Quantum Computing - An Introduction and Cloud Quantum Computing

[1]Samskruthi S Patil, [2]Dr. Vijayalakshmi M N
[1]Student, [2]Associate Professor,
[1]Department of Master of Computer Applications,
[1]RV College of Engineering®, Bengaluru, India.

Abstract: Quantum computing uses the phenomena of quantum mechanics to perform operations on data and it's a huge leap in the field of computation. A quantum computer is a computational device which uses quantum mechanical phenomena like superposition and entanglement of atoms, photons, electrons. The difference between Quantum computers and digital computers is that digital computers are based on transistors and require data to be encoded into binary digits (bits). Quantum computers use quantum bits (qubits) and use quantum properties to represent data. Quantum computers can solve certain computational problems like integer factorization faster than classical computers. Quantum computers can solve certain problems that no classical computer could solve in any feasible amount of time. The Quantum Computing Market was valued at USD 89M in the year 2016 and is expected to reach USD 949M by 2025. Industry leaders are trying to develop and launch an actual quantum computer and make it available for everyone. Many companies are working in this area and are providing platforms to build quantum algorithms. There could be around 2,000 to 5,000 quantum computers in the world by 2030. This paper provides an introduction to quantum computing, quantum mechanical phenomena used in quantum computing and quantum computing service providers

IndexTerms **- - Qubits, Superposition, Entanglement, Quantum Algorithms, Quantum Mechanics, Quantum Gates, Quantum Circuit, Q Sharp, Qiskit**

I. INTRODUCTION

Quantum computing started in the 1980s when physicist Paul Benioff proposed a quantum mechanical model of the Turing machine, named after Alan Turing. Yuri Manin and Richard Feynman opined that quantum computers had the potential to simulate things classical computers would never be able to. Peter Shor developed a quantum algorithm for factoring integers which can be used to decrypt RSA-encrypted communications. If a quantum computer is capable of performing Shor's algorithm it will manage to break current cryptography techniques in a matter of seconds. This algorithm provided motivation and the topic of quantum computing has gathered momentum and researchers around the world are trying to create a practical quantum computer. According to Chuang a supercomputer would take about a month to find a phone number from the database consisting of the world's phone books, whereas a quantum computer can solve this task in 27 minutes. Despite the ongoing experimental progress since 1990s, most researchers think that fault-tolerant quantum computing cannot be achieved.

