Quantum Computing: The Next Generation of Computing

Remya.S.P
Lecturer, Department of Computer Science,N.S.S.College,Ottapalam
University of Calicut, Kerala, India.

Abstract : Quantum computation and information is a new and rapidly developing field. Quantum computing is regarded as the future of computing and the game changer for a whole lot of fields depending on it from cryptography, to medicine all the way to applied sciences and computer science. It is the new field of science which uses quantum phenomena to perform operations on data. In the last decades of the twentieth century, scientists sought to combine two of the century's most influential and revolutionary theories: information theory and quantum mechanics. Their success gave rise to a new view of computation and information. This new view, quantum information theory, changed forever how computation, information, and their connections with physics are thought about, and it inspired novel applications, including some wildly different algorithms and protocols. Quantum mechanics has played an ever-increasing role in the development of new and more efficient computing devices. Quantum Computation is becoming a viable alternative for high complexity problems, too hard to address in classical computation, with or without acceleration. Quantum mechanics underlies the working of traditional, classical computers and communication devices, from the transistor through the laser to the latest hardware advances that increase the speed and power and decrease the size of computer and communications components. Quantum Computation represents an important change of paradigm, where the concept of bit gets transformed into a quantum bit, or qubit, which affords for an enormous information storage and processing capacity. In this paper, the basic concepts of Quantum Computation will be introduced and it's application in different fields.

Keywords **- Quantum computing, Classical computers, cybersecurity, Qubits, Superposition.**

I. INTRODUCTION

Quantum Computing is the process of using quantum-mechanics for solving complex and massive operations quickly and efficiently. As classical computers are used for performing classical computations, similarly, a Quantum computer is used for performing Quantum computations. Quantum Computations are too complex to solve that it becomes almost impossible to solve them with classical computers. The word 'Quantum' is derived from the concept of Quantum Mechanics in Physics that describes the physical properties of the nature of electrons and photons. Quantum is the fundamental framework for deeply describing and understanding nature. Thus, it is the reason that quantum calculations deal with complexity. Quantum Computing is a subfield of Quantum Information Science. It describes the best way of dealing with a complicated computation. Quantum-mechanics is based on the phenomena of superposition and entanglement, which are used to perform the quantum computations.

Quantum computing is radically different from the conventional approach of transforming bits strings from one set of 0's and 1's to another. With quantum computing, everything changes. The physics that we use to understand bits of information and the devices that manipulate them are totally different. The way in which we build such devices is different, requiring new materials, new design rules and new processor architectures. Finally, the way we program these systems is entirely different. This document will explore the first of these issues, how replacing the conventional bit (0 or 1) with a new type of information - the qubit - can change the way we think about computing.

Quantum computers are designed to tackle complex problems that would take supercomputers from days to being unable to solve. The post-COVID changes in global power-sharing and the recent technological developments to handle the crisis have brought a new technological trend. This paper will introduce quantum computers by initially providing a definition and brief history about the field then move on to explain potential applications that can utilize quantum computers to greatly advance in certain fields.

II. CONVENTIONAL COMPUTING VS QUANTUM COMPUTING

To understand quantum computing, it is useful to first think about conventional computing. We take modern digital computers and their ability to perform a multitude of different applications for granted. Our desktop PCs, laptops and smart phones can run spreadsheets, stream live video, allow us to chat with people on the other side of the world, and immerse us in realistic 3D environments. But at their core, all digital computers have something in common. They all perform simple arithmetic operations. Their power comes from the immense speed at which they are able to do this. Computers perform billions of operations per second. These operations are performed so quickly that they allow us to run very complex high level applications.

Although there are many tasks that conventional computers are very good at, there are still some areas where calculations seem to be exceedingly difficult. Examples of these areas are: Image recognition, natural language (getting a computer to understand what we mean if we speak to it using our own language rather than a programming language), and tasks where a computer must learn from experience to become better at a particular task. Even though there has been much effort and research poured into this field over the past few decades, our progress in this area has been slow and the prototypes that we do have working usually require very large supercomputers to run them, consuming a vast quantities of space and power.

