International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

Technological Survey on Quantum Computing

Vinaytej V G[1], Venugopal S[2], Manoj R[3], Vaishnavi M[4] Dr. Vikas Reddy S[5]

[1]*Student, Dept Computer Science And Engineering S J C Institute of Technology Chickballapur India*
[2]*Student, Dept Computer Science And Engineering S J C Institute of Technology Chickballapur India*
[3]*Student, Dept Computer Science And Engineering S J C Institute of Technology Chickballapur India*
[4]*Student, Dept Computer Science And Engineering S J C Institute of Technology Chickballapur India*
[5]*Assoc.Prof, Dept Computer Science And Engineering S J C Institute of Technology Chickballapur India*

Abstract - *The development of new technology depends on a good theoretical basis. At the initial stages of evolution of computers vacuum tubes ruled the generation, now nano chips are ruling the generation, in future atoms will be ruling the era of computing. Quantum computing is a paradigm which is a highly topical and fast-moving field. A Quantum Computer uses a different approach compared to classical computer, e.g., qubits, superposition which helps to extend the computational abilities to a higher level. Quantum computer directly exploits the principles of quantum mechanical phenomena to solve complex problems. Currently there are few algorithms which make use of quantum technology. This paper reviews about fundamentals of quantum computing, importance in various areas, difficulties involved implementation of quantum computer.*

Key Words: Entanglement, Super-Position, Qubit, Quantum, Quantum-Mechanics.

1. INTRODUCTION

Quantum computer is machine that use the collective principles of quantum state properties and information represented in quantum states. Quantum computation is fundamentally based on reversible computation and uses the quantum-bits or qubits (0 & 1 at the same time) by following the "superposition principle of quantum mechanics" with this we can speed up data processing by overriding the traditional computers. These machines are not yet commercially and still in its early stages of research and development. Quantum computers works based on the wave nature of the atom and spin of the magnetic field of the molecular and sub molecular form of the matter. Atoms are simplest form of the matter, which has electrons, neutrons and protons. Under electrons there will be a small amount of energy with air called Quartz

Some of the building blocks of quantum computing are:

1.1 Entangle States

Irrespective of distance between qubits they are always connected to each other which is known as entangled state. It is a primary feature of quantum mechanics. One qubit output an immediate information about the other no matter how far apart these qubits are. Increasing the number of qubits will not necessarily double the number of processes since processing one qubit will reveal information about multiple qubits. It's responsible for exponential speed of the quantum algorithm. Qubits increases in a exponential form(2n) Uses of entanglement in Quantum computing is:

- Quantum Cryptography
- Superdense Coding

Suppose consider a pair of hand-gloves, if you find the right glove alone in the drawer then other one will be the left one, we can push the two qubits into the same state even though the states are different and this increases the computational power and solution optimization. If we obtain entanglement, we can store many numbers of possible values, Entanglement and behavior of the Qubits can know with the help of the spin of an electron if the spin value is in negative then it is referred as a 'spin-up' and it represent '1'if spin is in positive value, then it is referred as a 'spin-down' and it represent '0'. If the electrons have opposite spins, then 2 electrons can occupy a same space exactly same time. Initially determining state of object and the qubits are then super positioned and entangled in order to make functional qubits

Fig -1: shows the IBM Quantum computer.

1.2 Qubit

The qubits are fundamentals in quantum computing, the operations of quantum computing are performed on qubits which can be in coherent superposition state. Coherence tells us defines how long a qubit retains its information. Qubit is a two-state quantum mechanical system. The illustration of bit (used in classical computing) and qubit is given below.

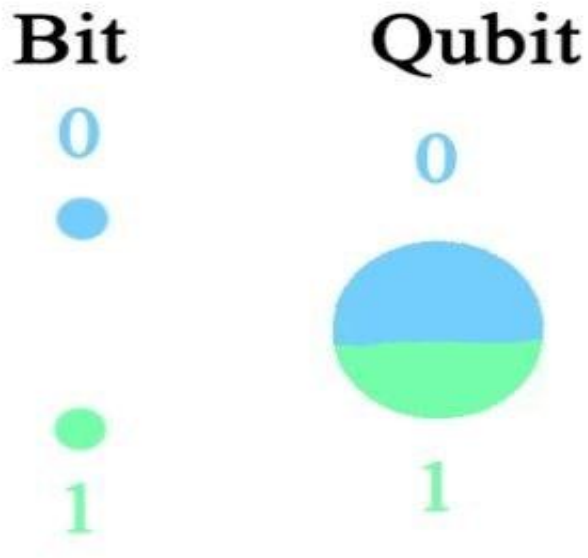

Fig -2: Illustration of bit and qubit.