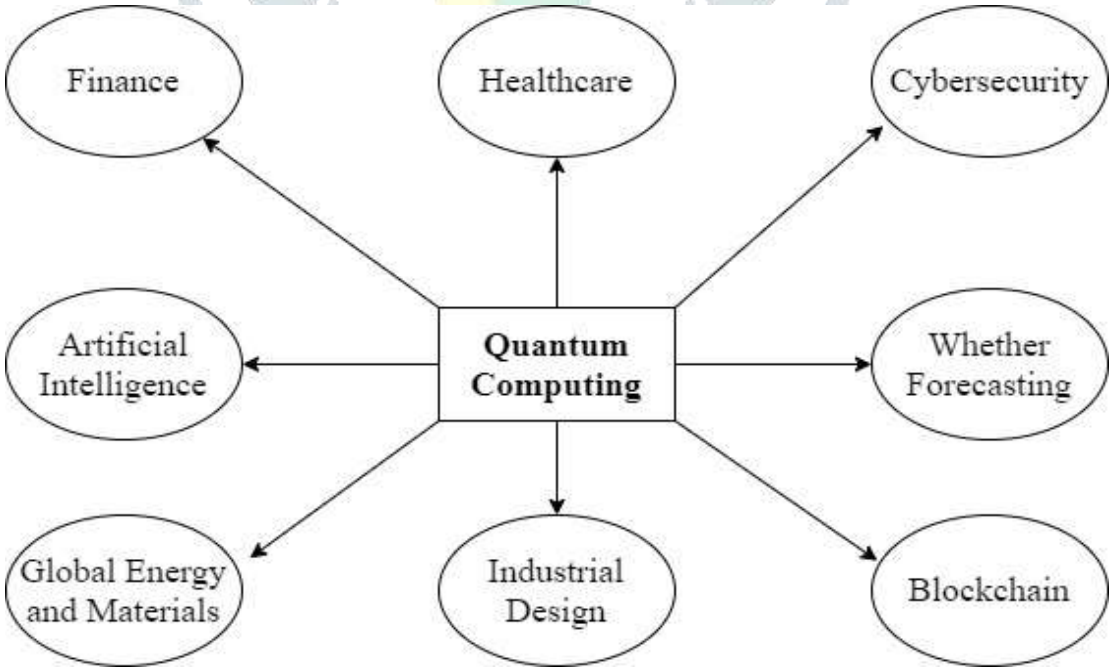

Fig 1: Applications of Quantum Computing

The technology employed in quantum computers is completely different. For operation on data, quantum computers use quantum bits (qubits). Qubit encompasses a quaternary nature. A qubit will exist within the states resembling the logical values zero or one as in the case of a classical bit, however additionally in an exceedingly superposition state. A qubit can be both zero and one at the same time (Superposition state). Thus, a computer functioning on a qubit can calculate on both values at the same time. A qubyte is formed of eight qubits and might have all values from zero to 255 at the same time. Forty qubits may have an equivalent power as trendy supercomputers. Multi-qubyte systems have huge potential and can surpass classical computers easily.

Recently, investment in the field of quantum computing has increased in both the public and private sectors. Google AI partnered with the U.S. National Aeronautics and Space Administration (NASA) and claimed to have performed a quantum computation that was not possible on any classical computer. The world's first commercial quantum annealing machine, operating on a 128-qubit, was developed by D-Wave in 2011 and its price was approximately USD 10M. In 2020, a Chinese team from the University of Science and Technology of China, reported that their quantum computer, named as Jiuzhang, is 10 billion times faster than that of Google's. Quantum computing can be applied in many areas, like Finance, Artificial Intelligence, Weather forecasting, etc.

The exponential growth in computational power has enabled quantum computing to get ready for its close up. Quantum computers are suited to solve complex problems, which are hard and time consuming for classical computers but are easy to factor on a quantum computer. Such an improvement in this field creates a world of opportunities, across almost every aspect of modern life. The Fig 1 represents all the different sectors where Quantum Computing can be used

II. LITERATURE SURVEY

A potentially new technology for future computing systems is quantum computing. Quantum computing offers a new approach to computation that can have capabilities which are not available with today's existing transistor-based processing. The theory of quantum computing has found significant speed up to a few prominent algorithms in modeling, simulation and mathematics, and experimental efforts in quantum computer science and have recently made huge achievements in illustrating quantum algorithms which can solve problems in physical simulation and applied mathematics [1].

Quantum computing has the potential to offer computational capabilities which will surpass existing supercomputers, and this has sparked huge interest from both industry and academia to build a world's first quantum machine. Today, many big companies such as IBM, Google, Microsoft, and Intel, as well as many ambitious start-up companies such as Rigetti and IonQ are actively pursuing the race to develop a first large scale universal quantum computer. In parallel to quantum hardware development, the area of quantum software and quantum algorithm development has also seen huge progress in the recent years [2].

Quantum computing is a subset of quantum information science. It's an area of study based on the idea that information science depends on quantum effects in physics and can be defined as the use of quantum properties which can solve complex problems much faster than conventional, or classical, computers. Quantum technology is a different way of storing and manipulating information when compared to conventional computers. Conventional computers use bits, or binary digits that are the basic unit of computer information storage and processing, quantum computers use quantum bits called as qubits. Bits are like switches, they can be either up or down, on or off. Qubits are like dimmer knobs, they can take on an infinite number of different values between on and off, and this, along with other mechanical properties, underpins their computational functionality [3].

In Quantum computing operations on data can be performed using the principle of superposition which is a quantum natural phenomenon. While classical or digital computers are supported by transistors, Quantum computers are different from classical computers which use theoretical discipline. Quantum computers use qubits and classical computer works on binary digits which are either 1 or 0. The qubit is a superposition of states which means it will take any value between 0 and 1. A quantum computer is a theoretical model of such computers. Quantum computers share theoretical similarities with both non-deterministic and probabilistic algorithms [4]. Quantum computers can be used anywhere, where there's an exponentially large, uncertain complicated system that needs to be simulated, the range of applications can be from predicting the financial markets, to improving weather forecasts, to modeling the behavior of individual electrons. This uses quantum computing to understand quantum physics [5].

