A Quantum Future: Preparing Canada for the Potential Impacts of Quantum Computing

by

Sahar Shoja

Bachelor of Business Administration, York University, Schulich School of Business, 2011

A thesis

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Digital Media,

in the Program of

Digital Media

Toronto, Ontario, Canada, 2017

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A THESIS

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my dissertation may be made electronically available to the public.

A Quantum Future: Preparing Canada for the Potential Impacts of Quantum Computing

Master of Digital Media, 2017

Sahar Shoja

Digital Media

Ryerson University

Abstract

Quantum computation has the potential to transform the way various Canadian industries do business. Unlike classical computers which use bits, computers built using the principles of quantum mechanics use qubits, which allows them to perform several complex tasks simultaneously and at an exponentially faster speed. This research will analyze the potential impact of quantum computing on Canada's cybersecurity and workforce. It will also highlight barriers to entry for this burgeoning technology and provide recommendations that address current and future challenges. It is proposed that if Canada embraces this technology's opportunities and addresses its challenges, it can continue to be a global leader in the field of quantum computing.

Acknowledgements

I would like to thank my academic supervisor, Professor Marcus Santos, who patiently guided me through the writing process, as well as my second reader, Christian Weedbrook, who answered all of my "quantum" questions. I would also like to thank the Master of Digital Media program and the 2016-2017 cohort.

Dedication

To my family, who moved across the world to give me the chance at a better life, and my husband, who supported me as I took on too much.

Table of Contents

Chapter 1

Introduction

1.1 Thesis Statement

Quantum computers are in many ways similar to classical computers. Every element that allows our laptops to function has a quantum equivalent [1]. Our current computer devices, also known as classical computers, use bits to perform tasks. Quantum computers use qubits, which can harness the power of quantum mechanics to complete certain tasks exponentially faster [1]. Although the technology is currently in its infancy, many large firms such as Google and IBM are working towards technology that would achieve quantum supremacy[1] [2]. Quantum supremacy would allow these revolutionary devices to go beyond speed-ups and complete calculations that would be impossible for any classical computer in existence today. In what some call the next space race, leading tech firms throughout Canada and the world are competing to be first to achieve quantum supremacy, with Google claiming that it will achieve this milestone by the end of 2017 [2].

The potential impact of quantum technologies has been recognized by the government of Canada, which has developed a quantum strategy through the National Research Council (NRC) [3]. Known as Quantum Canada, this strategy aims to "provide visible focus for Canada's national interests in quantum..." and to ensure that "...Canada's present-day advantage in quantum technologies is maintained and expanded for long-term economic prosperity" [3]. This focus by the Canadian government on fostering the development of this technology is yet another indication of the emergent significance of quantum technologies within the global landscape.

Yet, despite extensive investment by the government, the newness of the technology means

[1] Quantum Supremacy is the point at which a quantum computer can complete a defined task faster than any existing classical supercomputers [2]

there is a lack of clarity around its implications for the Canadian economy. This research aims to provide a better understanding of the technology's potential impacts – both negative and positive – on Canada's cybersecurity and workforce, while identifying key barriers to entry. This research objectives are divided into three parts:

1. *Investigate the Potential of Quantum Computing*: This research will use primary and secondary data to draw conclusions about the technology's current and potential impact on Canada [2]. A background on quantum computing's unique capabilities and potential limitations will be provided. In addition, a profile of several leading quantum computing firms and their recent technological accomplishments will be shared. In order to understand where the government should focus its support to ensure continual leadership in the sector, the current perceptions of industry leaders and researchers on the sector's future will also be provided.

2. *Understand the Impact of Quantum Computing on Cybersecurity*: In order for Canada to remain a leader within the global industry, it will be asserted that the Canadian government must prioritize funding research for quantum security. As this technology grows past infancy and becomes more widely available, hackers could utilize quantum technologies to threaten the privacy of Canada's government bodies, businesses and citizens.

3. *Identify Barriers to Adoption*: Several barriers will hinder the adoption of this new technology by Canadian businesses. It will be illustrated that the technology's novelty means there is a lack of understanding around its potential by those outside of the limited group of quantum researchers and business leaders. If Canada's quantum industry is to thrive, the government must work in partnership with Canada's tech industry and burgeoning quantum firms to educate and enable businesses to become early adopters of quantum computing.

1.2 Methodology

For the purpose of this thesis, the following methodology was used:

1. *Research Surveys*: In order to gather recent data on the quantum computing industry in Canada, individuals working at quantum computing firms, academic institutions or incubators and Machine Learning firms were surveyed. The surveys provided to these three distinct groups aimed to shed light on the current state of Canada's quantum computing industry, including its gaps and opportunities.

[2] Primary data is defined as data that is collected via surveying by the lead researcher of this work. Secondary data is defined as data found via literature review of existing works

2. *Literature Review*: In addition to surveys of individuals at private firms and academic institutions, a literature review of existing scientific publications and journals was conducted to provide a background on quantum computing's evolution over the years. This review of existing literature looks to highlight the technology's unique capabilities, limitations and possible risks and challenges.

1.3 Contributions

The NRC projects that quantum computing will have major impacts in fields from finance to materials design, but there is currently minimal understanding of the economic impact and challenges presented by this technology. This research provides a broad overview of the current state of quantum computing, highlight some of its key challenges through surveying of experts within the industry and provide recommendations on:

1. How government, academia and private firms can work together to identify the best opportunities for the early development and adoption of quantum technologies and address hurdles with the commercialization process
2. How the incoming Canadian workforce can be better prepared for work in a quantum age
3. How the government and private institutions can be proactive in protecting themselves against the potential security threats posed by quantum technologies

1.4 Roadmap

Chapter 2 provides background on the current state of quantum computing, some of its potential applications and several of the key firms competing in the global race for quantum supremacy. Chapter 3 is a survey of current literature that provide applicable learnings for the quantum computing industry. Chapter 4 will include an overview of methods and materials and an analysis of the survey findings. Chapter 5 provides recommendations on how the government, academic and private institutions can work together to address existing challenges and ensure the continual growth of the industry.

Chapter 2

Background

The first Quantum Revolution at the turn of the 20th century allowed us to understand that electrons and photons can behave both as particles and waves [4]. With the new understanding that light can be simultaneously spread out and localized, classical Newtonian dynamics were revised [5]. This new understanding made many scientific breakthroughs possible, and forms the basis for our understanding of quantum mechanics to date.

Today, we are living through a second Quantum Revolution, which will be integral to the development of many new technologies [4]. As a consequence of this new revolution, a universal quantum computer may have the capacity to take tasks performed by various industries in Canada and complete their functions in significantly less time. Theoretically, a universal quantum computer could take tasks that were previously deemed too complex to attempt – because they would take the age of our universe to solve — and complete them in a matter of minutes or hours [6].

Quantum computers are in many ways like classical computers, meaning that the elements that allow our laptops to function all have a quantum equivalent [1]. Classical computers use binary arithmetic, which means all numbers are a sequence of bits – either a 1 or a 0. A quantum computer uses quantum bits, or "qubits". Due to the quantum principle of superposition, a qubit can have "... the equivalents of 0 and 1 occurring at the same time" [1]. In addition, due to the concept of quantum entanglement, quantum correlations can be made that simply cannot be achieved using a classical computer [1]. Through entanglement, a qubit is entangled with another, which dramatically increases the number of qubits that can be processed at any time [7]. The concepts of superposition and entanglement, when paired together, allow for a quantum computer's unprecedented speed-ups.

Although a universal quantum computer has not been built, physicists have been working for years to harness the power of quantum mechanics to build the next generation of

computers. Many firms are currently focusing on solving specific optimization problems, and many are uncertain about the specific industries that would most benefit from the technology. However, once the technology is more firmly established, the next step for the evolution of quantum computers will be the development of universal quantum computers which use the quantum effects of entanglement and superposition to perform any given task exponentially faster than a classical computer [6].

There has been some success in commercializing quantum computers in recent years as D-Wave, a Canadian firm, built the world's first commercially available quantum computer: the D-Wave 2000Q [8]. There is also clear momentum within the technology industry as organizations like IBM and smaller quantum start-ups are working on building superior quantum computers.

2.1 Why Quantum Computing is Different

As previously mentioned, unlike classical computers which use bits, quantum computers leverage the laws of quantum mechanics in order to complete tasks. Key concepts and functions of quantum mechanics give quantum computers their unique capabilities and unprecedented potential. Those key concepts and characteristics will be covered in this section.

What is a Qubit?

As previously discussed, classical computers use binary arithmetic in the form of a sequence of bits. In a quantum computer, a similar type of measurement known as a qubit exists. Quantum bits or qubits are represented by single particles and can have many more states than a simple 0 or 1 value [9]. Due to another quantum phenomenon known as superposition, these values can be varying degrees of 1 and 0 at the same time. In fact, qubits can be in multiple states at once. [9]. This superposition of qubits is what allows quantum computers to have parallelism, which gives them the ability to work on many computations at once. This is why with each single qubit increase in speed, a quantum computer's processing power doubles [7].

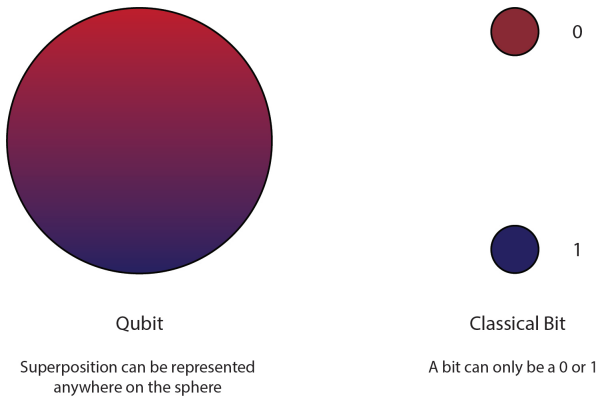

Figure 2.1: A visual representation of a qubit versus a classical bit [10]

Quantum Tunneling

In classical physics, if the gravitational potential of a barrier is too high - i.e. greater than the initial kinetic energy of a free particle such as an electron trying to pass over the barrier - the object simply cannot pass over the barrier [11]. In this scenario, the particle simply bounces against the barrier and eventually stops [12]. In quantum mechanics, the particle behaves as a wave [4]. This electron wave diminishes as it encounters the barrier, but despite the existence of a higher gravitational potential, there is always a probability that part of the wave will pass the barrier onto the other side [11]. This is due to a phenomenon known as quantum tunnelling. Through quantum tunnelling, the particle can move through the barrier as a wave and appear on the other side [12]. This quantum ability is what gives some quantum computers the potential to not only complete tasks faster but to potentially complete tasks a classical computer simply could not do within the confines of classical physics.

The phenomenon of quantum tunnelling can be explained through the macroscopic analogy of a rock rolling up a steep hill. In this scenario, we know that the ball can only go over the hill if its kinetic energy is higher than the gravitational potential of the hill itself. Otherwise, the ball will simply roll back down the hill. In order to pass over the hill, the ball will either need to surpass the gravitational potential of the hill through additional energy (e.g. an individual rolling the ball up the hill), or use quantum tunnelling to simply pass through the barrier as a wave.

