# A Survey:The Next Generation Of High Quantum Performance Of Quantum Computing Devices

Ms.Rashmi Dubey, Ms. Sugandha Agarwal,Mr.Rajesh Singh

**Abstract**— This Research paper gives a review of Quantum Computing Devices – How they uses quantum mechanical Phenomena to performs operations on data through Superposition and entanglement? What makes them different from Classical computer? How Q-bits play a necessary role? This review paper will also answer the needs of quantum computation and the benefits of its application and processing power as compared to the classical computer. Quantum Computers are working on qubits that makes it immensely powerful and even make Quantum Computers to break one of the secure Public-key cryptography RSA. What makes them so powerful? And what are the areas of Quantum Computing device in which it can be fruitful. This paper introduces all pros and cons of quantum computing and tell us why upto certain bits Quantum Computers are infeasible to build.

**Index Terms**— Quantum Computing Devices, High Performance Quantum Computers, Next Generation Computers, Qubits, Superposition, Entanglement, Reversible Quantum Gates, Shor's algorithm.

## 1 INTRODUCTION

**Q**uantum Computing is not the new concept, its roots lie in the era of 1970s, when it was coined by Richard Feynman and Yuri Manin. The tremendous amount of processing power generated by this computer has not been able to fulfill the demands for computing capacity and speed. Even an American Computer Engineer, Howard Aiken in 1947, said that the computing needs of United State would be satisfied by just six electronic digital computers [7].

Quantum Computing is totally based on quantum mechanics theory. Quantum Computers harness the powers of molecules and atom to do faster computation and to enhance the performance of memory at subatomic levels. Quantum Computers have the potential to do faster calculations than Silicon based computers.

Quantum Computers are computational devices that use quantum mechanical phenomena at subatomic level such as entanglement and superposition. Where a digital computer uses binary bits to encode the data, Quantum Computers uses qubits. Qubits has quaternary in nature. Laws of quantum mechanics are totally different than classical physics. Where binary bits remains in either 0 or 1 state, qubits can exist in both states i.e. what called superposition. Therefore computer which works on qubit can make calculations faster than the digital computers using both values simultaneously.


- *Ms. Rashmi Dubey,Assistant Professor, Computer Science and Engineering Department in Amity University, Iindia, PH-9999017210. E-mail: rash.monu@gmail.com*
- *Ms. Sugandha Agarwal,Assistant Professor, Computer Science and Engineering Department in Amity University, Iindia, PH-9873005445. E-mail: aga.sugandha@gmail.com*
- *Rajesh Prasad Singh, pursuing masters degree program in Computer Science and Engineering Department in Amity University, India, PH-08826074469. E-mail: rj.singh@live.in*


A qubit made of 8 bits can have all the values between 0-255 at a time while a binary bit can have the single value between 0-255 at a time. Almost Forty Qubits are equivalent to the power of the current modern computers [2]. A quantum computer takes only 27 minutes to find a phone number from the database consisting of world's phone number while "Chuang", a supercomputer takes a month to do the same [2].

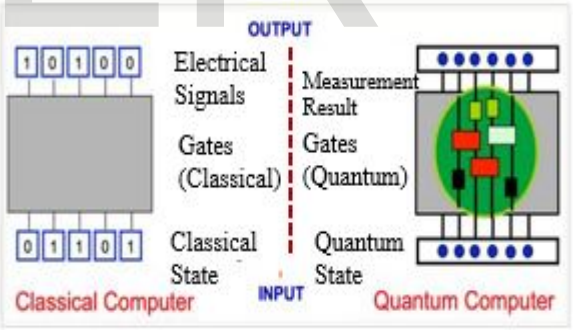



fig. 1: shows the possible states of classical and Quantum Computer after giving the set of inputs [6].

A Classical Computer takes input in the form of either 0's or 1's and process the information using electronic circuitry. It performs set of predetermined operation which can be further broken down into "gate operations" in which some bit changes based on the known values of others [6]. While the information is taken as a Quantum encoded form in Quantum Computer and gate operations are performed to produce new quantum state according to laws of Quantum.