With the technology growing rapidly at a high acceleration rate, huge companies nowadays like IBM, Google, Microsoft and Amazon are on pace to develop cloud quantum computers. They combine quantum computers with cloud computing which can be accessed by a network without having the physical quantum computer. It means that soon enough, people can act as a basic user will have the opportunity to taste the power of quantum computers in a cloud computing environment. This makes the quantum computing experience available to more number of people [6].

III. QUANTUM MECHANICAL PHENOMENA

Quantum Superposition

Quantum superposition is one of the fundamental principles of quantum mechanics and is based on superposition of waves. It states that, any two or more quantum states can be added together or superposed and the result will be another valid quantum state. That vice versa of it is also true, that every quantum state can be represented as a sum of two or more other distinct states.

Quantum Entanglement

Quantum entanglement is a phenomenon that could happen when a group of particles are generated and these particles are either interacted or have the same spatial proximity. In this condition the quantum state of each particle of the group cannot be described independently, excluding the state of the other particles in the group, even when the particles are separated by a large distance. The topic of quantum entanglement serves as a topic of disparity between classical physics and quantum physics. Entanglement is a primary feature of quantum mechanics that lacks in classical mechanics.

An entangled system is defined as a quantum state which cannot be factored as a product of states of its local particles which means, they are not individual particles but are inseparable as a whole. In entanglement, one particle cannot be fully described without considering the other particles in the group. The state of a composite system can always be expressed as a sum, or superposition, of products of states of local particles. It is entangled if the sum cannot be written as a single product term.

Quantum Circuit

A quantum circuit also known as quantum network or quantum gate array generalizes the idea of replacing the AND, OR, and NOT gates by elementary quantum gates. A quantum gate is a unitary transformation on a small usually 1, 2, or 3 qubits. The main 2-qubit gate is the controlled-NOT (CNOT) gate. The 3-qubit Toffoli gate is also called controlled-controlled not (CCNOT) gate. This gate negates the third bit of its input if both the first and second bits are 1. The Toffoli gate is very important because it is complete for classical reversible computation. Toffoli can also implement AND and NOT gates.

A quantum circuit is defined as a finite directed acyclic graph of input nodes, output nodes and gates. There are n nodes that contain the input which is classical bits. The internal nodes of the quantum circuit are usually quantum gates. Each quantum gate operates on at most two or three qubits of the state. The gates in this quantum circuit transform the initial state vector into a final state, which will be a superposition. The measurement of some dedicated output bits of this final state in the computational basis is done in order to obtain an output.

IV. QUANTUM ALGORITHMS

A quantum algorithm is an algorithm which can be run on a real model of quantum computation, the most used model is the quantum circuit model of computation. An algorithm is a finite set of instructions, or a step by step procedure for solving a problem and obtaining the solution, in which each step or instruction can be performed on a classical computer. A quantum algorithm is a step by step procedure, or a finite set of instructions in which each of the steps can be performed on a quantum computer. Even though all classical algorithms can also be performed on quantum computers, the phrase quantum algorithm is used for those algorithms which use features of quantum computation such as quantum superposition or quantum entanglement.

Shor's Algorithm

Shor's algorithm is a polynomial-time quantum algorithm for integer factorization. In 1994, American mathematician Peter Shor invented this algorithm. Basically, for a given integer N, this algorithm will find its prime factors.

The algorithm is made of two parts. The first part of this algorithm converts the factoring problem into the problem of finding the period of a function and can be implemented classically. The next part of Shor's algorithm finds the period using the quantum Fourier transform and is accountable for the quantum speedup.

