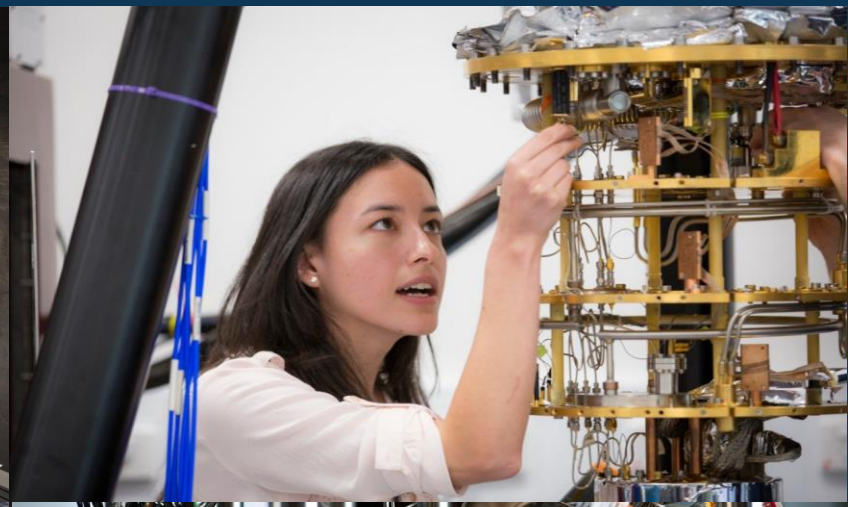
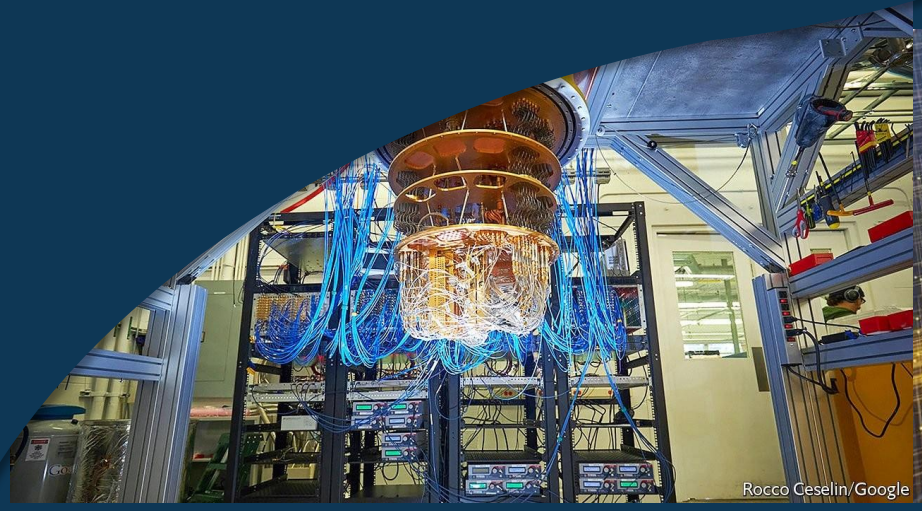
Citizen F1RST

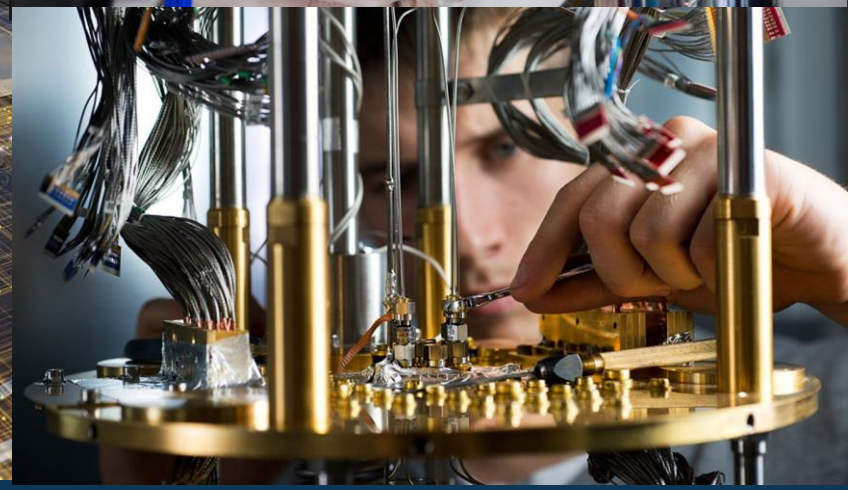
POWERED BY
Institute for
Citizen-Centred
Service