The question arises is that why we are looking for the computers and computational devices that obey quantum mechanics laws? According to Moore's law, in every 18 months the transistors on microprocessors continues to double. So by the year 2020 or 2030, circuits in microprocessor enters into an atomic

level [9]. And the only way to work at subatomic level is quantum mechanics. According to the evolution described by Moore's law if there is a digital computer in 2020, then it will run with the speed of 40GHz and with 160 GB RAM. And at the same time if applying analogue Moore's law in Quantum Computing then qubits would be double every 18 month. And adding a single qubit would increase the power and speed of Quantum Computer to double [2].

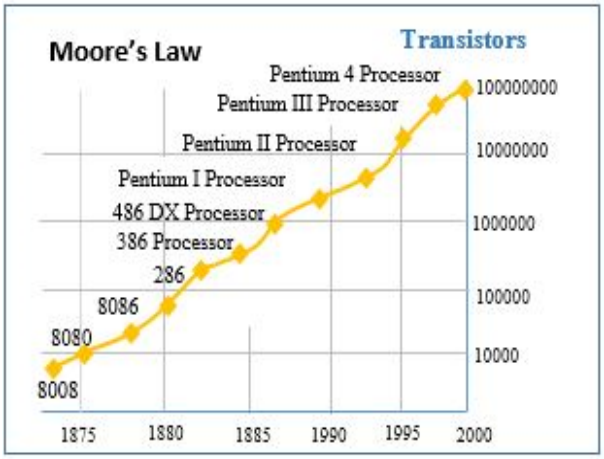



Fig. 2: Graphical representation of Moore's law showing that no. of transistors continues to double after every 18 month [9].

IJSER staff will edit and complete the final formatting of your paper.

## 2 RELATED WORK

This section give the review of previous work carried out by many scientist on qubits and their practical approach. There has been lot of research [5], carried out to explore the computational power of qubits and to make the Quantum Computers realistic upto a certain numbers of qubits.

### 2.1 Qubits

Qubits are also called quantum bits. The specialty of quantum bits is that it can be in the state of superposition of "0" and "1" or it can have more than two values at a time. A binary bit can either take 0 or 1 value while the qubit can hold both values at a time. States in which qubit are measured are known as basis vectors. Qubits are represented as |0> and |1> pronounced as ket 0 and ket 1.

.

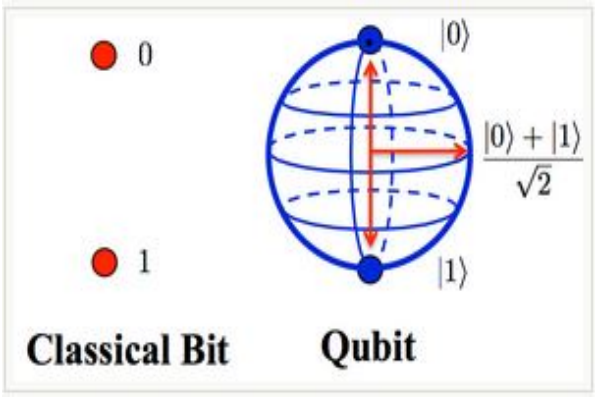



**Fig. 3:** Fig. 3: Graphical Representation of classical bit and Qubit showing the difference between their states [6].

Where a "bit" of information in Classical Computer can be represented by only two points, a "qubit" in a Quantum computer is instead represented by any point on the 3D surface of the "Bloch Sphere". As the whole system of the quantum computer runs on qubits, the system as a whole can be in the state of superposition and can be mapped anywhere on the surface of "Bloch Sphere". This is why Quantum Computer is extremely omnipotent, where each and every state could be stored and processed parallely. The number of states in superposition is very huge i.e. having N qubits in Quantum means having 2N states in superposition [2]. A Quantum computer having 30 qubits would have 1,073,741,824 states and a Quantum computer with 300 qubits would have roughly the same number of states as the total number of atom in the universe [2]. A qubit can be also visualized as a unit vector on the normal plane where α and β are complex numbers.

