Quantum Computing: What is it, How Does it Work and is it Viable?

Oliver J. Denton
Aston Academy

9th April 2018

[Click for Figure Booklet]

Table of Contents

[Click for Figure Booklet]

I. Introduction and Overview

"I am not young enough to know everything."

- Oscar Wilde

I have chosen to produce an academic report answering this question because of my deep desire to truly understand the elementary workings of the universe we observe every day, with or without knowing. I am truly fascinated by the hidden mechanics of this world and equally so by the discovery processes that uncover them. I want to explore the link between the astounding works of the founding fathers of modern physics and the way in which we envision our future through encompassing the laws of our physical reality as well as the mathematics we use to model it. Moreover, computer science is an ever-evolving field of which I wish to study alongside physics and there is no better way to incorporate both into an extended project. My chosen question is also inherently related to my current subjects of study.

"The history of the universe is, in effect, a huge
and ongoing quantum computation.
The universe is a quantum computer."

- Professor. Seth Lloyd

We are living in a wonderful era where new discoveries are still being made every day. More precisely, we call our shared period of human history the Digital* [1] Age. Yet, the race is on to take our species beyond binary. This should come as a surprise to most. After all, it has brought us unimaginably far by revolutionizing our industries, economies and essentially even the people within them. However, the foundations these systems are built upon are beginning to show lapses of their limitations of which we simply cannot overcome by applying the principles that we have discovered throughout the last seventy-two years of computer engineering and study. This paper discusses this, the solutions and, soon to become obvious, why it may take more than computer scientists to build on the work already being done to solve these problems using some of the discoveries regarding the fabric of the cosmos and the fundamental properties of the universe. Without them, we could potentially see the rise and fall of governments. But, with such solutions, comes the possibility of, not only an impending end being brought to the age of silicon* [2, 3], but also the whereabouts of the next Silicon Valley being determined by who can first conquer quantum circuitry and much more in order to engineer the technology we call quantum computers.

Within this report, I will discuss the need for definitive quantum computing, the origins of these concepts, how they work and the physical theories that have already proven to be crucial in their development, where we find ourselves in the race to accomplish such a feat as well as the viability of these systems. Amongst these, will be the information and examples required to understand each section. Prior to reaching an informed conclusion regarding the viability of this technology, from my research, one must decide how to quantify whether a system is to be classed as viable or otherwise. I will do so based on the difficulty to implement them, whether there is a place for them in modern society and, foremost, whether they are feasible and capable of working successfully.

- *Digital – "(of signals or data) expressed as series of the digits 0 and 1…". This series of 1s and 0s we call binary.
- *Silicon – A chemical element and semiconductor used to manufacture key components of circuit boards i.e. transistors.

II. The Need for Quantum

In the year 1965, co-founder of computing powerhouse corporation Intel, Gordon Moore, made an empirical observation leading to a prediction that has withheld until recent years - Moore's law. This states that the number of transistors* [4] in an integrated circuit doubles approximately every two years, while the cost halves [5]. Our digital society is based upon this law. However, Moore's law is coming to an end and this has already proven to be a huge issue that will not lend itself to being solved unless alternatives are found. But the question is why. Before this can be answered, some of the core principles of physics must be understood. Oxymoronically, these are some of the most accurate findings and models that, literally, describe the universe down to the most uncomprehensive of scales, yet they are a collection of the most counter intuitive in existence. Here are the two that can most closely be held responsible for the downfall of Moore's law:

"The greatest obstacle to discovery is
not ignorance – it is the illusion
of knowledge"

- Daniel J. Boorstin

The first of these is called particle-wave duality. Consider the seemingly innocent idea that even if none of us were there to see it, the world would still exist. Most of us do not believe that when we close our eyes, everything around us dematerializes only to come back into existence instantaneously upon reopening them. Assumptions like this are instinctively engrained in our minds. Yet in quantum theory, almost all of our basic assumptions are deemed false or invalid, including this very belief.

For this reason, one must let go of two conceptions in order to accept and comprehend what follows. Just because we know a particle looks and behaves like one when observed, doesn't mean it

does so whilst we are not observing it. Another assumption that we must disregard is that the experiments we perform simply unveil the reality that was already there, rather than changing it completely. One man in particular found this extremely difficult – Albert Einstein [6]. The experiment that uncovers these truths, the Double Slit experiment, lets these reassuring ideas go. It revealed the true nature of subatomic particles, such as electrons and photos, and is the most stunning illustration of how the quantum world is so different from the comfortable larger scale of our physical intuition.

The following equipment is set up: An electron gun facing a photosensitive screen where between them stands a plane with a slit cut into it [7, 8]. When a constant beam of electrons was fired at the plane, as expected, the following occurred (see figure 1.a) [9].

