QUANTUM COMPUTING: NEXT REVOLUTION IN COMPUTING IN COMPUTING

Aviral Mishra
Amity University, Lucknow,
Uttar Pradesh
E-mail : aviral.mishra1@s.amity.edu

Dr. Ranjana Rajnish
Amity University Lucknow,
Uttar Pradesh
E-mail : rrajnish@lko.amity.edu

ABSTRACT

Since the time idea of quantum computing was proposed, it has become a new field of interest for Physics and Computer Science researchers. Quantum computing is a conceptual change for the current day programmers, which includes the ways you think to solve a problem. It can be seen as the development of Object-Oriented Programming (OOPs) that changed the way programming was conceptualized. Unlike classic computing where the fundamental unit of storage is a bit that can store 0 or 1, quantum computing opens a way where, by superimposition and entanglement, qubit (storage unit in quantum computing) can store many intermediate stages between 0 and 1 also. Quantum processing is the utilization of quantummechanics to register and compute and is opening up a new world of computing and is seen as a revolution in computing technology and has various applications, issues, and challenges.

This paper is a study based on an exploration of the concept of quantum computing and tries to bring attention to emerging computing technology, its applications, issues and, challenges. It also discusses the concept of Qubit (Quantum Bit), Superposition and, Entanglement.

Keywords: *Quantum, Quantum Computing, Qubit, Superposition, Entanglement*

1. INTRODUCTION

Traditionally computers work based on a classical framework of 0's and 1's, but in the past few decades, classical computer chips and computing power have constantly improved. Moore's Law of computing talked about the way that the processing power of traditional

computers tends to double approximately every 18months. But now computing is evolving so fast that it seems it is the end of Moore's law. People are now talking about quantum computing which follows quantum mechanics as a framework to develop more powerful quantum computers. In quantum computing, the biggest revolution is that we can have a state between 0 and 1 also.

concept of quantum computation was firstly introduced by famous physicist, Richard Feynman in 1982. Quantum processing is the utilization of quantummechanics to register and compute and is opening up a new world of computing. A quantum PC is any PC apparatus that legitimately utilizes certain quantum mechanical wonders, for example, superposition and entanglement to perform different capacities in information. Quantum machines guarantee to release the best abilities of the present and future supercomputers.

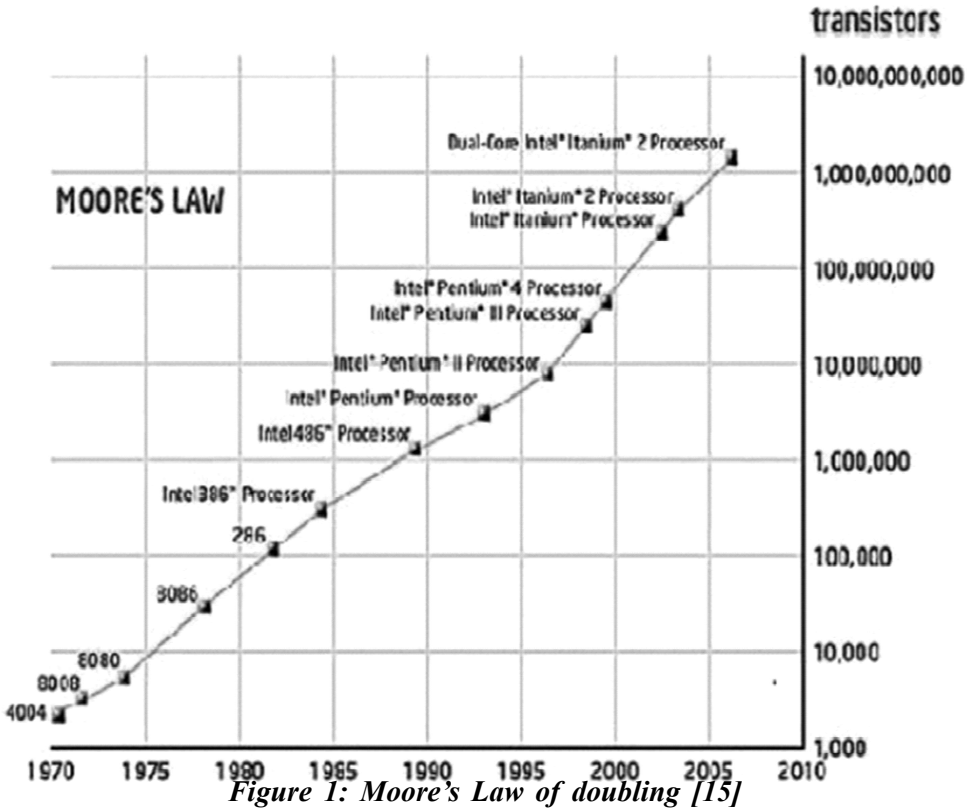

Figure 1: Moore's Law of doubling [15]