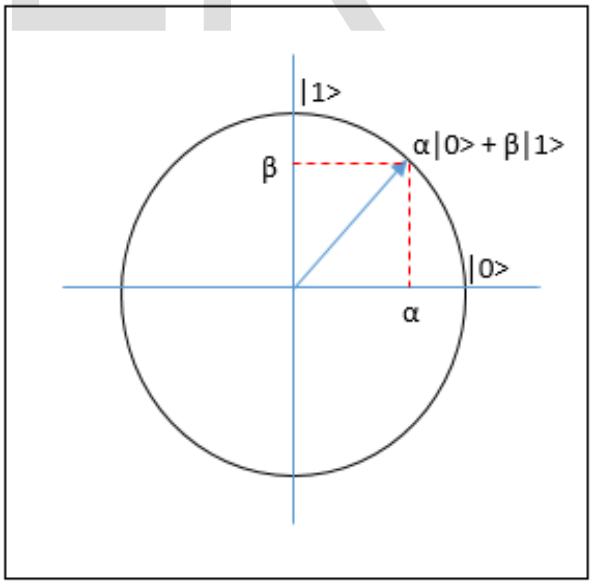



Fig. 4: Qubit Representation on a 2D sphere.

In pure state qubit is a superposition of the basis states. It can also be represented as linear combination of |0> and |1>.

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Where α, β are probability amplitudes. Also the outcome of |0> and |1> will be α2 and β2 respectively and then the whole equation can be written as

$|\alpha|2 + |\beta|2 = 1$

Any linearly independent pair of vectors $|\varphi>$, $|\psi>$ □ C2 serve as a basis. $\alpha|\ \varphi > + \beta|1> = \alpha|'0> + \beta'|\ \psi >$. Basis is determined by the measurement process or device. Measuring the state of $\alpha|0> + \beta|1>$ results in $|0>$ with the probability $|\alpha|2$ and $|1>$ with probability $|\beta|2$. After the quantification, the system is in the measured state. That is further quantification will always yield the same value. Fetching only one bit of information from the state of qubit. $\alpha|0> + \beta|1>$ and $\alpha|0> - \beta|1>$ are having almost the same probabilities for their measurements. However they belong to distinct states which behave differently in terms of how they evolve.

The possible state of single qubit can be also be represented on Bloch Sphere. A classical bit could be only at the North and South pole representing $|0>$ and $|1>$ and the rest of the surface is inaccsible, but a qubit in a absolute state can be represented anywhere on the surface [10].

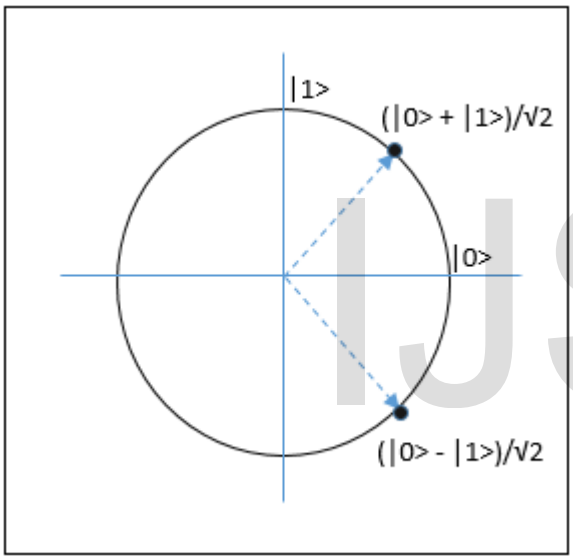



Fig. 5: Showing the measurments in qubits [13].

