Prabha Materials Science Letters
Vol. 4, No. 2, 235-258, 2025
https://doi.org/10.33889/PMSL.2025.4.2.020

Ram Arti Publishers

# Quantum Computing-The Underlying Principle Behind it

**Ansh Chawla**
Department of Artificial Intelligence and Machine Learning,
Vivekananda School of Engineering and Technology, Pitampura, Delhi, India.
*Corresponding author*: anshchawla.a1@gmail.com

**Sankalp Mathur**
Department of Artificial Intelligence and Machine Learning,
Vivekananda School of Engineering and Technology, Pitampura, Delhi, India.
E-mail: sankalpmathur4@gmail.com

**Harshit Rao**
Department of Artificial Intelligence and Machine Learning,
Vivekananda School of Engineering and Technology, Pitampura, Delhi, India.
E-mail: harshitrao5698@gmail.com

**Naman Mudgal**
Department of Artificial Intelligence and Machine Learning,
Vivekananda School of Engineering and Technology, Pitampura, Delhi, India.
E-mail: nmnmdgl@gmail.com

**Vanita Bhardwaj**
School of Engineering and Technology,
Vivekananda School of Engineering and Technology, Pitampura, Delhi, India.
E-mail: vanita.bhardwaj@vips.edu

(Received on March 30, 2025; Revised on July 1, 2025; Accepted on July 17, 2025)

**Abstract**
Computers have become an indiscipline part of our lives nowadays due to their versatile uses. The advent of computers took place due to the need of efficient mathematical computations. Solving complex problems and running complex algorithms requires powerful processors. Even these powerful processors come with a few limitations and fail to solve problems like simulation of atoms and molecules, solve multi-dimensional computational spaces. This aroused the need for even more efficient and powerful computing systems leading to the rise of quantum computers. The quantum computers are based on laws of quantum mechanics which allows them to leverage the benefits of various principles like Superposition, Coherence, Entanglement. The Quantum computers use qubits unlike bits which are used in computers and can explore multiple states parallelly thereby decreasing computation time exponentially. Multiple domains and fields will benefit from the usage of quantum computing like medicine, finance, logistics, artificial intelligence, and weather forecasting, ushering in a new era of scientific discovery and technological advancement. The paper provides insights into the developments of quantum computing, its underlying principle and the potential it holds.

**Keywords-** Quantum computing, Qubit, Superposition, Entanglement.

## 1. Introduction

Computers have become an indiscipline part of our lives nowadays due to their versatile uses. The advent of computers took place due to the need of efficient mathematical computations. As the technologies advanced and discovery of semiconductors occurred, the computers evolved significantly. The discovery

of semiconductors allowed for first revolution within the computers by switching from Cathode Ray Tube (CRT) (Ozawa & Itoh, 2003; Rajaraman, 2020) based computers to transistor-based computers. Computers began to come in compact sizes. This allowed the computers to become easily available to public.

The classical computers were being built using transistors and worked on digital logic i.e. 0 or 1. Our surroundings resemble the quantum systems and obey the laws of quantum mechanics. Thus, the computational power of the computer seemed limited. As faster, better and efficient algorithms were developed to solve our problems, the demand for more accurate solutions increased rapidly. Real world problems are extremely complex and keep varying thereby handling them on a classical computer produces unsatisfactory in many cases. This led to the need for further advancement in the computer technology. As the power of computer seemed to reach its limits, the field of quantum mechanics opened the gateway for a new discovery - Quantum computers (Ladd et al., 2010). Quantum computers are a recent advancement in the field of computer science. Unlike the classical computers which work on digital logic, these computers are based on laws of quantum mechanics. The classical computers store the data in the form of bits either 0 or 1; on the other hand, the quantum computers use qubits and stores the state of the data. The quantum computers have widened the scope of computers and increased its computational power manifold as they consider the ever-changing factors of the environment. **Table 1** mentions the key differences between classical computing and quantum computing.

