How Will Quantum Computers Affect Science and Technology?

Alexander Furmston

Abstract. The topic question for this project is "How will quantum computers affect science and technology?" and its aim is to understand and discuss the effects of quantum computing on science and technology, how likely these effects are to occur and how significant they are. This project will only examine effects which are likely to occur within the next decade. Quantum computers are a form of computer, similar to supercomputers, except they use quantum bits instead of the bits found in traditional computers. Quantum bits can represent one, zero or a combination of one and zero. This gives quantum computers the potential to perform different algorithms to traditional computers, making them more efficient at performing simulations or accessing data from a database. These advantages have many applications within science and technology, including engineering research, machine learning and the development of new medicines. This project will analyse these applications in order to answer the topic question. However, there are also drawbacks to quantum computers, such as their high cost and complexity. Furthermore, quantum computers may have a negative impact on cyber security, due to their ability to easily crack RSA encryption, which underpins much of modern communication on the internet. Some of these drawbacks may reduce the positive impact that quantum computers can have on science and technology and therefore it is necessary for this project to also discuss the drawbacks associated with quantum computers in order to answer the topic question.

0. Contents

Introduction

1.1. What makes quantum computers different from normal computers and what advantages do they hold?—Quantum computers differ from traditional computers in many ways, the main way being that they use quantum bits (qubits) to perform calculations, whereas a traditional computer would use bits. Bits are made of electricity and are only able to represent one of two states at once: on or off (one or zero) but qubits can represent a combination of one and zero at the same time. As a result of qubits' behaviour, quantum computers are able to take many more factors into account than a traditional computer when performing calculations, making them faster at many tasks.

Quantum computers are much better at simulations than classical computers. This is useful in applications such as chemical modelling and weather simulations. Furthermore, they are efficient at solving problems involving lots of variables, such as optimisation problems or calculating the dose of radiation to give to a radiotherapy patient. Also, they can perform calculations that normal computers aren't able to, such as quantum algorithms like Shor's algorithm or Grover's algorithm.[1] These algorithms have many applications in science and technology. For example, Shor's algorithm is able to factorise numbers in much less time than any traditional algorithm, allowing a quantum computer to quickly decrypt messages encrypted with the widely-used RSA encryption system, which relies on the computation difficulty of integer factorisation.

It is important to understand when considering the advantages of quantum computers that the best solution may not always be to use only a quantum computer or use only a classical computer, but instead to use a combination of the two where each works on the areas in which it is strongest, such as is the case in D-Wave's hybrid quantum computers. Additionally, due to the costs associated with building and running a quantum computer, they won't replace traditional computers at all for many everyday tasks, such as emailing or browsing the web and individuals may never have their own personal quantum computers.[2]

1.2. Why study quantum computers' effects on science and technology?—This topic is important to study due to the potential impacts of a fast and fully functional quantum computer. These impacts span many different industries including engineering, chemistry, medicine, cryptography, machine learning and big data processing. Possible applications of quantum computers range from developing new superconductors for more efficient circuits to learning what sort of videos to suggest to someone watching online videos. Additionally, the huge amount of resources being spent on research and development of quantum computers and other quantum technologies means new discoveries are constant, so there is plenty of material to help answer the question of this project. For example, China's government is investing $10 billion USD in the world's largest quantum research facility and the USA spends $200 million USD per year on quantum research.[3] These facts demonstrate that quantum computing is a developing area worthy of being studied.

1.3. Do we already have quantum computers and who is working on quantum computing?—D-Wave has already developed and sells quantum computers to companies, such as Volkswagen for use in a variety of ways, although primarily for optimisation problems. Other companies have also produced quantum computers, such as Rigetti, Google and IBM, who are approaching quantum supremacy with their 50 qubit computer[4] . Although large companies like IBM, who

have been working in this field for 50 years, play a significant role in developing quantum computers, governments also contribute to research, along with universities. Smaller companies and start-ups, such as IonQ or Xanadu are also developing new quantum computers and quantum algorithms and applications. According to Edgy Labs, the 11 companies set for a "quantum leap" in technology are: IBM, Google (Alphabet), Microsoft, Nokia Bell Labs, D-Wave, Rigetti, Airbus, Lockheed Martin, Raytheon, Amgen and Biogen.[5]

1.4. How will this project assess the impacts of quantum computers on science and technology?—In order to assess the impacts of quantum computing, this project will first discuss and analyse the potential impacts of a fully functional quantum computer and the different areas it could affect. To answer the topic question, this project will focus on the effects of quantum computers on science and technology and some of the applications of the changes they will bring about, rather than simply discussing the eventual impacts of quantum computers on all areas of life as this would involve more speculation and guesswork and would be too broad of a topic to explore. Secondly, it is necessary for this project to analyse what implications any advancements in quantum computing may have on cyber security. This is essential because if IT systems are not prepared to handle the threats introduced by fully functional quantum computers, they will provide new opportunities for hackers to obtain sensitive information from large companies or governments.

This project will also discuss the progress already made on quantum computers, including examples of where they are already used and breakthroughs in research. The purpose of this section is to analyse the effects they already have on science and technology and use this information to analyse better the practicality of the impacts discussed in the first section of the project. Next, it is essential to examine what developments are needed to develop better quantum computers and what is slowing research down in order to further analyse the practicality of these impacts.