Quantum computing is radically different from the conventional approach of transforming bits strings from one set of 0's and 1's to another. With quantum computing, everything changes. The physics that we use to understand bits of information and the devices that manipulate them are totally different. The way in which we build such devices is different, requiring new materials, new design rules and new processor architectures. Finally, the way we program these systems is entirely different. This document will explore the first of these issues, how replacing the conventional bit (0 or 1) with a new type of information - the qubit - can change the way we think about computing.

III. HISTORY OF QUANTUM COMPUTING

In the early 1980s, Paul Benioff(a physicist) proposed a quantum mechanical model of the Turing Machine. Since then, the concept of Quantum Computing came into existence. Later on, it was suggested that a quantum computer could simulate those things that a classical computer cannot. The suggestion was given by Richard Feynman and Yuri Manin. Peter Shor developed a quantum algorithm in 1994 for factoring the integers. The algorithm was strong enough to decrypt RSA-encrypted communications. More research is still going on in the field of Quantum Computing.

On October 23, 2019 Google AI, in partnership with NASA (National Aeronautics and Space Administration), US, published a paper in which it was claimed that they had achieved "Quantum Supremacy," meaning that they had used a quantum computer to quickly solve a problem that a conventional computer would take an impractically long time (thousands of years) to solve. Although some of them have disputed this claim, it is still a significant milestone in history.

IV. WHAT IS QUANTUM COMPUTING?

Quantum computing is an area of computing focused on developing computer technology based on the principles of quantum theory, which explains the behavior of energy and material on the atomic and subatomic levels.Classical computers that we use today can only encode information in bits that take the value of 1 or 0. This restricts their ability. Quantum computing, on the other hand, uses quantum bits or qubits. The basis of quantum computing is the Qubit. Unlike a normal computer bit, which can be 0 or 1, a Qubit can be either of those, or a superposition of both 0 and 1.It harnesses the unique ability of subatomic participles that allows them to exist in more than one state i.e. a 1 and a 0 at the same time. Superposition and entanglement are two features of quantum physics on which these supercomputers are based. This empowers quantum computers to handle operations at speeds exponentially higher than conventional computers and at much lesser energy consumption. According to the Institute for Quantum Computing at the University of Waterloo, the field of quantum computing started in the 1980s. It was then discovered that certain computational problems could be tackled more efficiently with quantum algorithms than with their classical counterparts.

The word 'Quantum' is derived from the concept of Quantum Mechanics in Physics that describes the physical properties of the nature of electrons and photons. Quantum is the fundamental framework for deeply describing and understanding nature. Thus, it is the reason that quantum calculations deal with complexity. Quantum Computing is a subfield of Quantum Information Science. It describes the best way of dealing with a complicated computation. Quantum-mechanics is based on the phenomena of superposition and entanglement, which are used to perform the quantum computations.

- **Superposition:** In the presence of a magnetic field, the electron may exist in two possible spin states, usually referred to as spin up and spin down. Each electron will have a finite chance of being in either state until it is measured. It can be observed to be in a specific spin state at the time of measurement. In common experience a coin facing up has a definite value: it is head or a tail. Even if you don't look at the coin you trust that it must be head or tail.
- **Entanglement:** When two particles are entangled or intertwined they behave collectively. i.e. at the time of measurement, if one entangled particle in a pair is decided to be in the spin state of 'down' (that is, the lowest energy state. When the electron is in alignment with its magnetic field), then this decision is communicated to the other correlated particle that now assumes the opposite spin state of 'up'. Quantum entanglement allows qubits, including those far away, to interact instantaneously with each other.

Quantum Computing leverages all the above-mentioned phenomenon to function. For example, it is easy to get the product of (500 * 187625) through a classical computer, but it is easy and quick to get the same result through a quantum computer. A classical computer will take approximately 5 seconds to get the result, whereas a quantum computer will take 0.005 seconds to get the result. Currently, researchers are working with Quantum computers in the field of cybersecurity to break codes and encrypt electronic communications to explore better cybersecurity and protected data. Data transfer using traditional computers has always been susceptible to hacking; however, photon-based packets are linked to each other and alert both the sender and the receiver about any possible intrusion by a third-party, thereby securing networks. Quantum computing could contribute greatly in the fields of finance, military affairs, intelligence, drug design and discovery, aerospace designing, utilities (nuclear fusion), polymer design, Artificial Intelligence (AI) and Big Data search, and digital manufacturing. Its potential and projected market size has engaged some of the most prominent technology companies to work in the field of quantum computing, including IBM, Microsoft, Google, D-Waves Systems, Alibaba, Nokia, Intel, Airbus, HP, Toshiba, etc.