Utilizing a traditional machine will at present be the least difficult and most remarkable answer for tackle numerous issues. Be that as it may, quantum PCs guarantee to empower energizing advances in an assortment of fields, from materials science to pharmaceutical exploration.

The mystery of quantum PC power lies in the capacity to form and use a quantum bit or qubits.

POTENTIAL OF QUANTUM COMPUTING – QUANTUM BIT (QUBIT)

A bit is the fundamental unit of storage in Computer Science, where a bit can hold only two values: a 0 or 1. In quantum space, there isn't a limited space for electrons. Atomic particles behave like a wave and do not have a specific position. In quantum computing, the basic unit of storage is "qubit" (instead of "bit" as used in classical computing). Everything from your destinations and messages to your Spotify songs and YouTube accounts is in all actuality long strings of these equal numbers (bits). But a qubit has a state that could be a 0 or 1, but it can have unlimited states that are a superposition of these two states. Quantum computing uses the principle of superposition, i.e. a qubit can be in a state if linear superposition of two logical states (0 and 1) at the same time, similarly two qubits can be in a state of superposition of four logical states (00,01,10,11) at the same time, similarly, multiple qubits can have an exponential number of states. These states are a mixture of two arbitrary states and are described by equation (1). The objective of quantum computing is to harness these quantum superpositions [1]. This means that more data can be stored in few bits in the case of qubits and more computations can be processed in a flash [2].

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{——} \quad \text{Eqn 1}$$

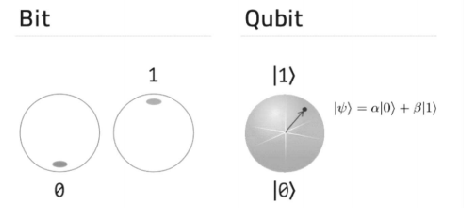

Figure 2: A comparison of states in a bit and Qubit

According to Hartmut Nevens the director of Google's Quantum Artificial Lab, growth in power with each new improvement to Google's best quantum processor is growing not just at an exponential rate (as stated by Moore) but at a doubly exponential rate. That is if qubits are used, he says, qubits are used in quantum computing to hold the same amount of data as 2n classical bits. For example, 2 qubits arethe same as 4 bits, 4 qubits as 10 bits, and so on.

Moore's Law is a doubling function, and its effect is seen every two years.

For example, for n year, computing power is 2^n.

Whereas Neven's Law is with double exponential growth.

For example, for each improvement in Google's quantum processor (n), computing power is 2(2n).

Table 1 represents quantum computing power relative to classical computing power. You may notice that after n=6, there is a tremendous improvement in the computing power. All this power will be of help to solve computational problems that were not possible with classical computers.

Table 1: Quantum Computing Power Relative to Classical Computing Power [3]

2n	$2^{(2n)}$	Quantum Computing Power Relative to Classical Computing Power
2	2^2	4
4	2^4	16
8	2^8	256
16	2^{16}	65,536
32	2^{32}	4,294,967,296
64	2^{64}	18,446,744,073,709,551,616
128	2^{128}	3.402823669209384634633746074317 7e+38
256	2^{256}	1.157920892373161954235709850086 9e+77
512	2^{512}	1.340780792994259709957402499820 6e+154
1024	2^{1024}	1.797693134862315907729305190789e+308

Qubits have some unconventional quantum properties which infer that their related assembling can give a way to deal with use more power than a comparable number of matched bits. One of those structures is known as superposition and the other is called a catch.

What is Superposition??

Qubits can speak to various blends of 1 and 0 simultaneously. Property of superposition says that, unlike bits that can have either 0 or 1, qubits can have a combination of 0s and 1s concurrently. We can say according to the quantum system, a qubit can be in a ratio of 0 or 1, and is not necessary that it be 0 or 1 only [4].