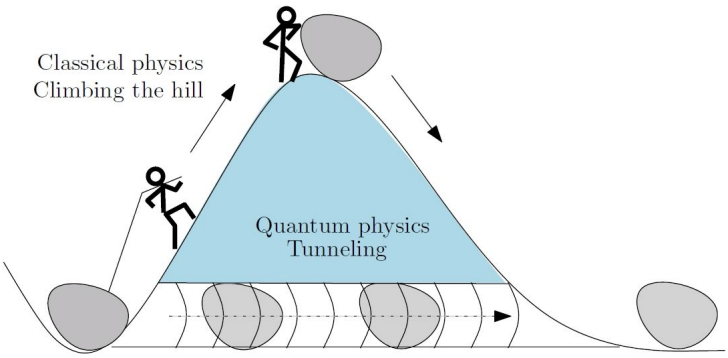

Figure 2.2: A visual representation of the concept of quantum tunnelling [12]

Quantum Superposition

We already know that quantum mechanics revolutionized our understanding of how atoms, photons and electrons behave [4] and that photons and electrons can behave as both particles and waves [4]. Some of this behaviour can seem strange when compared to our day-to-day understanding of how objects in our macroscopic world behave. One of these strange behaviours is explained by the concept of superposition. When electrons or photons are in a state of superposition, they can be in two states at once.[7]

What does this mean exactly? The concept of superposition states that these particles can be in different positions at the same time [7]. Instead of existing in a binary state, they exist along a spectrum of all possible states concurrently [13]. Even more strangely, we can never witness this state of superposition because it is lost as soon as the particles are observed [13]. Once their exact position or energy is known, they are no longer in a state of superposition. This is what makes quantum computers different, requiring their units of information to be represented by qubits rather than a classical computer's bits [13].

Quantum Entanglement

The concept of entanglement is another one that forms the basis for quantum mechanics and provides quantum computers with their powerful potential. Even Albert Einstein, who alongside fellow physicists Podolsky and Rosen penned the first academic paper proposing the concept in 1935, described it as "spooky action at a distance" and concluded that "no reasonable definition of reality could be expected to permit this." [14].

Today, quantum entanglement is widely accepted and has been proven by scientists to be in fact possible. Once a system is made up of more than one qubit, those qubits are likely to be entangled, meaning that the state of one qubit impacts the state of the other [15]. In this entangled state, the measurements of the qubits will be perfectly correlated, even at vast distances. To Einstein, this seemed to break the laws of physics, as it proposed that one

electron was sending information to the other instantly, thus meaning that the information was travelling faster than the speed of light [16]. This is why to him, entanglement was "spooky" and difficult to explain. Of course, despite entanglement, classical information still needs to be sent, so in fact the speed of light limit is not violated.

Tying this back to the aforementioned concept of superposition, entanglement puts objects in a state of quantum superposition. In this state, particles can be in multiple states at once - similar to the classic Schrödinger's cat thought experiment - simultaneously dead and alive [17]. This state is impacted and the superposition is lost once the particle is viewed and measured.[17].

The challenge presented by the paradox of quantum physics here is that while an algorithm can take entangled qubits in a state of superposition as an input, this state changes immediately upon observation, making it impossible for us to observe the output of an algorithm in a state of superposition [15]. This paradox is the challenge many scientists are trying to solve for: how to glean as much information as possible from a quantum algorithm while being unable to observe them in their state of entangled superposition[15].

2.2 The Current State of Quantum Computing

There are currently several established tech firms and some smaller, newer firms looking to become leaders in the global quantum race. Below is a summary of three major firms, the current state of their technology and their ultimate goals as it relates to quantum computing.

D-Wave

Based out of Vancouver, British Columbia, D-Wave was established in 1999 and claims to be the first quantum computing firm in the world [8]. The team at D-Wave believes that quantum computing has the potential for unprecedented breakthroughs in many fields including "...engineering, modelling and simulation, healthcare, financial analysis, optimization, logistics, and national defense applications."[8]

D-Wave sold the first ever commercially available quantum computer, the D-Wave One, to Lockheed Martin in 2010 [18]. At the time, Lockheed Martin's Chief Scientist, Ned Allen, was hoping to reduce the amount of time their engineers spent on verification and validation [19]. The team sent D-Wave a sample problem to test with its new 128-qubit computer. It is claimed that the same code that took Lockheed Martin's best engineers several months to resolve was solved by D-Wave's quantum computer in only six weeks[19].

Since then, D-Wave has consistently released newer quantum computers with higher qubit

capabilities. The 512-qubit D-Wave Two system was launched in 2013, the 1,000+ qubit D-Wave 2X system in 2015 and the 2,000 qubit D-Wave 2000Q system in 2017 [20].

D-Wave's quantum computers are annealers and specialize in solving optimization problems [21]. In the process of annealing, a series of magnets placed along a grid represent the problem being solved, and the magnets on the grid impact one another's magnetic fields [22]. The quantum computer's qubits are built out of superconducting loops [21]. At the beginning of the process, the qubits are in a high energy state [21]. The qubits are then put into their lowest possible energy state through a dramatic decrease in their temperature, until eventually they are frozen into their lowest energy state (also known as their ground state) [22]. The final orientation of the magnets in this low energy state allows them to pass through the energy barrier and provides the solution for the problem being proposed [21].

In the case of D-Wave's latest quantum computer, their cooling mechanism, known as "the fridge", provides a temperature close to absolute zero or 0.015 Kelvin - 180 times colder than interstellar space [8]. This allows them to reduce the energy state of the qubits to allow them to escape low energy valleys - making more accurate solutions possible. The aforementioned phenomenon of quantum tunnelling also allows the magnets to be cooled faster, because it reduces the chances of particles becoming trapped in energy barriers [22].

Another aspect of quantum computing currently being explored by D-Wave is how software can be developed to support quantum computers [23]. This software would need to be user friendly and available to those without extensive knowledge of quantum computing or quantum mechanics. D-Wave has begun to address this need by providing an open-sourced software known as Qbsolv [24]. This software can be shared and modified by anyone. By providing access to this and a D-Wave simulator, the company is allowing researchers and practitioners to test and shape its software [24].

Since the latest D-Wave quantum computer was released in January of 2017, D-Wave has continued to work towards newer, more powerful quantum computers [25]. Jeremy Hilton, SVP Systems, said in a recent interview that D-Wave will "continue to increase the performance of [its] quantum computers by adding more qubits, richer connections between qubits, more control features; by lowering noise; and by providing more efficient, easy-to-use software." [25] The latest D-Wave 2000Q has already been deployed for clients such as Temporal Defense System, Google/NASA/USRA and Virginia Tech and the Hume Centre which will use its system for defense applications [26].

Upon the launch of its first computer, D-Wave faced criticism for not proving that its technology uses quantum effects. It has now published studies that do show the use of quantum effects in their computers, but what remains to be seen is whether or not these effects are being used to provide a speed-up, or if the annealer model is capable of one day achieving quantum supremacy [27].

Figure 2.3: D-Wave's latest quantum computer, the D-Wave 2000Q [27]

IBM

IBM's quantum computing approach differs from D-Wave's, in that they are using the Universal Gate Model in place of the annealing model [28]. This model could theoretically be used to build a universal computer, versus one that places more focus on optimization problems [28]. IBM entered the realm of quantum firms by first fusing the capabilities of classical and quantum computers. In May of 2016, they introduced a 5 qubit quantum computer known as the IBM Quantum Experience [29]. Their online application-programming interface (API) allowed developers free access to the quantum computer housed at the BM T.J. Watson Research Center in New York via the IBM cloud [30]. Using the API, users could access IBM's quantum processor and conduct experiments, simulations and even complete tutorials on their desktop or mobile devices [29]. Using this hybrid approach, IBM aimed to engage developers who may not be as familiar or comfortable with quantum technologies and encouraged them to learn and experiment with quantum programming [30].

Within the first year, IBM reported to have had 40,000 users on the platform, with academic institutions such as MIT even using the API to teach quantum computing courses [31]. Physicist Jerry Chow, who leads the quantum computing laboratory at IBM, described this as an invaluable learning experience that helped them "build a community and an ecosystem" for the further development and adoption of quantum technologies [31].

In March of 2017, approximately ten months after the launch of the Quantum Experiment, IBM introduced a revised API and upgraded simulator for the Quantum Experiment [32]. In addition, it announced plans for the launch of a new initiative called the IBM Q [32]. Officially launched in May 2017, it is described as the pioneering industry initiative to build a universal quantum computer [33]. It introduced IBM's most powerful quantum computers to date: a 16 qubit processor for continued experimentation by developers via the IBM cloud, and a 17 qubit processor as their first commercial processor to date [33].

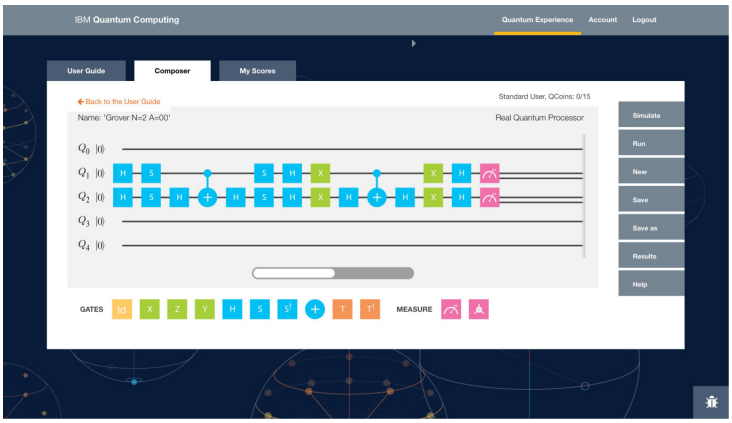

Figure 2.4: A screenshot of the quantum programming interface launched by IBM. The programmer allows users to visualize quantum objects and intuitively reposition them to write and test programs [29]

Despite D-Wave's impressive 2,000 qubit computer, every increase in qubits on a processor increases the chances for errors and the need for error corrections [26]. A Universal Gate Model quantum computer such as the one IBM has built can be built on as few as 50 qubits and need significantly less error correcting to potentially prove quantum supremacy [28]. As a result, although IBM's qubit numbers are significantly lower compared to D-Wave's 2,000 qubit computer, they are made using a different model and could form the basis for the world's first universal quantum computer.

In addition to building their qubit capabilities, IBM's focus remains on the quality of each additional qubit rather than just the total number of qubits. In their press release announcing the IBM Q, they specify that the computational power of a quantum processor is not solely dependent on the number of qubits. [33]. Due to the unstable nature of quantum data and the level of noise that can affect the coherence of the data, quantum errors must be minimized as each additional qubit is added to a circuit [33]. To reduce charge noise, IBM's quantum computers are built using a superconducting qubit known as the Transmon Superconducting qubit [34]. Invented by physicist Robert J. Schoelkopf in 2001, this type of qubit reduces charge noise and allows for a longer coherence – i.e. the length of time a qubit retains its quantum state [34].

IBM also uses a metric known as Quantum Volume to account for the quality of their "qubits, circuit connectivity, and error rates of operations" [33]. As an example, if a computer's processor were to be improved by 100 qubits while there is a zero error rate decrease, the Quantum Volume increase would be zero. In order to build a powerful quantum computer, the error rate must be decreased and the quantum volume should be increased with each added qubit [35]. IBM claims that their first commercial quantum processor has significantly better Quantum Volume than their previous processors and that

their focus remains on increasing this volume and qubit capabilities [33]. IBM's goal in the near term is to prove quantum supremacy, which they believe can be done once they reach 50-100 qubits of power on their quantum processors. Although IBM has not provided firm timing on this, they state that they expect to reach this milestone within the next few years [36].

