

**COURSEWORK COVER SHEET**

**FOUNDATION IN SCIENCE AND TECHNOLOGY**

**SUBJECT TITLE : BASIC COMPUTER CONCEPT**

**SUBJECT CODE : FSTM3054**

**INTAKE : JULY 2020**

**COURSEWORK TITLE : REVIEW 1 – INDIVIDUAL ASSIGNMENT**

**COURSEWORK** **:** **15%**

The objective of this assessment is:

* To evaluate student’s understanding on technology concepts.
* To encourage students to think critically about the way’s technology advancements can

improve our daily lives.

Student Name: Lester Koon Zhy Min.

Student ID: 20068813.

Table of Contents

[**TOPIC 1: Quantum Computing** 3](#_Toc48949078)

[**Introduction to Quantum Computing** 3](#_Toc48949079)

[**Background to Quantum Computing** 4](#_Toc48949080)

[**How Quantum Computing Functions** 6](#_Toc48949081)

[**Superposition** 6](#_Toc48949082)

[**Entanglement** 7](#_Toc48949083)

[**Application of Quantum Computing** 8](#_Toc48949084)

[**Cybersecurity & Cryptography** 8](#_Toc48949085)

[**Financial Services** 9](#_Toc48949086)

[**Artificial Intelligence & Machine Learning** 9](#_Toc48949087)

[**Healthcare** 10](#_Toc48949088)

[**Challenges of Quantum Computing** 10](#_Toc48949089)

[**Conclusion** 12](#_Toc48949090)

[**TOPIC 2: Biometrics** 13](#_Toc48949091)

[**References** 16](#_Toc48949092)

# **TOPIC 1: Quantum Computing**

## **Introduction to Quantum Computing**

Moore’s Law, which describes that the processing speed and computing power doubles every 18 months, has started to slow down as classical computers that work on classical mechanics are at their zenith of expansions. Due to this, “Quantum Computing” (QC) a novel subject over a decade ago, have surfaced in the imagination of the general population in recent years yet, it is still poorly understood by most. The question still stands, what exactly is Quantum Computing? Quantum computing is a branch of study that concentrates on the expansion of computer technology based on the theory of quantum mechanics such as superposition and entanglement. Quantum mechanics, one of the most counter-intuitive ways to describe the world that explores and explains the nature and behaviour of macroscopic phenomena on a fundamental level. However, instead of atomic and subatomic particles, quantum computing utilizes a combination of quantum binary digits, or qubits to carry out specific yet complex computational functions. A traditional computer uses bits that have the operational value of either 0’s or 1’s, on the other hand, qubits used in quantum computers can represent the values of 0’s, 1’s or both a 1 and 0 simultaneously or any value in between. As a result, qubits are enables quantum computers to perform particular calculation that would normally seem infeasible at a breakneck speed in contrast to classical computers. The power of quantum computing that lies in its ability to manage and generate qubits, also bring its own set of challenging problems from both a scientific and engineering aspects.



Figure 1.0: Google’s quantum computer

## **Background to Quantum Computing**

The development of quantum theory began in the year 1900 with a presentation by theoretical physicist Max Planck to the German Physical Society. During the presentation Planck introduced the idea that energy and matter exists in individual units. Over the next thirty years, several scientists began to further develop on Planck’s idea lead to the understanding of modern quantum theory. This discovery remains as a cornerstone on which condensed matter physics, chemistry and technologies ranging from transistors to emitting diodes. Decades later in the early 1980s, Paul Benioff, an American physicist, and a trailblazer of the quantum computing world, paved the way for a prospect of a quantum computer with his idea of the original quantum mechanical model of a computer. Through his findings, he describes that a computer could under the principles of quantum mechanics through a Schrödinger equation explanation of Turing machines, thus marking the starting point of quantum computing. Meanwhile, in 1981, Nobel laureate Richard Feynman pointed out in MIT during the First Conference on the Physics of Computation that it was paradoxical for a classical computer to stimulate the evolution of quantum phenomena easily and efficiently. As a result, from his observation on Benioff’s work, he proposed the idea of a basic model for a quantum computer. Feynman proceeded to conclude his lecture by saying that he was unhappy with the standard norm that all analyses needed to go with classical theory and state that quantum mechanics should be used to stimulate computing nature as it was a wonderful problem that was not so easily solved. Later, in 1985, David Deutsch, a British physicist at Oxford University, suggested a way to mathematically understand the possibilities that lie in quantum computers. While different Turing machines can be efficiently stimulated by a universal Turing machine through the Church-Turing thesis, therefore a universal quantum computer is in a position to simulate different quantum computer with at most a polynomial slowdown. In the year 1994, Peter Shor showed that multiple key computational problem that thought to be to difficult for ordinary computer to solve, in belief could be solved meaningfully more proficiently using quantum computing. The interest in quantum computing drastically rose when Shor developed a quantum algorithm to solve discrete logarithms problems and efficiently factorize large integers that could take even the most advance supercomputers today eons to compute. Theoretically, Shor’s algorithm suggested that anyone possess the power to break most of the cryptosystems used today with the help of a quantum computer in a matter of hours rather than a million years. Since this discovery was made, quick and practical quantum computer algorithms have been developed for many of our hard-classical tasks, such as but not limited to machine learning, simulating molecular systems in chemistry, and solving systems of linear equations. Then during the year of 1996, Lov Grover conceived a quantum database search algorithm that presented a 4x speedup for a variety of matters. Any issues that would normally be resolved by brute-force or random search would currently be 6completed at quadruple the speed. Two years later, in 1998, first quantum algorithms like Grover’s algorithm were solved by a working 2-qubit NMR quantum computer being built. The competition to develop an additional abundance of applications was heading into a development era for computer systems. Two decades later, the IBM Q System One was unveiled by IBM as its first commercial quantum computer. Later, IBM’s biggest quantum 53-qubit computer went online. Google announces the creation "Bristlecone”, a 72-qubit quantum chip, achieving a innovative height. Google then also publicized in October 2019 that it has achieved quantum supremacy after its 54-qubit Sycamore processor was ready to perform a calculation in 200 seconds. within the past, such a calculation would have required 10,000 years of a typical supercomputer. we've thus demonstrated how increasing global investment in quantum computing makes the longer term seem brighter and filled with possibilities.