For example, the pure qubit state $(|0> + i|1>)/2$ on the positive y axis would lie on the equator of the sphere,

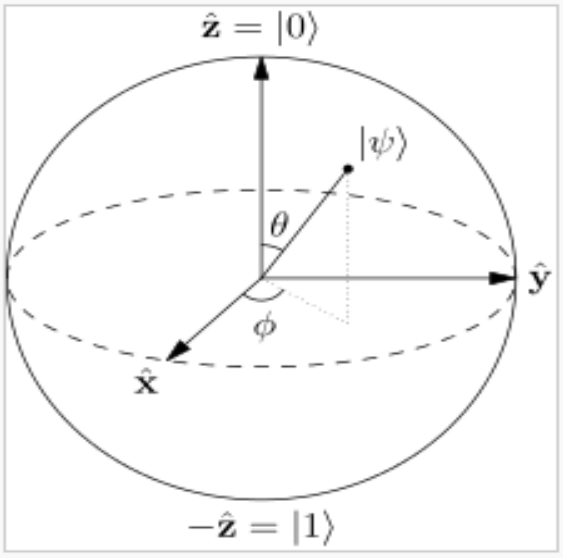



Fig. 6: The Bloch sphere representation of qubit [10].

Many implementation ideas of q-bits have been proposed:

- Spins of electrons in quantum dots
- Spins of nuclei in molecules (molecules)
- Floating of electron spins over liquid helium
- ions in traps
- Excitonic states of nanocrystals
- Polarization of photons ("flying qubits")
- Spins of impurity nuclei
- "Dual-rail" photon qubits
- Ions in optical lattices
- Collective spins of atom clusters

All of these implementations have their own pros and cons and are being actively experimentally pursued.

### 2.2.1 SUPERPOSITION

Superposition is a fundamental principle of quantum mechanics that holds an electron in partially all its possible states simultaneously, and when measured gives results corresponding to only one of the possible configuration. It refers to the property of solutions to the Schrödinger equation which says that any linear combination of solutions to a particular equation will also be a solution of it.

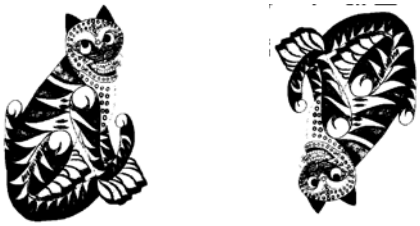


Fig. 7. Schrödinger's cat

The best example is Schrödinger's cat. Since both a dead and living cat are the valid solutions to the laws of quantum mechanics, a superposition of the two cat should also be valid. Schrödinger described an experiment that could give rise to such a state. If this state is measured, one can only see one or the other state (live or dead) with some probability. Consider a polarizing beam splitter which reflects all light of one polarization (say H) and transmits all light of the other polarization (say V). If light polarized 45° to Horizontal and Vertical, half of it is reflected and half transmitted. A Single photon will be reflected with 50/50 probability, if it arrives at 45°. Such a photon can be described as a superposition of H and V: (|H>+|V>)/sqrt (2) [11].

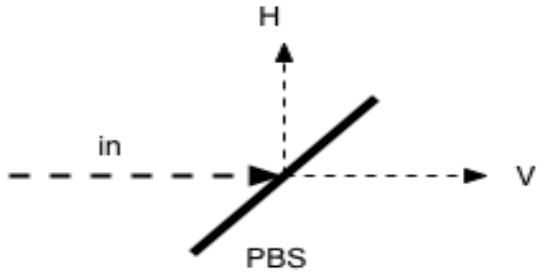



Fig. 8: A Polarizing Beam Splitter describing light as superposition of H and V [11].

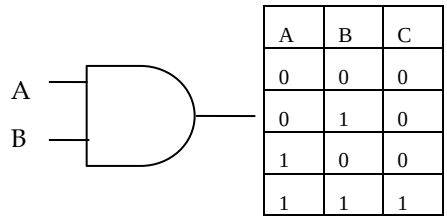
However, it is not just a simple matter of a photon going one way or the other with equal probability. In a beam splitter if two beams are passed, then the photon can recombine in such a way that the probability to go in one direction cancels out. This is interference. Thus splitting the beam and then recombining it again to get the desired final output serve the purpose of quantum bits operations.