V. APPLICATIONS OF QUANTUM COMPUTING

With the exponential growth in computing power, quantum computing is getting ready for its close up. Quantum computers are ideally suited to solving complex problems, which are hard for classical computers but are easy to factor on a quantum computer. Such an advancement creates a world of opportunities, across almost every aspect of modern life.In fact, Google has recently made headlines proclaiming the achievement of quantum supremacy, where its computers can perform a task

that a conventional computer can't. IBM is also making noise about their supercomputers, which are blazingly fast. Some of the top quantum computing applications in the real world. are:

5.1. Artificial Intelligence & Machine Learning

Artificial intelligence and machine learning are some of the prominent areas right now, as the emerging technologies have penetrated almost every aspect of humans' lives. Some of the widespread applications we see every day are in voice, image and handwriting recognition. However, as the number of applications increased, it becomes a challenging task for traditional computers, to match up the accuracy and speed. And, that's where quantum computing can help in processing through complex problems in very less time, which would have taken traditional computers thousand of years. Artificial Intelligence should have the option to pull from huge datasets of picture, video and content. Clearly, there isn't a lack of content. Big Data is out there to be processed; however, we need all more remarkable PCs to process the petabytes of unprocessed data. Quantum PCs could empower Machine Learning by enabling AI models to look through these huge datasets concerning clinical research, customer behavior, financial markets and comprehend them.

5.2. Analytical Chemistry

IBM, once said, one of the most promising quantum computing applications will be in the field of analytical chemistry. It is believed that the number of quantum states, even in a tiniest of a molecule, is extremely vast, and therefore difficult for conventional computing memory to process that. The ability for quantum computers to focus on the existence of both 1 and 0 simultaneously could provide immense power to the machine to successfully map the molecules which, in turn, potentially opens opportunities for pharmaceutical research. Take a simple molecule of Caffeine. It has approximately 248 states. We know we can't even understand the basic structure of molecules today with classical computing. We can use a Quantum computer to simulate a quantum system. This will not only help us understand but to simulate and even manipulate the process to get a new material which is let's say light and indestructible at the same time or selection of molecules for the creation of organic batteries or we might able to create drugs which might cure cancer or whatever our imagination allows us to create.Some of the critical problems that could be solved via quantum computing are — improving the nitrogen-fixation process for creating ammonia-based fertilizer; creating a room-temperature superconductor; removing carbon dioxide for a better climate; and creating solid-state batteries.

5.3. Drug Design & Development

Designing and developing a drug is the most challenging problem in quantum computing. Usually, drugs are being developed via the trial and error method, which is not only very expensive but also a risky and challenging task to complete. Researchers believe quantum computing can be an effective way of understanding the drugs and its reactions on humans which, in turn, can save a ton of money and time for drug companies. These advancements in computing could enhance efficiency dramatically, by allowing companies to carry out more drug discoveries to uncover new medical treatments for the better pharmaceutical industry.

5.4. Cybersecurity & Cryptography

The online security space currently has been quite vulnerable due to the increasing number of cyber-attacks occurring across the globe, on a daily basis. Although companies are establishing necessary security framework in their organisations, the process becomes daunting and impractical for classical digital computers. And, therefore, cybersecurity has continued to be an essential concern around the world. With our increasing dependency on digitisation, we are becoming even more vulnerable to these threats. Quantum computing with the help of machine learning can help in developing various techniques to combat these cybersecurity threats. Additionally, quantum computing can help in creating encryption methods, also known as, quantum cryptography. From managing money to huge datasets, applications of Quantum Computing are seemingly endless. The power of Quantum Computing could lead to more than just innovation; it also could lead to the minimization of risk.