However, when two slits were opened, hence the name of the experiment, and the same beam was projected, this time we observe what is called an interference pattern as seen on the optical screen (see figure 1.b) [9] which is a typical property of all waves and occurs when two or more of the same type are 'in phase'. This is where the crests, or troughs, of both waves meet each other when travelling through the same medium and are added together as a result (see figure 2.a) [10]. Two waves that are perfectly 'in phase' have 0 or 2π phase difference* (measured in radians* [11] or seconds) whereas, conversely, when the phase difference is π radians, they are said to be perfectly 'out of phase' or 'antiphase' and they cancel each other out [12] (see figure 2.b) [10]. To those conducting the experiment, it seemed the electrons had travelled through both slits behaving like waves, interacted with each's ulterior that passed through parallel to it and thus produced this pattern. So, they decided to fire the electrons at the plane one at a time with a sufficient time gap between the next, allowing it to either hit the screen or be blocked. Nonetheless, after doing so for a more substantial amount of time, the same pattern emerges (see figure 1.b) [9].

It seems that each electron is individually contributing to this wave-like behaviour which at the time physicists found profoundly shocking considering it appeared to later hit the screen again as a single particle. As a result, a measuring device was focussed on one of the slits so they could determine which slit it passed through. If it was not detected, it passed through the other slit. Anyhow, the electron reverted to behaving like a particle as no interference pattern formed on the screen (see figure 1.c) [9] and a particle was measured to have passed through the observed slit 50% of the time. It was as though the electron knew it was being observed. Meaning in this case, it most definitely travelled through only one slit and not both. We know where the particle is at both ends – the location of the gun and the localised point where it comes into contact with the screen, releasing all of its energy in the process at this spot. Be that as it may, it still acts wave-like in-between where this wave holds all the information, not only regarding possible final positions, but also those at every stage of the journey at any point in space and time. Essentially, it is a family of 'could be' trajectories. Only the act of observation collapses the wavefunction and causes the transition seen in this experiment and as described by the Copenhagen Interpretation* [13].

We have to conclude that each electron travels through both slits not as a particle, but as a wave that interacts and interferes with itself to produce the interference pattern. What separates this from any other interference pattern however, is what the crests and troughs represent; unlike in other types of wave, they represent regions of greater and lower probability, respectfully, that the particle will find itself there. Almost a wave of possible, yet undefined positions that at some point, for some reason can and will resolve itself into a single, well-defined particle of certain position [7, 8]. We call this wave-like distribution of properties the 'wavefunction'. Describing its behaviour lies at the heart of quantum mechanics.

The second of the physical theories necessary to understand why the reign of classical computers may soon come to an end is the Heisenberg Uncertainty Principle. It's core existence can be attributed to the dualistic nature of matter. Prior to delving into the explanation of the principle, I must begin with one key fact – it is impossible to measure something with greater accuracy than the resolution* of the apparatus being used to do so [14]. For example, if you are using a standard ruler to measure a straight line you will not be able to know its exact length to any quantity within a millimetre. This may seem obvious, but this simple fact has astounding implications of which also came to fruition ninety-two years ago.

Formulated in the year 1926, the Uncertainty Principle states that there is a fundamental limit to the precision with which the position and momentum of a particle can be known. It is defined by the following equation:

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

Where Δx = *the uncertainty in its position*
Δp = *the uncertainty in its momentum,*
{Both given as the standard deviation of the measured value from its expected one}.

And $\frac{\hbar}{2} = \frac{\textit{Planck's constant divided by } 4\pi}{2}$ *(an incredibly small number)**

It reads the uncertainty in the position of a particle multiplied by the uncertainty in its momentum must always be greater than or equal to a certain value. Again, this is all because of the act of making an observation, taking a measurement and the techniques we practice in order to do so.

The easiest way to accomplish this is to indicate the particle's position by shining light on it. Like everything in the universe, light is, both, a particle (known as a photon) and a wave. Therefore, it is impossible to use anything other than a minimum of one photon to do so. This means there must be a minimum amount of energy transfer take place and as a result, unpredictively disturb the particle and its velocity. As previously stated, one cannot be more accurate than the resolution of the equipment being used take such a measurement, which in this case turns out to be light itself. Therefore, to measure one of these attributes accurately, we must use light of a shorter wavelength (see figure 2.a/b) [10] which is the defining property of its resolution. And it is this change we make in the light we use to observe a particle's position more precisely that increases the change, and hence the uncertainty, in the particle's velocity which is proportional to the frequency* of the light wave. In other words, the more precisely one knows the momentum of a particle, the less precisely one can determine its position and vice versa [15].

As stated by Professor. S. Hawking, it is an "inescapable property of the world", that also "does not depend on the way in which one tries to measure the position or velocity of the particle, or on the type of particle" [16]. And the effect on our silicon-based computer chips are, yet another, small drop in the vast ocean of proof that keeps quantum theory alive.

It is these two fundamentals that have, and will be, responsible for the downfall of Moore's law. For this to withstand, it has been necessary that the size of the transistor halves every two years so that it can be made possible for twice as many to be placed on a circuit board of identical size which, subsequently, provides significantly more computing power. In the year 2017, we have reached new magnitudes of 14nm in width (approximately twenty-five atoms across). And arriving at this incomprehensively minute scale, marks the boundary to the quantum level.

It is here that these quantum behaviours begin to affect each of the billions of transistors found within our integrated circuits of which are the elementary building blocks of classical computers. A transistor is an electrically driven switch with no moving parts where the passage or denial of current is variable. Like any switch, it controls the flow of electrons by becoming that of an open one, and thus not allowing a flow of electrons, or a closed one where a conductive channel is formed, instead providing a means of transfer for moving charges. These charges move between two parts of the transistor named the source and drain and it can be set to one of two states represented by 0 and 1 where the 1/ON state is activated by applying a small voltage to a gate which removes a barrier previously blocking the current [4].