Quantum Computing 101

- What is quantum computing?
- Practical applicability
- Government and industry benefits
- Future implications of quantum computing







JOINT COUNCILS' EXECUTIVE MONTHLY REPORT

Developed by the Research Committee

April 2022

Images: University of Sydney, New Scientist, India Times, Nature, IBM.com, Investable Universe

1. Introduction and applicability

A quantum computer is a computer that uses quantum physics to execute computations faster than a traditional computer. Qubits, which are units of information, are used in quantum computers to complete tasks. Unlike traditional computer "bits," which are either 1s or 0s, qubits can be either - or both - at the same time. This is crucial for vastly faster processing speeds, which are required to model quantum physics at the molecular level. **Compared to regular computers, quantum computing will make a fundamental shift in the speed, efficiency, and quality of all sorts of calculations.** At this time, quantum computers are starting to be used by:

- **IBM:** weather prediction by analyzing a myriad of variables.
- **JPMorgan Chase:** calculation of price option contracts and risk assessment in the banking and financial industry.
- **Microsoft:** calculation of chemical and bacteriological processes to conserve energy and reduce CO2 emissions.
- **Daimler AG:** cell chemistry stimulation to improve battery longevity and resilience in electric vehicles.
- **ProteinQure:** drug discovery via stimulating molecules and molecular processes.
- **Post-Quantum:** improvement or hacking of cybersecurity algorithms.

Quantum computing has huge potential to enable massive system transformation. It's predicted that the transition from classical to quantum computing will be more momentous than the transition from abacus to regular computer. This is one of the reasons governments throughout the globe, including Canada, continue to invest in quantum computing research and development. Those efforts are intensifying now that quantum research is transitioning from the theoretical to the practical realm, similar to the AI development a decade ago.

Since late 2010s, the US and China have been at the forefront of state-led investments in quantum computing.

Why is this Report Important?

- Quantum computing, which is more powerful than regular computers, has the potential to revolutionise the world. It has the power to reshape digital services, accelerate data processing, and usher in a new era of communications and artificial intelligence. Companies such as IBM, Microsoft, and Google are vying with one another to develop reliable quantum computers. The National Quantum Strategy, worth $360 million, was launched in 2021 by the Canadian government to boost national innovation.
- Quantum computing may be used to help tackle challenges related to climate change, health care, and citizen-oriented policy outcomes. Quantum computing is still being tested on its exact applicability and relevance to various calculations that might be required by governments. At this time, the interest in quantum computing is shared between technology, academia, industry, and government, creating venues of collaboration and cooperation.

What is Covered in this Executive Report?

This report includes the following:

- Introduction and Applicability
- Unique Features of Quantum Computers
- Benefits of Quantum in Government
- Future Implications of Quantum Computing

Sources: "How Quantum Computing Could Change Financial Services." ; Quantum Computing 101; What Is Quantum Computing?

2. Unique Features of Quantum Computing

In calculations done by a quantum computer, all possibilities are feasible, and it can process all of them at once rather than in parallel.

Quantum computers are more powerful for some sorts of massive, complicated computations that a great number of traditional computers would otherwise be required to do equivalent job.

"If you're trying to solve a maze, you'd come to your first gate, and you can go either right or left. We have to choose one, but a quantum computer doesn't. It can go right and left at the same time."