Finally, this project will include a conclusion to present its answer to the topic question using the evidence outlined in the discussion and analysis section.

Research Review

The sources of information used in this project vary greatly in format and content. Scientific papers, news reports, websites and interviews were all used to gather information from which the conclusions of this project were drawn. Whilst some of the sources covered a broad range of areas within quantum computing, others focused on specific developments or applications. Furthermore, including a variety of sources was important so that the conclusions made in this project would be well-rounded and accurate.

2.1. Preliminary Research—Preliminary research was undertaken to assist in establishing what impacts and applications needed to be researched further during the research phase of the project. Also during the preliminary research phase, sources which covered a broad range of topics within quantum computing, such as YouTube videos and Wikipedia were used to gain a basic understanding of quantum mechanics and how quantum computers work as this understanding would help to evaluate the accuracy of sources of information during the research phase and therefore improve the accuracy of any conclusions drawn. Furthermore, a good understanding of classical computing had already been established which enabled evaluation of any comparisons made between quantum and classical computing in sources.

YouTube, Wikipedia and news articles proved to be useful sources information for initial research due to them covering a broad range of topics and providing explanations of some quantum mechanics. This helped during the research phase as sources requiring a foundation knowledge of quantum computing became easier to interpret, evaluate and make us of. However, these sources of preliminary research were not used for any facts or references in the project because they often didn't focus on any specific impacts or applications of quantum computing. Using many YouTube videos, news articles and a Wikipedia page for preliminary research ensured the understanding gained would be accurate and detailed.

2.2. Research Planning—Using the knowledge and understanding obtained from the preliminary research, a list of questions that would be worthwhile to research in order to answer the topic question was drafted to assist in structuring the research done in the research phase. These questions became the different headings within the discussion and analysis section of the project and they were: "Why are quantum computers important?", "What are the impacts of quantum computing on cyber security?", "What progress has already been made on quantum computers?" and "What will we need for better quantum computers?". They were considered when reading and evaluating every source used in this project to ensure that source was made use of as best as possible.

Preliminary research was also valuable in creating a list of subtopics within science and technology where quantum computers will have an impact. These were: chemical modelling, big data analysis, renewable energy and energy storage, artificial intelligence, medicine and optimisation problems. This list provided ideas for what to look for during the research phase, making research quicker, more detailed and ensuring it covered the subtopics relevant to the topic question and therefore the information used to draw conclusions from and the conclusions themselves were improved. During the research phase, this list was expanded where necessary to include other topics.

2.3. Research—The research for this project followed the plan created during the research planning phase. Sometimes sources were found by using the questions listed earlier, combining them with one of the subtopics into a search term and then searching for information relating to that using Google, Google Scholar or JSTOR. Google Scholar and JSTOR were the main sources of scientific papers for this project and Google provided most of the rest. This proved to be a quick way of finding the information needed for the project. However, occasionally sources were found by using more general search terms relating to quantum computers and the information from these sources was then sorted into the different questions and subtopics already created.
The research for this project focused mainly on what will happen soon (in less than a decade) and what has already happened, rather than focusing on the possible impacts of quantum computing in 30 years, which would be extremely difficult to accurately and objectively predict.

2.3.1 Why are quantum computers important?

A large portion of the overall research time was spent on this section of the project as it forms the largest question of the discussion and analysis section and thus requires the most evidence and information to support the points discussed. Scientific articles, websites and news articles were all used to provide information for this part of the project to ensure information came from a wide range of different sources with different focuses, styles and opinions. All the sources used in this section are from 2016 or later, meaning they are still relevant at the time of writing this project, except for one scientific paper from 2010. This paper from 2010 only focuses on the medical applications of quantum computing. The notes taken are considered reliable as the focus of the paper is still correct and relevant today. The fact that this paper was not entirely representative of all the uses of quantum computers as it only focuses on the medical applications was also considered when using information from it. Because this was done, the notes taken on this topic are still reliable.
All the sources used for this section agree that quantum computers will have many important effects. They also agree that the medical applications of quantum computation are immense. However, they disagree about what will be the most important way that quantum computers will affect science and technology. The scientific paper implies medical applications will be the most important, but one article gives evidence to suggest that AI and machine learning will be the most important. Most of the sources, other than the scientific article, provide a balanced perspective on the potential effects of quantum computers. Overall, these sources were very useful as they provided data and citations to back up all their projections, which was useful in providing evidence for the conclusions of this topic.

2.3.2 What are the impacts of quantum computing on cyber security and cryptography?

It was appropriate to separate the section of this project on cyber security from the section on why quantum computers are important because, as discovered in the preliminary research, this is a huge area to discuss and contains many challenges as well as applications of a fully functional quantum computer, mainly due to their ability to reverse RSA encryption. Scientific papers, an article on a website and the IBM website page on lattice-based cryptography were

the main sources of information for this section. All of the sources of information used in this section were written recently, with the oldest being a scientific paper from 2012. However, since this paper is only used for information on a mathematical principle on which encryption is based, all the notes taken from this paper are still valid at the time of writing this project. The IBM website page `https://www.research.ibm.com/5-in-5/lattice-cryptography/` on lattice-based cryptography was especially useful in explaining the challenges quantum computers will present for cyber security and how they can be dealt with. Furthermore, IBM is involved in this field so their evaluation of the impacts of quantum computing on cyber security are quite accurate.