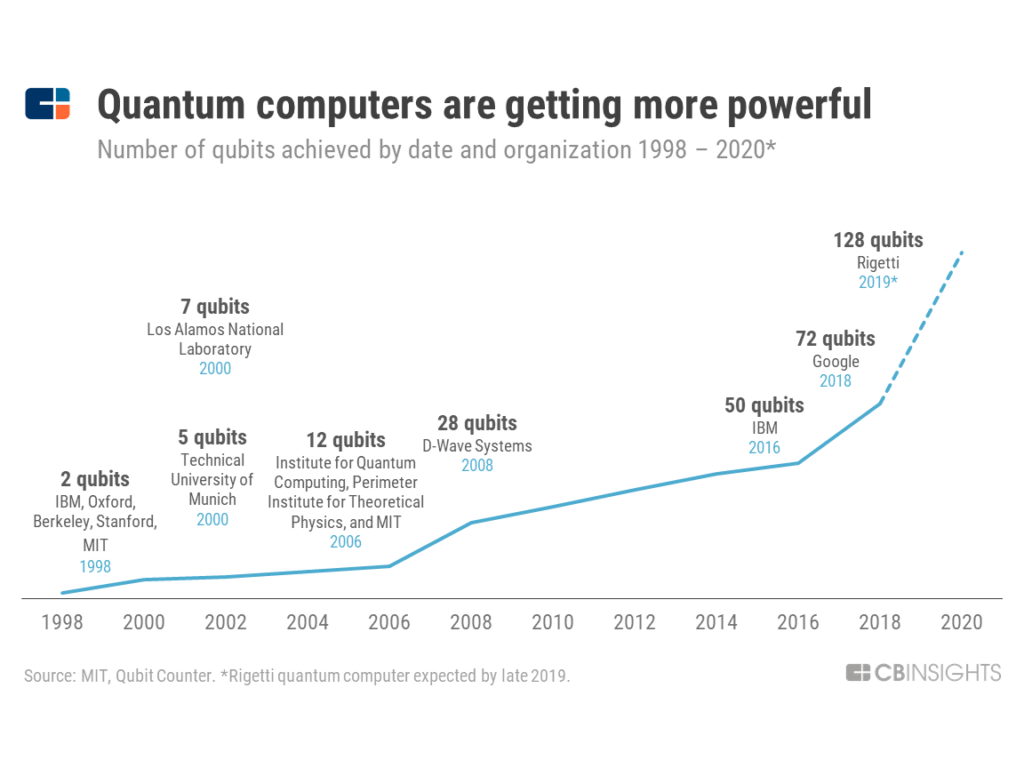


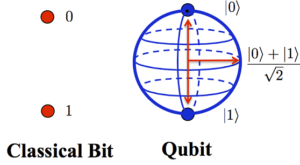
Figure 1.1 The advancement of the number of qubits achieved for quantum computers over the past 20 years

## **How Quantum Computing Functions**

Traditional computing depends on logic of the Boolean algebra, which uses a 3 or 7-mode gate principle as a basis to function. The data must be processed in a strictly binary state at any point of time which is either 1, on or 0, off . These values are better known as bits, which stands for binary digits. The million of capacitors and transistors that make up the heart of computers can only be in one state at any given time. Furthermore, there is still a glass ceiling as to how fast these components can be made to switch between states. As the progress of making smaller and faster circuits already reaching the molecular scale in the next few years, the threshold for classical physical laws of physics and the physical limit of materials in computing has begun to reach its zenith. Conversely, quantum computers operate with a two-mode logic gate, XOR and a mode called QO1, which is the ability to change the value 0 into a superposition. In a quantum computer, several subatomic particles such as photons or electrons can be used. Each of these particles is polarize or given a charge, so it is able to act representation of 0 and/or 1. The then polarized particles are called quantum bits, or qubits. The behaviour and nature of these particles form the foundation of quantum computing and quantum supremacy. The principles of entanglement and superposition are two of the most relevant aspect of quantum mechanics used in quantum computing.