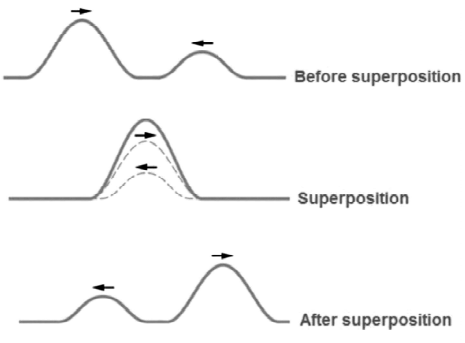

Figure 3: Principle of Superposition in waves

A quantum PC with few qubits in high goals can acquire countless outcomes

all the while. The last numerical outcome possibly shows up when the qubits are determined, causing their quantum state to be "acceptable" at 1 or 0.

What is Entanglement?

Nobody knows how or when it functions. It even incited Einstein, who portrayed this as "a misleading demonstration." But the key is in the intensity of quantum PCs. On an ordinary PC, it pairs the number of bits and copies its preparing power. Be that as it may, on account of the support, the option of extra qubits to the quantum machine builds a critical increment in the ability to create esteem.

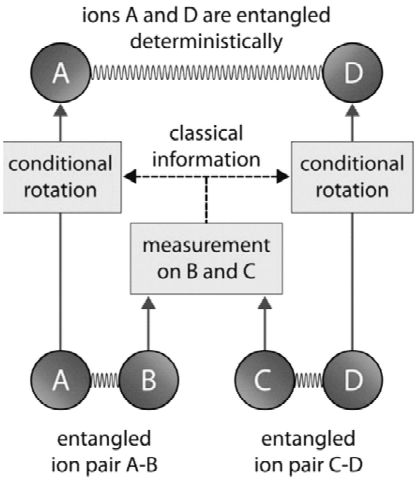

Figure 4: Entanglement Swapping with 4 ions. Image: University of Innsbruck [11]

Very powerful bonding between the quantum particles is called entanglement. This bonding or correlation is so strong that if they are being separated by a very long distance, it will be linked with another one. It leads to a very good communication system.

Agents can deliver sets of "bound" qubits, which implies that these 2 individuals from a couple exist in a similar quantum world. Changing the status of one of the qubits will change the status of the other in a sensational manner. This happens despite the fact that they are isolated by significant distances.

Quantum PCs pull q-bits as a quantum chain to accomplish their work. The intensity of machine speed counts utilizing exceptionally planned calculations is the reason there is such a great amount of cost to their capacities.

APPLICATION AREAS

With the exponential growth of computing power, quantum computing is ideally suited for solving complex problems. We will discuss some of the applications of Quantum computing in the real world.

Artificial Intelligence and Machine Learning:

The primary use of quantum processing is man-made reasoning and learning(AI& ML). Man-made intelligence depends on the rule of experiential learning, progressively exact as the appropriate response is given, to the point that the PC

framework appears to show "resourcefulness."

This depends on figuring the likelihood of numerous choices accessible, so AI is perfect for quantitative calculation. It vowed to grow the whole business, from car to clinical, and it was said that AI would be progressive in the 21st century.

For instance, Lockheed Martin intends to utilize his D-Wave quantum PC to test the auto-pilot programming that is as of now the most modern of old style PCs, and Google utilizes a quantum PC to plan programming that can recognize vehicles from marks. Some other common applications can be seen as voice, image and hand-writing recognition. We've arrived at a point where AI makes more Artificial intelligence, so it is worth will increment in less time.

Quantum artificial intelligence (QAI) is a field of methods focused on developing quantum algorithms for optimizing computational functions within artificial intelligence, including horizontal fields such as machine learning.

Quantum-improved AI alludes to quantum calculations that understand undertakings in AI, create and regularly quicken old style AI procedures. Such algos expect us to enter the predefined data set to the quantum PC to make it open to QI handling (quantum data).

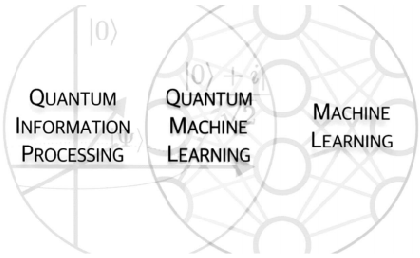

Figure 5: Representation of quantum machine learning research as a combination of research in quantum information processing and machine learning [11].