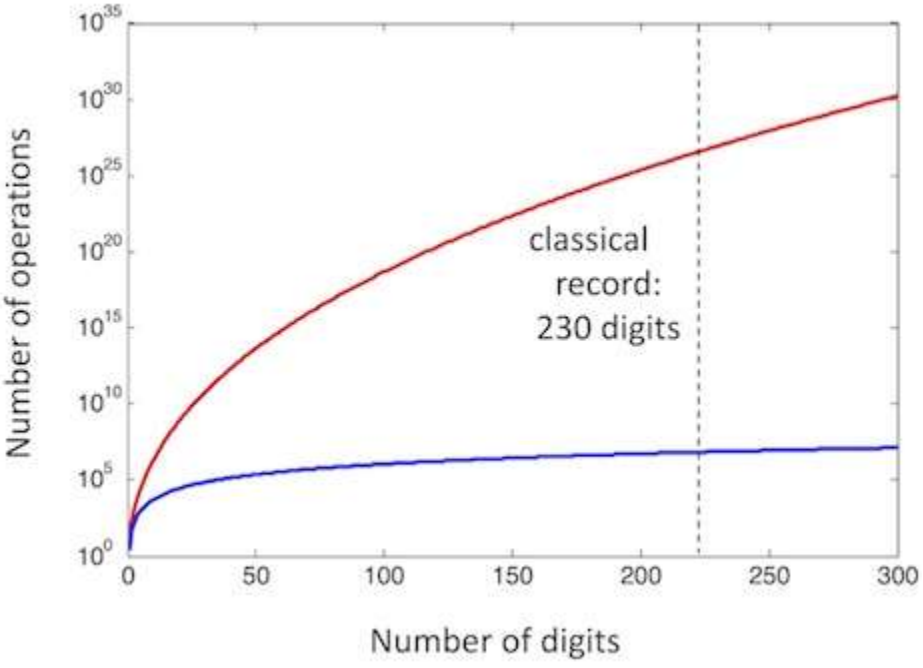

Fig 2: Quantum Algorithm and Classical Algorithms operations

The exponential runtime scaling limits the use of classical factoring algorithms to numbers with a few hundred digits. The world record is 232 digits. In contrast, Shor's factoring algorithm is polynomial-time and this version of the algorithm described, requires roughly 10 qubits, and has runtime roughly the cube of digits.

Grover's Algorithm

Grover's algorithm is also known as the quantum search algorithm. Lov Grover invented this algorithm in 1996. It refers to a quantum algorithm which is used for unstructured search and it finds with a high probability the unique input value to a black box function that produces a particular output value. Grover's algorithm has amplitude amplification. A quadratic speedup is a substantial time saver for finding items in long lists. The algorithm does not use the list's internal structure, that's why it is a generic algorithm. It gives a quadratic quantum speed up for many classical problems.

V. Q SHARP AND QISKIT

Q# (Q sharp) is a programming language used for writing quantum algorithms. It was released by Microsoft to the public as part of the Quantum Development Kit. Q# is available as an extension for Visual Studio, which can be downloaded separately and it can also be run as an independent tool from the Command line or Visual Studio Code. The Quantum Development Kit comes with a quantum simulator which is capable of running Q#.

In order to call the quantum simulator, a .NET programming language, usually C#, is used and it provides the classical input data for the simulator and reads the classical output data from the simulator.

Qiskit is an open source framework which is used for quantum computing. It enables the users the tools for developing and manipulating quantum programs and running them on prototype quantum devices provided by IBM on IBM Quantum Experience or on simulators on a local computer. It obeys the circuit model for universal quantum computation, and can be used on any quantum hardware but, currently the hardware is limited to superconducting qubits and trapped ions and follows this model. Qiskit was founded by IBM Research to permit software development for their cloud quantum computing service, IBM Quantum

Experience. Contributions are also made by external supporters, mostly from academic institutions. Python programming language was used by the primary version of Qiskit.

VI. CLOUD QUANTUM COMPUTING

Cloud quantum computing is the use of quantum emulators, simulators or processors through the cloud. In recent times, cloud services are being considered as a method for providing access to quantum processing. Quantum computers attain the huge computing power by combining quantum physics into processing power and when users are given access to this quantum powered computers through the internet it is known as Cloud Quantum Computing

Microsoft Azure Quantum: Microsoft provides tools such as QDK(Quantum Development Kit) and quantum script languages as Q# for quantum computing development. Microsoft has partnered with 1Qbit, Honeywell, IONQ, QCI for development of quantum computing systems. The capabilities of Azure Cloud provides access for quantum computers developed by its partners. Microsoft has also developed their own quantum system which is called as Station Q. This approach is called topological qubit method for stable quantum bits to serve for mass production of quantum computers.

Amazon Braket: Amazon Braket is a fully managed quantum computing service, provided by Amazon. It helps all the researchers and developers across the world to get started with the technology and to accelerate research and discovery. Amazon Braket gives access to a development environment for the users to explore and build quantum algorithms, test them on quantum circuit simulators, and run them on different quantum hardware technologies.