Google

Google's foray into the world of quantum computing began with a partnership with the previously mentioned Canadian firm, D-Wave. In 2009, Google's Technical Lead Manager, Hartmut Neven announced through a blog post that their team has been working with D-Wave to test quantum adiabatic algorithms to find better solutions for optimization problems than currently exist with a classical computer [37]. Google worked with their algorithms and D-Wave's hardware to detect cars in a series of images. They concluded that their algorithms in partnership with the D-Wave hardware was able to outperform any of their classically trained data centre computers [38].

In 2013, Google continued their work with quantum computing when they partnered with the Universities Space Research Association, a non-profit research corporation and NASA to launch the Quantum Artificial Intelligence Lab [39]. As part of this partnership, Google and the Universities Space Research Association purchased the 512-qubit D-Wave Two system [39]. Housed at NASA's Ames Research Center, the computer was used to further test machine learning algorithms [40].

In September of 2014, Google began shifting its strategy by announcing that it would be building its own quantum computer [41]. John Martinis, a professor at University of California, Santa Barbara's Physics department, was hired by Google to establish a lab which would produce a new type of quantum chip. Martinis is well known in the field of quantum physics and in July of that same year, had published a paper in Science Magazine where he tested the D-Wave Two system purchased by Google, and concluded that there was "... no evidence of quantum speedup when the entire data set is considered [42]." D-Wave of course challenges these findings and states that the wrong types of algorithms were used to test its technology [43].

Since joining Google, Martinis and his team have successfully built and tested a 9 qubit computer and are now scaling towards a 20 qubit computer [44]. The team's goal is to build a 49 qubit computer that achieves quantum supremacy by the end of 2017 [44]. This would be made up of 7 by 7 configuration of superconducting qubits [45]. The team hopes to simultaneously achieve a two-qubit fidelity of 99.7%, which put simply, means a system with lower error rate. They are currently working with a 99.5% fidelity [46].

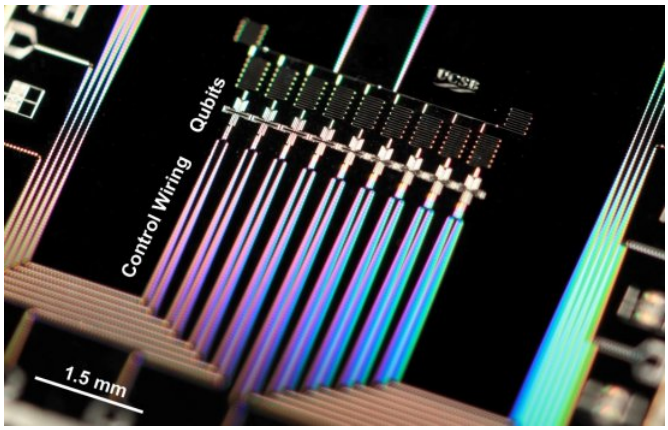

Figure 2.5: An image of Google's 9 qubit superconducting quantum chip[47]

In order to demonstrate that their quantum computers behave according to the laws of quantum physics, the team at Google begin with their qubits in a quantum state [48]. They then allow the qubits to evolve and compare their final states to the final states provided by the simulations of the experiment conducted on a classical computer. If the evolved state of the qubit aligns with the simulation created on a classical computer, they have successfully proven that they are performing quantum computations [48].

While focusing on demonstrating their computer's quantum computations at every step - a feat that D-Wave is often criticized for not doing - the team at Google also aims to build qubits that have a higher coherence - meaning that they can maintain a quantum state for a longer period of time [49]. Martinis' team builds qubits using tiny superconducting circuits and test their coherence with every qubit progression [50]. They describe their approach as different from D-Wave's, saying that the team at D-Wave focuses too much on the number of qubits and not enough on the coherence time [50].

Martinis believes that their team will be capable of proving quantum supremacy in 2017, but states that solving real world problems using quantum computers will not happen for another five to ten years [50]. Nevertheless, as unpredictable as things may remain in the quantum world, proving quantum supremacy will be an integral feat for the future of the industry, regardless of who achieves it first.

2.3 The Potential Applications of Quantum Computing

Although there is some uncertainty around which industries may benefit most from the advent of a powerful quantum computer - with some even asserting that we may discover new applications we couldn't fathom before - there are certain areas that most agree show promise. This section provides a broad overview of the potential applications of this technology. Please note that there is a wide range of potential applications for quantum computers. Although only three areas are covered here, quantum computers could revolutionize a wide range of fields, allowing for more efficient drug development, weather forecasting and even traffic control.

Data Processing and Quantum Machine Learning

Scientists have already proven that quantum computers could vastly improve our ability to process large amounts of data [51]. Using quantum superposition, a quantum computer could make several computations simultaneously, allowing it to identify patterns in data much faster than a classical computer [52]. As a result, quantum computers could be useful in any field where large amounts of data must be processed and understood.

Today, machine learning is a commonly used tool for managing big data. A familiar term within the tech and business communities, machine learning allows us to process large amounts of data and find patterns in that data to predict future behaviour [51]. With the increasing digitization of our society, this data is growing at a rate of approximately 20% per year [53]. This growth makes it more challenging to devise machine learning algorithms that are efficient and accurate [51]. This is where quantum machine learning could come into play.

When a quantum computer with a sufficient number of qubits is commercialized, quantum machine learning will allow us to tackle the problems currently handled by classical machine learning [53]. Quantum computers running quantum algorithms - due to their very nature - would be able to process our ever growing pool of data much more efficiently, saving both time and resources. This is especially true of nearest neighbour, kernel and clustering methods algorithms, which can see the most significant speedups through quantum computation [51].

Quantum Simulations

Currently, scientists use numerical simulations to predict the behaviour of our physical world, and can even use them to simulate simple molecules. However, there are many calculations that require more computing power than we currently have available [54]. This is especially true when attempting to simulate a quantum environment, as the simulations

are too complex and too exponentially large for a classical computer [54]. The power of a quantum computer could allow us to truly simulate a quantum environment.

Using a quantum computer, one could simulate the behaviours of the microscopic world, which would allow scientists to conduct virtual experiments, modelling the behaviours of atoms and particles in very specific conditions [55]. This would make modelling chemical or biological reactions a reality, which could result in groundbreaking discoveries [55]. By allowing scientists to simulate molecules, a quantum simulation can reduce the length of time currently spent testing the properties of a molecule for things like drug discovery. Currently, to develop a new molecule for a drug, scientists must test many of the existing millions or trillions of possible molecules for the right properties. A quantum simulator could help us understand how drugs may act within the human body, by simulating the behaviours of complex molecules like cholesterol and finding the "needle in a haystack" molecule with the desired properties much more efficiently.

In August 2016, Google and Harvard University announced that they had successfully modelled electron interactions in a complex molecule [55]. They believe this shows the true potential of quantum simulations, and that this area is "the most valuable application for a quantum computer." With the market for fine chemicals worth nearly $3 trillion, this is definitely one of the major areas of economic and scientific opportunity [55].

Quantum Security

Wireless communication systems are omnipresent in today's world and are used in our everyday lives as we conduct financial transactions, send e-mails or even browse the Internet. As you shop online and input your credit card number, you are giving away confidential information and trusting that the private firm is able to keep your data safe. As a result, any communication system must protect the confidentiality of data whilst providing proof of its authenticity [56]. This is especially important when dealing with large amounts of data, as their breach can put the security of businesses, institutions and governments in jeopardy.

Cryptography plays an important role in ensuring the confidentiality of our data. Through cryptography, an algorithm is used to protect a message with a "key." The resulting cryptogram is meant to be secure, only breakable by the those who have access to the key [57]. Today, cryptography is not only used to keep confidential information private, but it also serves other purposes including customer authentication or digital signature validation [56].

Although current classic communication and cryptography methods provide some protection for the massive amounts of data we are collecting today, they are far from perfect [56]. Despite encrypted keys, current cryptography methods are still vulnerable to outside forces, as evidenced by the growing number of data breaches taking place worldwide. An independent study by Ponemon Institute found that the cost of data breaches are increasing

every year. The per capita cost of data breaches increased from $250 in 2015 to $278 in 2016 and the total organizational costs went up from $5.32 million to $6.03 million year over year [58]. In addition, the potential introduction of a quantum computer could put these already vulnerable security mechanisms at an unacceptable level of risk.

This is where quantum security and quantum cryptography can come into play. As discussed earlier in this section, quantum computers have unprecedented potential due to quantum concepts of superposition and entanglement. Due to the very nature of quantum mechanics, if information is sent from one party to another using a quantum channel, and the encrypted key is tampered with by a third party in any way, the quantum state of the key changes, alerting both parties to tampering [59].

A simple example of how quantum encryption work is as follows: If Bob is sending a message to Alice, he would send Alice the key as binary numbers using polarised photons. He will choose a vertical polarisation for each zero and a horizontal polarisation for each one, at random [7]. Alice will receive the message and measure the polarisation on each photon using a vertical or horizontal filter [7]. Then, Alice and Bob can compare notes to see if Alice used the correct filters for each bit. They will then discard any bits for which the wrong filter was used, leaving the remaining bits which are the key for the quantum encrypted message [7]. By using photons to send and encrypt messages, quantum cryptography can allow for secure encryption that cannot be broken, regardless of future advances in mathematics or quantum computation [56]. This technology has the potential to safeguard the growing volume of data being collected, and could reduce data breach incidences which are costing businesses across Canada millions of dollars every year.

Chapter 3

Literature Review

Although quantum computers that could solve new, currently inaccessible problems are still years away (as few as five or as many as ten years based on the work being done by current firms), there are several important challenges that must be addressed to prepare for their eventual, broad commercialization.

This section covers academic works that address three such issues, 1) the proven challenges of commercializing new technology, 2) the security risk posed by quantum computing and 3) the need to prepare Canada's workforce for a quantum future. The findings in these academic works provide applicable learnings for the successful introduction and adoption of quantum computing by a broader public.

3.1 Identifying the Challenges in Commercializing Quantum Technologies

Quantum Key Distribution (QKD) technology has passed the stage of research and development to be more broadly commercialized in recent years. However, there are several challenges being faced by the commercialization of this new technology, which are relevant to quantum computing's foray into the mainstream [60].

QKD is used to send and receive encrypted information by firms and is key to the security of the firms using it. Although this technology is already being used by cybersecurity firms, there are no standard measurements or certifications in place for testing their validity. As a result, the European Union has funded a project called the "Metrology for Industrial Quantum Communications" (MIQC), which is aiming to provide standards for this

emerging technology.

In [60], Natesh, Gbadegeshin, Rimpilainen, Imamovic-Tokalic and Zambrano, examine the barriers present in commercializing QKD technologies. The aim of this research is not to specifically help QKD commercialization, but to help future researchers and innovators understand the challenges they may face as they develop and launch new products.

The researchers of [60] identified five potential challenges for the commercialization of QKD technology.