1.3 Quantum Gates

Quantum gates function similar to logic gates in classical computers. Unlike many classical gate quantum gates are reversible. Quantum gates are unitary operators and are described as unitary matrices.

Quantum full adder was given by Feynman in 1986 [1].

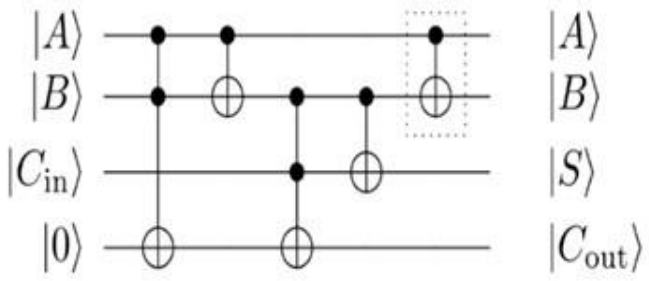

Fig -2: Feynman's Quantum full adder

1.4 Superposition

It's an ability of particle to be in two positions at a time. In classical computer the bit can be either 0 or 1, but in quantum computer the qubit can be in 0,1 at same time. Superposition is a linear combination of |0> and |1> if the system has A and B (A and B is a combination of 0's and 1's) states if the system chooses 0 from state A, the information apart from 0 in state A will be erased. Similarly for B system also, this property is called as super position principle. In Schrodinger's cat equation the cat is super position of being dead and alive, until the box is opened and forced to choose the state [2].

2. LITERATURE SURVEY

In 1992 at bell labs "Umesh Vazani" come up with "BersteinVazarani Algorithm" this algorithm shows how a quantum computer find the secret number in a step whereas a classical computer takes the steps based on the size of the bit which is inside an oracle[3].

"Peter Shor" After reading the "Berstein-Vazarani Algorithm" Shor came up with algorithm with the help of "Charlie Bennet" and "John Smolin" called "Shor's Algorithm". This algorithm explains how can we get a factor of large numbers using exponential form.

For saving the mouse stuck in Maze, the classical computer gives the solution based on the principle of Trail and error for reaching to the end, where as in quantum computer the bits are replaced with Qubits, Qubits works based on Quantum Mechanics. With 3 qubit system can store 8 possible solutions consider if we construct with just 20qubits we can store billions of possible solutions.

In classical computer the number of transistors will be increased to enrich the speed of the classical computer whereas in the quantum computer qubits are increased. When the Qubits are increased then the correlation also increases thus the computational power also increases [4]

The qubit represented mathematically as a 2Dimensional Vector (or state). We represent the states with word called vector. The Qubits is a combination of '0' and '1' it is not only meant for 0 and 1 states, it is the values in between 0 to 1 state, we can represent the quantum states with the "Dirac Notation" or "Bra-ket Notation" [5]. There are some factors that we need to discuss if we want to know about the Quantum computer Using only one wave function, we can't represent the states of the system. If we need to do so then we want to represent the states of the system we should have two or more wave functions. With these wave functions we have to superimpose the wave functions and there it produces another wave function of that system and this wave function is called as 'Eigen State'. Super position state is combination of many eigen states.

3. IMPORTANCE

As we observe the present situations the technology is growing in a faster phase and also complexity of implementing and computing those ideas are becoming

difficult which requires a high computational device which can meet the requirements of solving complex problems. That is where quantum computation comes into picture. By using Quantum computers, we can solve the problems that cannot be solved by traditional computers over so many years.

The major groundwork in the field of quantum computing was done by physicist "PAUL BENIOFF" in 1980.Quantum computers are 1000 times faster than the traditional computers are derived from Quantum Theory. The problems which cannot be solved from super computers those problems can solve by using Quantum computers. Quantum computers have the ability to give the potential to the industry by solving the problems that can't achieve from the modern-day computers. When Google developed first quantum computer with 53 qubits in 2019, the machine was able to solve a calculation in just 3minutes, where it would have taken 10,000 years for world's fastest computer to solve.