IBM Quantum: The IBM Quantum Composer and the IBM Quantum Lab are collectively known as the IBM Quantum Experience, form an online platform which allows public and premium access to cloud based quantum computing services and is provided by IBM Quantum. It provides access mainly to a set of IBM's prototype quantum processors. It also provides access to a set of tutorials on quantum computation, and a textbook. As of February 2021, there are around 20 devices which provide service actively, six of them are freely available for the public. This service can be used to run algorithms and experiments, and explore tutorials and simulations which can be done using with quantum computing

Quantum Computing Playground: Quantum Computing Playground is based on browser and its a WebGL Chrome Experiment. It features a GPU, which is accelerated by a quantum computer. It has a simple IDE interface and has its own scripting language along with debugging and 3D quantum state visualization features. Quantum Computing Playground is able to simulate quantum registers up to 22 qubits. It can run Grover's and Shor's algorithms and has a variety of quantum gates built into the scripting language.

Rigetti Forest: Rigetti Forest is a cloud computing platform, which gives developers access to quantum processors so that they can write quantum algorithms for testing purposes. The computing platform is mainly based on a custom instruction language called Quantum Instruction Language(Quil). Quil supports both quantum and classical computing, and programs can be built and executed using open source Python tools. This platform allows coders to develop quantum algorithms for a simulation of a quantum chip with 36 qubits.

VII. CONCLUSION

Quantum computing uses concepts of quantum mechanics like superposition and entanglement to perform operations on data. Quantum computers use quantum bits (qubits) instead of classical bits used in classical computers. A qubit will exist within the states resembling the logical values zero or one as in the case of a classical bit, and also in a superposition state. This enables Quantum computers to solve problems faster than classical computers. Q# (Q sharp) is a programming language used for writing quantum algorithms. Qiskit is an open source framework used for quantum computing. Many companies are providing cloud Quantum computing services, among them IBM provides free access for research and educational purposes. A lot of start-ups have also started to provide cloud quantum computing services. The existing Quantum Algorithms like Shor's Algorithm and Grover's Algorithm can be tested on any of the Cloud based platforms. Every platform provides its own development kit using which the user can test their Quantum Algorithms.

REFERENCES

[1] Alán Aspuru-Guzik, Wim van Dam, Edward Farhi, Frank Gaitan, Travis Humble, Stephen Jordan, Andrew Landahl, Peter Love, Robert Lucas, John Preskill, Richard Muller, Krysta Svore, Nathan Wiebe, Carl Williams. 2016. ASCR Report on Quantum Computing for Science. U.S. Department of Energy Office of Science Advanced Scientific Computing Research Program.

[2] Sukhpal Singh Gill, Adarsh Kumar, Harvinder Singh, Manmeet Singh, Kamalpreet Kaur. 2017. Quantum Computing: Taxonomy, Systematic Review and Future Directions. ACM Computing Surveys,

[3] Akhil Iyer. 2020. Quantum Computing. Technology and Public Purpose Project Belfer Center for Science and International Affairs Harvard Kennedy School 79 John F. Kennedy Street, Cambridge, MA 02138,

[4] Ganesh Vishnu Funde & Anil Vishwanant Yetonde, 2020. A Survey Study based on Quantum Computing, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 06.

[5] Mukesh Singh Yadav, Md. Akib Qureeshi, 2020. Quantum Supremacy. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 04.

[6] Haryono Soeparnoa, Anzaludin Samsinga Perbangsa. 2020. Cloud Quantum Computing Concept and Development:A Systematic Literature Review. 5th International Conference on Computer Science and Computational Intelligence.

[7] K. Bertels et al. 2020. Quantum Computer Architecture Toward Full-Stack Quantum Accelerators. IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-17.

[8] D. J. Egger et al. 2020. Quantum Computing for Finance: State-of-the-Art and Future Prospects. IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-24.

[9] C. Gambella and A. Simonetto. 2020. Multiblock ADMM Heuristics for Mixed-Binary Optimization on Classical and Quantum Computers. IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-22.

[10] S. Harwood, C. Gambella, D. Trenev, A. Simonetto, D. Bernal and D. Greenberg. 2021. Formulating and Solving Routing Problems on Quantum Computers. IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-17.

[11] J. C. Bardin, D. H. Slichter and D. J. Reilly. 2021. Microwaves in Quantum Computing. IEEE Journal of Microwaves, vol. 1, no. 1, pp. 403-427.

[12] D. Ferrari, A. S. Cacciapuoti, M. Amoretti and M. Caleffi. 2021. Compiler Design for Distributed Quantum Computing. IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-20.