The general consensus of the sources of information used for this section of the project is that quantum computers will easily break current encryption standards relying on integer-factorisation, presenting a risk if current computer systems are not prepared to handle the threats this presents. However, due to the high cost of developing a quantum computer, most hackers will not have the resources required to use a quantum computer to break encryption. Furthermore, the resources used for this section agree that it is possible for businesses and governments to secure their encryption, through methods such as lattice-based cryptography. There was little disagreement between the sources used in this section of the project.

2.3.3 What progress has already been made on quantum computers?

Research into the progress already made on quantum computers was important in order to ensure a balanced and well-rounded perspective was presented in the discussion and analysis section of the project. The research into this section focused on the technical achievements in quantum computing and included some research on current applications of quantum computing because understanding the current applications of quantum computers is essential in evaluating their potential effects. Furthermore, this information was useful in evaluating how feasible the applications of quantum computing discussed in the first section of the discussion and analysis would be. JSTOR.org was useful for research into quantum computing progress as it provided many scientific papers detailing the latest advancements in technology. However, news articles were the main source of information for this section as they tended to present information on a greater number of topics or advancements at once and in an easier to read format. All the articles used here were from 2013 or later so the information used in this section of the project is up-to-date, which is important when considering what progress has already been made. Furthermore, D-Wave's website discussed many of the current applications and advancements in quantum computing, making it an especially useful source for this section. One of the sources used in this section was an interview with Mikhail Lukin, a professor of physics at Harvard University. This source was particularly valuable in forming the arguments of this section as it contained statistics and opinions from a reliable source.

The general view of the sources used in this section was that although quantum computers are already useful for some applications, such as traffic flow prediction, because they are in the early stages of development, many of their potential applications have not yet been implemented. However, as the interview with Mikhail Lukin points out, it is important to consider that this was also true of traditional computers when they were in the early stages of their development.

2.3.4 What will we need for better quantum computers?

This area of research was also useful in determining how realistic the previously discussed potential applications of quantum computing will be. It would be impossible to determine this without researching and considering the current applications of quantum computers, as done in the previous section, and what advancements still need to be made. As with all sections of this project, a variety of sources were used to ensure a non-biased argument was presented in the discussion and analysis section. The oldest resource used was a report by the University of British Columbia from 2011 and it was important that the facts and viewpoints presented in this report were considered in the context of when they were published. However, as only relevant and accurate information from this source was included in the notes for this project, the conclusions drawn in this section can still be considered to be accurate. Furthermore, since all the other sources were more recent, they are all relevant at the time of writing.

There was some disagreement between the sources used in this section about how quickly quantum computing technologies will continue to advance. On the one hand, an article published on Science Daily by the University of California entitled "Plan for quantum supremacy" suggested in its title and opening paragraphs that Google was on the cusp of a technical revolution. On the other hand, later in the article, the author points out that quantum supremacy and Google's plans are not as impressive as they initially implied they were. Furthermore, another article notes the lack of trained researchers in the field of quantum computing and the effects this will have on its progress. Overall, the conclusion to be drawn from these sources is that with some more time and research quantum computers can be hugely significant. Although the exact time is unknown, it is likely to be several years before we see anything revolutionary but smaller advancements will occur in the meantime as businesses increasingly take advantage of quantum computers.

Discussion and Analysis

3.1. Why are quantum computers important?—This section of the project will examine the potential effects and applications of a fully functional quantum computer and use this information to help determine the effects that quantum computing will have on science and technology.

3.1.1 Engineering and chemistry

Due to their manipulation of qubits, quantum computers are far more efficient at performing simulations than traditional computers.[6] This presents a wide array of opportunities for chemists and engineers to run much larger simulations than they were previously able to. For example, quantum computational simulation has the possibility to be used by chemists to study the causes and effects of climate change and research ways to tackle this.[7] Developments in climate science aided by quantum computers would have the potential to affect science and technology as they would initiate the development of new technologies by governments and companies in order to slow down climate change or protect communities and habitats from its harmful effects, saving money and even lives.

Furthermore, the ability of quantum computers to simulate natural processes and chemical interactions may have many impacts on technology and help to meet the growing energy demands of the increasing global population. Natural processes, such as photosynthesis, could be exploited to make more efficient photovoltaic cells.[8] Combined with future battery technology, aided by the development of new superconductors researched through chemical modelling, quantum computers could become an invaluable tool for providing the additional energy needed to finally transition away from fossil fuels. Additionally, cost-effective superconductors would have a huge impact on technologies, such as the power grid and electric cars, which transfer huge amounts of electrical energy. Therefore, chemical modelling is a way in which quantum computers could have a great impact on the science and technology of energy. Also, cheap, reliable, clean energy would clearly have a huge effect on science and technology as it would make research and development cheaper and therefore would affect the daily life of many people too.