### 2.1.2 ENTANGLEMENT

Quantum Entanglement is a kind of phenomena where two or more than two particle act together in such a way that leave them entangled, later measurement on one system predicts the outcome of analogous measurement on the second system-no matter how much far they are separated in space[1]. Assume Two qubits, each in the state of |0> + |1>. Then the entanglement of both the qubits are related in such a way that the measurement of one qubit is always related the measurement of another qubit. It is the product of Quantum Superposition. However the vagueness of state totally depends in terms of spin, polarization, momentum etc. when one member of entangled pairs are measured and there outcomes are known, then the other member of the entangled pair at any subsequent time always found to have taken the suitably correlated value [4].

## 2.2 OPERATIONS ON QUBITS-REVERSIBLE LOGIC

As per quantum physics the devastation of information in gate cause the heat to raise which can spifflicate the superposition of qubits. For eg.




| A | B | C |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**Table 1. Logical Gate Operation Showing Loss of Information**

Lots of resemblance between quantum gates and classical gates, but their original input state can be specifically derived from their output state. They are reversible. That confirms a quantum computer can perform deterministic computation only if it is reversible which has been proved by Charles Bennet in 1973. Hadmard Gate, involves one qubit which is also called as square root of NOT gate, is used to put qubits into superposition. Two Hadmard gates in succession represent NOT Gate. A gate operating on two qubits is named as a Controlled-NOT Gate. If the bit on the target line is 1, then the bit on the target line is inverted. XOR gate is similar to the CN gate but CN gate has some extra information to make it reversible. Similarly the gate operating on three qubits is called Controlled Controlled NOT (CCN) Gate.

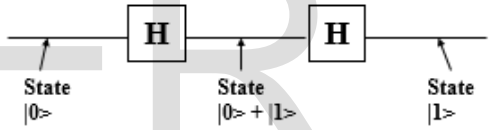



Fig. 10: Hadamard gate showing the states of |0> and |1> [11].

The target bit is inverted, if the bits on both of the control line is 1.

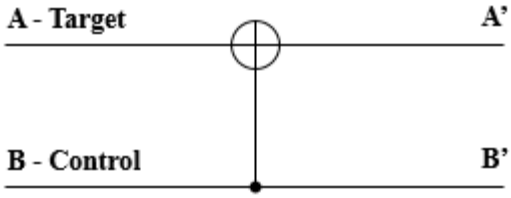



Fig. 11: Controlled Not Gate Operating on Two qubits [11].

For eg. Reversible logic circuit to caculate multiplication by 2 using CN gates arranged in the following manner :

**TABLE 2 : EXAMPLE OPEARTION-MULTIPLY BY 2**

| INPUT | | OUTPUT | |
|---|---|---|---|
| Carry bit | One Bit | Carry bit | One bit |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |

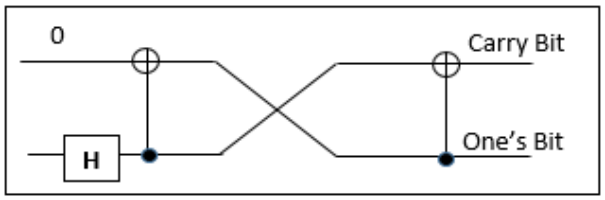



Fig. 12: Reversible Logic Circuit to calculate multiplication by 2.

The CCN gate is also a Universal reversible logic gate as it can be also used as a NAND gate.

### 2.3 SHOR'S ALGORITHM

Shor's algorithm is one of the most widely used quantum algorithm used in quantum computer to factorize a number N in O (log N)3 time and O(log N)space. Shor's algorithm is efficient in terms that it can break one of the most secured public key cryptography RSA, given a sufficiently large quantum computer. In RSA, the public key N is based on the product of two large numbers. And the only way to crack RSA encryption is to factorize N which is impossible using classic algorithm, as N grows large, factoring of a large number becomes time consuming. Currently no classical algorithm is known that can factor N in RSA in polynomial time [13]. While Shor's algorithm is the answer for all, and can factorize large prime number in polynomial time. Shor's algorithm is totally probabilistic. It always gives the accurate result with high probability and by repeating the algorithm continuously accuracy can be increase. It was also proven by the group at IBM, using a set of 7 qubits in quantum computer, which factored 15 into 3 and 5. The algorithm is fully dependent on