As we have approach these infinitesimally scales, the quantum effects that the uncertainty principle and particle-wave duality contribute towards become more apparent. When we do so, we can no longer consider the electron as a localised particle with a well-defined position because of its probabilistic comportments. At the source, where electrons are, supposed to be, abundantly trapped in this miniscule area within the transistor, its wavefunction 'spreads itself out' in space. This includes the other side of the boundary preventing the flow of electrons at any point in time when no current is being supplied to the gate. The amplitude (see figure 2.a/b) [10] of the electron's wave tells us the

probability it will be found in any previously undefined location meaning it can, and will, actually pass straight through the barrier [17]. This effect is called quantum tunnelling and provides our computers with unreliable results to any calculations or logic operations being performed, the pivotal roles of transistors. This occurs because if the electron(s) tunnels through the boundary unexpectedly, its state will invert.

Another way to consider this is like so; the size of the transistor decreases, as does the source. This implies our certainty in any given electron's position, and velocity, due to them being confined to a smaller region of space, increases. And by Heisenberg's uncertainty principle, there is a fundamental limit to the extent at which we can know these vector quantities. Therefore, for example, when the space in which the electron exists is reduced, its maximum possible displacement becomes more and more limited.

$$\bar{v} = \frac{d}{t}$$

Where d = *displacement*
t = *time*
And v = *velocity*

As shown in the velocity equation above, the displacement is a necessary quantity in calculating it. If this can take less values, as stated, we become more certain of it. This directly affects the certainty at which one can know an electron's position of which must subsidise and thence, quantum tunnelling becomes more probable.

The transistor is the underlying engine operating at inconceivable speeds and is constantly engaged in computing using raw binary data, accounting for anything and everything imaginable being done by a digital machine. If this is incorrect by reason of quantum tunnelling taking place (altering the state of transistors), the operations will yield erroneous results. The question evolves into at what point does this become so inefficient, it noticeably hinders performance? Our current systems' common flaw will allude upon the error correction adhering to doing so.

- *Transistors – The key electrical component in constructing 'logic gates' which are the arrangements of transistors that allow for calculations to be performed within a classical computer.
- *Phase difference – In basic terms, it tells us how far in front or behind one wave is in comparison to another referenced to the same point in time.
- *Radians – An SI derived unit for angular measure, also used to measure the phase difference of two waves.
- *Copenhagen Interpretation – "an expression of the meaning of quantum mechanics that was largely devised in the years 1925 to 1927 by Neils Bohr and Werner Heisenberg. It remains one of the most commonly taught interpretations of quantum mechanics".
- *Resolution – "the smallest interval measurable by a scientific instrument".
- *Frequency – the number of complete waves (oscillations) that pass a point in one second. The higher the frequency, the more energy the wave carries/transfers.
- *$\frac{\hbar}{2}$ = 5.27285863 x 10^{-35}

III. How Do They Work?

"The significant problems we have
cannot be solved at the same level of thinking

with which we created them."

- Albert Einstein

One should begin to notice the distinct relationship between the discoveries of our physical world and the implications they have on our technology, regardless of the time it takes us to realize them. The contents of this chapter follow this trend, also. It is two quantum behaviours that make computation by physical means a reality. These are quantum superposition and entanglement and are the phenomena that have already started to revolutionize the way in which we compute the algorithms we write.

"Computer Science is no more about computers
than astronomy is about telescopes."

- Edsger W. Dijkstra

Classical computers utilise the only method we've ever known. This is the elementary representation of data. It is information in its purest form and can take one of two values, 0 and 1. These are called bits. Quantum computers take this fundamental and put their own spin* on it. As appose to bits, they compute with quantum bits, 'Qubits'. We can use a multitude of things as qubits such as the nucleus of an atom and photons but here I will discuss how an outermost electron (see figure 3) [44] and its quantum mechanical behaviour enables extraordinary advances in solving computational problems by acting as our qubit.

Electrons and their movement within the orbitals of the nucleus generate their own magnetic fields. Because of this, they have a property called spin which is a quantum state representing the angular momentum and orientation in space with which the electron aligns itself with this magnetic field. This state has multiple pairs of names with the most common being the 'excited' and 'ground' states or 'spin up' and 'spin down'. We can assign a value to each of the states and, for example, say that when an electron is 'spin up', it serves as a 1 and when it is 'spin down', it is its counterpart, a 0. Quantum mechanics also states* that no two electrons at the same energy level, or orbital, can be in the same state at any one time. And we can also manually switch electrons between states at our will by shining light on them. We can do this because some energy is required in order for an electron to be placed in the excited state. A great way to think of this is like the electron is the needle of a compass which, of course, will always point towards magnetic north (e.g. the 0 state). But if one desires for it to instead point south (the 1 state), they would have to, given that the glass has been removed, take the needle and physically turn it until it does so, thus transferring energy to it in the process. The alignment of any electron therefore depends on length of time and amount of electromagnetic radiation we use. As a result, we can position these electrons anywhere between the two states. This quantum weirdness is called superposition and also means that an electron can be in any number of states simultaneously, theoretically making it infinitely more powerful as it is possible to assign any value between 0 and 1. It has, essentially, become analogue.

