest now, decrypt later": adversaries collect encrypted data today and wait for quantum capability to crack it retroactively. The National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Canadian Cyber Centre all treat this as a live threat requiring action. If your organization holds data with a long shelf-life: health records, proprietary research, industrial IP, the breach window is already open.

What is the opportunity for Canada?

Canada's quantum prowess is decades in the making. Waterloo's 'Quantum Valley', anchored by the Perimeter Institute and the Institute for Quantum Computing, has attracted over $1.5 billion in investment over 25 years and trained more than 3,500 quantum specialists.

The challenge is keeping that advantage at home. In December 2025, Ottawa launched the Canadian Quantum Champions Program, investing $92 million across four companies: Xanadu (Toronto), Nord Quantique (Sherbrooke), Photonic (Vancouver), and Anyon Systems (Montréal). This is part of the government's five-year quantum commitment of $334.3 million.

The projected payoff: by one estimate, quantum could contribute more than 3% to Canada's GDP by 2045, rivalling the aerospace sector, and support more than 200,000 jobs.

What challenges does quantum computing face?

There are technical challenges that need to be addressed. A qubit holds its quantum state for a tiny window, often tens to hundreds of microseconds, so you can only run a limited number of steps before errors drown out the signal. It's like solving a complex equation on a whiteboard that erases itself every fraction of a second.

To compensate, engineers use error correction: redundant qubits that check and protect the computation. But creating a single stable "logical qubit" can require hundreds to thousands of physical qubits, far more than current machines offer. This is where the race is being run – Google, Microsoft, and Canada's Xanadu are all competing to crack error correction at scale and unlock breakthroughs in molecular simulation, cryptography, and optimization that classical computers can't reach.

What to keep an eye on

- **Post-quantum cryptography deadlines:** Canada's roadmap for the public service requires migration plans by April 2026, high-priority systems quantum-safe by 2031, and full migration by 2035. Those dates will ripple into vendor contracts and supply chains.

- **Early commercial traction:** Drug discovery, materials science, and financial optimization are where pilots are emerging. Consistent advantages over classical methods will signal the technology is turning a corner.

Written by **Sabreena Shukul**, Research Assistant, RBC Thought Leadership