- Modular arithmetic
- Quantum parallelism
- Quantum Fourier transform

### 2.4 CLASSICAL VERSUS QUANTUM COMPUTER

**Table 3: Difference between classical and quantum computer.**

| | Classical Computer | Quantum computer |
|---|---|---|
| Fundamental unit | Bits | Qubits |
| State | Can be either in 0 or 1 state | Can be in both the states i.e. superposition state. |
| Possible permutations | One out of 2N | All of 2N |
| Laws obeying | Classical physics | Quantum mechanics |
| Algorithms used | Normal Algorithm | Quantum Algorithm |
| Circuit | Irreversible Circuits | Reversible Circuits |
| Cryptography problems | Unable to solve in Polynomial time | Solve most of the problem in polynomial time |

## 3 POTENUTIAL OF QUANTM COMPUTERS

Factoring Integer is considered as one of the hardest problem for Classical Computers. For digital computers the problem of factorization is difficult to solve in polynomial time while it could be easily done by quantum computer using Shor's algorithm. The ability makes quantum computer efficient to break the well-known RSA public key encryption in polynomial time. Almost all the public key cryptography technique are based on the difficulty of factoring the integers. They are used for the security of encrypted email and to protect the web pages, and many other types of data from vagueness. Cracking this would be a significant ramifications for high security and electronic privacy. Besides factorization, quantum algorithm offers more than polynomial speedup over classical algorithm. Groove's algorithm a well-known quantum algorithm uses almost half a quarter queries to the database than are required by the classical algorithms. For eg. To search the entire library of congress for one's name given an unsorted database takes 100 years by Classical Computer while the quantum computer takes only half second to do it [11]. Due to the ability of quantum computer to attain in multiple states simultaneously, it has the potential to be millions of times more powerful than today's most powerful supercomputer. According to David Deutsch, a physicist, a quantum computer can parallelly compute millions of computations at once while our Classical Computer does the calculations one at a time. A quantum computer having 30 qubits would equal to the processing power of conventional computer that could run at 10 teraflops while the Classical Computer runs at the speed measured in gigaflops [7]. To know the real power of Quantum Computing consider the case of Large Hydron Collider (LHC) which also uses the same technique i.e. to harness the power of atoms to reveal the mystery of universe found almost 5 trillion bits of data-more information than all than all of the world's library combined-every second. The four experiments of LHC produced a whopping 25 petabytes (25 x 1015) of data per year. This scale is far beyond the computing resources of any single facility, so the LHC scientist rely on vast computing grid of 160 data centers spread all around the world, a huge distributed network which is capable of transforming as much as 10 gigabytes per second at peak performance. Such is the power of Quantum Computing and its applications.

## 4 PROBLEM FOUND IN QUANTUM COMPUTING

One of the biggest problem that arises to deploy a quantum computer is quantum decoherence. It is the phenomena in which the quantum computer decay from a given quantum state into an incoherent state. Other sources of decoherence also exist like quantum gate lattice vibrations, spins of nucleus in background etc. it is also irreversible, as it is non-unitary and is usually that must be controlled [2]. Ratio of operating time to the decoherence time is directly proportional due to which operations must be completed much quicker than decoherence time which is hard to implement. If the problem of decoherence cannot be solved than the quantum computer will be similar to the silicon computer and are not better than the digital one. Also upto a certain qubit the quantum states

are more than the stars in our universe which is hard to store and analyze and thus Quantum Computers are limited upto a certain qubits. For eg. If considering a Quantum Computer of 500 qubit, then it would be equal to the 10150 processors which is impossible. Hardware is another problem of Quantum Computing because developing a quantum computer whose hardware works on subatomic level is a tough task to implement. The current technology used in quantum computer IS NMR i.e. Nuclear Magnetic Resonance Technology because of some fruitful experiments [10].