### **Superposition**

In the quantum universe, the state of a system, for instance, an electron or an atom is described by a state vector mentioned as a wave function. A probabilistic understanding of the wave function that describes the state of a system under investigation is employed to explain various quantum eﬀects like ﬁnding the system during a particular state. The fact that a wave function can define microscopic particles features a reference to a wave-particle duality, an idea that matter and energy can exhibit the properties of both a wave and a particle. This concept establishes the failure of classical concepts, such as a “wave” or “particle”, to elucidate the phenomena observes on small-scale objects. This principle, called quantum superposition, means that a quantum state can be represented as a sum of other distinct state. Conferring to the Copenhagen interpretation of quantum physics, valid only within the microscopic world, the physical properties of a system being investigated cannot be shown before it is measured, hence the only prediction is the probability of a given measurement possible. Furthermore, the act of measurement affects a system as it leads to the collapse of the system’s set of probabilities to just a single value. In quantum mechanics jargon, this phenomenon is dubbed “wave function collapse’. Erwin Schrödinger, however rejected this interpretation, sought to illustrate the absurdity of the notion that the laws of nature change in the conversion from subatomic systems to macroscopic systems. In the renowned thought experiment of Schrödinger’s cat, he proposed a situation where a cat is placed in a box along with a Geiger counter, a radioactive substance and a device that emits poisonous gas. The radioactive substance decays once an hour, which will impact the GM counter and triggers the device to release the poisonous gas, which in turns kills the cat. In reference to quantum theory, after 30 minutes the radioactive atom can either be decay or not. There’s no telling of its decay exact moment, but once it does decay, it is sure to release the poison and kill the cat. Until the box opens, an observer has no way of knowing whether the cat is alive or dead in response to the radioactive substance decay. Before a measurement is performed quantum mechanics tells us that the radioactive substance and the cat are in a superposition of being non-decayed/dead and decayed/alive. Therefore, before the measurement until the system collapses into a singular configuration the cat is in a peculiar state of both” living or dead in equal parts”. Quantum computing functions on a similar premise. The state of a qubit can be represented in numerous possible combinations of 0 and 1 simultaneously. They have a probability of being 0 and a probability of being 1, until the qubits are measured which results in the emergence of calculation, it immediately causes the “collapse” of their quantum state to either 1 or 0. This superposition of qubits allows for additional computational complexity, which allows a quantum computer to crunch through a number of potential outcomes at a single moment of time.



Source: [eyerys.com](https://www.eyerys.com/articles/news/google-introduces-openfermion-software-ease-scientists-using-quantum-computers)

Figure 1.2: Comparison between classical and quantum bits The Bloch sphere is used to represent the possible states of a single qubit.

### **Entanglement**

To make the huge advances that are assured by quantum computing, group of independents qubits singularly are not enough. The wonders of quantum computing comes into fruition when the quantum principle of entanglement is implemented. An industry expert used the description of a “very expensive classical computer” to represent qubits without entanglement. Entanglement is another counter-intuitive quantum phenomenon, which states that between quantum particles in superposition exist a very strong correlation that links them together in perfect unison no matter how far apart they are. For example, the result of the measurement of one qubit will always be correlated to the measurement of another qubit even if the particles are separated from one another by a great distance. Hence, Einstein coined the phrase “spooky action at a distance” to describe the theory of entanglement. Entanglement particles such as qubits that have interacted at some point becomes entangled with each other in pairs. Knowing the spin state of one entangled particle, either up or down gives away the spin of the other in the opposite direction. The measured particle has no single spin direction before being measured with the addition of the principle of superposition. The spin state of the particle being measured is determined at the time of measurement and communicated to the correlated particle, which simultaneously assumes the opposite spin direction. As a result, information is able to travel almost instantaneously even faster than the speed of light. This principle can be further supported by the thought experiment, the EPR paradox or the Einstein-Podolsky-Rosen Paradox. In terms of conventional computing, this is often a touch like having a gate connecting equally in bit memory with one another. The thought of how powerful this element is can begin to ascertain, which may be compared with a standard computer wanting to read and write from each element of memory separately before operating thereon. Quantum superposition and entanglement can be taken together to enhance computing power tenfold. A 2-qubit register during a quantum computer can store all configuration of 00, 01, 10, or 11 simultaneously, when compared to a standard computer where a 2-bit register can store only one of 4 binary configurations at any given time,. this is often actually because each qubit represents two values. If more qubits are added, the increased capacity is expanded exponentially.