Another area of engineering and chemistry in which quantum computers are set to excel is material science. In fact, Los Alamos National Laboratory and Volkswagen are already using D-Wave's quantum computers to research material science.[9] Due to the nature of the chemical modelling involved in material science research, classical computers take an exponentially longer time to simulate larger molecules. However, quantum computers do not, opening up the possibility of research into new materials which could be applied to any area of engineering, from stronger, lighter materials in vehicles or buildings to superconductors in batteries. Material science is evidently an area which will affect science, technology and everyday life and the US government agrees with this as it has invested over $250 million in the Materials Genome Initiative to "discover, manufacture, and deploy advanced materials twice as fast, at a fraction of the cost".[10] The fact that quantum computers can help to advance this area of research clearly demonstrates why they are important in chemistry and engineering.

3.1.2 Healthcare

Because quantum computers are capable of simulating chemical interactions far more efficiently and effectively than traditional computers, there is a strong potential for quantum computers to be used to better understand cellular processes.[11] This is essential as "biomolecular recognition, enzyme catalysis, self organization and molecular motors are central to all cellular processes but remain poorly understood theoretically" and with powerful quantum computers, it would be possible to create new drugs based on the better understanding provided by the simulations performed on quantum computers.[12] Non-quantum projects, such as `https://www.foldingathome.org` have already made medical advancements performing simulations on traditional computers. If powerful quantum computers were to be used for the same purpose, it is likely the rate of discovery of new medicines would increase considerably, making them significant to the fields of science and technology. However, it is important to remember that the work needed to run biomolecular simulations on a quantum computer is substantial enough to slow down the implementation of these technologies.

Quantum computing has more uses in healthcare than just chemical simulation. They can perform quantum algorithms, such as Grover's algorithm, enabling them to find answers from unstructured databases more quickly than traditional computers.[13] As a result, they present the possibility of mass-processing of patient data through an artificial intelligence to analyse trends in people with certain conditions or diseases to discover risk factors or lifestyle changes that reduce the risk of a condition or improve health. Obviously, this creates huge opportunities for new advancements in healthcare, including treatment and preventative measures to stop a patient from ever developing a condition, showing how important quantum computers are. As with most of the applications of quantum computers, there would be huge costs associated with the setup of quantum computer-based analysis of patient data. Furthermore, it presents data privacy issues with using a patient's sensitive data – such as whether healthcare companies or the NHS should be allowed to process this data without a patient's consent.

3.1.3 Machine learning and big data processing

As previously mentioned, due to quantum algorithms such as Grover's algorithm, quantum computers are extremely efficient at sorting through large sets of data to find information in a large database.[14] This has numerous applications in the fields of machine learning and big data processing. One way in which the machine learning opportunities of quantum computers are being used is to improve the artificial intelligence in driverless cars.[15] Quantum computers could improve the technology in driverless cars in several different ways. For example, they could reroute cars around a city to decrease traffic or they could analyse the huge quantity of data generated by self driving cars, which are packed with sensors and cameras to improve the artificial intelligence which drives the car, aiding developments in safety and, ultimately, saving lives. These applications clearly demonstrate the importance of quantum computers as they will save time, money and lives.

3.1.4 Summary

From the evidence presented above, it is evident that quantum computing has great potential to affect areas of science and technology positively including machine learning, data processing, healthcare, chemistry and engineering. The ways in which quantum computers aid the progression of these fields is usually related to using them to run complicated simulations but they can also be used for analysing data, as discussed in the "Machine learning and big data processing" section. However, the practicality of these potential applications needs to be evaluated in the following sections of this project.

3.2. What are the impacts of quantum computing on cyber security and cryptography?— It is important to include a separate section of this project on cyber security and cryptography due to the significance of some of the dangers presented by quantum computers in relation to cyber security. In fact, "If a quantum computer were to appear today, virtually all internet communication would become insecure".[16] This section of the project will analyse the dangers presented by quantum computers and also the ways in which they may positively affect areas of science and technology, such as cyber security and cryptography.

3.2.1 RSA encryption and lattice-based cryptography

RSA is a cryptosystem which many of our current methods of communication rely on. It is widely used across the internet in protocols, such as the very widely-used HTTPS which keeps website communications, including usernames and passwords, secure. With conventional computers RSA is extremely secure, as it relies on the computational ease of multiplying two numbers together to encrypt, but the computational difficulty of factorising a number into its prime factors without the key to decrypt.[17] However, quantum computers are much more effective at factorising numbers than traditional computers, since they are able to run quantum algorithms such as Shor's algorithm. Therefore, a powerful quantum computer may easily decrypt RSA-based communications, leaving most websites and many other methods of communication vulnerable.[18]

If RSA were to suddenly become unsafe, it could leave the whole internet in chaos. However, it's unlikely that a powerful quantum computer would suddenly appear, with no warning, in the hands of criminals. The first groups to have access to powerful quantum computers are likely to be governments and large corporations and whilst this may grant them more power than they should have, it is unlikely that they will suddenly start information. However, it would be extremely dangerous if criminals were to gain access to this. Therefore, it is still necessary to consider what would happen if a powerful quantum computer were to be misused before the internet has transitioned to safer methods of communication. It is important to remember that the high costs associated with developing a quantum computer would mean high-value targets would be the main targets of a quantum computer-based cyber-attack. Most online payment, which relies on RSA for security, would become insecure and any parts of government websites which rely on HTTPS would probably have to be shut down and reworked as they could pose a security risk. Many people could have their usernames and passwords decrypted and misused.[19] In fact, damages from cybercrime are predicted to reach $6 trillion globally by 2021 and with quantum computers in the wrong hands, this number would continue to rise considerably after 2021.[20]

Clearly, an alternative method of secure communication between computers on the internet is a necessity if people still want to be able to trust that online activity will not lead to their identity being stolen.
Quantum-safe cryptography is the name given to methods of encryption that are not broken by a quantum computer. One example of this is lattice-based cryptography, a technology which IBM has undertaken lots of research into. With lattice-based cryptography, there is a way for organisations to fully secure themselves against attacks from quantum computers or conventional computers, since lattice-based encryption methods have withstood all algorithmic attacks so far: both quantum and classical.[21] However, the transition to quantum-safe encryption methods will not be easy as RSA-based encryption is so wide-spread, meaning some organisations may still be at risk when a powerful quantum computer is developed.