One can only know the definite quantum state of an electron by observing it, more on this later. Until then, it exists in a superposition of all states where there are separate probabilities that it will resolve itself into the $|0\rangle$ or $|1\rangle$ state.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Where $|\psi\rangle$ *= the resolved quantum state, once observed,*
α *= the probability it will be observed as the* $|0\rangle$ *state,*
And β *= the probability it will be observed as the* $|1\rangle$ *state.*

This is how qubits can store more data than classical bits. For example, lets compare the amount of information two classical bits can store with the amount that two qubits are able to. Two bits could be any of the following: 00, 01, 10, 11. Whereas two qubits would take this form – as they can be in a superposition of all possible states: $\alpha|00\rangle, \beta|01\rangle, \gamma|10\rangle, \delta|11\rangle$. To know the overall state of the classical bits, two pieces of data are necessary – the state of the first and second bit. However, when two qubits are being used, we actually require four separate pieces as shown. These coefficients represent the relative probabilities of measuring the electron to be in one of the two states. Two qubits can store twice the information of two regular bits. This can also be modelled as:

$$2^x \qquad \textit{Where x = the number of qubits}$$

As you can see, this is an exponential (see figure 4) [45] law of which we will see how powerful they can be in a later chapter [18, 19, 20, 21, 22].

These four coefficients do not seem like answers to any problem we may pass to a quantum computer. Not only is this because they are not, but it is impossible to measure them. We cannot measure a superposition as they behave similarly to a particle's wavefunction; the moment it is observed it collapses into a definite state. Subsequently, we must design the logical operations compatible with qubits to be able to arrive at a final result in such a way that this is able to be measured. This is where the problem becomes less about the physics and instead more so about how we will begin to engineer such a system. The theory is known. The engineering is not.

Before we can harness the infinitely more powerful qubits, they must be built along with an environment that will still allow for communication with them. We have achieved this by creating artificial atoms, which is essentially how qubits behave inside what we call a superconducting Josephson Junction.

What would you say if I told you that the coldest place in the known universe is actually sitting on the other side of a rather large black box somewhere in Canada? It's true. To be operational, the qubits and their environment have to be cooled to a specific temperature of 0.015 K, where 0 K is the lowest physically attainable temperature (-273.15 °C). Without such an extreme temperature (which is a measure of the internal kinetic energy of any given particle), the electron, in our case, would be constantly switching between the ground and excited states and back again due to energy transfers caused by its surroundings, ever switching between being a 0 and a 1. Maintaining these conditions is the only way we can know for certain that an electron will be in its ground or lower energy state, unless the system executes instructions to alter it. Without them, computing would be impossible. Any change in its temperature, even by hundredths of a degree, can cause the system to fail as it is crucial in allowing the qubits to exhibit specific quantum mechanical behaviours.

The way in which we switch between states is, as established, by shining light (electromagnetic radiation) at the qubits. Therefore, we couple the Josephson Junction to a microwave* resonator so that we can communicate with any given number of qubits. We, simply, probe them with microwaves causing energy transfer. This resonator must, too, be kept supercooled but instead it is so by a dilution refrigerator.

All that is left is computing using our qubits. This requires the spin of an electron to be measured. The method used to attain such information relies heavily, again, on the transistor which is what the Josephson Junction is based upon. The qubit is simply embedded next to this special transistor and if the qubit is in the excited/spin up (higher energy) state, it will jump from the atom leaving the bare nucleus to the transistor. Otherwise known as the Josephson effect. As electrons have a negative charge, upon the its departure our artificial atom becomes positively charged. This in turn creates a positive voltage that is supplied to the transistor. As appose to the qubit itself, this is what we measure to observe its state. If the qubit was not in this state, it would not have sufficient energy to leave the atom and we would detect no change in voltage. However, it is no longer in any form of superposition. We can also extract similar information from our computations using "the quantum version of the Fourier transform" [23, 24, 25].

- *Spin – By the end of this chapter I sincerely hope you understand that pun. Many apologies.
- *States – I am, honestly, so sorry.
- *Microwave – a form of electromagnetic radiation (light).

IV. The Viability of Such Systems

In the concluding chapter of this academic report, I must discuss whether the envisions of computer engineers and physicists alike will ever be able to fully come to fruition. As aforementioned, this depends on three selected factors: the necessity for them within our modern society, any problems considering their implementation within it and whether they are feasible and capable of working successfully.

5.a Necessity

Classical computers have enabled amazing things. There's no denying it. Amongst other obvious systems, they have given us the internet of which has transformed into the paramount platform we take for granted every day. But its time to talk about what they can't do. There are countless problems our conventional machines cannot help us with, or that would take infinite amounts of computing time to arrive at a solution. But we can only solve small versions of such

complex problems, where as soon as it becomes large enough to be interesting and worthwhile, we simply run out of computing power.