A. Healthcare:

Quantum computing facilitate healthcare use case that fortify each other in a cycle. The convolution of human biological system, the customized medicine requiring other than standard medicine. Classical ML has limitations due to complexity of relation among features. The Quantum integrated ML, which may provide the accuracy in early detection of disease in detailed way and to have a precautionary measure over that particular disease The current diagnosis, treatment for most of the disease are costly and slow with deviations around 15-20% [6]. Quantum enabled diagnosis has ability to improve image-aided diagnosis. Quantum computing allows medical practitioner to differentiate large amount of grouped data and permutations to identify best pattern.

In drug research and discovery quantum computing allows medical partitioners to model the complex molecular interactions at an atomic level. It's now possible to encode approximately 20,000 proteins in the human genome and their interactions with existing drug can be simulated [7]

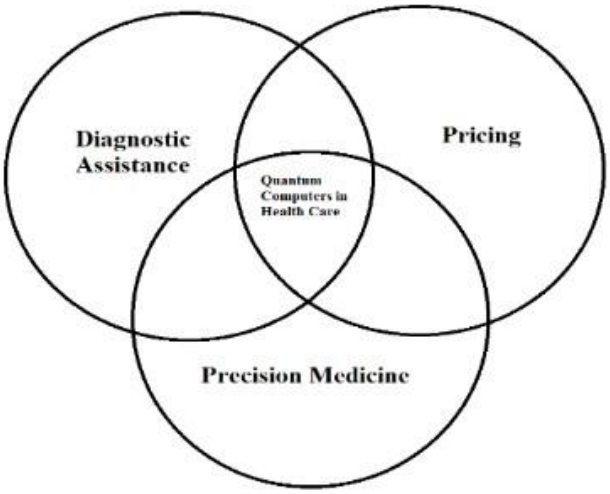

Fig -4: Venn Diagram of applications of quantum computer

B. Weather Forecast:

Forecasting is compact to be exactly according to the predictions, mostly when the weather is considered to be varying and when the information available is minimum. with exact predictions we can save many lives and we could help the farmers so that they can plan accordingly That can be achieved from the Quantum computers. Early warnings of dangerous weather and minimizing the effects of such events, but current model can predict regional scale weather like hurricanes and sandstorms. The IBM has jointly combined with The Weather company, University Corporation for Atmospheric Research and the National Centre for Atmospheric Research to develop the model which covers across the globe which will provide high resolution forecasts even in the most difficult and undeserved areas. In the future the combination on IBM supercomputing technology, geographical processing units with quantum computer will help to predict and track wild weathers, meteorological conditions in such a way that classical supercomputer are unable to achieve.

C. Cryptography:

Basically, cryptography refers to encrypting the data at sender side and receiver having the right key can decrypt it using the key using RSA, Symmetric key algorithm etc. But most of them are not 100% reliable, the recent example for this case is a Pegasus software which was used for surveillance on political leaders, journalist and many other people. Which proves that the current security is not enough to protect our data and our privacy. Quantum cryptography is a way of encryption which uses the naturally occurring properties of quantum mechanics to enhance secure and transmit data in a way that cannot be hacked [8]. Computer Scientist Lov Grover developed a algorithm called Grover's

algorithm which is an quantum search algorithm. Using this algorithm can impact or even break some symmetric algorithm, the main factors in this algorithm is key size and message digest which decides whether an algorithm is quantum safe or not. [9].

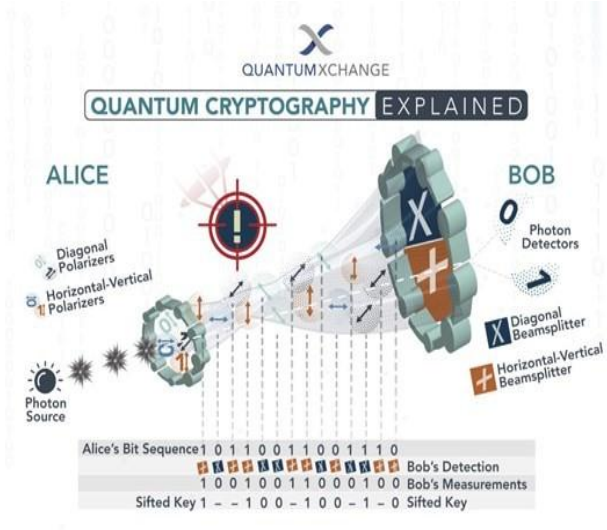

Fig -5: Working of Cryptography

There's a main reason why we should implement quantum computing as soon as possible because it's able to break the asymmetric encryption and signature algorithms which we are presently using in our infrastructure. The Fig 5 shows how quantum cryptography works.