5.5. Weather Forecasting

Currently, the process of analysing weather conditions by traditional computers can sometimes take longer than the weather itself does to change. But a quantum computer's ability to crunch vast amounts of data, in a short period, could indeed lead to enhancing weather system modelling allowing scientists to predict the changing weather patterns in no time and with excellent accuracy — something which can be essential for the current time when the world is going under a climate change.
Weather forecasting includes several variables to consider, such as air pressure, temperature and air density, which makes it difficult for it to be predicted accurately. Application of quantum machine learning can help in improving pattern recognition, which, in turn, will make it easier for scientists to predict extreme weather events and potentially save thousands of lives a year. With quantum computers, meteorologists will also be able to generate and analyse more detailed climate models, which will provide greater insight into climate change and ways to mitigate it.

5.6. Financial Modelling

For a finance industry to find the right mix for fruitful investments based on expected returns, the risk associated, and other factors are important to survive in the market. To achieve that, the technique of 'Monte Carlo' simulations are continually being run on conventional computers, which, in turn, consume an enormous amount of computer time. However, by applying quantum technology to perform these massive and complex calculations, companies can not only improve the quality of the solutions but also reduce the time to develop them. Because financial leaders are in a business of handling billions of dollars, even a tiny improvement in the expected return can be worth a lot for them. Algorithmic trading is another potential application where the machine uses complex algorithms to automatically trigger share dealings analysing the market variables, which is an advantage, especially for high-volume transactions.

5.7. Logistics Optimisation

Improved data analysis and robust modelling will indeed enable a wide range of industries to optimise their logistics and scheduling workflows associated with their supply-chain management. The operating models need to continuously calculate and recalculate optimal routes of traffic management, fleet operations, air traffic control, freight and distribution, and that could have a severe impact on applications. Usually, to do these tasks, conventional computing is used; however, some of them could turn into more complex for an ideal computing solution, whereas a quantum approach may be able to do it. Two common quantum approaches that can be used to solve such problems are — quantum annealing and universal quantum computers. Quantum annealing is an advanced optimisation technique that is expected to surpass traditional computers. In contrast, universal quantum computers are capable of solving all types of computational problems, not yet commercially available.

5.8. Solving Some Intractable Problems

Think about neural networks and the growing space of characterization using quantum computing for financial modeling and optimization of routes and logistics such as TSP problem that is considered to be insurmountable.

5.9. Making Room Temperature Semiconductor

Quantum computers rely on superconductors to function which have to be kept at extremely low temperatures(15 milli Kelvin).

VI. QUANTUM COMPUTING - PROS AND CONS

In this era of supercomputers, quantum computing is considered as the next big thing. It has been theorized that quantum computes will take a huge leap over the supercomputers. To put this into perspective, supercomputers have achieved a peak performance of around 200 petaflops or 200, 000 trillion calculations per second. Quantum Computers will be able to achieve a billion times more performance power.

A quantum computer will be able to perform any task that a classical computer is able to perform. The basis of quantum computing is the Qubit. Major Problem is that these Qubits are prone to errors. Errors caused by qubits decay and losing information stored on them and to make what's known as logical qubit that's more coherent requires hundreds and thousands of physical qubits whose errors cancel each other out. And a quantum computer capable of cracking encryption would require thousands of logical qubits. Last time I checked we had somewhere near 72 physical qubits available to us and that computer was pretty unstable. Another problem is the condition of isolating the system in which these qubits need superconductors to work on and superconductors needs to be maintained at 15 millikelvin to work as a superconductor and thus the giant quantum computer you see normally is mostly for maintaining this temperature and for sending microwave pulses some set up which is very hard a task.

Although, there is a catch. If we use classical algorithms on a quantum computer, it will simply perform the calculation in a similar manner to a classical computer. For a quantum computer to be utilized to its full potential, quantum algorithms need to be formulated. Quantum algorithms can exploit the phenomenon of quantum parallelism.These algorithms are not easy to create, requiring a lot of research and development. A well-known example for one of the algorithms is the quantum factorization algorithm created by Peter Shor of AT&T Bell laboratories. What the algorithm does is tackle the problem of factorizing large numbers into its prime factors. This task is classically very difficult to solve (base on current technology). Shor's algorithm cleverly uses the effects of quantum parallelism to give the results of the prime factorization problem in a matter of seconds.