One of these cases of problems are those of optimization. This is where one desires to find the best solution to a problem among many possible solutions. For example, imagine I am hosting a dinner party with ten rather fastidious guests of whom must sit where best fits them all. There are 10!* possible arrangements (3,628,800). In the present, our computers consider some solutions while making approximations as it is the only way I would end up seating guests at all! This is due to current processing speeds being unable to consider each of the three and a half million configurations individually and compare them all. With a quantum computer, however, its qubits would be taken into a superposition of all 3.6 million states and once the problem has been encoded, interference is used to calculate the results. This is possible because as the most optimal results' waves, thanks to particle-wave duality, will have been amplified and the least being left out of phase.

Now to look at a more complex problem we may turn to quantum computing for – researching the world around us in terms of its biology and chemistry. One example of current research within the fields regard enzymes such as nitrogenase. It is crucial to the N_2 to NH_4 reaction in ammonia production which will remain essential in the food, fertiliser and pharmaceutical sectors. It is made up of iron sulphide clusters (protein molecules) of three different sizes, yet we can scarcely simulate the smallest of the three which is made up of only eight atoms using the greatest supercomputer on Earth. The reason for this lies within the atom itself as we must account for every electron-electron repulsion and every attraction to the nuclei [26, 27]. Like in the previous problem, this number grows exponentially, the larger the molecule. An abundance of our problems share this issue of exponential scaling which has proven to be impossible to house a classical computer capable of overcoming.

Aside from these problems, quantum computers could be suitably tasked with making profound advances in research. This could involve modelling biological processes we don't fully understand such as photosynthesis of which is taught in every school across the country, yet we have no way of mathematically describing it like we do electromagnetism through Maxwell's equations that since enabled everything from power generation to wireless communication, for example. It is simply too complicated of a process, until then we remain without the knowledge of what lies on the other side of such a model and its applications [26, 27].

Thought to be caused by a genetic mutation that encodes for the production of amyloid proteins as well as the 'incorrect folding' of such strings of amino acids, there is no cure for Alzheimer's disease [28, 29]. There is no computer powerful enough to simulate this folding responsible for the condition, instead we conduct all our chemistry from first principles, when it could, alternatively, be reduced to software so as a species we do not have to play around with thousands of antibiotics to find an ideal candidate.

Previous large human initiatives include the Manhattan Project and the Human Genome Project of which were both deemed successful thanks to the creation the atomic bomb and mapping every strand of DNA. The next is said to, potentially, be the 'Human Connectome Project' where research teams and scientists poise themselves to tackle mapping the most complex object in the known universe, our brains and their neural circuits, thoughts and memories. Such colossal efforts may require a quantum computer to continue making new discoveries.

5.b Susceptibility

On the other hand, there are some potential problems I have found in relation to constructing such a powerful machine capable of truly unravelling seemingly enigmatic conundrums. One being whomever possesses this raw computing powerhouse, has simultaneously acquired the means to topple data security as we know it. Aside from the fact that a quantum processor would take mere seconds to bypass anything password protected in existence within a matter of seconds, at the most, the data we send between points may also be at risk.

Various groups of people may wish to view any given person's private data being sent via the internet. The way in which this is prevented is through public key encryption. This is where our information, whether it be text, i.e. an e-mail/message, or an image etc. is manipulated in such a way that the original pieces of data cannot be easily derived from what a complex, randomized mathematical hash function* [30] makes of them prior to being distributed.

The current approach that has been employed for a number of years now is called asymmetric encryption and is used in everything from banking to e-mail. Upon joining any system, for example creating an e-mail account, two 'keys' will be generated for each person on the system, one being a 'public' key and the other a 'private' key. Every public key can, and will, be broadcast to anyone you may wish to communicate with whereas private keys remain within the owner's possession only. Upon sending a message, the receivers public key is taken which encrypts the message and sends it. The only way to decrypt the message is to use this person's private key, which only they have access to. Each key is indistinguishable from the other. However, the keys can, and are, also used in reverse beforehand to allow users to verify the authenticity of a sender by encrypting data with your private key which can, conversely, only be decrypted with your public key. Both are achieved along with ensuring no modification has been made to the contents of the message by using your private key followed by the receiver's public key [31, 32].

Each key passes every bit data through a hash function in order to encrypt it. This what makes a quantum computer the ideal piece of equipment to use brute force* [33] in attempting to 'guess' the steps to such an algorithm. It and its qubits would be able to go into a superposition of all possible mathematical stages, resulting in the time it takes to crack the function to be reduced almost infinitely. Not only would this break the data protection act, but also the freedom to share data privately would be brought constantly into question.

5.c Feasibility

From researching why the reign of classical computers will soon fall and the inner workings of a quantum computer, it is evident to me that they are a feasible concept that has made leaps in recent years to becoming closer to the reality of a definitive, fully operational system. Additionally, it is more than merely me coming to this informed conclusion, the proven laws of physics that govern quantum mechanics, quite literally, also state this very fact.

Numerous of the largest and renowned corporate entities are jumping on the quantum computing bandwagon, each in an arms race against the other to be the team first arrive at the next evolutionary stage of our computational machines.