Rebecca Krauthamer, CEO, Quantum Thought

"Digital computers use Boolean logic, the language of 0s and 1s. A quantum computer replaces it with quantum law, getting faster operations. This allows us to do certain tasks with fewer steps."

Hartmut Neven, founder of the Google quantum lab

"A quantum machine is a kind of analog calculator that computes by encoding information in the ephemeral waves that comprise light and matter at the nanoscale."

Microsoft researcher David Reilly

Sources: Quantum Computing: Everything You Need to Know; 20 Mind-Boggling Facts About Quantum Computing Everyone Should Read; More Possibilities Than There Are Particles In The Universe

Here are some of the most important facts and figures on quantum computing.

Quantum computing needs extremely low temperatures because subatomic particles must be as close to a stationary state as feasible in order to be measured. D-Wave quantum computers' cores operate at -460 degrees F, or -273 degrees C, which is just 0.02 degrees above absolute zero.

Science fiction appears to become reality on a quantum level. Particles can teleport (quantum tunnelling) between two sites by travelling backwards or forwards in time.

Parallel universes could be one explanation for why quantum computers work. Because we are observing qubits in multiple universes at the same time, it has been hypothesized that they can exist in two states at the same time.

By 2028, intelligent machines may emerge that can perform any task that humans can. Quantum computers could aid in the development of an entirely new sort of intelligence.

3. Benefits of Quantum in Government

While the use of quantum computing is limited today, in the future it will be capable of significantly improving all areas of government activities where current computers are involved. A data collection that takes days or months to analyse now, would be able to provide responses in a matter of seconds, speeding up policy-making processes.

Quantum computers can handle a huge number of potential outcomes at the same time due to their technical nature and working method. These results are beyond what is feasible with the fastest version of a classical computer.

A quantum computer may solve a variety of issues, including chemical reactions in molecules and a better understanding of some of the unknowns surrounding climate change. This includes budgetary calculations and a variety of policy consequences of all levels of complexity.

Sources: Quantum Computing Holds Promise for the Public Sector; What Is Quantum Computing and How Can It Help Feds?; Quantum Computing and Communications

Examples of Potential Applications in the Public Sector

Efficiencies

By empowering the overall system, quantum technology will assist provincial and municipal governments in improving everything from resource allocation to budgetary calculations, to a myriad of other provincial and local operations. Quantum is particularly good at issues involving routing, logistics, and resource optimization.

Local examples vary from the most efficient routing of emergency operations to directing paramedics to an accident scene to sophisticated optimizations for public safety at the federal level with complex calculations.

Cybersecurity

Encryption techniques will be forced to alter as a result of quantum computers. On current most powerful supercomputers, today's methods are predicated on methodologies that may take millennia to solve. These sorts of issues might potentially be answered in hours or days on a quantum computer.

Quantum can assist governments in promoting the research of new and more diversified encryption tactics to defend national security, since quantum computers may be able to break all types of encryption systems.

Science and technology

Quantum will be a driving force, from weather forecasting and climate change analysis to improved treatment choices for pandemics like Covid-19 and discovering new and exciting prospects in research.

For all levels of government, labs, special institutes for healthcare innovation, and more, the possibilities are endless.

Financial services

Large or unstructured data collections will be easier to evaluate for the finance sector. Improved understanding of these areas might aid in better decision-making, customer service, and policy analysis. Capital markets, national finance, portfolio management, and encryption-related operations are all compelling application cases.

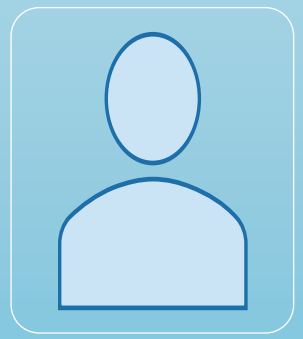
Quantum computers are especially useful when algorithms are fueled by live data streams with a high amount of random noise, such as real-time equities prices.