D. Financial Services:

The financial services industry has mathematical models and classical computing algorithms to manage business risks for decades. However, those systems weren't always fail-safe and have inaccurately predicted business risks several times, most notably during the 2008 subprime mortgage crisis [10]. Growth in data volumes, business risks, security threats, and regulations will soon make today's computers insufficient. Moore's law which says the number of transistors in an integrated circuit doubles every two years is expected to falter within the decade. The growth of computing power will have to come from other technological advances [11]. Quantum computing has long been seen as a solution — and several banks are already experimenting with it. Quantum encryption can prevent data breaches and thefts by even the most powerful classical or quantum computers. Quantum key distribution (QKD) uses quantum mechanics principles to encrypt and transmit data. With this approach, quantum cryptography encrypts data in a way that is believed to be unhackable. Spain's Caixa Bank developed a hybrid computing model where quantum and traditional computers work together at different calculation stages to classify credit risk profiles. The bank uses this model to improve its risk simulations and machine learning algorithms, which require vast amounts of data. This application helped the bank significantly reduce the time needed to complete risk analyses[12]. By applying the methods of classical computer to quantum computer can improve the research progress. Quantum computer has a potential to revolutionize the traditional system by achieving unimaginable speed, efficiency and reliability.

4. FUTURE WORK

The quantum computing is in early stages of development, it also enables great technological advancement. The main threat from using quantum computing is the ability of quantum computing to break the cryptographic algorithms very easily due to its high computational power of solving the complex problems very fast, so when it's used for breaking into any system or any server it can be done in no time. The only solution for this to change our current cryptographic methods. Using quantum computing it might even be possible to forecast weather conditions is your backyard.

5. CONCLUSION

In this paper we discussed the fundamentals of quantum computing and it has the capability to transform computation by solving the intractable problems which cannot to be carried in a classical or traditional computers. At present there is no Quantum computer that is sophisticated enough to solve the calculations that a classical computer can't. The more research and development can be carried out to make the quantum computing has real life implementation model.

REFERENCES

[1] Feynman, Richard P. (1986). "Quantum mechanical computers". Foundations of Physics. Springer Science and Business MediaLLC. 16 (6):507531. Bibcode:1986FoPh...16.507F. doi:10.100 7/bf01886518. ISSN 0015-9018. S2CID 122076550.

[2] Ofek, N., Petrenko, A., Heeres, R., Reinhold, P., Leghtas, Z., Vlastakis, B., … Schoelkopf, R. J. (2016). Extending the lifetime of a quantum bit with error correction in superconducting circuits. Nature, 536(7617),441–445. doi:10.1038/nature18949K. Elissa, "Title of paper if known," unpublished.

[3] https://qiskit.org/textbook/ch-algorithms/bernstein-vazirani.html

[4] https://www.scientificamerican.com/video/how-does-a-quantumcomp uter-work M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] ACM Computing Surveys, Vol. 32, No. 3, September 2000, pp. 300– 335.

[6] H. Singh, A. N. Meyer, and E. J. Thomas, "The frequency of diagnosticerrors in outpatient care: estimations from three large observationalstudies involving us adult populations," BMJ quality & safety, vol. 23,no. 9, pp. 727–731, 2014

[7] Quantum Computing for Healthcare: A Review, Rasool, Raihan Ur; Ahmad, Hafiz Farooq; Rafique, Wajid; Qayyum, Adnan; Qadir, Junaid (2021): QuantumComputing for Healthcare:A Review.TechRxiv.https://doi.org/10.36227/techrxiv.17198702.v2a

[8] https://quantumxc.com/blog/quantum-cryptographyexplained/#:~:text =Cryptography%20is%20the%20process%20of,way%20that%20cann ot%20be%20hacked

[9] https://www.ibm.com/cloud/blog/what-is-quantum-safecryptography and-why-do-we-need-it.

[10] https://www.wired.co.uk/article/ibm-barclays-bankingquantumcomputing.

[11] https://www.nature.com/news/the-chips-are-down-for-moore-s-law1. 19338.

[12] https://www.caixabank.com/comunicacion/noticia/caixabankbecomes-the-first-spanish-bank-to-develop-risk-classification-modelusing-quantum-computing_en.html?id=42234.