1. Market size
2. Possibility of building the supply chain
3. Availability of technology validation/certification
4. Availability of infrastructure for the new technology
5. Possibility of offering after sales services (especially product update and maintenance)

After defining these challenges, the team wrote five interview questions to be included as part of a larger survey for the MIQC's mandate of standardizing the technology.

1. Do you think that the market size of quantum cryptography can affect its commercial implementation?
2. How important is the development of standards and quality assurances related to the commercial QKD system in order to ensure the commercial success of this technology?
3. How important is the development of a metrological infrastructure for characterizing the optical components of QKD systems in relation to the development of standards for the market take-up of the QKD technology?
4. In your opinion, what do you think can hinder commercial implementation of quantum cryptography?
5. An empirical study on the commercial implementation of quantum cryptography revealed that building of supply chain, technology validation/certification, a lack of available or adequate infrastructure, and after-sales services are the most serious challenges facing successful commercialization of quantum cryptography. Do you agree?

100 employees of QKD technology firms were contacted and 60 participated in the survey. The survey collected both quantitative and qualitative data from participants.

The qualitative findings of the survey were as follows:

1. *Small market size and distribution channels*: Developing market for a net new technology is highlighted as a key challenge. This is especially problematic if the market for a product is scattered geographically as it increases marketing, sales and service costs.

2. *Building a supply chain*: Many QKD companies identified finding appropriate suppliers as a challenge. Due to the newness of the technology, many existing supplier products require tweaks in order to work with the new technology. The most challenging supply chain factor however, was the development of the correct supply chain as the new technology may have applications that cannot be provided by existing services.

3. *Technology validation or certification*: This was touched on earlier in the literature review and was in fact validated through the surveying of QKD employees. Setting validation standards for new technology can be expensive and time consuming, taking limited resources away from firms that are attempting to launch groundbreaking technologies. In addition, many metrics applied to existing technology cannot be applied to new technology, which means the involvement of the metrology community is required.

4. *A lack of available or adequate infrastructure*: Many participants flagged a lack of existing infrastructure to support QKD technologies. A comparable example would be the requirement for 3G technologies to support smartphone usage. Comparable infrastructure needs for QKD are preventing the technology from reaching its full potential.

5. *After-sales services such as product updates and maintenance*: Updating and maintaining the technology that has been sold to clients is also flagged as a challenge by many participants. This takes considerable time and resources, and only yields returns over the long term, which is a challenge when considering the niche market many QKD firms are currently serving.

The quantitative data highlighted the following findings:

1. 85% of participants believe market size impacts successful commercialization.

2. 82% of participants believed a lack of sufficient infrastructure, small market size, difficulties of building a supply chain and a lack of validation/certification standards were huge hinderances in the effective commercialization of QKD technologies.

3. A lack of customer awareness for the need of QKD technologies was also highlighted as a key challenge, with one respondent saying that most clients do not feel any urgency to switch to the new technology.

4. Government regulations and technical developments were also flagged as challenges, highlighting the importance of government support for innovation and the development of specialized talent.

Based on their research and primary and secondary surveying, Natesh et al. concluded that these findings could be applicable to other innovative technologies and advise that academics and entrepreneurs consider these challenges as they begin commercializing a new technology.

Implications for Quantum Computing

The findings in [60] by Natesh et al., highlight some key challenges for the commercialization of QKD technologies which can be applied to quantum computing. It is important that those developing quantum computers take these challenges into consideration as they test their products and prepare for mass commercialization. The Canadian government should also take note of these potential roadblocks as they further develop their innovation strategy, and invest more dollars into this emerging technology. The government should also be mindful of how current regulations can challenge the successful launch of quantum technologies and work closely with incubators, academic institutions and quantum firms to ensure the commercialization process addresses such challenges.

Natesh et al. highlight the lack of awareness amongst the general public as a challenge for QKD technology's commercialization. Quantum computing will face this same challenge as many even within the technology industry do not have a firm understanding of quantum computing's potential. Furthermore, a lack of standardized metrics for the capabilities of quantum computers will exacerbate these existing challenges. As covered in Chapter 2, many firms are using different models to develop their technologies and these differences, although significant to quantum physicists, are difficult to communicate to those without a physics background. As a result, it could be challenging to market such products and to benchmark performance.

For example, although IBM's goal is to build a quantum computer with 49 qubits, D-Wave's computers already boast 2,000 qubits. This of course is due to the fact that D-Wave's computers use the annealing model, whilst IBM's use the universal gate quantum model. These differences will not be distinguishable for the average consumer, highlighting the need for the appropriate validation of the technology ahead of mass commercialization. The lack of appropriate validation metrics could also impact the potential market size of the technology and slow the rate of adoption. If potential clients do not feel they understand the technology and its associate benefits and risks, they will be more hesitant to adopt the products, making the initial launch of quantum computers more resource intensive.

The challenge of building a supply chain and a lack of adequate infrastructure could also prove to be a challenge to quantum firms. As covered in Section 2, many firms are currently working on building and testing software that could be compatible with existing classical

infrastructure. This is one challenge that has already been identified by quantum firms. There may be other less predictable infrastructure and supply chain gaps that could arise as the technology becomes more commonplace, and as the products begin to require continued maintenance. Quantum firms should partner with academic and government institutions to conduct research that identifies these potential gaps prior to commercialization.

3.2 Quantum Computing's Threat to Cybersecurity

We know that the ultimate goal of many quantum firms is to build a quantum computer that can prove quantum supremacy and solve universal problems faster than even the fastest supercomputers in existence today. Although this could allow us to solve for many of humanity's most pressing problems, it will also prove challenging to the existing cybersecurity infrastructure in place at many firms and institutions. One of the most fundamental pillars of cybersecurity is cryptography, and a quantum computer could be capable of breaking all of a classical computer's public-key cryptography, leaving the international community's cybersecurity at risk [61].

in [61], a report by the Institute for Quantum Computing and the Department of Combinatorics and Optimization at the University of Waterloo, author Michele Mosca highlights some of the risks posed to cybersecurity with the advent of a more advanced quantum computer. The report estimates that based on the current work being done by quantum firms, a quantum computer advanced enough to threaten existing cryptography could be available in less than ten years.

In an example, the report defines the number of years cryptographic keys must remain secure – *the cryptographic shelf life* – by x. The amount of time it would take to build and deploy quantum safe cryptographic keys is defined by y or *migration time*, and the number of years before a quantum computer could break existing public-key cryptography tools is defined by z or *collapse time*. The team proposes that if $x + y > z$, our cybersecurity is at an unacceptable level of risk. Meaning that if the amount of time our current cryptography can remain secure plus the amount of time it takes for us to deploy new, quantum resistant cryptography is longer than the estimated amount of time it would take for a quantum computer to break existing keys, the very fabric of our cybersecurity is under threat.

This report proposes two possible sets of solutions:

1. *Post-quantum Cryptography*: These are conventional ciphers based on mathematical problems that we believe could resist a quantum attack. The benefit of this solution is that it works with existing classical software and hardware, but its ability to resist a quantum attack would be based on the assumed computational hardness of the

problem, which can be difficult to predict.

2. *Quantum Key Distribution (QKD)*: Covered briefly in Section 3.1, QKD uses a quantum channel to send and receive bits of information. Currently, QKD can send information between short distances, but could potentially send information over global distances in the medium and long term. With QKD, there is no need for computational assumptions of the hardness of a problem.

This report emphasizes that the best cryptographic ecosystem uses both sets of solutions in combination. Depending on the required *cryptographic shelf life* of a firm, they could choose to use one method or the other. In addition, using both methods in conjunction can allow for security features that would not be possible if using each in isolation.

As covered in Section 3.1, QKD is still in the earlier stages of commercialization, and is facing many challenges including a lack of certification standards for the technology. This report asserts that extensive research and development of QKD technologies is needed in order for them to become a widely deployable global security solution. The potential of this technology will be met only when the needed infrastructure, including satellite QKD and untrusted quantum repeaters, are widely available. Despite this, it is vital that any future cryptography standards are made compatible with QKD solutions.

Similarly, post-quantum cryptography requires further research and testing of its resistance to attacks using varieties of problem hardness and resource constraints. Without such studies, it is hard to say how resistant they could be to potential quantum attacks.

This report asserts that we are still many years from being able to deploy quantum resistant cryptography and recommends that a holistic approach to preparing cybersecurity for a quantum world begin right away. This approach must focus on:

1. Setting specific QKD validation standards
2. Training a new generation of cryptographers who not only understand conventional cryptography but are able to understand and deploy QKD technologies
3. Developing business and policy practices that encourage adoption of QKD technologies whilst driving businesses to focus on strengthening their cybersecurity strategies

Implications for Quantum Computing

The issues faced by QKD technologies provide learnings for the quantum computing industry. As Canada works to develop superior quantum technologies, it must work to concurrently protect the cybersecurity of the nation. In fact, the government has already taken steps to do so, announcing on April 27, 2017 that they would be investing $80.9 million in funding to the Canadian Space Agency [62]. Part of this investment is towards the Institute for Quantum Computing's Quantum Encryption and Science Satellite (QEYSSat)

project [62]. This project focuses on cybersecurity, aiming to solve the aforementioned challenge of sending secure cryptographic keys between larger distances using QKD [62].

The National Research Council Canada (NRC) also works with business and academic institutions to develop "quantum-enhanced cyber security solutions" [63]. Businesses are able to contract out the resources of the NRC to develop more stringent cybersecurity systems that could meet the increasing number of security threats, including quantum computing [63].

Canada also has a cybersecurity strategy which is a three pronged plan for preparing Canada for cybersecurity threats [64]:

1. Securing Government Systems
2. Partnering to secure vital cyber systems outside the federal government
3. Helping Canadians be secure online

Although both of these steps are vital to the development of quantum resistant cryptography, the government should also work to more actively promote the services provided by the NRC, and perhaps incentivize the strengthening of private firms' cybersecurity via a holistic public and private cybersecurity strategy. The ongoing development of quantum resistant cybersecurity measures will be key to protecting the interests of Canadians as we enter a quantum world.

3.3 Preparing Canada's Workforce for a Quantum World

[65] is a report by Lamb and Doyle for the Brookfield Institute for Innovation + Entrepreneurship (BII+E). It highlights the technological trends seen in the Canadian workplace and the challenges and opportunities this may present to young Canadians entering the workforce. It also provides potential solutions to the challenges and opportunities Canada's young workforce will face [65].

As our world becomes increasingly automated, the nature of work will also change. Some believe that this increase in automation will lead to extensive job losses, while others assert that some repetitive jobs may become automated, opening the way for net new roles that keep the level of employment consistent. Although it is hard to predict the net impact of new technologies on the economy, it is estimated that around 42% of the workforce is at risk of being affected by automation. While this number may sound alarming, it is likely that these roles will simply change from routine labour to providing valuable skills that cannot

be replicated by a machine [65].

Despite the uncertainty around the full impact of automation on the Canadian workforce, it is clear that the trend for employment is skewing towards technology driven roles that require specialized skills. Between now and 2020, it is projected that computer and mathematical jobs - mainly data analysts and software developer roles - will be in demand across many industries, including financial services and media and entertainment. Over the next ten years, more than 60% of job openings will be for roles that require post-secondary education. These very same roles are at a low risk of automation [65].