## 5 FUTURE OF QUANTUM COMPUTING

1. Cryptography and Petr's Shor's Algorithm: Shor's Algorithm is capable to break a well-known public key cryptography method RSA in Polynomial time. If the operation to break the RSA is performed on Classical Computer then it will take 1000 of years to break it as it is based on factorization. Taking consideration factor of factorization Shor's developed an algorithm for factorization that gave immense power of computation as well as high processing speed to the Quantum Computers

2 Artificial Intelligence: Due to the mammoth computational power and high processing speed, Quantum Computers has the ability to learn fast and perform large number of operations in short amount of time which forms the basis of Artificial intelligence. It not only increases the learning rate but also enhance the accuracy.

3 Military and intelligence information gathering

4 Simulation of high computational models such as nuclear explosion and oil discovery.

5 Grid Computing: Grid computing uses combined computational power. It might be possible that Quantum Computer could inherit computational power of different machines and may play a better role in Grid computing. There is also the possibility of grid-type networks that use Quantum Computers which give almost incomprehensible computing power [8],[14].

As Quantum Computers are made for giving high performance they will also support development of voice, image reorganizations, complex compression algorithms, molecular simulations, true randomness and quantum communications.

## 6 CONCLUSION

The field of Quantum Computing is growing very rapidly as many of today's leading computing groups, colleges, universities; leading IT vendors are researching on this topic. As more researches on Quantum Computing are turning in practical applications, its pace is increasing simultaneously. The current issue is not to build a high performance Quantum Computing devices or to build a quantum computer that obeys quantum mechanics law, instead to move away from the investigation in which one can simply observe quantum phenomena to the experiments in which one can control these phenomena. Advancement in Quantum Computer needs tremendous amount of money and lot of effortless efforts too. Even the wisest scientists can't answer a lot on Quantum Computing which is totally based on quantum physics. Building a fully working quantum computer is just a matter of time. There is no prediction that when the scientists will build the first Quantum Computer that fully obeys quantum laws, it could be this year or may be after next 10 years or centuries from now. But this will be one of the prominent steps in science and will revolutionize the computing world era.

## REFERENCES

[1] Cristi Stoica, Adirect interpretation of quantum mechanics.philsci-archive.pitt.edu/4194/direct_qm.pdf,2008.

[2] Ding, Archil Aviliani, Quantum Computers, International University, December 1,2012.

[3] Scott Aronson and Dave Bacon, Quantum Computing and the Ultimate Limits of Computation: The case for a National Investment, Computing Community Consortium, and Version 6: December 12,2008.

[4] Phillip Kaye, Raymond Laflamme, Michele Mosca, An Introduction to Quantum Computing, Oxford University Press.

[5] Scott Aronson, Research Papers and surveys, http://www.scottaaronson.com/papers.

[6] Andrew Daley, Quantum Optics and Quantum Many Body Systems, Research Group at the University of Pittsburgh, http://qo.pitt.edu/research_qc.html.

[7] How Quantum computer works, http://computer.howstuffworks.com/quantum-computer1.htm.

[8] Richard Murch, Quantum Computing: The Hype and the Reality, IBM press release.

[9] Michael Karbo, PC architecture, Chapter 9, Moore's Law, http://www.karbosguide.com/books/pcarchitecture/chapter09.htm.

[10] Kaufman, Leon .1983 .Advances in imaging technology: Nuclear magnetic resonance ,IEEE Journals & Magazines ,Magnetics transactions ,Volume:19 Issue:3

[11] Todd A. Brun, Quantum Computers, Communication Science Institute, USC Viterbi

[12] Max Tegmark and John Archibald Wheeler,100 Years of Quantum, Issue of Scientific American, p.68-75.

[13] Quantum Computing Metaphysics Research Lab, CSLI Stanford University.

[14] M. Z. Li, M.Baker ,Kernel Technology of Computing Grid Tsinghua University Press,Beijing,2006.