3.2.2 Quantum entanglement

Quantum entanglement is a quantum phenomenon in which two quantum particles can be related in such a way that any change in one will cause a change in the other. The No Cloning Theorem states that qubits cannot be copied without first measuring them, which would cause a change in their state and therefore mean that any intruder into the transfer of information between two quantum computers would be detected. When considering this, along with the fact that quantum entanglement has been demonstrated to work over 143km, quantum computers could provide virtually unbreakable security.[22] Due to the small amount of data that can be transmitted this way and the huge costs associated with it, this would not be at all practical for transferring data between average internet users. The main application of this technology would be for governments communicating either with each other or different branches of their own governments without the possibility of hostile nations intercepting their messages. This is another way in which quantum computers will have an effect on cyber security and communications technologies.

3.2.3 Summary

It is evident that powerful quantum computers will have a much greater effect on the science and technology of cryptography and cybersecurity than one might initially expect. The fact that Shor's algorithm could break most modern encryption based on RSA shows that these impacts may be negative and extremely significant. However, through technologies such as lattice-based cryptography, these negative consequences can be minimised, and quantum computers could even bring a positive change through quantum entanglement.

3.3. What progress has already been made on quantum computers?—In order to fully evaluate how quantum computers will affect science and technology, it's important to look at what quantum computers can already do and what technical achievements have recently been made. This section of the project will use information on the progress already made on quantum computing to determine the practicality of a powerful quantum computer.

3.3.1 Recent breakthroughs and current applications

In 2015, the world's first quantum logic device based on silicon was made by the University of New South Wales.[23] This was seen as so significant that the UK Institute of Physics named it one of 2015's top 10 breakthroughs. The reason for this is that quantum logic gates on silicon, made with the conventional semiconductor manufacturing process, open up the possibility of scalable and cheaper quantum computers. This technology is still in its infancy, as the breakthrough was made in 2015 so it will be a while before we see any fully-fledged quantum computers based off of it but it opens up new opportunities for the development of more powerful quantum computers. D-Wave produced and sold a 512 qubit hybrid quantum processor to a collaboration between Google, NASA and the Universities Space Research Association in 2013.[24] This is an example of where quantum computers already exist and are already being used for research. However, this is only a hybrid quantum processor, meaning it can't do everything that a full quantum computer could do. That being said, Volkswagen proved that a D-Wave quantum computer is able to solve a difficult quantum chemical problem, showing that their computers are still very capable and acting as a proof of concept that more is possible with these machines.[25] The power of these machines is only going to get more impressive, as D-Wave sold a 2000 qubit machine in 2017.[26] Furthermore, companies already use D-Wave's computers, usually to solve optimisation problems. For example, Volkswagen uses them to calculate and optimise traffic flow in Beijing, NASA is using it for machine learning and D-Wave themselves use their computers for material science simulations.

There are currently 11 main companies focused on the development of quantum computation. These are IBM, Google (Alphabet), Microsoft, Nokia Bell Labs, D-Wave, Rigetti, Airbus, Lockheed Martin, Raytheon, Amgen and Biogen.[27] In a race for quantum supremacy between these 11 companies, Google unveiled a 72 qubit quantum computer and IBM made a 50 qubit quantum computer.[28] Both of these quantum computers are fully-quantum, in contrast to D-Waves hybrid approach, meaning they mark a huge milestone as 50 qubits is the point at which it becomes nearly impossible to simulate quantum computers on traditional computers.

3.3.2 Summary

The examples listed above clearly demonstrate that quantum computing is a rapidly developing area of science and technology. Quantum computers already have uses and are already changing science and technology so it's clear that in time, they will have a huge impact. As Mikhail Lukin (a professor of physics) points out, "When classical computers were first developed, they were mostly used to do scientific calculations, numerical experiments to understand how complex physical systems behave. Right now, quantum machines are at this stage of development.".[29] Therefore, it's not unreasonable to expect quantum computers to develop into something which will change science and technology, similar to conventional computers.

3.4. What is needed for better quantum computers?—This section of the project will analyse the technical advancement needed for more powerful and error-resistant quantum computers and the current limiting factors on progress with the same intention as the last section: to determine how realistic it is to expect a powerful quantum computer within the next 10 years. It is also

necessary to analyse how people working with quantum computers are dealing with these issues.