In addition to the changes being driven by technology, the way we work is also changing, with the "gig economy" making the state of work more precarious for many young people. Holding temporary contract positions is beginning to become the norm, with some youth saying they choose to freelance and enjoy the flexibility it provides, whilst others describe feeling uneasy at the prospects of not having a stable job [65].

Aside from these changes, there are also concerns that there is unequal access to opportunities for youth. Youth between the ages of 20-24 who are members of a visible minority have higher unemployment rates. Women are also underrepresented in science, technology, engineering and math (STEM) fields and are much less likely to enrol in such programs in university. In order for Canada to grow its potential and become a leader in the technology sector, it must ensure a more diverse representation of individuals across industries [65].

Another challenge faced by young workers entering the workforce is the paradox of trying to gain hands-on work experience but needing work experience in order to land their first job. Educators who were surveyed feel students are being well prepared for work, whilst employers and students themselves feel unprepared. This suggests that employers should provide some of the training needed to complement the formal education young Canadians receive. However, most employers in Canada are reducing the investment in skills development, with the amount firms provided in employee training declining by 40% since 1993 [65].

Overall, the report asserts that youth will need to have a broad set of hard and soft skills in order to succeed. They must have a high degree of digital literacy and gain hard skills such as coding which are becoming increasingly important. An entrepreneurial mindset that allows them to take risks and manage change will also be valuable. Young Canadians should know that upon entering the workforce, it is vital for them to continue updating their skills and set a pattern of lifelong learning in order to keep up with the rapid pace of change [65].

The authors of this report propose that all sectors including government, the public sector and the non-profit sector work together to remove the boundaries that can silo them from the work they are doing to train young Canadians.

The report provides the following recommendations for preparing Canada's youth for the workplace:

1. *Develop work-integrated learning (WIL) models applicable to different sectors*: WIL would allow students to apply the theories being taught in school in a practical work environment. This could address the increasing need for both hard and soft skills in the workplace, and allow employers to play a more active role in preparing their own workforce. This is especially important as the Canadian workforce is aging and traditional entry level roles are declining.

2. *Explore digital literacy programs for youth across Canada, including in urban, rural and remote communities*: Access to formal and informal digital literacy education, especially in underrepresented communities, will be key to preparing Canada for the future of work.

3. *Identify and address potential barriers to youth entrepreneurship and intrapreneurship*: Youth should be taught entrepreneurial skills from an early age to allow them to prepare for a world with increasing risk. There should be an understanding of how different demographic groups learn in order to ensure a diverse group of Canadians have these key skills.

4. *Provide timely labour market data, career planning and mentorship support for youth entering the labour force*: Given the fast pace of change in today's workforce, youth need to know about the available opportunities in a timely manner. They should be given access to labour market information before, during and after their formal education and provided with mentorship that allows them to navigate an increasingly complex work environment.

5. *Enable lifelong learning and rapid, job-specific upskilling and retraining*: Employers, government and educators need to provide resources that allow Canada's young workforce to develop habits of lifelong learning that prepare them for the rapid pace of change in technology.

6. *Develop a data strategy to build a stronger evidence base for policy and program solutions*: New research is needed to get a clear understanding of today's workforce needs across Canada. By tracking key trends in the labour market, governments, employers and educators can better intervene and prepare Canada for the future of work.

Implications for Quantum Computing

As Canada's technology sector continues to grow, there is an increasing need for specialized talent that can fill the high demand roles of the sector. The technology sector in Canada alone is responsible for $117 billion in output and will need a continued flow of specialized

talent in order to continue its success [66]. Quantum computing falls under this sector and will continue to grow if the investment seen to date continues.

As quantum computing firms establish themselves in Canada and begin to grow, they will need increasingly specialized talent or Highly Qualified Personnel (HQP). HQPs are individuals in the fields of science and technology who have university degrees at the bachelor's level or higher [67].

Some of the challenges highlighted by authors Lamb and Doyle in [65], directly affect quantum computing firms, including the need for training youth to be prepared for computer and mathematical based jobs. Ensuring digital literacy and continued learning will also be key, as quantum technologies are rapidly advancing. Quantum computing firms will require a wide range of experts including quantum physicists, software developers and business professionals with an up-to-date understanding of quantum technologies, their capabilities and challenges. It is important that the government, employers and academics work together to ensure Canada's young workforce is ready for the specialized skills of this emerging field.

Chapter 4

Methods and Materials

4.1 Survey Participants

In order to gain a better understanding of the current state, capabilities and perceptions of quantum computing, online surveys were sent to three distinct group of participants. Please refer to Appendix A in chapter 6 to see the list of questions for each survey group. The participant criteria and logic for the selection of each group is detailed below:

1. *Quantum Computing Firm Employees*: Canada is home to some of the world's leading quantum technology and quantum computing firms. Seven individuals employed at five firms building quantum computers or working with quantum technologies completed an online survey. The survey for this group asked about the size and value of their technologies and services, the types of industries they serve, and how they see the future of quantum computing evolving over the next 0-10 years.

2. *Academic Institution Employees*: Several of the world's leading research universities and quantum computing institutions are located in Canada. Six individuals from three such institutions completed an online survey. The survey asked about their research, in addition to their perceptions of quantum computing's evolution in Canada over the next several years.

3. *Employees of Firms Using Machine Learning*: If quantum supremacy is achieved, quantum computers could provide exponential speed-ups to firms using machine learning algorithms. As a result, nine individuals from nine unique firms using Machine Learning algorithms completed an online survey about their work. Individuals surveyed work at firms that provid B2B or B2C services through the use of machine learning algorithms. Those using machine learning to optimize aspects of

their work were also included in this pool. In addition to asking about their industry and the specific algorithms they use in their work, the survey aimed to gauge their understanding and openness to adopting quantum technologies.

Potential survey participants were reached out to via e-mail and social media. Experts in each field were found using online searches of university websites and LinkedIn. Snowball sampling was also used to reach out to possible participants. If individuals expressed interest in participating, some sample questions were provided to them to ensure they were aware of the types of questions they would answer. They were notified that they had the option to opt out of completing the survey at any time and were given the option to skip questions they believed asked for potentially confidential information.

Quantum Computing Firm Employees

The seven participants for the quantum specific survey hailed from five unique firms and each held the following positions within the industry:

- Quantum technology consultant at a quantum computing firm
- Quantum computing programmer at a quantum computing firm
- CEO and founder of a quantum computing firm
- Two research leads at a quantum software company
- Software developer at a quantum cryptography firm
- CTO at a quantum cryptography firm

Academic Institution Employees

The six individuals from three unique academic institutions specialized in the following:

- Three academics at the Institute for Quantum Computing
- Faculty member at the Perimeter Institute
- Academic at the Centre for Quantum Information and Quantum Control (CQIQC) at the University of Toronto
- Academic at the Institute for Quantum Science and Technology, University of Calgary

Employees of Firms Using Machine Learning

The nine individuals from nine firms using machine learning algorithms had a variety of roles within the Information Technology (IT) industry. They all have direct experience working with machine learning algorithms:

- Vice President at a leading IT firm

- Machine Learning expert at a private equity firm
- COO at a machine learning firm
- Software developer at a leading computer software firm
- Machine learning researcher at a leading financial institution
- Machine learning engineer at an IT firm
- Co-Founder at a firm using machine learning algorithms
- Data scientist at a machine learning firm
- Director of machine learning at a computer software company

4.2 Key Findings

Quantum Computing Firm Employees

The qualitative responses to the survey highlight several trends, including uncertainty around the market size (volume and value) of quantum industries. Amongst those surveyed, 71.4% are not certain about the volume and values of the firms they are employed at, and highlight this area as something that is currently being investigated. 28% of respondents opted to skip this question.

Several respondents flag regulatory and security implications for the increasing prevalence of quantum technologies. When asked if they foresee any potential regulatory hurdles for the government, 43% mention the need for updated encryptions and security measures as this technology matures. One respondent states that "[security] vs Privacy will continue to be a big issue that governments will grapple with."

When it comes to increased interest and investment in the field, 71% of respondents have noticed a spike in Venture Capital (VC) funding, which one respondent believes is indicative of the technology "...tipping into being a 'real' area. Much like AI 5 years ago." 71.4% of respondents believe there will be continued VC investment in the field in the medium (5-9 years) and long term (10+ years).

The quantitative data highlights some interesting trends. Only 28.6% of respondents believe a lack of needed talent is hindering the production of quantum technologies today, while 85.7% of respondents identify a lack of understanding of quantum technologies by organizations and the public as the biggest barrier for the effective post-launch adoption of quantum technologies. Although a need for specialized talent at this time is not flagged,

71.4% of respondents believe a skills gap will exist for the future needs of the technology. Physicists (80%) and academics (60%) are the two skills seen as the most scarce.

Financial services (85.7%), health and medicine (71.4%) and security (71.4%) were ranked as the top three industries to benefit most from the successful adoption of quantum technologies.

Academic Institution Employees

The qualitative results of the academic survey also highlight some interesting trends. 83% of respondents believe that there is a need for the planning and development of new academic programs for the future skill needs of the industry. 80% of those respondents believe the field of engineering will be most impacted with one respondent saying that "[Quantum] technologies [are] becoming more of an engineering problem than a fundamental problem. Thus engineering expertise is becoming much more relevant." Another respondent who also highlighted quantum engineering as an area of need, believes significant investment is needed to train talent to design and develop new devices and technologies, and states that although quantum technology research has been conducted, there is a need to "...get this science out of the laboratory."

Only 33% of respondents identify security and cryptographic concerns as having regulatory implications for the government, with 50% stating that they see no regulatory implications and 16% stating that they do not know if there are any regulatory implications. The 33% who identify cryptographic concerns believe quantum technologies "... have significant cryptographic implications which governments need to deal with" and that there is a need ".... for policy development around privacy, communications, and standards development and adoption."

The quantitative data for the academic survey group reflects some similar trends as the quantum computing group. Only 16.7% of respondents believe a lack of technical talent is a barrier to the launch of quantum technologies, whilst 50% believed prohibitive production costs can hinder development. The biggest barriers for the adoption of the technology are identified as a lack understanding of quantum technologies by organizations and the public, as well as prohibitive purchasing costs. In addition, 66.7% of respondents believe there will be a need for more physicists and computer programmers as the technology matures.

83% of academic respondents state that they have noticed an increase in government funding in quantum technologies, with 66.6% expecting increased funding over the short term (0-4 years), 83.5% over the medium term (5-9 years) and 83.4% over the long term (10+ years).

100% of respondents identify security and health and medicine as industries that would benefit most from quantum technologies. 66.6% identify communications and 50% financial services as priority sectors.

Employees of Firms Using Machine Learning

The qualitative responses by employees of firms using machine learning algorithms show that 55% of respondents would like to automate some tasks that currently cannot be automated due to their complexity. Respondents highlight the following in the open answer section of the survey:

- "We would always like to automate more complex dialogue interactions"
- "Autonomous Agents"
- "Clique detection"
- "...manufacturing and warehouse automation thru [*sic*] robotics"
- "Monitoring if the model went stale or not"

The quantitative results showed that respondents currently use a wide variety of machine learning algorithms in their work. The most commonly used are Support Vector Machine (SVM) (100%), linear and logistic regression (88.9%), decision trees (77.8%) and random forest (77.8%).