## **Application of Quantum Computing**

Figure 1.3: Distribution of quantum computing uses in various fields

### **Cybersecurity & Cryptography**

Quantum computing has the potential to interrupt the encryption on which most enterprises, digital infrastructures and economies believe. Cybersecurity is one key term regrading advancement in technologies. At this moment, the web security world has been quite vulnerable thanks to the increasing number of cybercrimes occurring across the world a day. Although companies and organizations are creating necessary security framework, the method becomes impractical and daunting for classical digital computers as even the massive companies like Twitter and Facebook are victims of cyber-attacks. Therefore, cybersecurity has continued to be an important concern round the world with the increasing dependency on digitalisation. Quantum computing possesses the power break cryptographic codes that's want to keep sensitive data and transmission secure. The implementation of Shor’s algorithm in quantum computers are eligible to open large-scale and methodical breaches of security and governance related mechanism using current cryptosystems. If the market contributors don't properly forestall and manage their crypto-mechanisms, such developments would be devastating for them. Conversely, quantum computing could even be wont to enhance theses important data from quantum hacking, a way referred to as quantum encryption. Nowadays, most online security of public cryptographic systems is underpinned by the problem of huge integer factorisation into prime numbers. However, the immense time used to ‘crack the code’ is both costly and impractical, as currently it is being accomplished by using conventional computer by rummaging through every possible factor. additionally, it's computationally infeasible for a classical computer to factorise large integers if they're the merchandise of two 3000-digit primes. In contrast a quantum computer can efficiently solve this through Shor’s algorithm. This ability would allow a quantum computer to interrupt many of the cryptographic systems in use today, within the sense that there would be a polynomial time algorithm for solving the matter. Through this, the RSA, Diffie–Hellman, and elliptic curve Diffie–Hellman algorithms that are popular foundation for many public key ciphers today can easily be broken. However, other cryptographic systems couldn't be broken through the facility of quantum computing. As an example, lattice-based cryptography that uses huge grids with billions of individual points across thousands of dimensions. Breaking the lattice cryptosystem means getting from a selected point to a different, which is entirely impossible unless the precise route is understood. Cybersecurity and encryption are often improved by quantum computing through quantum encryption. Quantum encryption is that the thought of sending entangled photon particles over an outsized distance in what is referred to as Quantum Key Distribution (QKD) for the aim of securing communications. the foremost important advantage of using QKD is that the ability to detect eavesdropping because the encryption key will show any sign of disruption instantly and reveal that the communication is vulnerable. This relies on the principle that the act of measuring a quantum system disrupts the system. Thus, quantum-based cryptographic systems could, be safer than classical systems against quantum hacking, as quantum cryptography can potentially fulfil a variety of public key cryptography functions.

### **Financial Services**

The modern marketing world is one of the most complicated systems to ever exist. While the development of mathematical and scientific tools to preachify this is seemingly increasing, it still faces one major hurdle that other fields do not have, which is an everchanging setting to run experiments. This issue has caused investors and analyst to investigate quantum computing to solve this. Investors often wish to gauge the distribution of outcomes under a particularly sizable number of scenarios generated randomly to be able to sustain a living in the market. The technique of ‘Monte Carlo’ simulations is used to achieve that, by being run continuously on classical computers, which consumes a large computational time. However, in addition to improving the standard of the solutions and reducing the development time of them, companies can also perform these massive and sophisticated calculations through the application of quantum technology. This system is being utilized by companies like D-wave and JPMorgan Chase for risk management and complex financial modelling within the financial industry. Quantum computing can also effectively interconnect dependencies and identify key fraud patterns, which can be used to determine tempting portfolios given thousands of assets. For conventional computers working in the mathematically complex world of the banking sector, this is often time-consuming and wishes tons of computer power to process such algorithms. Fraudulent activity could also be detected by using quantum computers supporting fast-learning algorithms that was previously thought to be inconceivable using classical computers given the sheer volume of big-data.

### **Artificial Intelligence & Machine Learning**

Machine learning and Artificial intelligence (AI) are becoming some of the most prominent areas of technological advancements in recent times, as technology have been implemented into all aspect of humans’ lives. Artificial intelligence is a prime application of quantum computing. AI is when a computer program appears to exhibit “intelligence” through the principle of learning from experience, and becoming even more precise as responses are given. This feedback is based on calculating probabilities for many possible choices by pulling large datasets of images, videos, and text. However, with the overabundance of content available both in the virtual and physical world, it becomes a challenging task for conventional computers. Therefore, machine learning empowered by quantum computers enables AI programs and application to search through these petabytes of datasets concerning fields such as medical research, financial market and human behaviour and make sense of them. Its been said that AI in the twenty-first century will be as revolutionary the invention as the wheel in every industry. For example, quantum computers are planned to use to test autopilot software that is currently too complex for classical computers by the Lockheed Martin and its quantum computer, D-wave, and on the other hand, a quantum computer is being used by Google to design software that can distinguish cars from landmarks.

