# Quantum Computers – an Approach to Reduce Time Complexity?

Lokesh Saini
B.Tech Student
Dept. of CSE
HMRITM New Delhi, India

Ravi Shankar
B.Tech Student
Dept. of CSE
HMRITM New Delhi, India

Dayanand
Assistant Professor
Dept. of CSE
HMRITM New Delhi, India

***Abstract*-Quantum computers are the outcome of upgraded technology used to remove time complexity. Quantum computers are expert in its own the field which investigates computational and other properties of computer based on mechanical principles. In quantum computers important objective is to find quantum algorithms that are significantly faster than classical algorithms. Here we give a brief introduction to quantum computers considering some physical system that can be i N different mutually exclusive classical states. Call these states |1i,|2i,... ,|Ni. Classical states .A pure quantum state is a superposition of classical states, written |φi = α1|1i+ α2|2i+···+ αN|Ni [1].**

***Keywords: Quantum Computers, Classical Computers, High Performance.***

## I. INTRODUCTION

**Quantum computing** or computation systems [quantum computers] that make direct use of quantum mechanical phenomena, such as superposition and entanglement, such as to perform operation on data.

Quantum computer are different from binary digital computer system [electronic computer based on transistors].Whereas common digital computing requires that the data be encoded into binary digits

(bits),each of which is always in one of two definite states[0 or 1],quantum computer use quantum bits, which can be superposition of state , A quantum Turing machine is theoretical model of such a computer ,and is known as the universal quantum computer.

The field of quantum computing was initialize by the work of Paul Benioff and Yuri manin in 1980, Richard Feynman in 1982, and David Deutsch in 1985. Quantum Computer, a computer that uses the effect of quantum mechanics to its advantage.

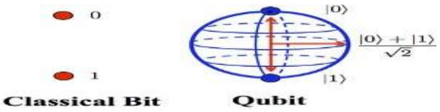

Fig.1.1

A computer which makes use of that Quantum states of subatomic particles to store information. Recent development of quantum computer have bought the idea to everybody attention. One such development was the invention of an algorithm to factor large number on a quantum computer by peter shor[Bell Laboratories].By using this algorithm, a quantum computer would be able to crack codes much more quickly than other ordinary(or classical) computer could. In fact a quantum computer capable of performing short's algorithms would be able to break current cryptography techniques in a matter of seconds. With the motivation provided by this algorithm the topic of quantum computing has gathered momentum and researches around the world are racing to be the first create a practical quantum computer .As we are in 2017, the development of actual quantum computer is till infancy, but experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits.

Both practical and theoretical research continues, and many national government and military agencies are funding quantum computing research in an effort to develop quantum computers for civilian, business, trade, environment and national security purpose, such as cryptanalysis.

## II. CONCEPTS OF QUANTUM COMPUTERS

### *Qubit*

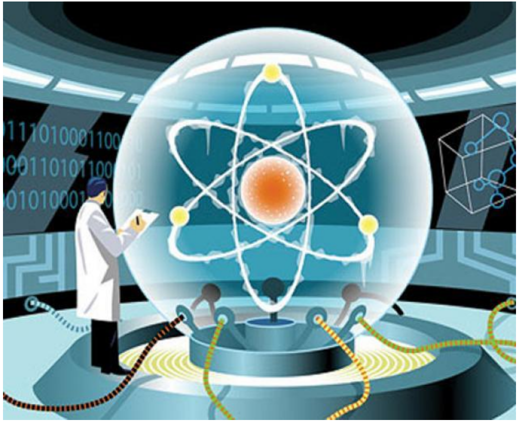

Fig.1.2

- A quantum bit or qubit is a unit of quantum information.
- Many different physical objects can be used as qubits such as atoms, photons, or electrons.
- Exists as a '0', a '1' or simultaneously as a superposition of both '0' & '1'

### ***Quantum information***

- Quantum information is physical information that is held in the "state" of a quantum system.
- Though the amount of information that can be retrieved in a single qubit is equal to one bit, the difference lies in the processing of information

### *Quantum entanglement*

- In Quantum Mechanics, it sometimes occurs that a measurement of one particle will effect the state of another particle, even though classically there is no direct interaction.
- When this happens, the state of the two particles is said to be entangled.