Computational Chemistry

According to IBM, the most promising application of quantum computing is in computational chemistry. It is understood that number of quantum states in the tiniest molecule is extremely vast and is thus difficult for traditional computing to process. Quantum computing willsolve this problem. 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].

Drug Design and Development

Researchers believe that advancements in computing will provide an effective way of understanding the drug and its reaction to humans. The use of quantum computing for the same will save a lot of time and money and will give better results.

Cryptography& Cyber Security

Security of online space has been quite vulnerable due to the large number of cyber-attacks across the globe on a regular basis. Using machine learning algorithms and quantum computing, new techniques may be developed to make online space more secure.

Most online security is as of now subject to the trouble of breaking huge numbers into primes. Although this can be accomplished right now by utilizing old PCs to look through all the potential issues, the tremendous time required makes "breaking this code" more costly and reasonable. Quantum computing can help in devising new and complex encryption methods, known as quantum cryptography.

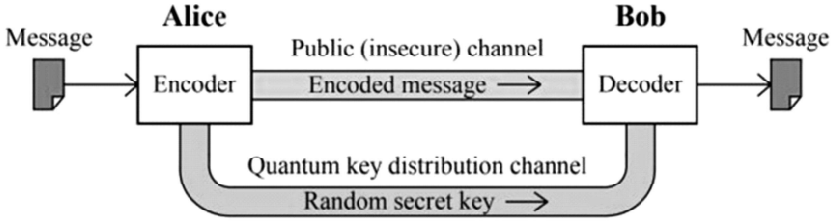

Figure 6: Quantum Cryptography [14]

There are likewise better quantum encryption strategies that are created utilizing a solitary normal info technique. Systems around urban communities have just appeared in different nations, and some Chinese researchers have recently reported that they have effectively transmitted pictures concentrated on the changing quantum satellite to three distinct stations accessible on Earth.

A superb and improved application for quantum cryptography is quantum key distribution (QKD) which is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics.

Financial modelling

The present markets are one of the most mind-boggling frameworks in presence. While we have built up some logical and numerical apparatuses to tackle this, there is as yet one significant contrast between different sciences - there is no controlled game plan to run tests. Researchers are working on preparing models that could find the right mix of investment based on expected return, associated risk, and factors that are important to surviving in market. Current algorithms take a lot of resources and time. It is believed that the application of quantum computing to handle computation complexity involved in financial modelling will reduce the time of computations.

Logistic Optimization

Improved algorithms and modelling will help in better data analysis. Many

organizations will be benefitted to optimize their logistics, scheduling workflows, and supply chain management. Traffic management, Air traffic control, freight and distribution, fleet operations are various other domains that require optimization, thus these all may be benefitted from quantum computing.

Weather Forecasting

In traditional computing, analyzing weather data takes a lot of time and makes accurate weather prediction a problem. Quantum computing's ability to process a vast amount of data in a very short span of time could lead to better weather prediction modeling systems, that could help weather scientists to make better predictions with respect to changing patterns in no time and with improved accuracy.This becomes especially important for the current time when the world is undergoing abrupt climate change.

While quantum computing has already had an impact on the above-mentioned fields, the list is by no means exhausting, and that's the most exciting part. As with all new technologies, un-imaginable current applications will be developed as the Hardware continues to emerge and create brand new opportunities.

