QUANTUM COMPUTING – NEXT GENERATION COMPUTING TECHNOLOGY – A GENTLE INTRODUCTION

Abstract

The limitations of traditional CMOS-Technology for bulk and high-performance computing applications may be solved by quantum computing. More scholars are turning to this topic as a result of its potential to change the modern computing industry. However, because quantum aspects are involved, many newcomers find it challenging to understand the field. Therefore, an effort has been made in this research note to introduce researchers, quantum engineers, and scientists to the many features of quantum computing research, quantum scientists and engineers. The historical context and fundamental ideas required to comprehend quantum-computation and processing of information have been clearly introduced. This paper also discusses various quantum computing physical implementations and prospective application domains.

Keyword: Qbits, Quantum Mechanics, Quantum Gates, Classical Computing, Quantum Computing

Authors

Prabhash Kumar
Database and Infrastructure Architect
Bangaluru, Karnataka, India
prabhash@eywrnd.org.in

Dr. Shailaj Kumar Srivastava
Principal
Anugrah Memorial College
Gaya , Bihar, India
shailajshri68@gmail.com

Dr. Narendra Kumar
Assistant Professor
Department of Computer Application and Information Technology
A. M. College
Gaya, Bihar, India
nar.electron@gmail.com

Dr. Ajay Kumar Singh
Associate Professor
Department of Physics
A. M. College
Gaya, Bihar, India
amcphysicsas@gmail.com

Dr. Neeraj Kumar Kamal
Assistant Professor
Department of Physics
A. M. College
Gaya, Bihar, India
neeraj.arnold@gmail.com

I. INTRODUCTION

The term "quantum computing" connotes a system that computes outputs using quantum mechanics. The tiniest distinct unit of any corporeal (Physical) attribute is known in physics as a quantum. The majority of the time, it alludes to the characteristics of atomic or sub-atomic particles like photons, electrons, neutrinos, etc.. Quantum bits, or qubits, are used in quantum computing. It takes advantage of sub-atomic particles' special capacity to exist in several states such as 1 and 0 exist concurrently. The study of quantum computing focuses on finding new ways to compute by utilizing quantum physics phenomena. Qubits make up quantum computing. Either I or 0 or superposition of both of them can be a Qubit. When compared to supercomputers and conventional computers, quantum computers are many times quicker. The supercomputers are based on two aspects of quantum physics: superposition and entanglement. This enables quantum computers to do processes at speeds that are exponentially faster than those of traditional computers while consuming significantly less energy.

There are some fundamental aspects of quantum physics. These are:

1. **Superposition:** A quantum system can have numerous states at once thanks to superposition. The standard illustration of superposition is coin flip, which always results in either heads or tails—a fairly binary idea. But while the coin is in the air and up until it touches the ground, it is simultaneously heads and tails. The electron is in quantum superposition prior to measurement.

2. **Entanglement:** As a quantum property, entanglement connects items by keeping them bound together indefinitely. A 50-cubit quantum machine may study $\mathbf{2^{50}}$ states at once when an extra qubit is added to it. Quantum computers are able to solve issues quickly and with a great deal less calculations thanks to the rise in power and qubit entanglement.

3. **Interference:** Interference is used to manipulate quantum states, increase signals pointing in the proper direction, and suppress signals pointing in the wrong direction.

4. **Coherence and De-coherence:** Quantum computers are particularly susceptible to noise and other influences in terms of coherence and de-coherence. Unfortunately, quantum state of information is finite. There are only so many processes that can be carried out prior to the data being lost It is essential to be aware of how long will quantum information persist before losing coherence.

   To establish superpositions, qubit entanglement, and retention for as long as possible, quantum circuits must be maintained at temperatures lower than those in space. It is possible to communicate with qubits that are housed inside a dilution refrigerator by applying calibrated microwave pulses that superposition the qubit or flip its state from 0 to 1 by passing a microwave pulse between two qubits.

   Quantum computing is a herculean task, a real challenge and a genuine potential field of Physics and IT. Undeniably, based on what we now as of now, the underlying nature of our physical universe is quantum mechanical. Real computations are physical processes performed on physical equipment, which includes all computers. Therefore, its a basic challenge, it is our duty to investigate the possibilities, rules, and constraints of quantum physics in order to carry out information processing and communication.

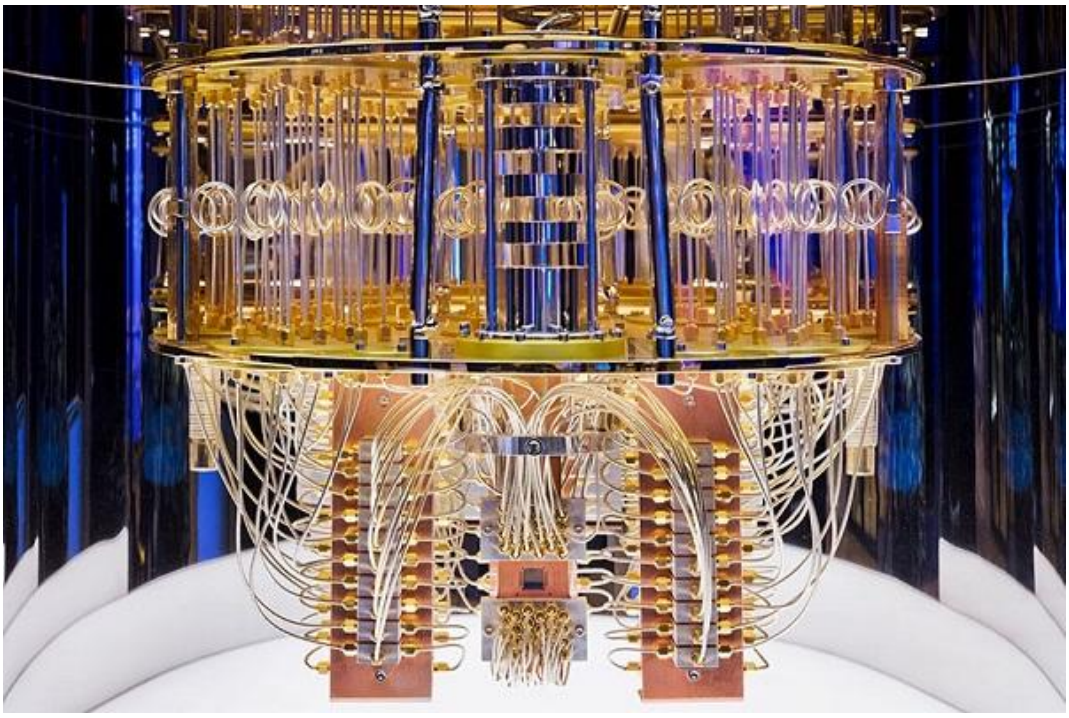
Beyond the doubt, one of the trendiest issues in computing today, if not the entire field of science, is quantum computing. It looks really promising and has an alluring sound. Before we begin to investigate the ideas and fundamentals, as well as the mystique and prospective of quantum computing, there are a few obvious fundamental questions to ask. There appears to be no end in sight to the tremendous progress being made in the development of traditional computers. Additionally, it appears that quantum computer design is highly dubious and virtually certainly extremely expensive. Even though it is rarely stated directly, all the classical computers and computer models are based on classical physics, making them insufficient in high-performance processing. Classical computing is working well, but they don't seem to completely utilize the physical world's capability for processing information. Although they are beneficial and effective, they must not be considered as representing our whole understanding of information processing systems.

The Church-Turing thesis' contemporary, efficiency-focused iteration is also shown to be facing its first significant challenge from quantum computation, according to theoretical results. There are already results that show conclusively that quantum computers are hypothetically exponentially more powerful than conventional computers for some significant practical challenges.

Quantum parallelism, complex probability amplitudes, quantum entanglement, quantum interference and the unitarity of quantum evolution are a few examples of quantum phenomena and laws that are fundamentally distinct from those found in classical computing and underpin the power of quantum computing. One needs to understand a number of fundamental principles upon which quantum mechanics is based, as well as the fundamentals of Hilbert space formalism, which serves as the mathematical framework for quantum mechanics, in order to comprehend these features and use them to design quantum algorithms, networks, and processors.

The current status of quantum computer is restricted with the IT giants only and still it is a big dream to have a commercial Quantum Computer. Some examples of real quantum computers are:

1. **Sycamore (53 QB)** – Developed by Google in the year 2019
2. **Tangle Lake (49 QB)** – Developed by Intel in the year 2018
3. **D-Wave 2000Q (2048 QB)** – Developed by D-Wave in the year 2017
4. **D-Wave Advantage (5760 QB)** – Developed by D-Wave in the year 2020
5. **IBM Eagle (127 QB)** – Developed by IBM in the year 2021
6. **Borealis (216 QB)** – Developed by Xanadu in the year 2022



Source: Google

Figure1: Google's Quantum Computer

II. BACKGROUND

Since 1945, we have seen a sharp increase in the speed and memory capacity of computers, as well as their overall raw performance. The creation of transistors, which already make use of some quantum property in their operation, was a significant milestone in this progression.

However, it is evident that if the performance of computers persists to rise at this rate, our processors will need to have 1016 gates and run at a clock rate of 1014 Hz to offer 1030 logic operations per second after 50 years. The only way to do that, it would appear, is to develop the ability to construct computers solely on the principles of quantum physics.

A number of conceptual obstacles have to be surmounted in order for the concept of quantum based information processing to be taken seriously and progress so quickly. The most fundamental one dealt with reversibility, a crucial aspect of quantum physics. All existing universal computer models were irreversible. Bennett (1973) was the first to break through this barrier by demonstrating the existence of universal reversible Turing machines.

Benioff(1980, 1982, 1982a), who demonstrated that quantum-mechanical computational processes can be more powerful than that of classical computational processes, and hence overcame the second intellectual handle. He accomplished this by demonstrating the ability of a quantum system to mimic the operations of classical and reversible Turing machines. His "quantum computer" could not, however, outperform classical ones since it was not yet totally quantum. The repercussions of overcoming these fundamental intellectual obstacles were enormous and far-reaching. A more comprehensive and in-depth investigation into the connections between physics and computation has begun. Reversibility results revealed the theoretical viability of zero-energy computing, which has also contributed to this.

Lack of a suitable model for a functional universal quantum-computing device that could accurately simulate any other quantum computer constituted the third conceptual hurdle that needed to be surmounted. By expanding on Feynman's ideas and creating a quantum-physical analogue of a probabilistic Turing machine that fully exploits the quantum superposition principle and produces a random sample from a probability distribution for any given input, Deutsch (1985) took the first step toward overcoming this barrier. The awareness of the dangers and incomplete understanding of quantum computing has also been aided by quantum cryptography. Through their contributions, Cirac and Zoller were able to get beyond another conceptual hurdle (1995). They demonstrated it in the search for technology to create quantum processors, at least on a laboratory scale.

III. Understanding QUBITS

A quantum bit, or qubit, is the binary digit or bit of classical computing’s quantum counterpart. A qubit is the fundamental informational building block of a quantum computer, just as a bit is in a classical one. Any bit made from a quantum system, such as an electron or photon, is referred to as a quantum bit. A quantum bit must have two different states, one representing "0," and the other representing "1," much like classical bits.

Each qubit measures around 0.2 millimeters across, making them large enough to be seen under a standard microscope. Two bits can be represented by one qubit. Four-bit values can be represented by two qubits. n qubits can typically take values between 0 and 2n. Data "bits" are units of storage in traditional computers that consist of a string of 1s and 0s. However, "qubits" in a quantum system are kept in "superposition state" where they can be both 1 and 0, allowing them to carry out several calculations at once.

1. **2D representation:** We are entirely unable to know the state of a Qubit until we measure it properly. The process of measuring a qubit, however, changes its state from one of 0 to 1 (inclusive), where it always exists. An image of a qubit is a complex vector of size 2.

   Typically written as:

   $$\begin{bmatrix} \alpha \\ \\ \beta \end{bmatrix}$$

   Where **α** and **β** representing height of the signal, i.e., amplitudes, indicating the two states 0 an 1 respectively. It’s a probability between 0 and 1.

   The vector can be normalized as:

   $$[\alpha]^2 + [\beta]^2 = 1$$

The state (0) can be represented as:

$$\begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix}$$

While state (1) is represented as:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

The quantum states |0> and |1> combine to produce orthogonal basis, also known as computational basis or canonical basis.

2. **Dirac's Notation:** It is a simplified way to represent a qubit. A ket is used to represent a vector.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

In dual form, we may also write:

$$|0\rangle = [1 \quad 0] \text{ and } |1\rangle = [0 \quad 1]$$

Hence, the arbitrary state will be:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Or

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

3. **Bloch's representation:** A point on the unit sphere is referred to as the Bloch sphere in geometry to represent pure single-qubit states. The Bloch sphere can be used to represent common quantum information processing operations on single qubits. The orthonormal computational basis states |0⟩and |1⟩ are defined as the north and south poles of the Bloch sphere, respectively, and an arbitrary single-qubit pure state, up to the global phase, is represented by a point on the unit sphere, linking the superposition of the basis states to the angular coordinates of the point. Any unitary operation transforming a single-starting qubit's state into its final state is comparable to composing one or more straightforward rotations on the Bloch sphere.

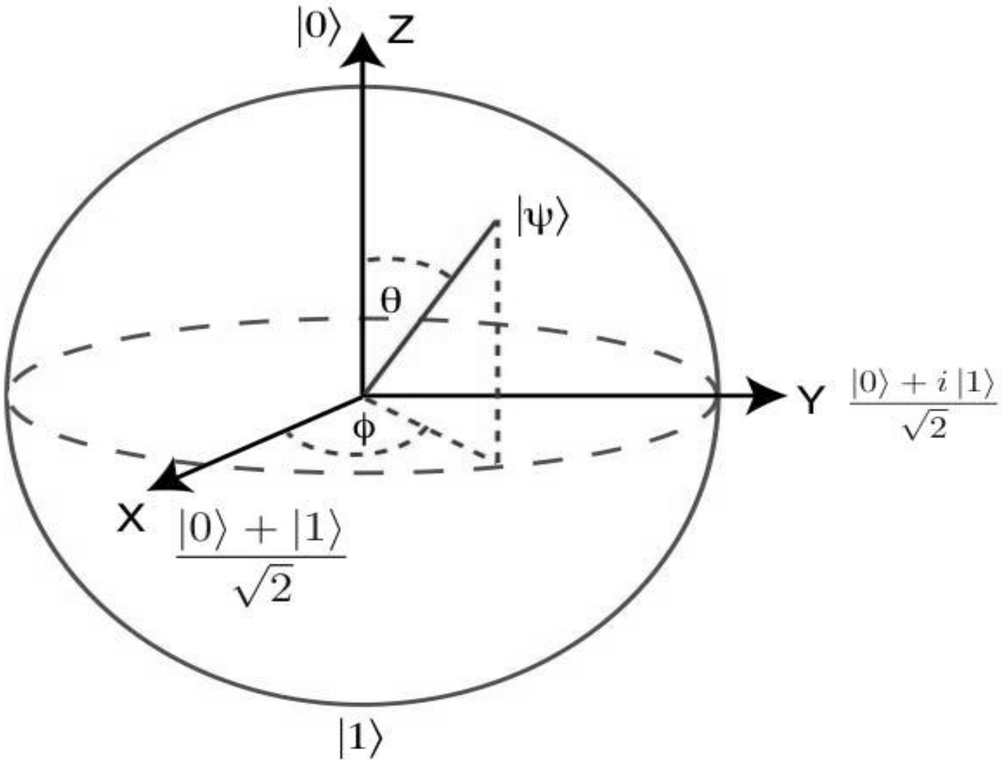


Figure 2: Bloch Sphere Representation of Qubit Glosser.ca, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

IV. QUANTUM GATES

An elementary quantum circuit that uses a few qubits is known as a quantum gate. Also known as quantum logic. They serve as the analogues of classical logic gates in traditional digital computers for quantum computers. To the contrary of many conventional logic gates, quantum gates are reversible. Some global classical logic gates offer reversibility and can be directly transferred onto quantum logic gates, for example, the Toffoli gate. Unitary matrices are used to depict quantum logic gates.

The first silicon-based quantum-logic device has been disclosed by scientists in Australia and Japan. They used standard semiconductor manufacturing techniques to create CNOT gate, which is considered most crucial part of a quantum computer. The technology will now be scaled up by the researchers in order to produce a complete quantum-computer chip.
Some quantum gates are briefly summarized below:

1. **Hadamard gate:** A Hadamard Gate can be used to put a qubit in superposition. This is the function of the gate in quantum computing. When a single qubit enters the gate, it is in both states, i.e., 0 and 1 as shown in Fig. 3.

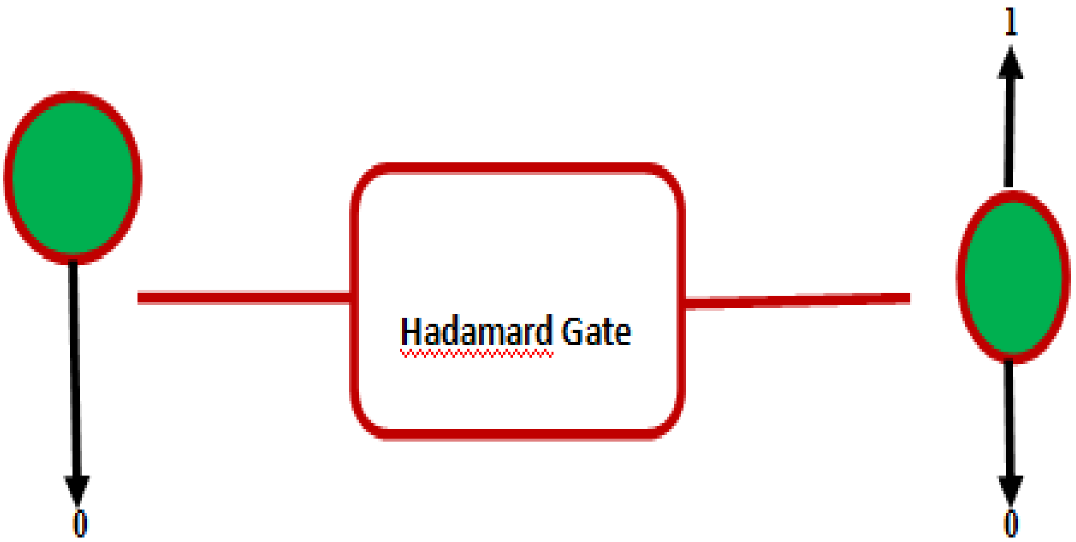
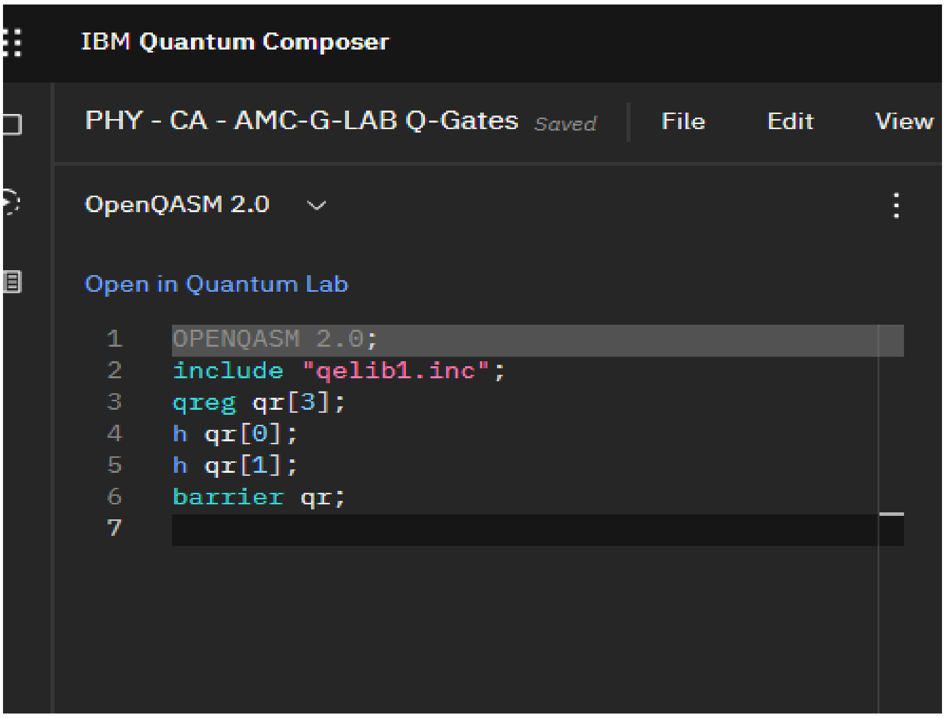


Figure 3: Bringing qubit in superposition state using Hadamard Gate

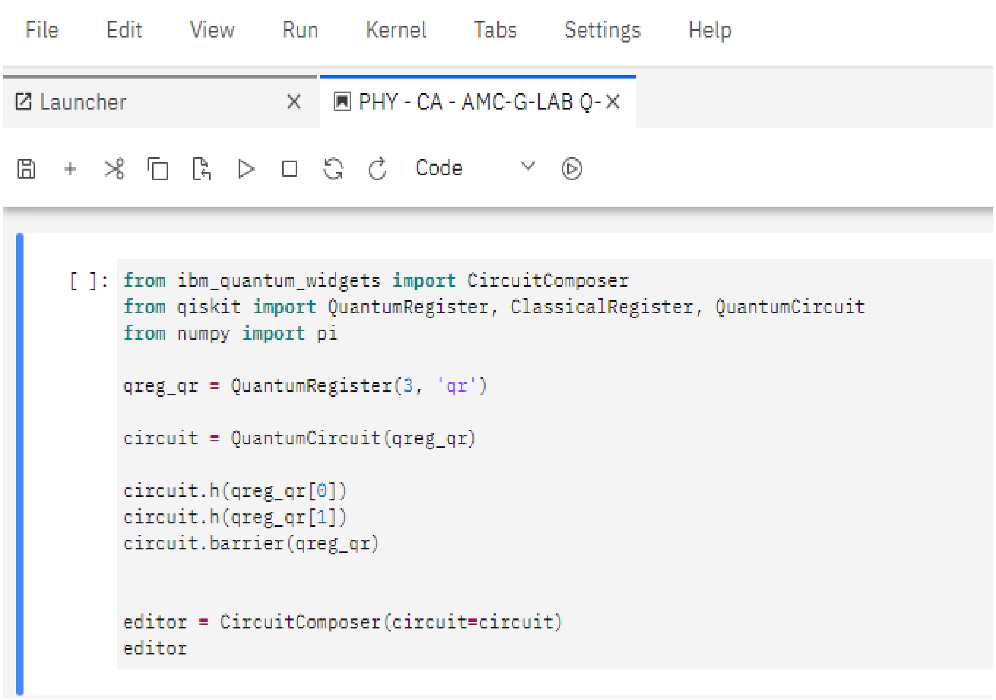
Here is an example of practical Hadamard gate approach using IBM Quantum Composer with OpenQSAM programming language.



```
OPENQASM 2.0;
include "qelib1.inc";
qreg qr[3];
h qr[0];
h qr[1];
barrier qr;

```

Figure 4 (a): Quantum Composer



```
from ibm_quantum_widgets import CircuitComposer
from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
from numpy import pi

qreg_qr = QuantumRegister(3, 'qr')

circuit = QuantumCircuit(qreg_qr)

circuit.h(qreg_qr[0])
circuit.h(qreg_qr[1])
circuit.barrier(qreg_qr)


editor = CircuitComposer(circuit=circuit)
editor
```

Figure 4 (b): Source Code on IBM Quantum Lab

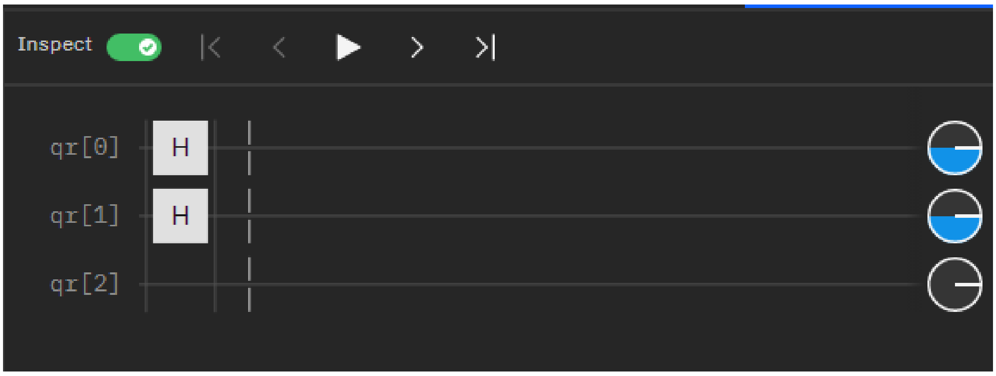


Figure 4 (c): Circuitry of Hadamard Gate

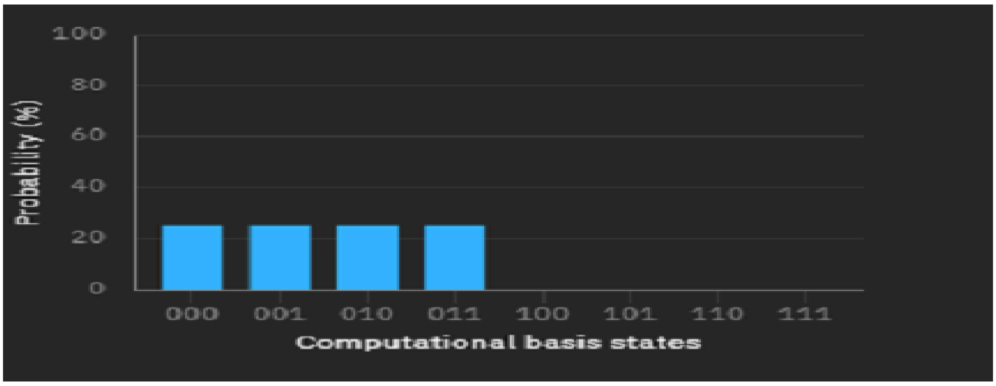


Figure 4 (d): Probabilities

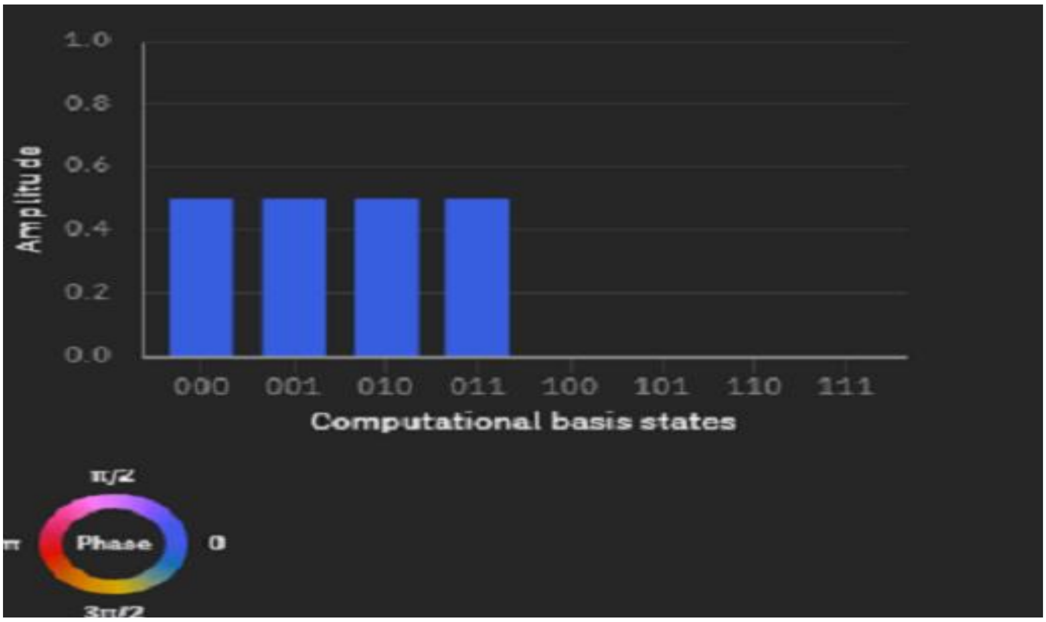


Figure 4 (e): State Vector of Hadamard Gate

Below is the output state of above configuration: [1+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j]

2. **Pauli Gates:** The Pauli gates, i.e., X, Y and Z Gates, are three different Pauli Matrices that operates on a single bit. Some of the most often used quantum gates can be represented using Pauli matrices. The Pauli-X gate, when compared to the standard basis that separates the z axis on the Bloch sphere, is the quantum counterpart of NOT gate in classical computing.

   - **X – Gate**
   - **Y – Gate**
   - **Z – Gate**

   These corresponding Pauli matrices are usually represented as

$$X = \sigma_X = \mathrm{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

3. **CNOT Gate:** It's a two bits operation. The first qubit in the CNOT gate is generally referred to as the control qubit, and the second qubit is usually termed as the target qubit. When the control qubit is in state |1⟩, the CNOT gate carry out a Pauli-X gate on target qubit while leaving the control qubit intact, and if the control bit is in |0⟩ state, leaves the target qubit unaffected.

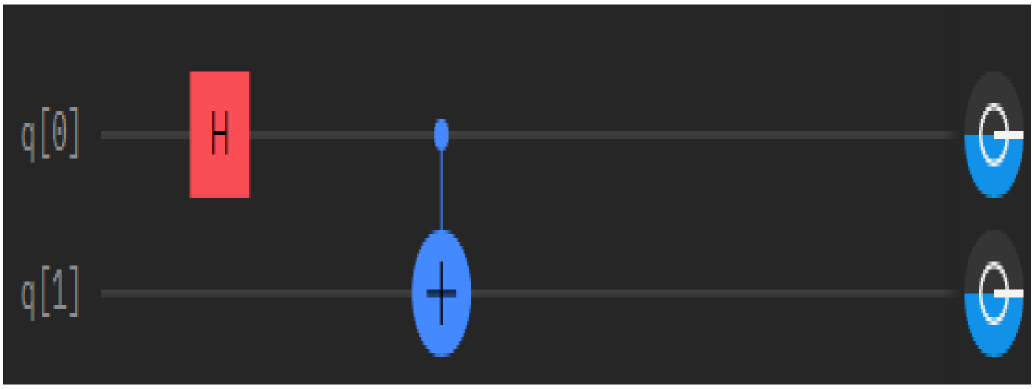


Figure 5 (a): CNOT Gate Operation

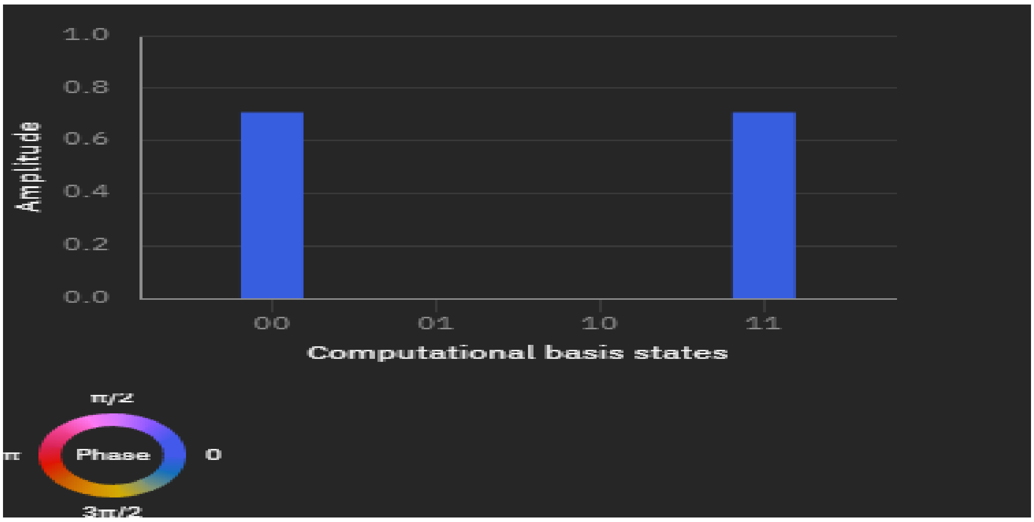


Figure 5 (b): State vector of C – NOT Gate

4. **P-Gate:** This is a parameterized gate and hence it requires a number (ϕ) to instruct it precisely what to do. Around the direction of the Z-axis, the P-gate rotates ϕ (A real number). The matrix form of P-Gate is given below.

$$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{ei}\varphi \end{bmatrix}$$

Besides above mentioned quantum gates, there are various other quantum gates, such as, I-Gate, S-Gate, T-Gate, U-Gate, etc, that can be used to design quantum operations.

V. APPLICATION AREAS

There are abundant application area of Quantum Computing and Information Processing. It can offer a number of applications to the advance industrial applications, it can be applied to AI and ML, cryptography, health sector, weather forecasting, cyber security, computational chemistry, machine design, medicine development and invention, solar panel design, etc. A variety of intelligent tasks are waiting for the quantum system. The IT industry could be a massive user of quantum system throughout its cloud environment. The datacenters will also be a giant user of quantum information system. Complex problems in mathematics, physics and chemistry, genetic engineering, bio-technology and medicine could enjoy manifold development for the interests of the human society. The information processing offered by the quantum computing will imprint enormous growth while reducing the cost of service.

VI. BOTTLENECKS

The parallelism that quantum computing can offer is immense. Harnessing the power of quantum parallelism, however, also poses significant challenges. A (projection) measurement procedure can only extract one classical result from a (big) quantum superposition, and the other quantum data is subject to irreversible destruction, according to the fundamentals of quantum physics. The so-called de-coherence effects are caused when a quantum system interacts with its surroundings, and they have the power to significantly alter or even destroy tiny quantum interference systems. Long dependable quantum computations seem to be basically unattainable as a result.

VII. CONCLUSION

In light of the aforementioned findings and discussion, the article offers a broad overview of the development of quantum advances as well as specific inclinations for quantum computing. Recent years have seen an exponential growth in quantum research. Global companies including IBM, Microsoft, Intel, D-Wave and Google fiercely compete for quantum computing. In terms of quantum computing research, the United States, China, and Germany are now the three leading countries. We catalogued the quantum computer structure squares, the most recent research findings on the practical use of quantum computers, and potential applications. This paper also discusses various quantum computation physical implementations and prospective application domains.

Quantum computing requires significant research and expenditure, but the good news is that big businesses and governments are putting money into projects to advance the development of practical quantum computing. By modifying the fundamental nature of information, quantum information processing creates new opportunities for computers, networking, and communications. It is merely a matter of time before a practical quantum computer is built.

REFERENCES

[1] Gate Types in Quantum Computing: Hadamard, Controlled & CNOT. (2021, November). Retrieved from https://study.com/academy/lesson/gates-types-in-quantum-computing-hadamard-controlled-cnot.html.
[2] R. P. Feynman (1982), “Simulating physics with computers,” *Int. J. Theor. Phys.*, vol. 21, no. 6, pp. 467–488,
[3] Hyun Cheol Koo *et al.(2009)*, “Control of spin precession in a spin-injected field effect transistor,” *Science*, vol. 325, pp. 1517–1519.

[4] M. A. Nielsen and I. L. Chuang (2000) – *Quantum Computation and Quantum Information*. Cambridge University Press.
[5] A. Peres (2000) – Reversible logic and quantum computers. *Physical review*, (32):3270–3277.
[6] Chris Lomont (July 2003) Quantum circuit identities.
[7] D. M. Miller et al (2003), Spectral techniques for reversible logic synthesis. In *Proc. RM*, pp., 58–61.
[8] https://vector.me/browse/280210/qubit_bloch_sphere
[9] https://physicsworld.com/a/silicon-quantum-logic-gate-is-a-first/