One of the definitions of business is the following – "trade considered in its volume or profitability" [34]. And all enterprises and businesses alike all share one common goal – to increase profit margins. So, as seen in the previous chapter, why would four of the world's leading technology companies place not only their reputation on the line, but also the cash of their investors in attempt to establish a quantum computer if world leading experts and teams that the aforementioned corporations house didn't think one day manufacturing such machines was profitable, let alone possible?

"The days of the digital watch are numbered."

- Tom Stoppard

On the verge of 2018, the research being undertaken by these entities continues to produce staggering advancements. For example, IBM have been studying such technology for over thirty-five years and have recently formed a new division names IBMQ in attempt to deliver commercial quantum systems. They currently sit at the seventeen-qubit mark with this processor available to purchase over the web [35]. Furthermore, their sights are still set upon quantum supremacy through developing a 50-qubit processor (the speed of a current classical computer can be matched by a quantum computer of forty-nine qubits) [36].

However, the fact alone that prestigious tech-companies are ploughing resources into this research does not prove its viability. In one case it can achieve quite the opposite like in the case of D-Wave systems (another enterprise dedicated to producing them for a commercial market). Despite their 'milestones' in terms of qubit-count which thus far peaks at the two thousand level and selling this system to Temporald Defence, a cybersecurity firm, as well as other previous models to their famous customers Google and NASA, they remain controversial. This is because they use adiabatic quantum computing through quantum annealing* [37] that many in the field have dismissed such as IBM who claim it is 'restrictive' and a 'dead end'. Their technology differs from what I and many others believe to be true quantum computing as it waivers too far from other companies' gate-based approach, as discussed, when manipulating qubits similar to the current classical method.

A direct result of this system making use of quantum annealing is that it cannot control its qubits whatsoever. This should make you wonder how they work at all, but the answer lies in the fact that all physical systems tend towards a minimum energy state. Much like a cup of tea that can be boiling hot, but if left for an hour or so will have turned stone cold or be at the same temperature as the surrounding environment (its minimum energy state). This is a good analogy as temperature is only a measure of internal kinetic energy of the atoms making up a substance and annealing is a concept used in the first law of thermodynamics. D-Wave take advantage of this as their qubits also tend towards a minimum energy state so while they cannot control them, they know what their behaviour is going to be. They express their problems, write their algorithms and encode this data as 'energy minimization problems' which is indeed restrictive [38, 39].

Therefore, it wouldn't be entirely unreasonable to say that it is not improbable that D-Wave systems, as a company solely dedicated to quantum computing, encountered problems others simply haven't yet and deviated from these attempts as a result of assessing any possible method of accomplishing true quantum computing as unviable. Essentially settling for separate standards of quantum computation instead. Alternatively, there was a paper published by Google engineers of which states that certain algorithms can be run up 100,000,000 times faster than a single-cored classical computer [40]. In spite of this, as customers of D-Wave systems, the authors of this paper could have held biased opinions on the matter despite developing a hybrid quantum system of their own, as stated by another paper published in March 2017 in 'Mohensi et al, Nature' (Vol 543 9th March) which was taken by the industry as a statement of intent and importance. Nonetheless, this remains impressive.

Aside from this controversy, other companies on this quantum frontier are Microsoft who on its own campus are banking on technology called topological quantum computing [41]. And lastly, the masters of silicon, Intel, are reinforcing this title by developing silicon qubits inside transistors based on the existing classical tech they pioneered themselves [42]. Each company has experienced modest success, leaving me to think much more is, yet, to come.

"An opinion should be the result of thought,
not a substitute for it."

- Jef Mallett

Finally, in my opinion, the most difficult part of making quantum computation a reality is their implementation. A common misconception regarding this technology is that in twenty years' time we will be walking round with quantum mobile phones in our pockets and coming home to quantum desktop computers sitting at our desks. This is rather far from what will become of such systems, in actuality, and is not feasible. This is because of the delicate conditions required for computation to remain possible as well as the sheer scale of them. It would be impossible to retain temperatures of -273.135 °C in such a confined space and to shrink a microwave resonator down to such a scale would be an engineering achievement in itself. Quantum computers currently take up whole laboratories and will continue to do so, but this may not be a problem.

From my research, current areas of study and intuition I suggest a solution and an alternative to the misconception the majority seem to hold. This would be that in the future, quantum computers act much like servers or cloud computing services do today. They are centralized and connected to regular PCs or local servers via the internet.

Classical computers and their operating systems use scheduling algorithms in order to designate processor time both efficiently and fairly amongst all 'jobs' the system must compute at any point in time. There are numerous of such which may include allocating a 'time slice' to each job in the queue, first processing any jobs that will take the shortest estimated time to complete or even a mixture of multiple algorithms [43]. Once quantum computing systems have been established in a similar manner to other centralized services, operating systems' scheduling algorithms could be reworked to account for their extraordinary capabilities. For example, when a huge job or complex problem is passed to a classical computer, the scheduler can off-load this to a quantum computer located elsewhere in the world for processing, much like we can remotely access cloud storage servers and pull our relevant requested data from it anytime, anyplace. This is already possible. Anyone with internet access can actually begin to compute their own algorithms on a quantum computer located at IBM New York online. This way anyone with such access can accomplish quantum computation and allow for not only scientists, researchers etc. the ability to process their convoluted, exponentially growing, problems without estimated processing time starting to approach the age of the universe. Not to mention the obvious application of quantum computers within laboratories and research centres across all fields, as discussed.