55.6% of machine learning firm employees surveyed identify Information and Communication Technologies (ICT) as one of the industries their products cater to. 33.3% identify finance and 22.2% also identify energy, automotive and healthcare.

77.8% of respondents use machine learning algorithms for computer vision (object recognition) and information retrieval, and 55.6% use them for translations and language learning.

The survey had interesting results regarding the amount of time spent running algorithms. 44.4% of respondents spend more than 62 minutes running any one algorithm. It must be noted that 22.2% of respondents opted not to answer this question.

44.4% of respondents show some uncertainty about using quantum technologies if they became available to them. Uncertain data security (55.5%) and a lack of understanding of the technology's capabilities or limitations (55.5%) are listed as the top reasons for this hesitation.

4.3 Analysis

Investment Trends in Quantum Computing

Overall, both academic institution employees and quantum firm employees have noticed a marked increase in investment by both private VCs and the government institutions. This is not surprising, given that D-Wave alone has raised $200 million from investors to date, and the government has funded millions of dollars in research at academic institutions like the Institute for Quantum Computing at the University of Waterloo [68]. What this reaffirms is that there is marked interest in the development of this technology, and the continued investment into it could help the technology move past its current niche applications, impacting a variety of industries.

In order to prepare for this likelihood, Canada must address the uncertainty around the potential impact of this technology on the economy and the workforce. The majority of those at quantum firms are not certain about the potential size and volume of their technologies, making it difficult to project the monetary and workforce implications of quantum technologies at this time. Although this research shows that academics and quantum firm employees believe health and medicine, communications, financial services and security are the major areas that could benefit from the technology, the sample size of this study is small. By partnering with academic institutions and quantum firms, the government could lead research that will allow us a better understanding of the realities of a quantum world. This would allow Canada to understand which industries may be most impacted, allowing the government to anticipate and plan for potential areas of investment.

Preparing the Canadian Workforce

The research results show that although a shortage of HQP is not hindering the development of quantum technologies today, it is a concern for both academic institutions and quantum firms as the technology becomes widely commercialized. Based on the qualitative responses from academics, engineering is a field that will be widely impacted by quantum computing. Significant investment is needed to train engineers who have a comprehensive understanding of quantum computers, and who can design and develop devices based on quantum models. Both groups also flagged the need for more physicists, which should be a consideration for both academic institutions and government bodies.

Improving Quantum Literacy Amongst Businesses

Both academic respondents and quantum firm employees identify a lack of understanding of quantum technologies by organizations and the public as a major barrier to their adoption. This concern is reflected in the survey results of machine learning firms, as nearly half expressed uncertainty around using the technology and 55.5% cited a lack of understanding

of the technology as the reason for potential hesitation.

As a result, it is key that government and academic institutions work closely with quantum firms based in Canada to educate the business community on the potential of quantum technologies. It is important that businesses that could benefit from this technology have a preliminary understanding of it, making them more likely to be early adopters. This is also reflected in the literature review in section 3.1, which highlights one of the key barriers to the adoption of QKD technologies as a lack of general public awareness.

Addressing the Threat to Cybersecurity

Academic and quantum firm employees flagged the need for analyzing and preparing for the impact of quantum computing on cybersecurity. This risk has already been covered in section 3.2 where it was established that we are still many years from being able to implement quantum resistant cryptography. There is a need to proactively prepare our cybersecurity systems for potential quantum hacks, and to understand the regulatory implications this technology will have on Canada. It is important that the government, academic institutions and quantum firms work together to understand and prepare for the risks posed to existing security infrastructures.

Chapter 5

Recommendations and Conclusion

This chapter provides recommendations on how Canada can continue to be a leader in the quantum computing industry and how specific industry challenges can be addressed through meaningful partnerships between governments, academic institutions and private firms.

5.1 Addressing the Challenges of Commercializing Quantum Computers

As highlighted in Section 3.1 by [60], there are key barriers faced when commercializing a new technology. Some of these challenges includes small market size and distribution channels (in part exacerbated by a lack of awareness and understanding of a new technology), technology validation and a lack of adequate infrastructure to support new technologies.

Some of these same challenges are present for quantum computing and could present as barriers for the adoption of this technology. As discussed in chapter 4, the survey results of our study found a lack of awareness by machine learning firms about the capabilities of quantum computers. In addition, the background research conducted in chapter 2 of this work highlights that a lack of standardized validation methods for quantum computing technologies can make it difficult for the general public to understand and compare the capabilities of various quantum computers (for example, comparing D-Wave's 2,000 qubit annealing quantum computer with IBM or Google's universal gate quantum computers).

Furthermore, there is a lack of clarity around the best industry applications of the technology, which can make it difficult to grow the market size and associated distribution channels. As a result, it is recommended that the following steps be taken to address barriers in the commercialization process of this new technology:

- *Understanding the Best Applications of the Technology*: Many of the quantum firm employees surveyed were not clear on the size and volume of their firms, and there is general uncertainty around the best applications of this new technology. It is vital that academic institutions and quantum firms work in partnership to gain a more clear understanding of the potential impact of this technology on specific industries. This will not only help drive new areas of research, but will allow quantum firms to better target potential clients as they enter the early stages of commercialization. This is especially important for quantum startups in the early stages of commercialization, as their market size is smaller and the initial success of a product launch can impact their long term success.

- *Building Quantum Literacy Programs for Businesses*: In order for a broad range of Canadian industries to adopt this new technology, it is important that they are aware of the differentiating factors between a quantum and a classical computer. The government must work with quantum computing firms and academic institutions to host awareness workshops with businesses that could benefit from the use of this technology. These workshops can provide a broad overview of the technology and its benefits. These can be hosted at the offices of quantum firms or at academic institutions and incubators such as the Institute for Quantum Computing at the University of Waterloo, Ryerson University's tech incubator the DMZ, or the University of Toronto's Creative Destruction Lab. These workshops will not only improve quantum literacy amongst the business and technology communities in Canada, but can serve as a channel for quantum firms to connect with potential clients.

- *Setting Technology Validation Standards*: Setting clear technology validation standards is vital not only from a regulatory perspective, but will ensure that potential clients can reliably compare the differences between the future quantum computers available to them. It is important for government institutions to work with quantum firms and academic institutions to gain a better understanding of the various types of quantum computers in the market, their key differences and the best methods for their validation. It is difficult to regulate a new technology or protect consumers from their potential downfalls if there are no validation standards in place.

5.2 Educating Canada's Workforce

As a younger generation of Canadians enter post-secondary studies and begin entering the workforce over the next 5-10 years, we must prepare them for the growing needs of the quantum computing industry. The below recommendations address this challenge to ensure that Canada's future workforce is prepared for a quantum world.

- *Updating Academic Curriculums*: As seen by the results of the academic survey, specific academic fields will be impacted by the increasing prevalence of quantum computing. The key field highlighted by several academic respondents is engineering. However, a holistic analysis of university STEM curriculums must be conducted to better understand the updates that may be required for all academic curriculums. This will ensure that the next generation of Canadian workers understand quantum computing and can help grow Canada's quantum industry in the long term.

- *Building Quantum Specific Work Integrated Learning Programs (WIL)*: The literature review in Section 3.3 highlighted WIL as an effective approach to teaching the required soft and hard skills youth need in an increasingly technical work environment. WIL could be an effective approach to introducing the future workforce to quantum fields at a younger age. Through a partnership with academic institutions and quantum computing firms, students could apply their academic learnings in a professional setting, preparing them for work in a quantum field. There are various models of WIL including systematic internships, co-ops or even shorter term initiatives through bootcamps or hackathons. Academic institutions and quantum firms should work together to better understand the current and future needs of this new field and build WIL programs that best address short and long term needs.

5.3 Addressing the Cybersecurity Threat

The increasing prevalence of quantum computers will pose a threat to Canada's cybersecurity. If Canada wants to lead in a quantum world, it must be proactive in preparing for its security implications. The below recommendations can help prepare Canada for the security challenges it may face.

- *Prioritizing Investment in Quantum Cryptography Validation and Quantum Cryptography*: As highlighted in Section 3.1, validation standards are needed for QKD technologies. The European Telecommunications Standards Institute has been working on such standards, but none currently exist in Canada [69]. If we are to be leaders in the field of quantum computing, we must also address the need for validating quantum cryptography standards. Such efforts should also help with the

adoption rate of quantum computers, as they will address the security concerns that were flagged by many of the machine learning firms surveyed. If the Canadian government, academic institutions and security experts work together to set appropriate post-quantum and QKD cryptography standards, they can better prepare Canada for a post-quantum world.

- *Incentivizing Private Investment into Quantum Enhanced Cybersecurity*: The need for cryptography that is secure in a post-quantum world is key if we are to protect the cybersecurity of the nation. Currently, the NRC works with businesses and academic institutions to help them develop more stringent cybersecurity systems that could be ready for a quantum world [63]. However, there is no holistic strategy built to encourage the use of the NRC's services by private institutions. The government should consider incentivizing the use of such programs by more openly marketing the services and providing potential tax benefits to those who do update their security systems to address future quantum concerns.

- *Training the Next Generation of Cryptographers*: As discussed in Section 3.1, there is a need for a new generation of quantum cryptographers who not only have an understanding of conventional cryptography methods, but who can build and deploy QKD technologies. This need can be addressed by the update of academic curriculums recommended in Section 5.2.

5.4 Summary

The Canadian government has made a concerted effort to make Canada a leader in quantum technologies. This is a wise investment, as the development and launch of a universal quantum computer could revolutionize many industries and one day solve some of humanity's most pressing problems. Although the reality of a universal quantum computer is still years or perhaps decades away, it is important that Canada continue to prepare for the realities of a quantum world. If the government, academic institutions and quantum computing firms in Canada can work together to proactively address the barriers to adoption highlighted in this research, Canada can emerge as a quantum computing trailblazer and reap the unprecedented rewards such leadership could bring.