3.4.1 Technical advancements

As well as being something that quantum computers can help to develop, better superconductors are something which are needed for more powerful quantum computers. It is believed that the properties found in superconductors could make quantum computers "more robust".[30] Therefore, better superconductors could lead to less error-prone quantum computers with longer qubit decoherence times which would allow for quicker and more accurate computation. Although progress is being made in the technology of superconductors, with hydrogen sulphide being used as the warmest ever superconductor at 203 K (-70°C) in 2015 even better superconductors would allow for even better quantum computers.[31] Clearly, although more progress is needed here, superconductors will not be a major roadblock for the development of a powerful quantum computer. Furthermore, the research conducted in order to develop superconductors for quantum computer can be used in other fields of science and technology, such as batteries.

Qubit decoherence is a significant barrier that quantum computers need to be able to overcome. Long qubit decoherence times are important as they are required for quantum computers to be able to perform long calculations. According to the University of British Columbia, "Until now, all efforts to achieve such superposition with many molecules at once were blocked by decoherence", referring to a recent breakthrough they made in extending qubit decoherence times.[32] Despite their breakthrough, more time and research are needed if these discoveries are to be improved upon and applied to quantum computers. Therefore, bad qubit decoherence times may slow down the development of quantum computers somewhat but are not an impossible barrier to overcome.

3.4.2 Other limiting factors

Perhaps the greatest limiting factor on the development of quantum computers is the cost to benefit ratio of quantum computers over conventional computers. Currently, quantum computers can cost in the region of tens of millions of pounds to develop and run. D-Wave have been important in trying to bring this cost down by producing hybrid quantum computers, but their 2000 qubit machine still sold for $15 million USD in 2017, showing that their machines are definitely not cheap.[33] Cost will certainly be a great limiting factor in the development of quantum computing due to the resources required to develop such a complicated computer and it's unlikely that this will change any time soon.

There is a severe shortage of sufficiently skilled and trained researchers in the field of quantum computing. So much so that companies working in the field have been having trouble hiring people to get research done.[34] A shortage of people means research will progress slower than it could have if there were enough people. One positive outcome of this is that high-paying jobs are being created, which could attract more researchers. However, the high level of education needed for these jobs is likely to put many people off attempting this career route. In order to deal with this shortage of researchers, organisations have attempted to share more of their knowledge, rather than keeping it to themselves as this should enable quantum computing to

develop quicker. This can be seen in the increasing amount of open source quantum computing products.[35] However, the lack of sufficiently trained researchers is still likely to slow down the progress of quantum computers, meaning their impacts on science and technology will be less significant and later than they would have been if there were enough researchers.

3.4.3 Summary

To summarise, a lack of sufficiently trained researchers and the high costs associated with the production of a quantum computer are likely to inhibit their development. However open sourcing can be used to try and tackle this. Furthermore, from the examples of superconductors and qubit decoherence discussed above, it's clear that plenty of progress is still being made in quantum computing research, meaning the effects discussed earlier in the project are still likely to occur.

Conclusion and Evaluation

4.1. Conclusion—When conducting initial research into this project, it was important to consider all the ways in which quantum computers could affect science and technology. However, during further research, this was narrowed-down, leaving only the significant ways in which quantum computers will affect science and technology. Therefore, all the impacts of quantum computing discussed in this project are important. Furthermore, there are multiple answers to the question "How will quantum computers affect science and technology?" depending on where one decides to focus their interest. However, from the examples discussed in this project, engineering and chemistry is the most important area of impact of quantum computers. The fact that quantum computers make larger and more complex simulations possibly has a very wide range of applications in engineering and chemistry: including material science, energy production and storage and climate change. In fact, Volkswagen already use D-Wave quantum computers for material science purposes, as previously discussed in this project.[36] Therefore, it is logical to expect that quantum computers will have significant effects on science and technology through chemistry and engineering within the next 10 years.

Despite that, quantum computing will still have massive affects on science and technology through machine learning, due to quantum algorithms such as Grover's algorithm. This will enable many AI technologies and more analysis of big data within the next 10 years. Furthermore, quantum computing will change cyber security considerably, forcing organisations to update their IT systems to quantum-safe encryption methods, such as lattice-based cryptography but also enabling secure communication through quantum entanglement. From the fact that lattice-based cryptography is already under development, one can assume that the effects of quantum computers on cyber security previously discussed will occur within a decade.

Overall, although there are still many technical problems for quantum computers to overcome, researchers have demonstrated that they are capable of solving them, as shown by the improvements in superconductors, decoherence and the use of open-sourcing to minimise the impacts of a lack of sufficiently trained researchers. Therefore, it is likely that many of the technical issues discussed in this project will be solved within the next 10 years, enabling the effects of powerful quantum computers to occur. To summarise, the conclusion the research for this project has lead to is the same as the view expressed by Mikhail Lukin, a professor of physics at Harvard. He says that "They [the general population] assumed that it will take a long time before we create any useful quantum machines… I think that this is just not the case. I think we are already entering the new era with tremendous potential for scientific discoveries".[37]

4.2. Evaluation—The conclusions drawn in this project show that the project's aim has been accomplished: to understand what the effects of quantum computing are, how likely these effects are to occur and how significant they are. Furthermore, the structure and detailed planning of this project meant that the all parts of the discussion and analysis section were relevant to the topic question because all parts were either directly answering the topic question or evaluating the reliability of an effect previously mentioned. The lack of ability to conduct any primary research was unfortunate but it would have been difficult to perform any primary research as, although several emails were sent to experts on quantum computing, no replies were received. In hindsight, perhaps a different approach to primary research would have worked better but it is

unclear what this would be. However, the lack of primary research did not significantly hinder the writing of this project as the quality of the secondary research used was very high. Lots of research evaluation was conducted on each source during the research phase of the project to ensure this. Overall, the high quality of secondary research and the conclusions drawn mean this project can be considered a success and the conclusions can be considered both accurate and reliable.