Intrinsically linking countless problems, as well as the future of our race, quantum computation could unlock the door to the fourth wave of wealth generation; after the steam engine gave us the Industrial revolution, electricity and the Electric revolution and finally the transistor

giving us the Digital revolution. This wave could be anything from artificial intelligence to bio/nano-tech and the sheer establishment of a true, functioning computer harnessing the behaviours of the quantum realm lends itself to all of them.

In assessing the viability of a quantum system, it would be unreasonable to say there is no need for one, in fact quite the opposite. As laid out, the benefits, that we've realized so far, it would bring greatly outweigh potential issues. The foundations were laid by theorists and built upon by engineers. They have become more than a concept and are on the brink of conforming to a reality. Their viability is as assured as their potential.

- *10! = 10x9x8x7x6x5x x3x2x1 = 3,628,800.
- *Hash function – A type of algorithm specifically designed for use in cryptography that "is designed to be a one-way function… is infeasible to invert".
- *Brute force – Where "automated software is used in a trial-and-error method to generate a large number of consecutive guesses to obtain information".
- Quantum annealing – "a classical randomized algorithm which provides good heuristics for the solution of hard optimization problems", very similar to the ones already discussed in this chapter.

Bibliography

1. (2018). Digital. In: English Oxford Living Dictionaries, n.d. Oxford: Oxford University Press. Available at: https://en.oxforddictionaries.com/definition/digital [Accessed Thursday 22nd February 2018].
2. (2018). Silicon. In: English Oxford Living Dictionaries, n.d. Oxford: Oxford University Press. Available at: https://en.oxforddictionaries.com/definition/silicon [Accessed Thursday 22nd February 2018].
3. Wikipedia, (2006). Silicon. [online] Available at: https://en.wikipedia.org/wiki/Silicon [Accessed Thursday 22nd February 2018].
4. Wikipedia, (2003). Transistor. [online] Available at: https://en.wikipedia.org/wiki/Transistor [Accessed Thursday 22nd February 2018].

5. Schaller, R.R., (1997). Moore's law: past, present and future. IEEE spectrum, 34(6), pp.52-59.
6. Reid, M. (2014). Einstein vs quantum mechanics, and why he'd be a convert today. [online] Physics.org. Available at: https://phys.org/news/2014-06-einstein-quantum-mechanics-hed-today.html [Accessed Thursday 22nd February 2018].
7. Bach, R., Pope, D., Liou, S.H. and Batelaan, H., (2013). Controlled double-slit electron diffraction. New Journal of Physics, 15(3), p.033018.
8. WhatTheBleep. (2006). What The Bleep Do We Know!?: Down The Rabbit Hole – Dr Quantum – Double Slit Experiment. [video] Available at: https://www.youtube.com/watch?v=DfPeprQ7oGc [Accessed Friday 23rd March 2018].
9. The Royal Institution. (2013). Stages of Double Slit Experiment. [image].
10. Wikipedia, (2010). Wave interference diagrams. [images] Available at: https://en.wikipedia.org/wiki/Wave_interference#/media/File:Interference_of_two_waves.svg [Accessed Sunday 18th March 2018].
11. Wikipedia, (2004). Radian. [online] Available at: https://en.wikipedia.org/wiki/Radian
12. Benn, M. and George, G. (2015). Edexcel A Level Physics. London: Hodder Education, pp.212-215
13. Heisenberg, W., (1958). Physics and philosophy.
14. Benn, M. and George, G. (2015). Edexcel A Level Physics. London: Hodder Education, pp.10-12
15. Heisenberg's uncertainty paper has been translated into English by Wheeler, J. and Zurek, H. (1983) Quantum Theory and Measurement. Princeton: Princeton Univ. Press, pp. 62-84.
16. Hawking, S. (1988). A Brief History of Time. 6th ed. London: Transworld Publishers, pp.61-70.
17. Wikipedia, (2005). Quantum tunnelling. [online] Available at: https://en.wikipedia.org/wiki/Quantum_tunnelling [Accessed Sunday 18th February 2018].
18. Nielsen, M.A. and Chuang, I.L., (2010). Quantum computation and quantum information.
19. DiVincenzo, D.P., (2000). The physical implementation of quantum computation. arXiv preprint quant-ph/0002077.
20. Feynman, R.P., (1982). Simulating physics with computers. International journal of theoretical physics, 21(6-7), pp.467-488.
21. Feynman, R.P., (1986). Quantum mechanical computers. Foundations of physics, 16(6), pp.507-531.
22. Steane, A., (1998). Quantum computing. Reports on Progress in Physics, 61(2), p.117.