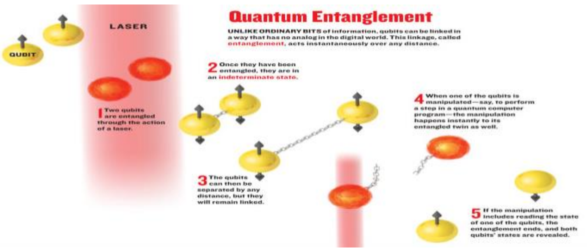
Quantum Entanglement
UNLIKE ORDINARY BITS of information, qubits can be linked in a way that has no analog in the digital world. This linkage, called entanglement, acts instantaneously over any distance.
QUBIT
LASER
1 Two qubits are entangled through the action of a laser.
2 Once they have been entangled, they are in an indeterminate state.
3 The qubits can then be separated by any distance, but they will remain linked.
4 When one of the qubits is manipulated—say, to perform a step in a quantum computer program—the manipulation happens instantly to its entangled twin as well.
5 If the manipulation includes reading the state of one of the qubits, the entanglement ends, and both qubits' states are revealed.

Fig.1.2

### *Need for Quantum computers*

- Quantum computers work on an atomic level that is roughly 200 times smaller than Intel's brand new 45nm architecture.
- Would be very useful in research and algorithm computation

### *Quantum teleportation*

- Quantum teleportation is a technique used to transfer information on a quantum level, usually from one particle to another.
- Its distinguishing feature is that it can transmit the information present in a quantum superposition, useful for quantum communication and computation.

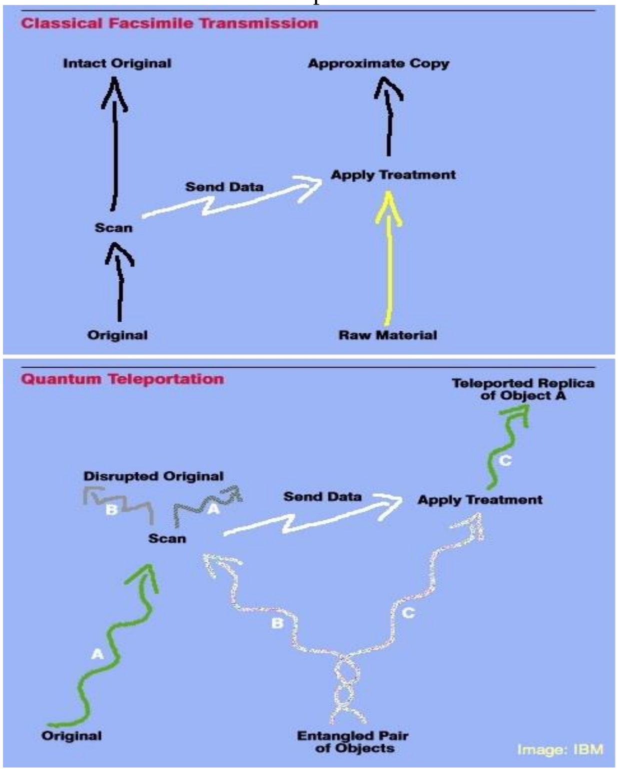

Fig.1.1

### *Representation of Data - Qubits*

A bit of data is represented by a single atom that is in one of two states denoted by **|0>** and **|1>**. A single bit of this form is known as a ***qubit***

A physical implementation of a qubit could use the two energy levels of an atom. An excited state representing |1> and a ground state representing |0>.

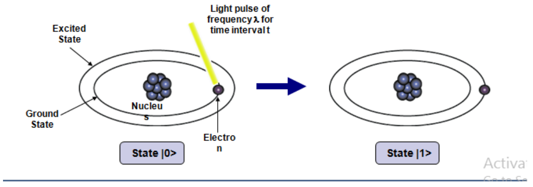

Fig.1.3

### *Future prospects*

- When processor components reach atomic scale, Moore's Law breaks down
  - Quantum effects become important whether we want them or not

But huge obstacles in building a practical quantum computer!