Glossary of key terms

Quantum bits (qubits): A quantum bit is similar to a normal bit on a conventional computer. The difference is, whilst bits can represent only 1 or 0, quantum bits can represent 1, 0 or any combination of the two.
RSA encryption: Rivest–Shamir–Adleman (RSA) is a form of encryption widely used on the internet for secure data transmission.
D-Wave: D-wave is a company which sells quantum computers based on hybrid quantum processors, which use quantum annealing.
Big data: Big data is the name given to the huge amounts of data generated by millions of online users, such as the data which Facebook holds on its users or, in some medical cases, the data a hospital may have on patients.
Optimisation problem: An optimisation problem is a type of mathematical problem in which the aim is to find the best possible solution from all feasible solutions. Quantum computers are very efficient at solving them.
Lattice-based cryptography: Lattice-based cryptography is a form of cryptography which is not broken by a quantum computer. It is based on lattices.
Photosynthesis: Photosynthesis is the process by which plants generate energy from sunlight.
Photovoltaic cell: The electrical cell in a solar panel which generates electrical energy from sunlight.
Superconductor: A conductor of electricity which, below its critical temperature has no resistance to current.
Protocols: A set of rules or instructions that allow two computers to interact.
Hypertext transfer protocol secure (HTTPS): HTTPS is the secure extension of HTTP. It allows secure communication over a computer network, such as the internet. It is widely used for websites.
Quantum algorithm: A quantum algorithm is an algorithm which uses quantum computation to run.
Shor's algorithm: Shor's algorithm is a quantum algorithm, named after Peter Shor, which factorises integers into their prime factors.
Quantum entanglement: Quantum entanglement is a quantum phenomenon in which two particles become correlated.
Qubit decoherence time: Qubit decoherence time is the time taken for a qubit to lose coherence and therefore lose any useful information in a quantum computer.
Open source: Open source software is software for which the source code is available to anyone.

Notes and References

[1] "shor's algorithm — experience documentation 2.0 documentation". 2017.https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/110-Shor's_algorithm.html quantumexperience.ng.bluemix.net. [accessed 2 jan. 2018].

[2] "what are quantum computers and why are they important? — ict reverse". 2018. ictreverse.com. https://ictreverse.com/what-are-quantum-computers-and-why-are-they-important/. [accessed 23 oct. 2018].

[3] "china's growing investment in quantum computing - id quantique". 2018. id quantique. https://www.idquantique.com/chinas-growing-investment-in-quantum-computing/. [accessed 2 jan. 2018].

[4] Knight, will. 2018. "serious quantum computers are finally here. what are we going to do with them?". mit technology review. https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/. [accessed oct. 2018].

[5] Guedim, zayan. 2017. "11 companies set for a quantum leap in computing". edgy labs. https://edgylabs.com/11-companies-set-for-a-quantum-computing-leap. [accessed 23 oct. 2018].

[6] Harris, sarah a., and vivien m. kendon. "quantum-assisted biomolecular modelling." philosophical transactions: Mathematical, physical and engineering sciences 368, no. 1924 (2010): 3581-592. http://www.jstor.org/stable/25699187.

[7] Peter h. diamandis, md. 2016. "massive disruption is coming with quantum computing". singularity hub. https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/. [accessed sep. 2018].

[8] Peter h. diamandis, md. 2016. "massive disruption is coming with quantum computing". singularity hub. https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/. [accessed sep. 2018].

[9] "applications — d-wave systems". 2019. dwavesys.com. https://www.dwavesys.com/quantum-computing/applications.

[10] "materials genome initiative — www.mgi.gov". 2019. mgi.gov. https://www.mgi.gov/. [accessed 9 feb. 2019].

[11] Harris, sarah a., and vivien m. kendon. "quantum-assisted biomolecular modelling." philosophical transactions: Mathematical, physical and engineering sciences 368, no. 1924 (2010): 3581-592. http://www.jstor.org/stable/25699187.

[12] Harris, sarah a., and vivien m. kendon. "quantum-assisted biomolecular modelling." philosophical transactions: Mathematical, physical and engineering sciences 368, no. 1924 (2010): 3581-592. http://www.jstor.org/stable/25699187.

[13] Shah, agam. 2017. "quantum computers are here – but what are they good for?". pcworld. https://www.pcworld.com/article/3180194/hardware/with-quantum-computers-here-developers-seek-uses.html.

[14] Shah, agam. 2017. "quantum computers are here – but what are they good for?". pcworld. https://www.pcworld.com/article/3180194/hardware/with-quantum-computers-here-developers-seek-uses.html.

[15] "thompson, p. (2018).

[16] Lyubashevsky, v. (2016). preparing for the next era of computing with quantum-safe cryptography. [online] security intelligence. available at: https://securityintelligence.com/preparing-next-era-computing-quantum-safe-cryptography/ [accessed 24 sep. 2018].