23. PD Knowledge. (2014). Quantum Computer in a Nutshell (Documentary). [video] Available at: https://www.youtube.com/watch?v=0dXNmbiGPS4 [Accessed Friday 23rd February 2018].
24. Ponnath, A., (2006). Difficulties in the implementation of quantum computers. arXiv preprint cs/0602096.
25. Ackland, R. (2015). How to build a quantum computer. [video] Available at: https://www.youtube.com/watch?v=_dvByciEwT0 [Accessed Friday 23rd February 2018].
26. IBM Research. (2017). Quantum and Chemistry. [video] Available at: https://www.youtube.com/watch?v=qarc7AA4-wM [Accessed Saturday 10th March 2018].
27. Popkin, G. (2017). Quantum computer simulates largest molecule yet, sparking hope of future drug discoveries. [online] Sciencemag.org. Available at: http://www.sciencemag.org/news/2017/09/quantum-computer-simulates-largest-molecule-yet-sparking-hope-future-drug-discoveries [Accessed Saturday 10th March 2018].
28. Department of Neuroscience, Istituto di Ricerche Farmacologiche Mario Negri. (2002). Protein misfolding in Alzheimer's and Parkinson's disease: genetics and molecular mechanisms. [online] US National Library of Medicine/National Institutes of Health. Available at: https://www.ncbi.nlm.nih.gov/pubmed/12392798 [Accessed Friday 10th March 2018].
29. King Fahd Medical Research Center, King Abdulaziz University. (2014). Protein misfolding and aggregation in Alzheimer's disease and type 2 diabetes mellitus. [online] US National Library of Medicine/National Institutes of Health. Available at: https://www.ncbi.nlm.nih.gov/pubmed/25230234 [Accessed Friday 10th March 2018].
30. Wikipedia, (2004). Cryptographic hash function. [online] Available at: https://en.wikipedia.org/wiki/Cryptographic_hash_function [Accessed Sunday 18th February 2018].
31. Microsoft TechNet. (2005). Understanding Public Key Cryptography. [online] Available at: https://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx [Accessed Sunday 18th February].
32. Wikibooks. (2014). Crptography/A Basic Public Key Example. [online] Available at: https://en.wikibooks.org/wiki/Cryptography/A_Basic_Public_Key_Example [Accessed Sunday 18th February].
33. Techopedia. (2018). Brute Force Attack. [online] Available at: https://www.techopedia.com/definition/18091/brute-force-attack [Accessed Friday 10th March 2018].

34. (2018). Business. In: English Oxford Living Dictionaries, n.d. Oxford: Oxford University Press. Available at: https://en.oxforddictionaries.com/definition/business [Accessed Saturday 14th March 2018].
35. IBM Research. (2017). The Future is Quantum. [online] Available at: https://www.ibm.com/blogs/research/2017/11/the-future-is-quantum/?utm_source=ibmqwebsite&utm_medium=web&utm_campaign=ibmq&utm_content=2050qubit [Accessed Friday 23rd March 2018].
36. IBM Research. (2017). Quantum Computing: Breaking Through the 49 Qubit Simulation Barrier. [online] Available at: https://www.ibm.com/blogs/research/2017/10/quantum-computing-barrier/ [Accessed Friday 23rd March 2018].
37. Tamascelli, D. and de Falco, D. (2011). An introduction to quantum annealing. [online] Cornell University Library. Available at: https://arxiv.org/abs/1107.0794 [Accessed Friday 23rd March 2018].
38. Gibney, E. (2017). D-Wave upgrade: How scientists are using the world's most controversial quantum computer. [online] Available at: https://www.nature.com/news/d-wave-upgrade-how-scientists-are-using-the-world-s-most-controversial-quantum-computer-1.21353 [Accessed Friday 23rd March 2018].
39. D-Wave Systems. (2018). Quantum Computing – How D-Wave Systems Work. [online] Available at: https://www.dwavesys.com/quantum-computing [Accessed Friday 23rd March 2018].
40. Denchev, V.S., Boixo, S., Isakov, S.V., Ding, N., Babbush, R., Smelyanskiy, V., Martinis, J. and Neven, H., (2016). What is the computational value of finite-range tunneling?. Physical Review X, 6(3), p.031015.
41. Linn, A. (2017). With new Microsoft breakthroughs general purpose quantum computing moves closer to reality. [online] Microsoft News. Available at: https://news.microsoft.com/features/new-microsoft-breakthroughs-general-purpose-quantum-computing-moves-closer-reality/ [Accessed Friday 23rd March 2018].
42. Intel Newsroom. (2018). Intel Sees Promise of Silicon Spin Qubits for Quantum Computing. [online] Available at: https://newsroom.intel.com/news/intel-sees-promise-silicon-spin-qubits-quantum-computing/ [Accessed Friday 23rd March 2018].
43. Heathcote, P. and Heathcote, R. (2016). Oxford Cambridge and RSA AS and A Level Computer Science. Dorset: PG Online Limited, pp. 30-33.

44. GCSEScience.com. (2015). Annotated diagram of atom. [image] Available at: http://www.gcsescience.com/a3-electron-shell-energy-level.htm [Accessed Thursday 29th March 2018].
45. Google. (2018). Graph of 2^x. [image] Available at: https://www.google.co.uk/search?q=2%5Ex+graph&rlz=1C1CHBF_en-GBGB778GB778&oq=2%5Ex&aqs=chrome.2.69i57j0l5.8429j0j4&sourceid=chrome&ie=UTF-8 [Accessed Thursday 29th March 2018].