### **Healthcare**

One of the most pivotal application of quantum computing would be in the field of healthcare. First and foremost, quantum computing with the help of machine learning would be able to create a prefect and safe decision support system. Quantum computers would be able to skim through every research, reports, and medical history, and find any correlation or causation that the human eye would never find. It would then be able to produce precise and suitable a diagnoses or treatment options that the human doctor could have never discover by themselves. Drug design and development is a challenging problem in quantum computing. Normally, drug development is carried out via trial and error method, which are not only both very dangerous and risky but also expensive and difficult task to complete. Quantum computer could help determine the best medical treatment possible by speeding up the process of comparing the effects of different drugs on a wide scope of diseases. Additionally, quantum computing could also lead to the production of highly personalized medicine through genome sequencing. The representation of a person’s whole DNA strand requires massive storage capacity and computational power, as genome sequencing produces a lot of data. A quantum computer could piece together and filter through all possible gene variants simultaneously and find all nucleotide pairs, making the process quicker and easier. Synthesizing patterns within the world’s DNA data to achieve a breakthrough in the understanding of our genetic makeup and potentially uncovering previously unknown disease patterns, might all be made achievable by the usage of quantum computers.

## **Challenges of Quantum Computing**

The main challenges faced by quantum computing is its sensitivity to its surrounding, since any interaction, or measurement leads to a collapse of the state function. A quantum system is said to be coherent if it is not interwoven with its surrounding, so it can be in a state of superposition that can entangle. The system losses its coherence once it interacts with the surrounding, in a process called quantum decoherence. An example of decoherence can be found in the double-slit experiment: when abeam of particles, say electrons, passes through two slits and then hits the screen, an image of the interference pattern is reﬂected on the screen. The accumulated different phases that creates the pattern determines, whether the interference is constructive or destructive once the particle hit the screen. However, a measurement made to determine through which of the slits the particles went through before reaching their destination will cause the state function to collapse, causing decoherence. Hence, during the computation phase, total isolation from all external forces id a necessity for quantum computers. Little breakthroughs have been achieved with the use of qubits in intense magnetic fields, using ions. The next challenge faced would be error correction. Errors which are either internal or externally induced is a norm for computing of all sorts. The traditional computers have the capability to perform well because the hard-limiting of computation process makes it possible to correct small errors, which in turn eliminates large bit errors using error-correction coding. However, qubits are not ordinary bits of data and thus cannot be solved through classical error correction. Error correction is proven to be vital in quantum computing as even a solitary error in a calculation can cause the entire computation to collapse in validity. There has been progress in this area through an error correction algorithm that utilizes a combination of computational and correctional qubits. For instance, IBM made a breakthrough that uses a total of 5 qubits, 1 computational and 4 correctional. In addition, as a result of the sheer complexity and how advance quantum computing is, it faces major hurdles the design and creation of its software and hardware. Quantum algorithms must leverage uniquely quantum features like interference and entanglement to reach the ultimate classical result, if quantum computers are to be taken advantage of. Thus, achieving quantum speedup requires totally new sorts of algorithm design principles and clever algorithm design. As with all computers, building a beneficial machine is far more intricate than simply creating the hardware tools are needed to make and debug QC-specific software. Quantum programs are different from programs for traditional computers, thus further research and development is required to create the software tool stack. Contemporaneous development of the software and hardware tool chain will shorten the event time for a useful quantum computer, as these software tools are driving the hardware. In fact, using early tools to finish the end-to-end design helps illuminate issues in the dark corner and drives toward designs with the sole chance for overall success, an approach utilized in the design of conventional computer. Building perfect qubits may be a challenge to current engineering because it is extremely diﬃcult to isolate them from the external environment to enable the generation and manipulation of qubits. Some companies, like Google, IBM and Rigetti Computing, uses cold temperatures to cool superconducting circuits. Others, like IonQ, uses ultra-high-vacuum chambers to ensnare individual atoms in electromagnetic fields on a chip. The objective of isolating the qubits during a controlled quantum state are the same for these two cases.