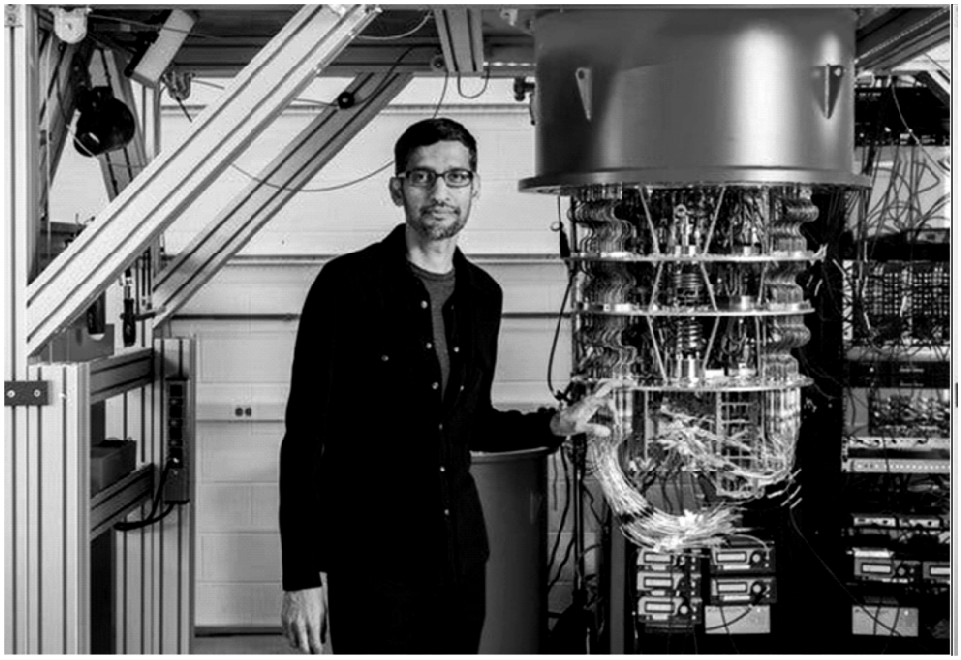

Figure 7:Google's chief executive, Sundar Pichai, with one of its quantum computers[6]

QUANTUM COMPUTING ISSUES

Quantum PCs are hard for a designer to construct and program. Thus, they are loaded up with blunders as commotion, mistakes, and loss of quantum intelligence, which are basic to their activity but separate before any nontrivial framework has the chance to dispatch to be finished.

The loss of attachment (known as decoherence) brought about by development, temperature variances, electromagnetic waves, and different cooperation with the outside condition, in the end, annihilates complex PC structures. Given the current commonness of decoherence and different blunders, present-day quantum PCs are probably not going to bring back the correct responses for basic tedious programming. While contending advancements and contending structures tackle these issues, no current equipment stage can control the attachment and give the strong mistake remedy required for huge incorporations. Achievement presumably kept going for quite a long while.

Reactions have emerged from broad examinations in a few fields, with agents in the industry, foundations, and national workshops following different techniques to lessen mistakes. One route is to think about what an immaculate computation will resemble dependent on the consequences of blends with various sound levels.

A totally extraordinary methodology, mixture quantum-traditional calculations, just apply the touchiest pieces of programming work to a quantum PC, with the greater part of the program running on a ground-breaking advanced PC. These and different methods end up being useful in managing the boisterous condition of numerous advanced PCs.

While old-style PCs are likewise influenced by different wellsprings of blunders, these mistakes can be explained with a restricted measure of extra stockpiling and rationale.

Quantum conspire change plans exist yet devour such countless qubits (the number of bits) of which just a couple qubits are left in the first mix. That decreases the size of the PC's work to a little part of what may deal with a standard imperfection-free convenient gadget.

QUANTUM COMPUTING CHALLENGES

Quantum computing seems to be a promising field, but looking at it practically, there are few challenges that are seen as big stops to quantum computing becoming reality. Few of the challenges are as below:

Sensitivity to interaction with the environment:

Quantum computers are way more

sensitive to interactions with their environment because any kind of interaction leads to a deterioration of the state function. It is very difficult to distinguish a quantum system, especially one designed for computation without getting it entangled with the environment. The larger number of qubits leads makes it difficult to maintain coherence.[8]

Reliable matrix conversion:

Lots of computations in quantum bits are accomplished using arrays of transformation using small gates [8]. It is expected that there will be no error in such transformations, but in practical schemes error may be introduced. Also, classically there is a lack of precision in matrix transformation. This lack of precision may not be compensated by quantum computing.

Qubic quality

Qubit is still at a nascent stage and has been tested only on the small system. There is a need to develop them to handle instructions or gate operations on a large scale. The qubits are still generating errors while running the operations. Though they are processing the instructions faster, they are producing the wrong results. Results obtained cannot be distinguished from the noise[9].

Error correction

Since the qubits are producing errors, error correction algorithms need to be implemented to get the correct result. Error correction has yet not been proven for quantum computing and is a priority research area. A full-scale commercial-scale quantum system can only be developed once this is taken care of.

Major Players working on Quantum Research

Google, INTEL, IBM, Microsoft and many other giants are working on various aspects of quantum technologies.