Chapter 6

Appendix A - Survey Questions

Group 1: Quantum Computing Firm Employees

1. Please describe how you are involved with quantum technologies.
2. What is the market size (volume and value) for your company's quantum technology?
3. Which types of products does your product or service cater to?
    - Security
    - Chip Products
    - Cloud Services
    - Computational Simulations
    - Machine Learning
    - Software Solutions
    - Other (Specify)
4. What do you estimate are the number of jobs in today's Canadian marketplace because of the continuing investment in quantum computers?
    - 1-50
    - 51-100
    - 101-200
    - 201-300

- 301-400
- 401-500
- 501-1,000
- 1,001-2,000
- 2,001-3,000
- 3,001-4,000
- 4,001-5,000
- 5,001-9,999
- 10,000 +
- I don't know

5. Which of the following statements best describe your product or service?
    - Net New: Exponential Technology that will disrupt and replace existing ones
    - New: Exponential technology that will work in tandem with existing technologies
    - Other (Specify)
6. How many employees do you currently have in Canada?
    - 0
    - 1-5
    - 6-10
    - 11-20
    - 21-50
    - 51-80
    - 81-100
    - 100-150
    - 151-200
    - 201-300
    - ...
    - 10,001+

7. How many new hires do you anticipate in Canada within the next year?
    - 0
    - 1-5
    - 6-10
    - 11-20
    - 21-50
    - 51-80
    - 81-100
    - 101-150
    - 151-200
    - 201-300
    - 301-400
    - 401-500
    - 501+
    - Not sure
    - I'd rather not share
    - Other (Specify)
8. What do you think is the single biggest barrier for the deployment (launch of a product) of quantum technologies in Canada?
    - Prohibitive Production Costs
    - Lack of understanding of quantum technologies by investors
    - Lack of needed technical talent for production
    - Insufficient government or academic funding
    - Other (Specify)
9. What do you see as the single biggest barrier for the adoption (post-launch) of quantum technologies by organizations and individuals in Canada?
    - Prohibitive purchasing costs

- Security concerns
- Lack of understanding of quantum technologies by organizations/public
- Other (Specify)

10. Which industries do you foresee benefiting the most from this technology? Select all that apply.
    - Business Services
    - Security
    - Law
    - Health and Medicine
    - Financial Services
    - Communications
    - Machinery and Equipment
    - Other (Please specify)
11. Do you see currently see a skills gap in Canada when it comes to the future need of the quantum industry?
    - Yes
    - No
    - I don't know
12. If answered yes, which skills do you anticipate a gap for? Select all that apply.
    - Academics
    - Physicists
    - Computer Programmers
    - Design and UX Experts
    - Marketers
    - Data Scientists
    - Machine Learning/AI Experts
    - Computer Language and Simulator Programmers

- Business Professionals with understanding of Quantum Technologies
- Other (Specify)

13. Do you anticipate quantum technologies will ever shift from B2B into B2C products and merchandise?
    - Yes
    - No
    - I don't know
14. If answered yes, what do you estimate is the time frame for the adoption of B2C products and merchandise?
    - 0-9 years
    - 10-20 years
    - 21-31 years
    - 32-42 years
    - 43-53 years
    - 54+ years
15. If answered yes, what type of B2C products and services do you anticipate quantum technologies to be used for?
    - Personal computers
    - Cloud services
    - Security
    - Other (Specify)
16. What is the percentage increase that you have noticed in VC funding (if any) of quantum technologies over the past year? What do you attribute this increase (or lack-there-of) to?
    - No increase
    - 1-5% increase
    - 6-10%
    - 11-15%

- 16-20%
- 21-25%
- 26-30%
- 31-35%
- 36-40%
- 41-45%
- 46-50%
- 51% or more
- I don't know

17. What are your estimates for the increase in VC funding of quantum technologies over the medium term (5-9 years)?

    - No increase
    - 1-5% increase
    - 6-10%
    - 11-15%
    - 16-20%
    - 21-25%
    - 26-30%
    - 31-35%
    - 36-40%
    - 41-45%
    - 46-50%
    - 51% or more
    - I don't know

18. What are your estimates for the increase in VC funding of quantum technologies over the long term (10+ years)?

    - No increase

- 1-5% increase
- 6-10%
- 11-15%
- 16-20%
- 21-25%
- 26-30%
- 31-35%
- 36-40%
- 41-45%
- 46-50%
- 51% or more
- I don't know

19. Do you anticipate regulatory implications for the government once quantum technologies are adopted in the future? Example: The way in which the sharing economy (Airbnb, Uber) has functioned outside of existing regulatory frameworks. Please comment.

Group 2: Employees of Firms Using Machine Learning

1. What is the market size (volume and value) for your company's quantum technology?
2. Which industries does your service/product cater to?
    - Information and communication technology
    - Education
    - Psychology and Behavioural Sciences
    - Finance
    - Law
    - Energy
    - Automotive
    - Healthcare
    - Other (Specify)
3. Do you presently use any of the below algorithm(s) at your organization? Please select all that apply.
    - Linear Regression
    - Logistic Regression
    - Decision Tree
    - SVM
    - Naive Bayes
    - KNN
    - K-Means
    - Random Forest
    - Dimensionality Reduction Algorithms
    - Gradient Boost and Adaboost
    - I would rather not share
4. In what type of problem(s) do you use ML algorithms? Please select all that apply.
    - Adaptive websites

- Affective computing
- Bioinformatics
- Brain-machine interfaces
- Cheminformatics
- Computational anatomy
- Computer vision, including object recognition
- Fraud detection
- Detecting technological anomalies
- Game playing
- Information retrieval
- Marketing
- Machine learning control
- Medical diagnosis
- Translations/Language learning
- Economics
- Other (Specify)

5. For the above type(s) of problem(s), how long does it typically take to complete needed tasks on a computer?
    - 0-15 minutes
    - 16-31 minutes
    - 31-61 minutes
    - 62-92 minutes
    - 93-123 minutes
    - 124-154 minutes
    - 155-185 minutes
    - More than 186 minutes
    - I would rather not share

6. Are there any other tasks you would like to automate using algorithms that is not currently possible due to the level of complexity involved? Please specify.

7. Quantum computers are currently being built, and are estimated to provide exponential speed-ups over current classical computers when solving complex algorithmic problems. If a quantum computer's capabilities were available to your organization via an encrypted cloud, would you be likely to use it?

    - Yes
    - No
    - Not sure

8. What hesitations, if any, would you have around using this technology? Please select all that apply.

    - Uncertain Data Security
    - Lack of understanding of technology?s capabilities or limitations
    - Perceived High costs
    - Other (Specify)

Group 3: Academic Institution Employees

1. Please describe how you are involved with quantum technologies.
2. What do you estimate are the number of jobs in today's Canadian marketplace because of the continuing investment in quantum computers?
    - 1-50
    - 51-100
    - 101-200
    - 201-300
    - 301-400
    - 401-500
    - 501-1,000
    - 1,001-2,000
    - 2,001-3,000
    - 3,001-4,000
    - 4,001-5,000
    - 5,001-9,999
    - 10,000 +
    - I don't know
3. What do you estimate are the number of jobs to be created in the short or medium term? (1-9 years)
    - 1-500
    - 501-1,000
    - 1,001-2,000
    - 2,001-3,000
    - 3,001-4,000
    - 5,001-9,999
    - 10,000 +

- I don't know

4. What are your estimates for the number of jobs to be created in the long term? (10+ years)
    - 1-500
    - 501-1,000
    - 1,001-2,000
    - 2,001-3,000
    - 3,001-4,000
    - 5,001-9,999
    - 10,000 +
    - I don't know
5. What do you think is the single biggest barrier for the deployment (launch of a product) of quantum technologies in Canada?
    - Prohibitive Production Costs
    - Lack of understanding of quantum technologies by investors
    - Lack of needed technical talent for production
    - Insufficient government or academic funding
    - Other (Specify)
6. What do you see as the single biggest barrier for the adoption (post-launch) of quantum technologies by organizations and individuals in Canada?
    - Prohibitive purchasing costs
    - Security concerns
    - Lack of understanding of quantum technologies by organizations/public
    - Other (Specify)
7. Which industries do you foresee benefiting the most from this technology? Select all that apply.
    - Business Services
    - Security

- Law
- Health and Medicine
- Financial Services
- Communications
- Machinery and Equipment
- Other (Please specify)

8. Do you see currently see a skills gap in Canada when it comes to the future need of the quantum industry?
   - Yes
   - No
   - I don't know
9. If answered yes, which skills do you anticipate a gap for? Select all that apply.
   - Academics
   - Physicists
   - Computer Programmers
   - Design and UX Experts
   - Marketers
   - Data Scientists
   - Machine Learning/AI Experts
   - Computer Language and Simulator Programmers
   - Business Professionals with understanding of Quantum Technologies
   - Other (Specify)
10. Do you anticipate quantum technologies will ever shift from B2B into B2C products and merchandise?
    - Yes
    - No
    - I don't know

11. If answered yes, what do you estimate is the time frame for the adoption of B2C products and merchandise?
    - 0-9 years
    - 10-20 years
    - 21-31 years
    - 32-42 years
    - 43-53 years
    - 54+ years
12. If answered yes, what type of B2C products and services do you anticipate quantum technologies to be used for?
    - Personal computers
    - Cloud services
    - Security
    - Other (Specify)
13. What is the dollar increase to date that you have noticed in academic funding (if any), due to investments in quantum research? What has been the source of this funding?
14. What are your estimates for the increase in funding expected in academic research because of quantum technologies over the short term (0-4 years)?
    - No increase
    - 1-5% increase
    - 6-10%
    - 11-15%
    - 16-20%
    - 21-25%
    - 26-30%
    - 31-35%
    - 36-40%
    - 41-45%

- 46-50%
- 51% or more
- I don't know

15. What are your estimates for the increase in funding expected in academic research because of quantum technologies over the long term (10+ years)?
    - No increase
    - 1-5% increase
    - 6-10%
    - 11-15%
    - 16-20%
    - 21-25%
    - 26-30%
    - 31-35%
    - 36-40%
    - 41-45%
    - 46-50%
    - 51% or more
    - I don't know
16. Do you anticipate regulatory implications for the government once quantum technologies are adopted in the future? Example: The way in which the sharing economy (Airbnb, Uber) has functioned outside of existing regulatory frameworks. Please comment.
17. Do you foresee the need for the planning and development of net new academic programs for future skills needs? Example: Quantum Programming. Are you aware of any such plans by your academic institution? Please comment.

Bibliography

[1] Christian Weedbrook. How to build a universal photonic quantum computer. Unpublished white paper by CEO of quantum firm, Xanadu, 2016.

[2] Rachel Courtland. Google plans to demonstrate the supremacy of quantum computing. http://spectrum.ieee.org/computing/hardware/google-plans-to-demonstrate-the-supremacy-of-quantum-computing/, 2016. IEEE Spectrum.

[3] National Research Council Canada. Quatum canada. http://www.nrc-cnrc.gc.ca/eng/solutions/collaborative/quantum/quantum_canada.html/, 2017.

[4] Jonathan P. Dowling and Gerard J. Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.

[5] Linda Enciu. Learning programs for the quantum computer. Master's thesis, Ryerson University, Toronto, ON, Canada, 2014.

[6] Peter Byrne. Analog simulators could be shortcut to universal quantum computers. https://www.scientificamerican.com/article/analog-simulators-could-be-shortcut-to-universal-quantum-computers/, 2015. Scientific American; Online; Accessed June 22, 2017.

[7] n.d. Quantum power: The future of computing and how it will change your world. page 12, 2017. How It Works Magazine; Print; Accessed May 17, 2017.

[8] The d-wave 2000q system, the most advanced quantum computer in the world. https://www.dwavesys.com/d-wave-two-system, 2017. D-Wave Corporate Website; Accessed June 24, 2017.

[9] n.d. Quantum what? the future of computing and electronics is all about qubits. https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/, 2016. Academic Blog, Online; Accessed June 19, 2017.

[10] Kellie Lu. The rise of quantum computing. `https://columbiasciencereview.com/2013/11/19/the-rise-of-quantum-computing/`, 2013. Columbia Science Review; Online; Accessed June 19, 2017.

[11] Andrey Kopot. Quantum tunneling. `https://www.youtube.com/watch?v=gNdIQVJhFoM`. Online Lecture; Accessed July 23, 2017.

[12] n.d. The curious quantum world: Part 6 - quantum tunneling. `https://steemit.com/science/@pjheinz/the-curious-quantum-world-part-6`, 2016. Quantum Tunnelling Image; Online; accessed July 15, 2017.