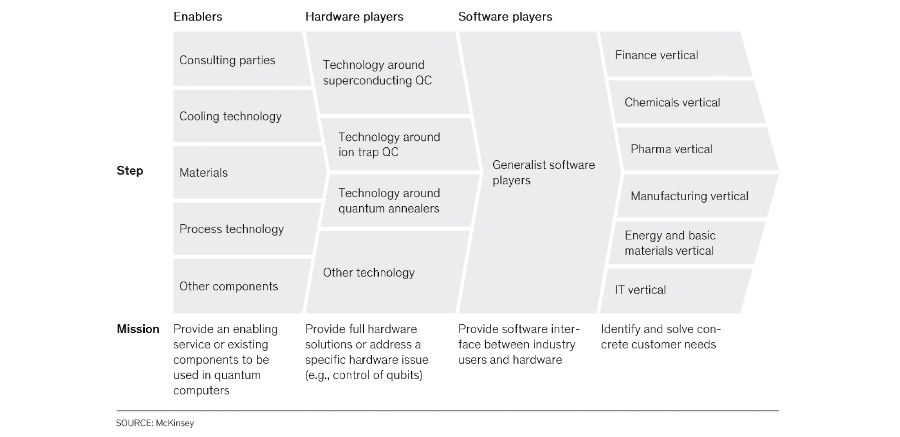


Figure 1.4: The steps in achieving effective quantum computing

## **Conclusion**

In conclusion, Quantum Computing will soon reach a state of quantum supremacy, which ask the hypothetical speedup advantage of a quantum computer in comparison to a standard computer. The vast potential of quantum computing with the essential concepts of quantum physics like superposition entanglement and decoherence would theoretically be ready to forever revolutionize every field from finance to medical within the future. Thus, companies and organizations should be quantum-ready to be ready to smoothly incorporate quantum computers into their business process. Quantum computing has various possible applications that might be ready to solve currently unsolvable or less efficiently solvable by conventional computational situation. However, the presence of noteworthy technical challenges of building such a system and to further improve it to practical advantage for a valued task still remains. Hence, making quantum computing no cakewalk, because it has its own set of limitation and challenges within the path of creating quantum computing a totally useable commodity. Not everyone has faith during a feasible upcoming for quantum computers. The hurdles of eliminating quantum errors are seen by some as simply being too high to overcome. Hence, only time will tell if quantum computing supremacy will become a revolutionary point of modern technology in the near future or will it still remain as a theoretical fantasy.

# **TOPIC 2: Biometrics**

In the recent years, the security and privacy of every aspect of the world has reach a critical turning point, which is with the implementation of biometrics security systems. Biometrics is known as unique behavioural or physical human trait and characteristic that can be utilize to digitally identify a person. These characteristics and traits compromise of inimitable measurements and calculations of definite technical processing of the physiological, behavioural, or physical characteristics that differs from one person to another. The technology of biometric security is a security system used for the identification and access control of individuals under surveillance. Biometric systems will store and gather biometric data to utilize it as a basis to automatically evaluate and authenticate personal identity. The biometric security system functions based on a lock and capture mechanism to ingress a particular data. A unique characteristic or traits is needed to be provided by an individual so it can be matched to a database in the system, in order to access biometric security system. If a match can be found, the user will be given access by the locking system. The locking and capturing system will trigger and record information of each user that has accessed the info. This interaction between biometric security system and the biometric date is additionally referred to as the lock and key system with the biometrics is a key and the biometric security system is the lock opened by that key. Hence making this security system a robust and fool proof physical security technique used for biometric identification.

Biometrics can be mainly categorised into two types, which Physiological Biometrics and Behavioural Biometrics. Physiological biometrics are those that rely on a person physical characteristic to determine identity. Physiological biometrics can be further divided into two subcategories. This biometrics type includes but is not limited to fingerprints, hand geometry, the shape of the face, vein pattern and the iris and retina of the eyes, for morphological analyses. On the other hand, for biological analyses saliva, blood, urine or DNA may be used. Behavioural biometrics, however is the scientific study of how living organism function. Voice recognition, gaits, signature recognition, gestures, the way objects are used, the sound of footfalls, and keystroke dynamics. However, the various kinds of biometrics do not have an equivalent level of reliability. The advantage being that physiological measurements have a more stable consistency. For instance, they are not affected by emotions or stress, in comparison to identification by behavioural measurement.

Historically, criminal, or civil identification and military access control where the only application of biometrics that was initiated by the authorities. However, today a broad spectrum of sectors from banking to healthcare are showing growing interest in biometric technology and its advantages . One of the largest sectors that have implemented biometrics into its system would be border control. Many countries across the globe have already implemented biometric border security systems for quick and precise identification of both domestic and international travellers, thus preventing the entry of illegal immigrants. Additionally, in current times, the growth of transnational crime and terrorism have led to a rise of security worries, which peaked the interest to make more precise identity checks through biometric technology. One of the most prominent events that sparks biometric development in this case would be the terror attacks of September 11, 2001. As a result, through the USA Patriot Act, all international travellers are required to provide machine-readable, travel documents with biometric information while travelling through either airports, seaports, or other border control environments. Biometrics serves as an undeniable link between the travel documents and its holder. Being on the border with Mexico, which is notorious for its high criminal activity such as assault and drug trafficking, the USA’ Federal Bureau of Investigation have implemented biometric security system into its border control management. The FBI’s Integrated Automated Fingerprint Identification System (or IAFIS) is an electronic database that contains electronic fingerprint information from all level of law enforcement agencies throughout the mainland. It allows these fingerprint records to be easily spread and recorded. In addition, IAFIS also holds photographs, mugshots of criminals, information about a person’s criminal background and information about employees of the federal government. Thus, it can identify criminals from positive identification from records of ten-print submissions or latent print submissions. Through this system, the FBI was able to score matches on 118,557 criminal suspects that were trying to illegally enter the United States, between September 2005 and December 2005.These statistics proves that many loopholes in border security were successfully closed through the implementation of biometric technology border control.