IBM took the first industry initiative in March 2017 to build a commercially available Quantum Computing system. These systems will be designed to tackle complex problems to demonstrate the viability of quantum computing and its utility across industries. In Sept 2017, IBM was successful to simulate the largest molecule till date i.e. Beryllium hydride (BeH2) on IBM quantum processor [10]. In 2019, designed and build IBM Q System One, the first integrated quantum computing system for commercial use. IBM Q System One was more reliable and stable and enables universal approximate superconducting quantum computers to operate beyond the confines of the research lab for the first time.

Researchers at Microsoft are also pursuing big questions related to quantum computing.Microsoft's Azure Quantum team isworking on tosolve customer problems using new algorithms and computing hardware. Mandate is

to develop computing systems to solve currently unsolvable problems. The Microsoft Quantum team innovates across every layer of the quantum stack, from software and applications to control and devices. This includes the pursuit of fault-tolerant topological qubits that scale towards a general-purpose quantum computer [17].

Intel Labs are doing lot of experiments since 20th century. The research has led to the development of Tangle Lake, a super conducting quantum processor that incorporates 49 qubits in a package that is manufactured at Intel's 300 millimetre fabrication facility in Hillsboro, Oregon. This device represents the third generation of quantum processor produced by Intel, scaling upwards from 17 qubits in its predecessor [18].

S.J. Pauka et al are working on the design of cryogenic CMOS chips for generating control signals for multiple qubits, which will be of great help in scalingup quantum computers [16].

CONCLUSION

The field of quantum figuring is quickly growing as increasingly more present-day with professional groups, colleges, universities, and all the main IT giants are exploring the subject. Experts believe that the development of quantum computers will be completed by 2025 or 2030, but a major issue to this is that the available software'sare developed to do computations on classical computers. There is a need to work on software that could harness the power of quantum computing.

Clearly, this degree of computational force hasenormous business, modern and logical applications, however, there are some significant issues that must be settled first. Looking at the huge benefits, it is worth solving these challenges.

REFERENCES

[1] *https://www.huawei.com/en/publications/communicate/86/quantum-computing-ai*

[2] *https://www.livescience.com/65651-quantum-computers-get-scary-fast.html*

[3] *https://community.hitachivantara.com/s/article/moores-law-is-replaced-by-nevens-law-for-quantum-computing*

[4] Hemant Bhatt, Shubhra Guatam, "Quantum Computing: A New Era of Computer Science", *https://ieeexplore.ieee.org/document/8991254*

[5] *https://analyticsindiamag.com/top-applications-of-quantum-computing-everyone-should-know-about/*

[6] *https://www.nytimes.com/2019/12/06/technology/what-is-quantum-computer.html*

[7] Franklin D., Chong F.T. (2004),"Challenges in Reliable Quantum Computing", In: Shukla S.K., Bahar R.I. (eds) Nano, Quantum and Molecular Computing. Springer, Boston, MA. *https://doi.org/10.1007/1-4020-8068-9_8*

[8] Abhilash Ponnath, "Difficulties in the Implementation of Quantum Computers", *https://arxiv.org/ftp/cs/papers/0602/0602096.pdf*

[9] Jim Clarke, "An optimist view of the challenges to Quantum Computing", *https://spectrum.ieee.org/tech-talk/computing/hardware/an-optimists-view-of-the-4-challenges-to-quantum-computing*

[10] *https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/*

[11] *https://phys.org/news/2008-10-deterministic-entanglement-swapping-successful-technique.html*

[12] *https://www.amirsariri.com/blog/2017/5/9/quantum-machine-learning-path-to-a-better-artificial-intelligence*

[13] *https://towardsdatascience.com/how-may-quantum-computing-benefit-machine-learning-c96de0bef0d4*

[14] *https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography*

[15] S. Jafar, P. Kumar, R. Rajnish and M. Jafar, "Architectural scheme for future embedded systems involving large number of processing cores", 2017 *7th International Conference on Cloud Computing, Data Science & Engineering - Confluence,* 2017, pp. 392-396, doi: 10.1109/CONFLUENCE.2017.7943181

[16] S. J. Pauka, K. Das et al,"A cryogenic CMOS chip for generating control signals for multiple qubits", *Nature Electronics, January 2021,* Vol 4: pp. 64-70.

[17] *https://www.microsoft.com/en-us/research/research-area/quantum-computing/?facet%5Btax%5D%5Bmsr-research-area%5D%5B0%5D=243138&sort_by=most-recent*

[18] *https://www.analyticsinsight.net/top-10-quantum-computing-companies-2020/*