4. Current limitations of quantum computing

The fragile nature of quantum information needs complicated and costly facilities to house quantum computers. Most quantum systems can only operate in vacuum-like settings that are colder than deep space. This requires the installation of specialized, energy-intensive refrigerators in laboratories. Some quantum systems are created with rare materials, posing ethical and environmental issues.

Researchers around the world are advancing in solving some of quantum computing's most persistent technical obstacles, as daunting as they may appear. Quantum processors may soon be able to function at more normal temperatures, thanks to recent research, and quantum error correcting codes are already being created.

The landscape of quantum development is highly diversified, with numerous stakeholders, nations, and even disciplines contributing to unique solutions.



Technical difficulties
Although the potential of simple quantum computing was first identified in the 1980s, it has yet to be realized. Engineering, building, and programming quantum computers are complex matters. As a result, there are flaws such as noise, malfunctions, and the loss of quantum coherence, which causes quantum computers to break down.

Qubit quality
Today's cloud-based quantum computers, with their few qubits, are insufficient for large-scale systems. When they conduct operations between two qubits at a pace significantly higher than what we would need to successfully compute, they nevertheless produce mistakes. More research is needed to determine the best conditions required to generate correct answers.

Error correction
Error correction algorithms are needed that verify and then correct random qubit mistakes as they arise, since qubits aren't quite good enough for the scale required for their functioning. Although error correction in quantum computing has yet to be shown as a complete picture, it remains to be a high-priority area of research for many countries.

Sources: Quantum Computers: Limits, Options, and Applications; The Limits of Quantum; Limitations in Quantum Computing from Resource Constraints; Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It

5. Future considerations for the use of quantum computing

An educated workforce will be needed with the talent to maintain growth and prevent a skills deficit if Canada wants to take advantage of the economic and political benefits quantum can provide. Education in quantum mechanics and machine learning is a must in order to encourage high school, college, and post-graduate students to pursue professions in this field.

Quantum computing should be further promoted to have bipartisan support at all levels of government. Bringing quantum computing to life in order to meet real-time use cases would need more than simply quantum hardware expenditures.

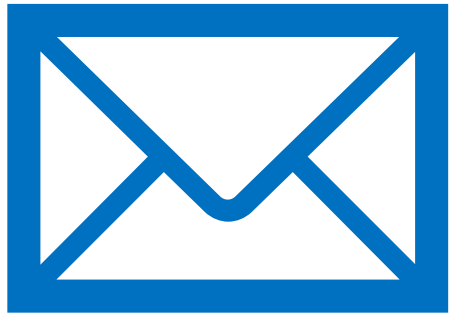
All levels of government may promote quantum computing in a variety of ways, not just for future possible improvements in the way cities and provinces function and breakthroughs in citizen safety, but also for economic growth and efficiency that will benefit everyone long into the future. Some of them are difficult to fathom now.

These are all reasons why quantum governance is important to the public sector's future.

Organizational Steps to Prepare for the Quantum Era

Build awareness of quantum's security risks.	Quantum computing poses a threat to existing cryptography and encryption methods. To garner broad support for investing in a quantum-safe cryptography infrastructure, it is recommended to bring this information to other company leaders at the board, C-suite, and operational levels.
Take a fresh approach to cryptographic governance.	A major technical difficulty is preparing cryptography systems for the quantum computing age. A more agile approach to cryptographic governance can build more flexible enterprises that can swiftly pivot and reprioritize in response to new security concerns, just how Agile software delivery principles help create more adaptable technological teams. This shift in mentality can lead to a more flexible, dynamic cryptographic infrastructure that can adapt to changing security challenges and requirements in the company, industry, and technology.
Assess the enterprise's readiness to become crypto-agile.	A more crypto-agile organization - one that can efficiently update cryptographic algorithms, parameters, processes, and technologies to better respond to new protocols, standards, and security threats, including those utilizing quantum computing methods - can be enabled by a refreshed approach to cryptography.
Practice good cyber hygiene.	Be proactive in controlling and eliminating cybersecurity risks, as always. Establish and maintain strong cybersecurity foundational concepts and practices, as well as situational awareness of data, infrastructure, and other assets.