VII. FUTURE OF QUANTUM COMPUTING

The future of Quantum Computing seems quite enhanced and productive for world trade. The above-discussed points tell that it is the beginning of the concept and will surely become a part of our life. It is not the mainstream yet. In the future, the quantum systems will enable the industries to tackle those problems, which they always thought impossible to solve.

According to reports, the market of quantum computing will grow strongly in the coming decades. In recent news, India has announced its partnership with Finland to work towards quantum computing. The digital partnership between the Indian Institute of Science Education and Research (IISER) at Pune and Finland's Aalto University has created a high probability of getting its first quantum computer.According to a report, the quantum computing market is currently reaching $2,545 million by 2029. Alongside, the Government of India's allocation of ₹8,000 crores towards quantum computing under the National Mission on Quantum Technologies and Applications further strengthens the desire of the country to be not left behind. Aligning to the vision, the Department of Science and Technology (DST) has also recently launched the Quantum-Enabled Science & Technology (QuEST) programme to lay the groundwork for building quantum computers in India.

Google is showing a great focus and interest in the theory of quantum computing. Recently, Google has launched a new version of TensorFlow, which is TensorFlow Quantum (TFQ). TFQ is an open-source library. It is used to prototype quantum machine learning models. When it will be developed, it will enable developers to easily create hybrid AI algorithms that will allow the integration of techniques of a quantum computer and a classical computer. The main motive of TFQ is to bring quantum computing and machine learning techniques together to evenly build and control natural as well as artificial quantum computers. Scientists are still facing some new and known challenges with quantum computing, but it will surely lead to software development in the coming years.

VIII. CONCLUSION

In this era of supercomputers, quantum computing is considered as the next big thing. It has been theorized that quantum computes will take a huge leap over the supercomputers. A classical computer would take, in some cases, more than the age of the universe to produce a result. Quantum computation promises the ability to compute solutions to problems that, for all practical purposes, are insoluble by classical computers. However, the quantum promise is still a long way from achieving practical realization. The some properties of quantum mechanics that enable quantum computers superior performance also make the design of quantum algorithms and the construction of functional hardware extremely difficult. It is clear that breakthroughs are required not just in technology, but also in algorithm and we do require other supporting technology such as leverage of machine learning (ML), artificial intelligence (AI), Big Data, Cloud Computing to accelerate Quantum Computing development.

IX. REFERENCES

[1] Quantum Computing: A Short Course from Theory to Experiment, by Joachim Stolze, Dieter Suter,Wiley publications

[2] Bertels, K., "Quantum computing: How far away is it?," in High Performance Computing & Simulation (HPCS), 2015 International Conference on July 2015

[3] Paler, A.; Devitt, S.J., "An introduction into fault-tolerant quantum computing," in Design Automation Conference (DAC), June 2015

[4] Wu, C.H., "Qubits or Symbolic Substitutions for General-Purpose Quantum Computing?," in Information Technology - New Generations (ITNG), 2015 12th International Conference on , April 2015

[5] Barila, A., "From classical computing to quantum computing," in Development and Application Systems (DAS), International Conference 2014.

[6] Hahanov, V.I.; Hyduke, S.M.; Gharibi, W.; Litvinova, E.I.; Chumachenko, S.V.; Hahanova, I.V., "Quantum Models and Method for Analysis and Testing Computing Systems," in Information Technology: New Generations (ITNG), 2014 11th International Conference on April 2014

[7] Kaizer Vizzotto, J., "Quantum Computing: State-of-Art and Challenges," in Theoretical Computer Science (WEIT), 2013 2nd Workshop-School Oct. 2013

[8] Morimae, T., "Basics and applications of measurement-based quantum computing," in Information Theory and its Applications (ISITA), 2014 International Symposium on Oct. 2014

[9] Grodzinsky, F.S.; Wolf, M.J.; Miller, K.W., "Quantum computing and cloud computing: humans trusting humans via machines," in Technology and Society (ISTAS), 2011 IEEE International Symposium on , May 2011

[10] Singh, H.; Sachdev, A., "The Quantum way of Cloud Computing," in Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on Feb. 2014

[11] Ying, M.; Yuan Feng, "An Algebraic Language for Distributed Quantum Computing," in Computers, IEEE Transactions on June 2009