Figure 2.1: A fingerprint scanner used at a border

Following that, the ever-expanding sector of e-commerce in the marketing world, has deemed the usage of card payments as a standard norm. However, the current method of swiping a card to make a transaction is slowly becoming obsolete in the advancing world today. The usage of chip-enabled cards across Europe and North America, that was thought to solve this issue, came with its own set of problems such as consuming time as the user is required to enter the PIN in every purchase made. Near-Field Communication (NFC) transaction, is another alternative method to make transaction, the user would only need to tap their cards on a terminal. NFC transaction is fast yet convenient compared to pervious card payment methods. However, as it does not need a PIN or signature to function, it has some serious security risk especially to fraud. These systems mentioned also do not have the ability to differentiate between type of transactions made. All these problems can be solved with the implementation of biometric payment cards. These cards functions based on a tap-and-go payment and are supported with biometric security. For instance, to make a purchase the user only needs to register their fingerprint on the card’s sensor. One of the big names in this industry, Visa is working with the Bank of Cyprus and Mountain American Credit Union to roll out these biometric cards. These cards would be used for testing fingerprints recognition to authenticate the identity of the holder during transactions and will include an on-card biometric sensor to support contactless payment. Another application of biometrics, would be on electronic card payment like Apple Pay or Samsung Pay. These services are able to be used as an e-card that supports facial and voice recognition or iris scanning to finalize a transaction. As a result, a highly secure yet simpler method for card payments can be utilize. Biometric card would have the ability to differentiate between payments made and prevent any fraudulent transactions from taking place.



Figure 2.2: A biometric card

Furthermore, biometrics is also used in physical and logical access control. The use of Biometric access control systems can help manage who is able to access facilities and computer systems and when they are access. A normal access control system uses keypads and passwords to safeguard the system. The problem faced is that the password codes can be guest or stolen and the key cards may also be stolen or lost. In addition, codes can be found out through the pattern of hand movements when the code is dialled on the keypad or slight fading in the numbers on the keypad. So, it can be concluded that in a normal access control system an unauthorised personal maybe able to gain access. Thus, biometric access systems are significantly harder to breech, as biological data cannot be mimicked or be randomly guest unless an exact replica of the biological system data is stolen. A biometric access system can be based on various types of biometrics from 3D face recognition to iris scanning and to hand geometry recognition. The most basic form of this system can be found on modern smartphones. Fingerprint recognition introduced on the iPhone 5 and facial recognition popularized by the iPhone X, together with iris scanning on android phones are features found in most phones today. These biometrics help protect the security and privacy of the user by preventing any access to the phone from anyone other than the owner of the phone. Google also uses biometric access systems in their physical data centres. To gain access into the data centre, authorized Google employees must go through a fingerprint scanner and an iris scanner.

In a nutshell, biometric technology can serve as a pivotal point in improving our security and privacy in various sectors. Biometric security is not a futuristic technology but is a concept that is already implemented by multiple organizations in countless fields around the globe. Despite the risk and controversial issues of biometrics, the system is a practical and simple yet hard to duplicate. In addition, biometric security will only continue to develop from here on out.