Sources: 5 Steps to Prepare Security for the Quantum Era; What Businesses Need to Consider Today for the Quantum Era



For Further Reading

- What is quantum computing?
- What Makes Quantum Computing So Hard to Explain?
- Quantum computers and quantum supremacy, explained
- Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It
- Race Not Over Between Classical and Quantum Computers
- The Basics of Quantum Computing
- The Quantum Computing Era Is Here. Why It Matters—And How It May Change Our World.

Other noteworthy articles:

- "Quantum computing: how to address the national security risk“
- The Commercial Prospects for Quantum Computing
- Industry quantum computing applications
- Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment
- The road to quantum computing

Research Repository

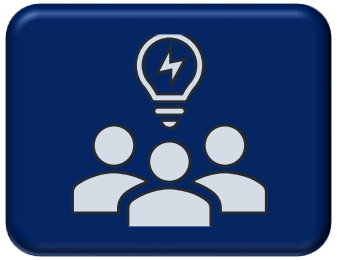
Access the Citizen First Research Repository.

Recent entries on the research repository:

The Future of the Workplace in Government - Joint Councils’ Executive Report March 2022

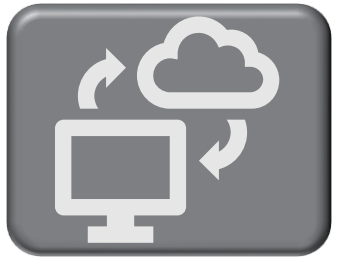
This report includes the following: Overall Trends, The Work-from-Anywhere Model, Key Considerations, Strategies to Prepare for the Workplace of the Future.

Trends in the Daily Newsletter

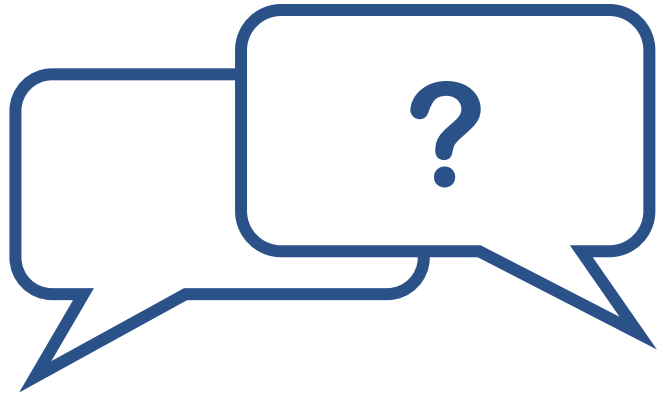


Citizen experience continues to represent a major point of interest for governmental agencies to improve their own effectiveness. Citizens are increasingly interacting with the world through digital channels, and that means dealing with agencies in the same way. Having seen how good things can be in the commercial world, their expectations have risen accordingly. And when they see that agencies experience challenges when it comes to the data that describes them, their confidence in the agency and government overall can decline.

Digital ID initiatives are being considered and developed by a range of international actors. The UK government, for example, has led efforts to create a digital identify system that can be used to help access public services. The new program represents a shift in the UK government's approach. It will allow users to create a government account to access services online. This initiative builds on a range of previous proposals and international experience, and it could represent a useful learning experience for other jurisdictions.



Canada, Mexico, and the United States have a chance to forge a regional agenda to position North America as a global leader in digital government services. Having already established a solid foundation for cooperation, these countries are now encouraged to build on it. The Canadian federal government rapidly developed a secure COVID-19 exposure notification service and launched the Find Financial Help During COVID-19 website, used by millions of Canadians. The US and Mexican government introduced similar initiatives, all of which can bring North America closer to a greater scope of digital integration.



We would love to hear from you!

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report. If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up. Send your questions to info@iccs-isac.org.

Follow: