International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 12, Number 8 (2019), pp. 1191-1199

An Overview on Quantum Computing: The Next Generation in Computing Technology

[1]Chikodili H. Ugwuishiwu, [2]Jideofor Ujah, [3]Albert E. Egi

[1]Department of Computer Science, University of Nigeria, Nsukka, Enugu State, Nigeria.
ORCID of Author 1: 0000-0003-3166-6633

[2]Department of Computer Science, University of Nigeria, Nsukka, Enugu State, Nigeria.

[3]Department of Computer Science, University of Nigeria, Nsukka, Enugu State, Nigeria.

Abstract

Quantum computers have gained attention as the way forward in the advancement of computing speed and complexity. Quantum computer is the next generation of computers expected to overcome the limitations of today's largest computers. Theory behind quantum computing has proved that it will outperform the conventional classical computers in practice. In this article, the researchers x-ray the limitations of the classical computers that makes it no longer feasible to further advance its computational prowess. Studies was also carried out on the quantum phenomenon, its principles, features that gives it super computational prospects and a breakdown of its components. The researchers compared the quantum and classical computers and the state of research in both computers. Quantum computers show potential supremacy over supercomputers of today due to its superposition features that leads to quantum parallelism. When quantum is successfully built, the classical computers may be rendered outdated. However, reliability of a quantum computer remains a research focus and as it is still in the theoretical stage.

Keywords: Classical computing, superposition, quantum gate, quantum mechanics and entanglement

1.0 INTRODUCTION

According to Moore, classical computer has improved in computing power and speed since its inception by constantly decreasing the sizes of its distinct components [1]. Based on Moore's prediction in 1965, as the number of transistors on a chip continues to double on almost every twelve months, then the computational power also increases almost every two years [1]. The trend is from vacuum tubes to discrete semiconductor devices and now integrated circuits. Again, as the processing speed of a classical machine approaches 4GHz, the cost of cooling is no longer economical [2]. It has been estimated that integrated circuit transistor sizes will shrink to single-digit nanometre (one millionth of a meter) by the year 2019, that means that the transistor sizes will be reduced to the size of a few atoms each (A two-nanometre transistor may be about ten silicon atoms wide.)[1]. Therefore, the limits achievable under Moore's Law may be reached in just a few years. This means that the semiconductor industry will reach its limit that the transistors making the basic logic gates can no longer be reduced resulting to the inability to improve on the computational power of the Boolean-algebra-based computers. It follows that, at this point, which is estimated not to be too long, semiconductor-based computers will be rendered obsolete and physical properties of matter give way to the effects of quantum mechanics [3]. This gives birth to a new technology called quantum computing that will enable further enhancement on the computer performance.

A Quantum machines function at molecules level, or distinct atoms or ions and their elemental particles based on the theory of quantum physics [3][1]. As we continued to advance in technology, we create new computational problems. Examples are the modelling of molecular behavior, complex mathematical analysis among others. In 1982, Richard Feynman proposed the idea of using photons for computations, he conceived the idea of a quantum computer as a machine which will use the principles of quantum mechanics in solving computational problems [3][5][6].The notion of quantum computer was primarily of theoretical importance, however, recent research has bought the idea to everybody's attention. The theory of quantum physics enables the physical machine to concurrently compute a vast number of possibilities as though it were extremely parallel hardware performing some types of computation millions or even billions of times faster [1]. Quantum computers have a new type of hardware and a computational mechanism which are radically different from their classical counterparts, this implies that, both the hardware and software should be constructed based on the principles of quantum mechanics [5].

1.1 Brief History of Quantum Computing

In late 1970s and early 1980s, scientists started thinking of building computers based on the theory of quantum mechanics, since Moore's prediction is that silicon transistors must eventually result in devices no larger than a few atoms. The idea is that the device properties and behaviour on an atomic scale is governed by the principles of quantum mechanics, not classical (Newtonian) physics. This observation led researchers to wonder whether a new and completely different type of computer could be invented based on quantum principles. Paul Benioff, a scientist at the Argonne National Laboratory, is generally credited with being the first to apply the ideas of quantum physics to computers. Other scientists include Richard Feynman of the California Institute of Technology, who conceived the idea of a quantum computer as a simulator for experiments in quantum physics, and David Deutsch of the University of Oxford, who extended Feynman's idea and indicated that any physical process could, in theory, be modelled by a quantum computer. Deutsch's work was very important: His findings presented that it is possible to build a general-purpose quantum computer that is capable of solving problems that are impossible with the fastest supercomputers of today.

Section 2 discusses the principles of quantum computing; section 3 describes how a quantum computer works; section 4 deals with the implementation of quantum computer; section 5 explains common quantum algorithm; section 6 discusses the advances of quantum computing and finally, conclusion was discussed in section 7.

2.0 PRINCIPLES OF QUANTUM COMPUTING

2.1. Quantum Bit (qubits):

In the classical computer model, the most fundamental building block is the bit, it can only exist in one of two distinct states, a '0' or a '1'. This is not so with quantum computers, here, the rules are altered. Not only can a quantum bit (qubit) exist in the classical '0' and '1' states, it can be in a coherent superposition of both or a state with a certain probability of a being either '0' or '1'. When a qubit is in this state it can be thought of existing in two universes, (i.e.) as '0' in one universe and as a '1' in the other. An operation on such a qubit effectively acts on both values at the same time. The important point here, is that by performing a single operation on the qubit, we have performed the operation on two different values. Also, a two-qubit system would perform the operation on 4 values, a three-qubit system on eight. Therefore, increasing the number of qubits exponentially increases the 'quantum parallelism' we can obtain with the system [3]. The qubits exist in quantum Computer as photons or nucleuses of certain elements. In a quantum computer a qubit is directed into two distinctive spin directions, a spin up for 0 and spin down for 1 [7] as shown in fig 1. The first spin state represents |1> and the second represents |0> [7]. The essence of this distinctive spin is to ensure that data is demarcated properly when superposition and entanglement occur on the same qubit [8][9]. A quantum computer must be able to adept different internal states, have the means of necessary transformations on them and be able to generate an output of information. The correlations between the logical and physical state of the machine is arbitrary and requires interpretation. Information is represented directly as the common quantum state of many subsystems. Wherein each subsystem is described by a combination of two pure states interpreted as $|0\rangle$ and $|1\rangle$. This can be achieved by the polarization of a photon, or by the ground state and an excited state of an ion [5][10].

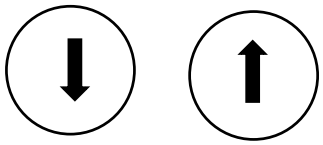

Fig 1: Two distinctive spin directions

2.2. Entanglement of states:

The one to one relation between logical and physical state in a quantum computer makes a quantum register containing more than one qubit to be impossibly described by listing the states of each qubit. In fact, the 'state of a qubit' is a meaningless term. Entanglement is the way energy and mass become correlated to interact with each other regardless of distance [5][9].

2.3. Reversibility:

To maintain a coherent state of computation, quantum registers must be kept isolated, to avoid entanglement with the environment. The entropy of the system has to be kept constant given that no dissipation of heat is possible, hence, state changes have to be adiabatic, requiring all computations to be reversible [2][9].

2.4. Initialization:

To set a quantum computer to the desired state Ψ, it suffices to provide means to initially 'cool' all qubits to |0) and then apply a unitary transformation μ which matches U|0) = | Ψ). One might think of μ as a base transformation which trivially exists for any desired | Ψ) [8].

2.5. Measuring states:

Measuring n qubits reduces the dimensionality of Ή by a factor of 2^n. The outcome of the measurement is biased by the probability amplitude for a certain bit configuration. The measurement of qubits is the only non-unitary operation a quantum computer must be able to perform during calculation [11].

2.6. Superposition:

This is a fundamental principle in quantum mechanics. It states that any two quantum states can be added together ('superposed) and the result will be another valid quantum state, and conversely every (except pure state) valid quantum state can be represented as a sum of two or more other distinct states [12].

All superposition of two quantum states of a system are not stable. If the superposition is to be stable, then there should be some sort of coherence between the two states that are being superpositioned. Such a superposition is called coherent superposition

Note that a pure state is one that cannot be represented as a sum of any two other quantum states [12]. In measuring that state of a quantum, only one of its constituent part can be measured at a time. Hence the probabilistic amplitude. The sum of the squares of the probabilistic amplitude of a quantum state should always be one. $a^2 + b^2 = 1$.

3.0. HOW DOES QUANTUM COMPUTERS WORK?

The basic unit of information that all classical computers store or process is a binary digit, or bit which may be grouped to form bytes or words, but all the basic combinational and sequential logic devices (gates, latches, flip-flops, etc.) operate on or store individual bits. The fundamental building block of a quantum computer is a quantum bit (qubit)[9] which entails that a quantum computer uses qubits for its computations [13].

Classical computers conform to the laws of classical physics, just like all other matters, Quantum computers conforms to the principle of quantum physics. Laws of quantum physics in most cases, results to effects that seems exceptionally against nature (classical physics). Experiments with photon beam splitting have proved the existence of quantum interference, which results from the superposition of the several possible quantum states. Based on theoretical physics, it may be said that subatomic particles do not have a certain existence like the macroscopic objects (a book is on a table or not). Instead, such a particle may be assumed to exist at a certain place and time with a certain probability. It has no certain existence or nonexistence (on the other hand, it both exists and don't exist) till it is observed, when the probability resolves to 1 (it exists) or 0 (it does not). The atoms and their subatomic particles in a quantum computer are basically used as processors and memories simultaneously. Though, there is only one set of some number of qubits in the computer, the quantum bits were not limited to be in only one state at a time as in the bits of binary register. A 3-bit binary machine can only take one of the eight states 000 through 111 at a time, a 3-qubit quantum register may be in all eight states at once in coherent superposition. With quantum parallelism, a set of n-qubits can store 2n numbers at once, and once the quantum register is initialized to the superposition of states, tasks can be executed on all the states at the same time. Therefore, addition of more qubits makes a quantum machine more powerful. Researchers are really exploiting in the world of quantum. While Google, IBM and D-wave systems are battling with creating stable quantum computers, Intel announced that they have found ways to fabricate quantum chips from silicon [14].

4.0 IMPLEMENTATION OF QUANTUM COMPUTERS

A quantum computer may be implemented using analog or digital approach. Just like the classical computer. The digital quantum computer has quantum logic gates as its building blocks.

Analog approach to implementation of quantum computer may take any of the following form: Simulation, quantum annealing or, Adiabatic Quantum computation [5].

4.1 Quantum Logic Gates:

Quantum digital computers are built using quantum logic gates [15][16]. Just as we have different types of logic gates in classic computers, there are various types of quantum logic gates. Quantum logic gates are represented as unitary matrices. Some of these are:

1. **Hadamard Gate:** This gate operates on a single qubit, it is denoted by the Hadamard matrix which is graphically given as $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
2. **Pauli-X gate:** This acts on a single qubit. It is the equivalent of the Classical NOT gate. And it maps |0) to |1) and |1) to |0). It is represented as $X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
3. **Pauli-Y gate**: While the Pauli-X equates rotation along the X-axis, this rotates in the Bloch sphere by II along the Y-axis. It maps |0) to i|1) and |1) to –i|0). It is represented as $Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
4. **Pauli-Z gate:** This gate equates a rotation around the Z-axis of the Bloch sphere by II radians. It is a peculiar case of the phase shift gate with O =II. It leaves |0) unchanged and maps |1) to -|1). It is represented as $Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
5. **Phase shift gate:** This leaves the basis state |0) unchanged and map |1) to $e^{i\Phi}|1)$. The probability of measuring |0) or |1) is unchanged after applying this gate. It is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by theta radians. it is represented as $R = \begin{bmatrix}1 & 0\\ 0 & e^{i\Phi}\end{bmatrix}$
6. **Swap Gate:** The swap gate performs half-way of a two-qubit swap. I is a universal in that many qubit gate can be constructed from only the swap and a single qubit gate,
$$\sqrt{SWAP}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0\\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$
7. **Controlled gate:** This acts on 2 or more qubits. In this case, one or more qubit acts as a control for some operation. It is represented as $U = \begin{bmatrix}U00 & U01\\ U10 & U11\end{bmatrix}$

4.2 The Quantum Computer Analyzed

4.2.1 Hardware Structure of Quantum Computing:

To aid in conceptualization, the hardware can be modelled in four abstract layers viz:

1. The "quantum data plane," where the qubits reside;
2. The "control and measurement plane," which carries out operations and measurements on the qubits as required;
3. The "control processor plane," responsible for determining the sequence of operations and measurements which the algorithm requires, potentially using measurement outcomes to inform subsequent quantum operations; and
4. The "host processor," which is a classical computer that coordinates access to networks, large storage arrays, and user interfaces. The host processor runs a conventional operating system/user interface, which facilitates user interactions, and has a high bandwidth connection to the control processor [4].

4.2.2 The Data Plane

The quantum data plane is the "heart" of a quantum computer. The data plane includes the physical qubits and the structures needed to hold them in place. It also must contain any support circuitry necessary to measure the qubits' state and perform gate operations on the physical qubits for a gate-based system or control the Hamiltonian for an analogue computer. Control signals routed to the selected qubit(s) sets the Hamiltonian it sees, and thus control the gate operation for a digital quantum computer. For gate-based systems, given that some qubit operations require two qubits, the quantum data plane must

provide a programmable "wiring" network that enables two or more qubits to interact.

4.2.3 Control and Measurement Plane:

The control and measurement plane of the quantum computer converts the control processor's digital signals, which indicates the quantum operations that are to be performed, to the analogue control signals needed to perform these operations on the qubits in the quantum data plane. It also converts the analogue output of measurements of qubits in the data plane to classical binary data that the control processor can work with.

4.2.4 Control Processor Plane and Host Processor:

The control processor plane captures, identifies and triggers the proper Hamiltonian or sequence of quantum gate operations and measurements (that are subsequently carried out by the control and measurement plane on the quantum data plane). These sequences execute the program, as provided by the host processor, for implementing a quantum algorithm. Programs have to be customized for the specific capabilities of the quantum layer by the software tool stack.

Building a control processor plane for large quantum machines is an area of ongoing research. One of the known approach is to split the plane into two parts. The first part is a classical processor, which "runs" the quantum program. The second part is a scalable customized hardware block that directly interfaces with the control and measurement plane, combining higher level "instructions" output by the main controller with the syndrome measurements to calculate the next operations to be performed on the qubits. The challenge is in creating scalable customized hardware that is fast enough and can scale with machine size. And also in creating the right high-level instruction abstraction.

4.3 Software Components of a qubit Computer

As an addition to creating the hardware functionality to support quantum computing, a functional quantum computer will also need extensive software components. This is analogous to the operation of classical computers, however, new and different tools are necessary to support quantum operations, including programming languages that enable programmers to describe QC algorithms, compilers to analyze the quantum codes and map them onto quantum hardware, and additional support for analysis, optimization, debugging, and testing of programs for implementation on specific quantum hardware. Prototype versions of some of these tools have been developed to support the QCs currently available on the web [17]. Ceteris paribus, these tools should be accessible to software developers without a background in quantum mechanics. The tools should offer abstractions that allow programmers to think at an algorithmic level with less concern for quantum details like control pulse generation. Lastly, the tools should in ideal circumstances enable programming of any quantum algorithm in a code that can translate to any target quantum architecture.

The software ecosystem for both classical and quantum computers includes the programming languages and compilers used to map algorithms onto the machine, and also much more than that. Simulation and debugging tools are necessary to debug the hardware and software (especially in situations where the hardware and software are developed concurrently); optimization tools are needed to help implement algorithms efficiently; and verification tools are required to help work towards both software and hardware correctness.

4.3.1 Operating Systems

The classical computer uses operating systems as the mother system upon which other software are built and embedded. This enables us to have a platform for programmers to build user end applications. Common Operating systems for Classical computers include Ubuntu, Windows, Apple, Andorid etc. Programing of the operating system is done with varieties of languages such as Java, C#, Python, C, Prolog etc.

The first Operating System, **t|ket>,** for quantum computer was developed in 2015 by Cambridge Quantum Computing Limited [18]. The Operating system comes with a compiler and a python toolkit. [19].The python toolkit enables programmers to interface with the operating system to develop programs.

4.3.2 Programming Language

Quantum programming languages are used to express quantum algorithms in high-level constructs. Quantum programming is the assembling of sequences of instructions, called quantum programs, with the capability of running on a quantum computer[20]. Contrary to a rather widespread belief that quantum computers have limited applications, the field of quantum algorithms has developed into an area of study large enough that a diverse sectors of economic industry are tapping into its potentials [21].

4.3.3 Algorithms

A core notion in the field of algorithms is in the principle that the total number of computational steps necessary to solve a problem is (roughly) independent of the underlying design of the computer. Remarkably to a first approximation what is designated, a single step of computation is a matter of convenience and does not affect or alter the total time to solution [4]. This basic principle is called the extended Church-Turing thesis. It shows that to solve a computational problem faster, one may

1. Reduce the time to implement a single step;
2. Perform many steps in parallel; or
3. Reduce the total number of steps to completion via the design of a clever algorithm.

Quantum computers do not violate the original Church-Turing thesis. Church-Turing thesis defines the limits of what is possible to compute at all (independent of time required to perform the computation) [4].

4.3.4 Debugging:

Debugging in an important aspect of programming. The use of breakpoints and interval analyisi of result is a core method of debugging. Methods to debug quantum hardware and software are of critical importance. Current debugging methods for classical computers relies on the memory, and the reading of intermediate machine states. Neither is possible in a quantum computer. A quantum state cannot simply be copied (due to the no-cloning theorem) for cross-examination, and any measurement of a quantum state collapses it to a set of classical bits, bringing computation to a halt. New approaches to debugging are essential for the development of large-scale quantum computers.

4.4 Quantum and Classical Computing

Table 1 shows the major differences between the quantum and classical computing.

Table 1: Quantum Verses Classical Computing

Description	**Classical Computing**	**Quantum Computing**
Information storage and representation.	Information is stored in bits which takes discrete value of 0 and 1. If storing one number takes 64bits, then storing N number s take N times 64 bits.	Information is stored in Quantum bits, qubits of qbits. A qubit can be in a state labelled |0} and \1}, but it can also be in a superposition of these states, a|0} + b|1}, where a and b are complex numbers, If we think of qubits as vectors, then superposition of states is just vector addition. For every extra qubits, you can twice as many numbers. E.g with 3 qubits, you get 8 new coefficients.
Delivery of information	Information can be copied without distributing.	Information cannot be copied without distributing
Behavior of information	Unidirectional	Multidirectional
Security	Hacker can break into communication	System is proposed to be more secure than any known process.
Noise Tolerance	Noisy channel can be used to deliver the information.	Noiseless channel is required.
Computation Cost.	Directly proportional to the computation	Not Directly proportional to the computation
Stability	Very Stable	Currently Unstable

4.4.1 Advantages in Quantum over Classical Computers

It has been established in 2018 that Quantum computer has computing advantages over Classical computer. The Shor's algorithm which is only available in quantum computing is said to just not have a classical equivalent yet. Some of the areas where Quantum Computing has prospects to outperform classical computing are:

Graphics (Modelling): Classical computing finds it hard to perform complex modellings, especially the behavior of chemical compounds [22]. Google was able to model the behavior of hydrogen molecule using quantum computer in 2016. Since then, IBM has also been able to model other molecules. It is believed that the actualization of a quantum computer will help in simulating new molecules for use in Medicine and can also be used to increase efficiency of Haber-Bosch process [23].

Mathematics: Quantum computer can be used to solve very complex mathematical problems in a very short time. This is

established in the Shor's algorithm which generates very large Prime numbers [6].

Search Functions: Grover's Algorithm can be used to reduce the number of queries that is being sent to the database. This speeds up the time taken to search the database and return result to the user [12].

Cryptography: Given the Shor's algorithm an encryption built on Prime numbers will be easily cracked by the quantum computer. This implies that such communication systems will no longer be considered encrypted once a quantum computer is used [24].

Encryption: There are no known examples or algorithm for this but it is expected that systems encrypted using a quantum computer will be more secure than those encrypted using a classical computer [25].

4.4.2 Advantages of Classical Computers over Quantum computers

Advantages of classical computers over quantum computers are as follows:

Simple Mathematical computation: Whereas the quantum computer is very good with complex computations, evidences show that the classical computer is faster with simple calculations such as addition of numbers and basic multiplication. As such it is safe to say that the Classical computer accelerates faster but has low computing ability while the Quantum computer accelerates slower but has high computing ability [25].

Cost: Most quantum computers that have been created are sold for tens of millions of US dollars. This is absurd given that such computers are not considered efficient. However, they are mainly for research purposes. However, the classical computer is available for as low as $100 USD [12].

Availability: Quantum computer are not in commercial production. Whereas the classical computer is available in all markets with different specifications.

Ease of Comprehension: The classical computer algorithm performs tasks which the human mind can also perform. The classical computer only outperforms humans in terms of accuracy and time of execution. As such, it is easier to understand how the classical computer operates. The quantum computer focuses on what the human hand cannot achieve, hence it is more difficult to understand its algorithm.

Ease of Programming: While there is only one known quantum programming language (QCL), there are many high level programming languages for the classical computer. This helps gives programmers a sense of choice and the ability solve numerous problem using a language of choice.

General Purpose: Most classical machines are used for general purpose tasks such as word processing, Internet, email, etc. However quantum computers by its nature are suitable for tremendously numerically rigorous calculations such as factorization of large integers.

5.0 COMMON QUANTUM ALGORITHMS

5.1 Shor's Algorithm

We study Peter Shor's Algorithm as presented in 1994. This algorithm is expected to be of help to the cryptography community [26][27]. One example is integer factorization using Shor's algorithm; it is composed of two parts; the first part alters the problem from finding the factor of a prime number to finding the period of the function. The second part of the algorithm is responsible for finding the period using the quantum Fourier transform. The problem can be assessed in five steps to deduce a prime factor of a given integer [28].

The algorithm is given as follows:

1. A random positive integer $m < n$ is chosen and the gcd (m, n) is calculated in polynomial time using the Euclidean algorithm. If $\gcd(m, n) \neq 1$, then a significant prime factor of n has been found and the problem is done. If $\gcd(m, n) = 1$, then proceed to step 2.

2. A quantum computer is used to deduce the unknown period P of the sequence.

x mod n, x2 mod n, x3 mod n, x4 mod n, ...

3. If P is found to be an odd integer, step 1 is repeated. If P is even, then proceed to step 4.

4. Since the period P is even,

$(m^{P/2}-1)(m^{P/2}-1)=m^{P}-1=0 \bmod n$

If $m^{P/2} + 1 = 0 \bmod n$, then step 1 is repeated. If $m^{P/2} + 1 \neq 0$, then proceed to step 5.

5. Finally, $d = \gcd(m^{P/2} - 1, n)$ is computed using the Euclidean algorithm. Since $m^{P/2} + 1 \neq 0 \bmod n$ was proven in step 4, it can be shown that d is a significant prime factor of n.

5.1.1 An Example

Below is an example of how n = 91(=7*13) can be factorized using Shor's algorithm

1. A random positive integer m = 3 is chosen since gcd(91,3) =1
   The period P is given by
   f(a)=3a mod 91
2. Shor's algorithm is used to find the period on a quantum computer to find the period P = 6.
3. Since the period P is even, we proceed to step 4.
4. Since the equation does not equal 0 mod 91, we proceed to step 5.
   $3^{P/2}+1=27+1=28\neq 0 \bmod 91$
   See below
5. $d=\gcd(3^{P/2}-1,91)=\gcd(33-1,91)=\gcd(26,91)=13$

Through careful calculation and the use of a quantum computer, the significant prime factor of d = 13 was found of n = 91.

5.2 Grover's Algorithm

Described in a paper published by Lov Grover in 1996, the eponymous algorithm solves the problem on unstructured search. Given a set of N elements for a set X = {x_1, x_2, x_3,…, x_n} and given a Boolean function f : X→ {0,1}, the goal is to find element x* in X such that f(x*) = 1. According to Grover, the algorithm solves this problem in O(/N) queries using quantum computation. This is possible because of the superposition feature of quantum computing [29] [30] [31].

The quantum operator, also called oracle, is defined as follows:

$|x\rangle \rightarrow |x\rangle$ (first register)

$|y\rangle \rightarrow |y \otimes f(x)\rangle$ (second register)

Then, we can write Grover's algorithm as follows:

Grover's Algorithm

(1) Initialize the first register in the superposition state:$(1\sqrt{N},1\sqrt{N},...,1\sqrt{N})$

(2) Repeat the following operation $O(\sqrt{N})$ times:

(a) Apply the quantum operator.

(b)Apply the matrix $Dij=-\delta ij+2\ 1/N$

(3) Measure the resulting state of the fist register.

6.0 ADVANCEMENT IN QUANTUM COMPUTERS

The ubiquity of research in quantum computing has not however yielded the much expected breakthrough since the maximum stability level that has been achieved by a true quantum computer is about 90 microseconds, decoherence sets into play almost immediately the quantum machine is set up [32]. The top researches in quantum machines are at Los Alamos, the University of Oxford Caltech, IBM, Los Alamos and National Laboratories. The latest quantum Computing produced available today is with a few qubits. In 1992, the first Quantum algorithm was proposed by David Deutsch and Richard Jozsa. It was called the Deutsch-Jozsa algorithm and was used to solve a proposed computational problem efficiently in quantum computer as against the classical computer [33].

In 1994, Peter Shor designed an algorithm that allows a quantum computer to factor large integers quickly. This algorithm solves both the factoring problem and the discrete log problem and had the potential of breaking most of the existing cryptosystems. This algorithm was first executed in 2001. The concept of factorisation has relevant application in the area of cryptography. Crypto systems such as Rivest, Shamir, and Adelman (RSA) exist today because classical computers are not able to factor large integers, thereby finding it very difficult to crack the RSA. RSA is the most commonly used Internet security and with the Shor's algorithm on quantum computer, one can crack into encrypted data and have access to the secured data. Hence, the existing method of encryption today may be rendered obsolete when the quantum computers become a reality. Quantum machines are capable of deploying codes that would encode information with much stronger encryption that today's fastest computer and the encryption cannot be cracked. Lov Grover introduced the quadratic speed up algorithm for quantum database search.

It was not until 1998 when a demonstration of quantum algorithm was possible [33]. The Deutsch problem was solved using a 2-qubit Nuclear Magnetic Resonance (NMR) quantum computer. This same year, a 3-qubit computer was used to execute Grover's algorithm. However, since the NMR, did not contain any entanglement, it is being debated if such quantum systems can offer quantum computational speedup. The quantum no-deleting theorem is established and 7-qubit NMR quantum computers were established in 2000[33]. In 2000, IBM produced a 5-qubits machine used to compute a single-step solution to an "order-finding" equation. To solve this on the classical computer, this must take several iterations. IBM also produced a 7-qubit quantum computer used to process Shors Algorithm. A few other scientist built intelligible quantum registers of 12 and 14 but these machines were not practically used showing that quantum computing research is still on the experimental level. David Deutsch predicted that 30 qubit quantum machine is required to have computing power of a10-teraflip classical machine.

D-Wave Systems manufactured and sold computers of high qubits that it claimed to be quantum computer. The blueprint for a quantum RAM was unveiled in 2007 as D-Wave systems demonstrated a 16-qubit quantum annealing computer, the same year, D-wave produced a 28-qubit machine. In 2011, the company demonstrated a 128 qubits followed by 512qubit in 2013 and D-Wave 2X (1000 qubits) in 2015. Researchers were doubting that the computers manufactured by D-wave were not actually quantum computers, though it might have certain quantum effects, but are not accomplished the expected speedup which is the focal aim of quantum computing research. The D-Wave machines cannot achieve those complex tasks (e.g. factorization of big number) that are not achievable in the classical computer.

Decoherence was suppressed in 2011[7]. In 2018, Robert Koining was able to create a quantum circuit that can solve a specific "difficult" algebraic problem which cannot be solved using classical constant-depth circuits. He proved that quantum computing outperforms Classical Computing [34]. Quantum processor were successfully produced in 2018. IBM makes its IBM Q System one Commercial in January 2019[35].

Quantum computers can also be used in areas such as include signal processing, answering differential equations, and large databases searching. Quantum computers by nature sees all data simultaneously, it could probably execute the same type of associative search with no additional cost of hardware. When the quantum computers actually exist, there is no doubt that it profits must be unlimited.

6.1 Some Challenges of a Quantum Computers

Quantum machines are difficult and costly to build. Researchers find it difficult to distinguish one or a few atoms from others for computations using methods including cavity quantum electrodynamics, ion traps nuclear magnetic resonance, and optical lattices), theory behind atom makes it difficult to achieve a steady state of an atom to manipulate its energy level or to observe the spin direction after other Features. To retrieve result after computation is one of the major challenges in having an actualised quantum machine. Furthermore, to measure an output of a quantum calculation is also a big challenge because interference with atom used for the computation may change the values of the result. Therefore, measurements on qubits must be made indirectly. One method is to cool the atom in the computer to a very low temperature (near absolute zero) [1]. This is a very expensive method and difficult to actualised.

Error correction is another problem that has hindered practical quantum machine due to decoherence. Decoherence occurs due to interaction with the surrounding is that destroy the atoms and decay the quantum state to an incoherent mixed state. This introduces error in computation and significant effort should be made to have a functional quantum computers.

7.0 CONCLUSION

While quantum computing has gained enough ground in modern research, there is still a long way to go in developing a viable quantum computer system. Google and NASA have been using the D-Wave to build their quantum computing hardware. It has been published that these quantum computers aren't actually conforming to the principles of quantum mechanics; they are compared to be the same as classical computers and in most cases, the quantum processor was found to be 100 times slower than a classical computer. It is observed that it is the superposition nature of quantum computer that distinguishes it from the conventional classical computer. The degree of research done so far indicates that we may have to wait for about a decade before we achieve a stable and viable quantum computer. This work educates new researchers in the field of quantum computer on the current status of quantum computing research and also identified some challenges encountered that contribute to non-realization of a reliable practical quantum computer. Research findings shows that the dynamic nature of molecules has made it very difficult to keep an atom and their subatomic particles in a stable state to be able to take the measurement or determine the state at that point in time. It is clear that scientist have a long way to go before a practical quantum is commercially available but it promises to be a wonderful future architecture if the challenges are overcome.

REFERENCES

[1] J. D. Dumas II, (2008). Computer Architecture: Fundamentals and Principles of Computer Design, Tailor and frances group, second edition, pp 279-385.

[2] B. Charles Y. L. Michael L. J. Apuzzo(2012). Quantum Computing: A Prime Modality in Neurosurgery's Future. World Neurosurgery Vol. 78, (5), pp 404-408. [online]. Available at https://doi.org/10.1016/j.wneu.2012.07.013

[3] Achintya A Paradkar, Vipul V. Joshi (2013). A report on Quantum Computing. International journal of Students in Technology & Management Vol 1(6), pp 627-634.

[4] Ashly Montaro [2016]. Quantum algorithms: an overview [online] Available at https://www.nature.com/articles/npjqi201523

[5] S. Akama (2015). Elements of Quantum Computing[online]. Available: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149203392.pdf

[6] Z. Hussain (2016). Strength and Weakness of quantum computing [online] Available: https://www.researchgate.net/publication/308414229_Strengths_and_Weaknesses_of_Quantum_Computing

[7] Robert Perkins (2011). Scientists take the next major step toward quantum computing. [online] Available at https://www.nanowerk.com/news/newsid=22174.php

[8] N. Drakos, R. Moore (1996). A procedural formalism for Quantum Computing [online] Available: http://tph.tuwien.ac.at/~oemer/doc/qcldoc/node4.html

[9] P. S. Menon, M. Ritiwik (2014). A comprehensive but not complicated survey on quantum computing [online] Available: https://www.sciencedirect.com/science/article/pii/S2212667814001178

[10] M. Ying (2009). Quantum Computation, Quantum Theory and AI [online] Available: https://ac.els-cdn.com/S0004370209001398/1-s2.0-S0004370209001398-main.pdf?_tid=6a6b29d8-1ddd-4371-a0ea-b73f297952d6&acdnat=1551878410_5776efccf043d1d7b4297906b8898a54

[11] N. A. Sinitsyn (2018). Computing with a single qubit faster than the computation quantum speed limit. Physics Letters A Vol. 382, (7), pp 477-481 [online] Available at: https://doi.org/10.1016/j.physleta.2017.12.042

[12] A. Majot, R. Yampolskiy (2015). Global catastrophic risk and security implications of quantum computers. Futures Vol. 72, pp 17-26. [online] Available at : https://doi.org/10.1016/j.futures.2015.02.006

[13] A. C. Thomas (2017). Quantum Computer Explained [online] Available: https://hackernoon.com/quantum-computing-explained-a114999299ca

[14] D. Krambeck (2015). Fundamentals of Quantum Computing [Online] Available: https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing/

[15] Wikipedia, (2018). Quantum logic Gates [online] Available https://en.wikipedia.org/wiki/Quantum_logic_gate

[16] Quantiki, (nd) Quantum gates [online] Available: https://www.quantiki.org/wiki/quantum-gates
[17] Peter Wittek [2014]. Quantum Machine Learning University of Boras, Sweden. DOI https://doi.org/10.1016/C2013-0-19170-2
[18] Rafia Shaikh [2015]. *First Quantum OS Brings Super-Fast Quantum Computing Closer to Reality* [online] Available at https://wccftech.com/operating-system-for-quantum-os-designed/
[19] CQCL[2019] Python toolkit for quantum [online] Available at https://github.com/CQCL/pytket
[20] Wikipedia [2019]. Quantum Programming Language [online] Available at https://en.wikipedia.org/wiki/Quantum_programming
[21] M.D. Purkeypile(2009). Cove: A Practical Quantum Computer Programming Framework, PhD thesis, Colorado Technical University, Colorado Springs, USA.
[22] Matthias M ̈oller, Cornelis Vuik (2019). A Conceptual Framework for Quantum Accelerated Automated Design Optimization. Microprocessors and Microsystems
[23] Intel (2018). Intel Sees Promise of Silicon Spin Qubits for quantum computing[online] Available: https://newsroom.intel.com/news/intel-sees-promise-silicon-spin-qubits-quantum-computing/#gs.QGRXw7gD
[24] K. Keplinger (2018). Is quantum computing becoming relevant to cyber-security? Network Security Volume 2018, Issue 9, September 2018, Pages 16-19 [online] Available: https://doi.org/10.1016/S1353-4858(18)30090-4
[25] A. Ho, J. McClean, S. P. Ong (2018). The Promise and Challenges of Quantum Computing for Energy Storage. Joules Volume 2, Issue 5, 16 May 2018, Pages 810-813. [online] Available at https://doi.org/10.1016/j.joule.2018.04.021
[26] B. Auburn (2019). Quantum computing- A means to perfect security? SANS Institute Information Security Reading Room. [online] Available: https://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986
[27] R. Orús, S. Mugeld, E. Lizaso (2019) Quantum computing for finance: Overview and prospects. Reviews in Physics Volume 4, November 2019, 100028
[28] Peter W. Shor (2001). Introduction to Quantum Algorithm [online]. Available: https://arxiv.org/pdf/quant-ph/0005003.pdf
[29] Wikipedia (2018). Grover's Algorithm. [online]. Available at: https://en.wikipedia.org/wiki/Grover%27s_algorithm
[30] J. Hui, (2018). QC- Grover's Algorithm [online] Available: https://medium.com/@jonathan_hui/qc-grovers-algorithm-cd81e61cf248
[31] J. Wright, (2015). Lecture 4: Grover's Algorithm [online] Available: https://www.cs.cmu.edu/~odonnell/quantum15/lecture04.pdf
[32] Scott Fulton (2008). What a quantum computer is, and why it needs to be more [online] Available at https://www.zdnet.com/article/what-a-quantum-computer-is-and-why-it-needs-to-be-more/
[33] Wikipedia (2019). IBM Q System One. [online] Available at https://en.wikipedia.org/wiki/IBM_Q_System_One
[34] Munich, Germany (2018). First proof of quantum advantage (2018). http://www.spacedaily.com/reports/First_proof_of_quantum_computer_advantage_999.html
[35] Wikipedia (2019). Timeline of quantum computing. [online] Available at https://en.wikipedia.org/wiki/Timeline_of_quantum_computing#cite_note-151