# **References**

1. (n.d.).
2. Bacon, M. (2019). *Biometric authentication terms to know*. Retrieved from SearchSecurity: https://searchsecurity.techtarget.com/feature/Biometric-authentication-terms-to-know
3. *Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review*. (2020). Retrieved from Thales: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics
4. Braun, M. C. (2018). *A brief history of quantum computing*. Retrieved from Medium.com: https://medium.com/@markus.c.braun/a-brief-history-of-quantum-computing-a5babea5d0bd#:~:text=In%201994%2C%20Peter%20Shor%20developed,classical%20algorithm%20on%20traditional%20machines.&text=In%201998%2C%20a%20working%202,algorithms%20such%20as%20Grover's
5. Cardinal, D. (30 January, 2019). *How Does Quantum Computing Work?* Retrieved from extremetech: https://www.extremetech.com/extreme/284306-how-quantum-computing-works
6. Das, S. (2020). *Top Applications Of Quantum Computing Everyone Should Know About*. Retrieved from analyticsindiamag.com: https://analyticsindiamag.com/top-applications-of-quantum-computing-everyone-should-know-about/
7. Davis, S. (2019). *How Does Biometric Access Control Work?* Retrieved from TEDsystems: https://www.tedsystems.com/how-does-biometric-access-control-work/
8. Giles, M. (2019). *Explainer: What is a quantum computer?* Retrieved from MIT Technology Review: https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/
9. Group, Q. C. (2015). *ASCR Report on Quantum Computing.* Caren Susut.
10. Jacksom, M. (2017). *6 Things Quantum Computers Will Be Incredibly Useful For*. Retrieved from SingularityHub: https://singularityhub.com/2017/06/25/6-things-quantum-computers-will-be-incredibly-useful-for/
11. Katwala, A. (2020). *Quantum computing and quantum supremacy, explained*. Retrieved from Wired.co.uk: https://www.wired.co.uk/article/quantum-computing-explained
12. Korolov, M. (2019). *What is biometrics? 10 physical and behavioral identifiers that can be used for authentication*. Retrieved from CSO: https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html
13. Le, C. (2011). *A Survey of Biometrics Security Systems.* Chien Le.
14. Marr, B. (2017). *What Is Quantum Computing? A Super-Easy Explanation For Anyone*. Retrieved from Forbes.com: https://www.forbes.com/sites/bernardmarr/2017/07/04/what-is-quantum-computing-a-super-easy-explanation-for-anyone/#7ded937e1d3b
15. Martin, E. (2018). *4 Amazing Quantum Computing Applications*. Retrieved from Devops: https://devops.com/4-amazing-quantum-computing-applications/#:~:text=Financial%20Services,is%20already%20on%20its%20way.&text=The%20systems%20could%20be%20used,factors%2C%E2%80%9D%20according%20to%20IBM.
16. McKinsey. (2020). *Quantum computing market to reach $1 trillion by 2035*. Retrieved from Consultancy.uk: https://www.consultancy.uk/news/24361/quantum-computing-market-to-reach-1-trillion-by-2035
17. Memoria, F. (8 August, 2020). *Bitcoin vs Quantum Computers: Real and Imagined Fears*. Retrieved from Cryptoglobe: https://www.cryptoglobe.com/latest/2020/08/bitcoin-vs-quantum-computers-real-and-imagined-fears/
18. O'Neillarchive, P. H. (2020). *The quest for quantum-proof encryption just made a leap forward*. Retrieved from MIT Tchnology Review: https://www.technologyreview.com/2020/08/03/1005891/search-for-quantum-proof-encryption-computing-nist/
19. Phillip Kaye, R. L. (2007). *An Introduction to Quantum Computing.* New York: Oxford University Press.
20. Ponnath, A. (n.d.). *Difficulties in the Implementation of Quantum Computing.* Retrieved from https://arxiv.org/ftp/cs/papers/0602/0602096.pdf#:~:text=This%20phenomenon%20is%20called%20decoherence,it%20to%20maintain%20the%20coherence.
21. Press, G. (11 August, 2020). *Honeywells Wants to Show What Quantum computing Can Do For The World*. Retrieved from Forbes: https://www.forbes.com/sites/gilpress/2020/08/11/honeywell-wants-to-show-what-quantum-computing-can-do-for-the-world/#255333012916
22. Raudaschl, A. (2017). *Quantum Computing And Health Care*. Retrieved from blogs.bmj.com: https://blogs.bmj.com/technology/2017/11/03/quantum-computing-and-health-care/
23. Rouse, M. (2013). *biometrics*. Retrieved from SearchSecurity: https://searchsecurity.techtarget.com/definition/biometrics
24. Rouse, M. (2020). *quantum computing*. Retrieved from WhatIs.com: https://whatis.techtarget.com/definition/quantum-computing
25. Smith, D. (2020). *Biometrics: The Future of Payment Authentication*. Retrieved from Infosecurity: https://www.infosecurity-magazine.com/opinions/biometrics-payment-authentication/#:~:text=Since%20the%20fingerprint%20data%20is,sensor%20device%20in%20the%20bank.
26. Thomas, R. (2005). *Biometrics, Migrants, and Human Rights*. Retrieved from MPI: https://www.migrationpolicy.org/article/biometrics-migrants-and-human-rights
27. Trader, J. (2015). *5 Ways Biometric Technology Impacts Our Everyday Life: A Statistical Representation*. Retrieved from m2sys: https://www.m2sys.com/blog/workforce-management/5-ways-biometric-technology-impacts-our-everyday-life/
28. *Types of Biometrics*. (n.d.). Retrieved from javatpoint: https://www.javatpoint.com/types-of-biometrics
29. Vishalxviii. (2018). *Introduction to quantum computing*. Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/introduction-quantum-computing/
30. *What Can Quantum Computing Do To Healthcare?* (2019). Retrieved from medicalfuturist.com: https://medicalfuturist.com/quantum-computing-in-healthcare/
31. *What is Biometrics Security: How It Works*. (n.d.). Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/definitions/biometrics
32. (2020). *What Is Quantum Computing?* cbinsights. Retrieved from cbinsights.com.
33. Elani, Zion. (2020). Qubit, Quantum Entanglement and all that: Quantum Computing Made Simple. 10.6084/m9.figshare.11778444.
34. Wikipedia contributors. (2020, August 19). Quantum computing. In Wikipedia, The Free Encyclopedia. Retrieved 15:52, August 21, 2020, from <https://en.wikipedia.org/w/index.php?title=Quantum_computing&oldid=973759666>
35. Wikipedia contributors. (2020, August 12). Timeline of quantum computing. In *Wikipedia, The Free Encyclopedia*. Retrieved 16:04, August 21, 2020, from <https://en.wikipedia.org/w/index.php?title=Timeline_of_quantum_computing&oldid=972589528>
36. Nagy, Marius. (2006). Quantum computation and quantum information. IJPEDS. 21. 1-59. 10.1080/17445760500355678.
37. UKEssays. (November 2018). Look At Quantum Computing Information Technology Essay. Retrieved from <https://www.ukessays.com/essays/information-technology/look-at-quantum-computing-information-technology-essay.php?vref=1>
38. National Academies of Sciences, Engineering, and Medicine 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196