[13] n.d. What is superposition? `http://www.physics.org/article-questions.asp?id=124`. Institute of Quantum Physics; Online; Accessed June 25, 2017.

[14] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[15] How does quantum computing work? `https://plus.maths.org/content/how-does-quantum-commuting-work`, 2015. Plus Magazine; Online; Accessed July 6th, 2017.

[16] Peter Mosley. Physicists prove quantum spookiness and start chasing schrodinger's cat. `http://theconversation.com/physicists-prove-quantum-spookiness-and-start-chasing-schrodingers-cat-48190`, 2015. The Conversation - Independent Academic News Website; Accessed July 18, 2017.

[17] Gabriel Popkin. China?s quantum satellite achieves ?spooky action? at record distance. `http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance`, 2017. Science Magazine; Online; Accessed July 8, 2017.

[18] Quantum computing. `http://www.lockheedmartin.ca/ca/what-we-do/emerging-technologies/quantum-computing.html`, 2017. Lockheed Martin Corporate Website; Accessed June 24, 2017.

[19] Our customers. `https://www.dwavesys.com/our-company/customers`, 2017. D-Wave Corporate Website; Accessed June 25, 2017.

[20] Tom Simonite. Meet d-wave: Our vision and history. `https://www.dwavesys.com/our-company/meet-d-wave`, 2017. D-Wave Corporate Website; Accessed June 26, 2017.

[21] Matthew Braga. New canadian quantum computer called twice as powerful as last one, but what does that mean? http://www.cbc.ca/news/technology/dwave-new-quantum-computer-twice-as-fast-so-what-1.3949886/, 2017. Online; accessed June 18, 2017.

[22] Chris Lee. Explaining the upside and downside of d-wave's new quantum computer. https://arstechnica.com/science/2017/01/explaining-the-upside-and-downside-of-d-waves-new-quantum-computer/, 2017. Ars Technica; Online; accessed June 12, 2017.

[23] QSoft. The quantum software group at iqc. https://qsoft.iqc.uwaterloo.ca/, 2017. Institute for Quantum Computing; Online; Accessed June 12, 2017.

[24] Dom Galeon. D-wave just open-sourced quantum computing. https://qsoft.iqc.uwaterloo.ca/, 2017. Institute for Quantum Computing; Online; Accessed June 12, 2017.

[25] D-Wave. D-wave announces d-wave 2000q quantum computer and first system order. https://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order, 2017. D-Wave Corporate Website; Accessed May 23, 2017.

[26] John Russell. Quantum bits: D-wave and vw; google quantum lab; ibm expands access. https://www.hpcwire.com/2017/03/21/quantum-bits-d-wave-vw-google-quantum-lab-ibm-expands-access/, 2017. HPC Wire; Online; Accessed June 27, 2017.

[27] Google says it has proved its controversial quantum computer really works. https://www.technologyreview.com/s/544276/google-says-it-has-proved-its-controversial-quantum-computer-really-works/, 2015. Technology Review; Online; Accessed June 27, 2017.

[28] Anastasia Marchenkova. What's the difference between quantum annealing and universal gate quantum computers? https://goo.gl/YDXemt, 2016. Accessed June 25, 2017.

[29] Ron Miller. Ibm launches quantum computing as a cloud service. https://techcrunch.com/2016/05/03/ibm-brings-experimental-quantum-computing-to-the-cloud/, 2016.

[30] IBM. Ibm makes quantum computing available on ibm cloud to accelerate innovation. http://www-03.ibm.com/press/us/en/pressrelease/49661.wss, 2016.

[31] Ron Miller. Ibm adds new api to quantum computing cloud service. https://techcrunch.com/2017/03/05/ibm-adds-new-api-to-quantum-computing-cloud, 2017.

[32] Ibm building first universal quantum computers for business and science. https://www-03.ibm.com/press/us/en/pressrelease/51740.wss, 2017. IBM Corporate Website; Accessed July 15, 2017.

[33] Ibm builds its most powerful universal quantum computing processors. https://www-03.ibm.com/press/us/en/pressrelease/52403.wss, 2017.

[34] Chow Jerry M. Gambetta, Jay M. and Matthias Steffen. Building logical qubits in a superconducting quantum computing system. *npj Quantum Information*, 3(1):2, 2017.

[35] A quantum computer's power depends on more than just adding qubits. https://www.research.ibm.com/ibm-q/resources/quantum-volume.pdf. IBM Corporate Website.

[36] Jamie Condliffe. Ibm nudges ahead in the race for quantum supremacy. https://www.technologyreview.com/s/607887/ibm-nudges-ahead-in-the-race-for-quantum-supremacy/, 2017. MIT Technology Review; Online; Accessed July 23, 2017.

[37] Hartmut Neven. Machine learning with quantum algorithms. https://research.googleblog.com/2009/12/machine-learning-with-quantum.html, 2009. Google Research Blog; Online; Accessed July 13, 2017.

[38] Jason Mick. Google, d-wave team up to unveil world's first quantum image search. http://www.dailytech.com/Google+DWave+Team+up+to+Unveil+Worlds+First+Quantum+Image+Search/article17112.htm, 2009.

[39] Nicola Jones. Google and nasa snap up quantum computer d-wave two. https://www.scientificamerican.com/article/google-nasa-snap-up-quantum-computer-dwave-two/, 2013.

[40] Quentin Hardy. Google buys a quantum computer. https://bits.blogs.nytimes.com/2013/05/16/google-buys-a-quantum-computer/, 2013. The New York Times; Online; Accessed June 2, 2017.

[41] Jeremy Hsu. Google hires quantum computing expert john martinis to build new hardware. http://spectrum.ieee.org/tech-talk/computing/hardware/google-hires-quantum-computing-expert-john-martinis-to-build-new-hardware, 2014. IEEE Spectrum; Online; Accessed June 7, 2017.

[42] Troels Ronnow, Zhihui Wang, Joshua Job, Sergio Boixo, V. Sergei Isakov, David Wecker, M. John Martinis, A. Daniel Lidar, and Matthias Troyer. Defining and detecting quantum speedup. `https://arxiv.org/abs/1401.2910`, 2014. Cornell University Library; Online; Accessed June 10, 2017.

[43] Tom Simonite. Google launches effort to build its own quantum computer. `https://www.technologyreview.com/s/530516/google-launches-effort-to-build-its-own-quantum-computer/`, 2014.

[44] Karla Lant. Google is closer than ever to a quantum computing breakthrough. `http://www.businessinsider.com/google-quantum-computing-chip-ibm-2017-6`, 2017.

[45] Tushna Commissariat. Google's supreme 20-qubit quantum computer. `http://blog.physicsworld.com/2017/03/17/googles-supreme-20-qubit-quantum-computer/`, 2017.

[46] Paul Ratner. Google to achieve "supremacy" in quantum computing by the end of 2017. `http://bigthink.com/paul-ratner/google-to-achieve-supremacy-in-quantum-computing-by-the-end-of-2017`, 2017.

[47] Tushna Commissariat. Google gains new ground on universal quantum computer. `http://physicsworld.com/cws/article/news/2016/jun/10/google-gains-new-ground-on-universal-quantum-computer`, 2016. Image of Google's quantum chip; Physics World; Online; accessed July 11, 2017.

[48] Sophia Chen. Big plans ahead for quantum computing. `https://www.aps.org/publications/apsnews/201705/quantum.cfm`, 2017. APS Physics; Online; Accessed June 23, 2017.

[49] Tom Simonite. Google's quantum dream machine. `https://www.technologyreview.com/s/544421/googles-quantum-dream-machine/`, 2015. MIT Technology Review; Online; Accessed June 25, 2017.

[50] Kathryn Nave. Quantum computing is poised to transform our lives. meet the man leading google's charge. `http://www.wired.co.uk/article/googles-head-of-quantum-computing`, 2016.

[51] Sinayskiy Ilya Francesco Schulda, Maria and Rimpilainen Petruccione. An introduction to quantum machine learning. *Contemporary Physics*, pages 1–19, 2014.

[52] Andris Ambainis. What can we do with a quantum computer? `https://www.ias.edu/ideas/2014/ambainis-quantum-computing`, 2014. Institute for Advanced Study; Accessed August 19, 2017.

[53] Martin Hilbert and Priscila López. The world's technological capacity to store, communicate, and compute information. 332:60–5, 02 2011.

[54] Munro J. William Brown, L. Katherine and M. Vivien Kendon. Using quantum computers for quantum simulation. *Entropy*, 12(11):2268–2307, 2010.

[55] Peter Reuell. New way to model molecules. `http://news.harvard.edu/gazette/story/2016/08/new-way-to-model-molecules`, 2016. Harvard Gazette; Accessed August 12, 2017.

[56] Guihua Zeng. *Quantum communication private communication*. Beijing : Heidelberg ; New York : Higher Education Press ; Springer, c2010, 2011. Accessed August 3, 2017.

[57] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[58] 2016 cost of data breach study: Canada. `https://www-03.ibm.com/security/ca-en/data-breach`, June 2016. Ponemon Institute and IBM; Accessed August 3, 2017.

[59] Institute for Quantum Computing. Quantum cryptography. `https://uwaterloo.ca/institute-for-quantum-computing/research/areas-research/quantum-cryptography`, 2016. Institute for Quantum Computing; Accessed July 23, 2017.

[60] Natesh, Gbadegeshin, Rimpilainen, Imamovic-Tokalic, and Zambrano. Identifying the challenges in commercializing high technology: A case study of quantum key distribution technology. *Technology Innovation Management Review*, 5(1):26–36, 2015.

[61] Michele Mosca. Cybersecurity in an era with quantum computers: will we be ready? *IACR Cryptography ePrint Archive Report*, pages 1–4, 2015.

[62] Raymond Laflamme. Statement on government of canada support for quantum space innovation. `https://uwaterloo.ca/institute-for-quantum-computing/news/statement-government-canada-support-quantum-space-innovation`, 2017.

[63] Quantum cyber security solutions. `https://www.nrc-cnrc.gc.ca/eng/solutions/advisory/quantum_cyber_security.html`, 2016. National Research Council Canada; Accessed July 8, 2017.

[64] Canada's cyber security strategy. `https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf`, 2010. Government of Canada Report; Accessed July 28, 2017.

[65] Creig Lamb and Sarah Doyle. Future-proof: Preparing young canadians for the future of work. Technical report, Brookfield institute for innovation + entrepreneurship, 20 Dundas St. W, Suite 921, Toronto, ON, 2017. Accessed June 28, 2017.

[66] Creig Lamb and Matthew Seddon. The state of canada?s tech sector, 2016. Technical report, Brookfield institute for innovation + entrepreneurship, 20 Dundas St. W, Suite 921, Toronto, ON, 2016. Accessed June 27, 2017.

[67] A profile of canada's highly qualified personnel. `http://www.statcan.gc.ca/pub/88-003-x/2007002/10331-eng.htm/`, 2008. Statistics Canada; Accessed August 24, 2017.

[68] Stephen Lam. B.c. quantum computing firm d-wave systems raises $21-million. `https://beta.theglobeandmail.com/report-on-business/small-business/startups/d-wave-systems-a-bc-quantum-computing-firm-raises-21-million/article32203708/`, 2016. The Globe and Mail; Accessed July 7, 2017.

[69] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2:16025 EP, 2016.