[17] L, adleman, rivest r.l., and shamir a. (2019). "a method for obtaining digital signatures and public-key cryptosystems". people.csail.mit.edu. https://people.csail.mit.edu/rivest/Rsapaper.pdf [accessed feb. 2019].

[18] Vamosi, r. (2018). "mind the gap – how quantum computers may leave today's online services vulnerable". forbes.com. https://www.forbes.com/sites/robertvamosi/2018/02/27/mind-the-gap-how-quantum-computers-may-leave-todays-online-services-vulnerable/#386b641852ce. [accessed jan. 2019].

[19] Frenkel, e. (2013). "online credit card security". slate magazine. https://slate.com/technology/2013/06/online-credit-card-security-the-rsa-algorithm-prime-numbers-and-pierre-fermat.html. [accessed jan. 2019].

[20] Morgan, s. (2018). "cybercrime damages $6 trillion by 2021". cybercrime magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. [accessed jan. 2019].

[21] Lyubashevsky, v. (2016). preparing for the next era of computing with quantum-safe cryptography. [online] security intelligence. available at: https://securityintelligence.com/preparing-next-era-computing-quantum-safe-cryptography/ [accessed 24 sep. 2018].

[22] Herbst, thomas, thomas scheidl, matthias fink, johannes handsteiner, bernhard wittmann, rupert ursin, and anton zeilinger. "teleportation of entanglement over 143 km." proceedings of the national academy of sciences of the united states of america 112, no. 46 (2015): 14202-4205. https://www.jstor.org/stable/26466427.

[23] Commissariat, t. and johnston, h. (2015). double quantum-teleportation milestone is physics world 2015 breakthrough of the year – physics world. [online] physics world. available at: https://physicsworld.com/a/double-quantum-teleportation-milestone-is-physics-world-2015-breakthrough-of-the-year/ [accessed 20 sep. 2018].

[24] Jones, n. (2013). [online] nature.com. available at: https://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999 [accessed 20 sep. 2018].

[25] "ieee spectrum: Vw solves quantum chemistry problems on a d-wave machine — d-wave systems". 2017. dwavesys.com. https://www.dwavesys.com/media-coverage/ieee-spectrum-vw-solves-quantum-chemistry-problems-d-wave-machine. [accessed dec. 2018].

[26] Gartenberg, chaim. 2017. "d-wave is now shipping its new $15 million, 10-foot tall quantum computer". the verge. https://www.theverge.com/circuitbreaker/2017/1/25/14390182/d-wave-q2000-quantum-computer-price-release-date. [accessed feb. 2019].

[27] Guedim, zayan. 2017. "11 companies set for a quantum leap in computing". edgy labs. https://edgylabs.com/11-companies-set-for-a-quantum-computing-leap. [accessed 23 oct. 2018].

[28] Greene, tristan. 2018. "google reclaims quantum computer crown with 72 qubit processor". the next web. https://thenextweb.com/artificial-intelligence/2018/03/06/google-reclaims-quantum-computer-crown-with-72-qubit-processor/.

[29] Ossola, alexandra. 2018. "quantum computing is going to change the world. here's what this means for you.". futurism. https://futurism.com/quantum-computing-qa. [accessed 23 oct. 2018].

[30] Article by rosén, susanne, and quotation from annica black-schaffer. 2016. "superconductors for the quantum computers of the future — knut and alice wallenbergs foundation". knut and alice wallenbergs foundation. https://kaw.wallenberg.org/en/research/superconductors-quantum-computers-future. [accessed sep. 2018].

[31] Commissariat, t. and johnston, h. (2015). double quantum-teleportation milestone is physics world 2015 breakthrough of the year – physics world. [online] physics world. available at: https://physicsworld.com/a/double-quantum-teleportation-milestone-is-physics-world-2015-breakthrough-of-the-year/ [accessed 20 sep. 2018].

[32] "discovery may overcome obstacle for quantum computing: Ubc, california researchers". 2011. ubc news. http://news.ubc.ca/2011/07/20/discovery-may-overcome-obstacle-for-quantum-computing-ubc-california-researchers/. [accessed 5 oct. 2018].

[33] Gartenberg, chaim. 2017. ”d-wave is now shipping its new $15 million, 10-foot tall quantum computer”. the verge. https://www.theverge.com/circuitbreaker/2017/1/25/14390182/d-wave-q2000-quantum-computer-price-release-date.

[34] Chen, sophia. 2018. ”quantum computing will create jobs. but which ones?”. wired. https://www.wired.com/story/national-quantum-initiative-quantum-computing-jobs/. [accessed dec. 2018].

[35] Jackson, mark. 2017. ”quantum computing progress will speed up thanks to open sourcing”. singularity hub. https://singularityhub.com/2017/01/28/quantum-computing-progress-will-speed-up-thanks-to-open-sourcing/#sm.0001no55brbe6fe7uwr2qgni8yq59. [accessed nov. 2018].

[36] ”applications — d-wave systems”. 2019. dwavesys.com. https://www.dwavesys.com/quantum-computing/applications. [accessed jan. 2019].

[37] Ossola, alexandra. 2018. ”quantum computing is going to change the world. here’s what this means for you.”. futurism. https://futurism.com/quantum-computing-qa. [accessed 23 oct. 2018].