## III. BACKGROUND OF QUANTUM COMPUTER IV.

- **1982:-**Feynman proposed the idea of creating machines based on the law of quantum mechanics instead of the law of classical physics.
- **1985:-**David Deutsch developed the quantum turing machine, shwing that quantum circuits are universal.
- **1994:-**Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.
- **1997:-**Lov Grover develops a quantum search algorithms with O(√N) complexity.

## V. APPLICATIONS OF QUANTUM COMPUTER

1. **Cryptography:** Cryptography is a cornerstone of information security. It is used to encode and decode data in order to fulfill the requirement for confidentiality, integrity, authentication as well as non-repudiation. Together, these are frequently referred to as cryptography services.

Fig.1.4

2. **Artificial intelligence:** Over the past few decades, quantum effects have greatly improved many areas of information science, including computing, cryptography, and secure communication.

Fig.1.5

3. **Teleportation:** Quantum teleportation relies on something called an **entangled state**.

4. **Quantum communication:** In quantum communication via noisy channels, the error probability scales exponentially with the length of the channel. We present a scheme of a quantum repeater that overcomes this limitation.

## VI. SHOR'S ALGORITHM

Shor's algorithm shows (in principle,) that a quantum computer is capable of factoring very large numbers in polynomial time.
The algorithm is dependant on

- Modular Arithmetic
- Quantum Parallelism
- Quantum Fourier Transform

### Shor's Algorithm – Periodicity

- An important result from Number Theory:

F(a) = x mod N is a periodic function

- Choose N = 15 and x = 7 and we get the following:
- 7 mod 15 = 1
- 7 mod 15 = 7
- 7 mod 15 = 4
- 7 mod 15 = 13
- 7 mod 15 = 1

### Shor's Algorithm - In Depth Analysis

To Factor an odd integer N (Let's choose 15) :

1. Choose an integer $q$ such that $N < q < 2N$ let's pick 256
2. Choose a random integer $x$ such that GCD($x$, N) = 1 let's pick 7
3. Create two quantum registers (these registers must also be entangled so that the collapse of the input register corresponds to the collapse of the output register)
   - Input register: must contain enough qubits to represent numbers as large as q-1. up to 255, so we need 8 qubits
   - Output register: must contain enough qubits to represent numbers as large as N-1. up to 14, so we need 4 qubits

## VII. CONCLUSION:

To conclude the study, we found that the concept of quantum computers is upcoming concepts of high performance quantum computer. [1]Many research groups have discovered qubit and quantum computers as discussed in literature. Practical quantum computers are expected to give better results in comparison to classical computer that operates on a practically large number of qubits[2]. The research of quantum computer is very limited in literature and the concept is in its novel stage which requires more attention. This sector needs more architectural solutions or algorithms to advancement to make this concept usable in art for computational and logical reasoning [3].

## REFERENCES

[1] Devitt, Simon J., William J. Munro, and Kae Nemoto. "High performance quantum computing." *arXiv preprint arXiv:0810.2444* (2008).

[2] Fortnow, Lance. "One complexity theorist's view of quantum computing." *Theoretical Computer Science* 292.3 (2003): 597-610.

[3] Kanamori, Yoshito, et al. "A short survey on quantum computers." *International Journal of Computers and Applications* 28.3 (2006): 227-233.

[4] Beals, Robert, et al. "Quantum lower bounds by polynomials." *Journal of the ACM (JACM)* 48.4 (2001): 778-797.

[5] Steane, Andrew. "Quantum computing." *Reports on Progress in Physics* 61.2 (1998): 117.

[6] Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen, eds. *Post-quantum cryptography*. Springer Science & Business Media, 2009.

[7] Ambainis, Andris. "Quantum lower bounds by quantum arguments." *Proceedings of the thirty-second annual ACM symposium on Theory of computing*. ACM, 2000.

[8] Pavicic, Mladen. *Quantum Computation and Quantum Communication:: Theory and Experiments*. Springer Science & Business Media, 2007.

[9] Briegel, H-J., et al. "Quantum repeaters: the role of imperfect local operations in quantum communication." *Physical Review Letters* 81.26 (1998): 5932.