**Table 1.** Difference between classical computing and quantum computing.

| Feature | Classical computing | Quantum computing |
|---|---|---|
| **Usage** | Used by versatile, everyday computers and devices | Used by high speed computers based on quantum mechanics |
| **Information Storage** | Stores information as bits (0 or 1) | Stores information as quantum bits (qubits) |
| **Possible states** | Has a limited number of distinct states (0 or 1) | Has an infinite, continuous range of possible states |
| **Calculations** | Performs deterministic calculations with predictable outputs | Performs probabilistic calculations with multiple potential outputs for the same input |
| **Data Processing** | Processes data using logic in a step-by-step sequence | Processes data using quantum logic in a parallel instance |
| **Operations** | Operations are based on Boolean algebra | Operations are based on linear algebra over Hilbert space |
| **Circuit Behaviour** | Circuit behaviour is governed by the principles of classical physics | Circuit behaviour is covered by the principles of quantum mechanics |

Richard Feynman theorized that the computational power of the classical computers can be improvised greatly by incorporating quantum effects into them in 1982 (Feynman, 2018). Working on top of this, David Deutsch developed the basis for quantum computing between 1984 and 1985. However, not much focus was done in this field and no major breakthrough was achieved until 1994. In 1994, Peter Shor devised an algorithm (Shor's algorithm) to solve a popular number theory problem of integer factorization (Shor, 1994). The Shor's algorithm allowed for factorization in polynomial time complexity while the best algorithm at that time consumed exponential time complexity. This algorithm was too complex for regular computers, but quantum computers could process using their ability to process multiple states parallelly.

Shortly after this, Lov Grover developed a fast database search algorithm (known as Grover's algorithm) in 1996 (Grover, 1996). Qubit correction techniques (Vedral & Plenio, 1998), Quantum complexity classes and quantum turing machine (Bernstein & Vazirani, 1993) followed these developments, thereby contributing in advancement of quantum computing. All these proposals were tested on quantum computers developed in the Bell labs and IBM. The invention of three qubit quantum machine in 1999 and seven qubit

quantum machines in 2000 further optimized these techniques (Zohuri, 2020). **Figure 1** represents the timeline of quantum computing.

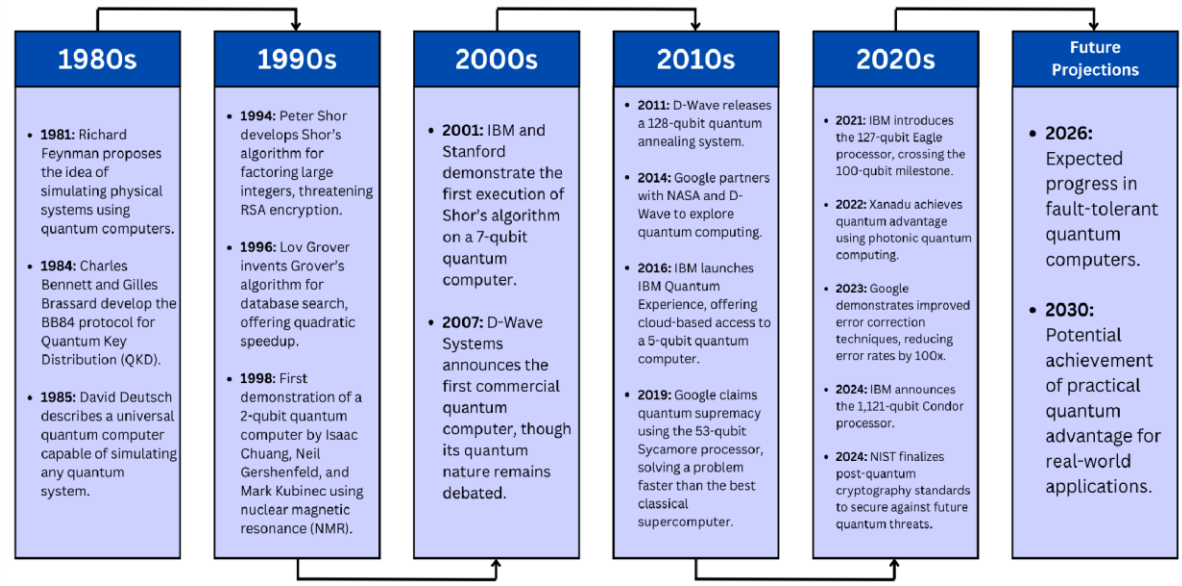


**Figure 1.** Timeline of quantum computing.

The field of quantum computing is experiencing rapid and significant advancement, driven by breakthroughs in quantum communication infrastructure and the development of more stable and scalable quantum hardware. Notably, China continues to lead in record-setting long-distance teleportation using the Micius quantum satellite, a cornerstone of their ambitious satellite-based quantum networks. Researchers have demonstrated quantum teleportation over vast distances exceeding 1,200 kilometres (Yin et al., 2017; Li et al., 2022). These ongoing efforts are crucial for establishing the foundation of a global quantum internet, enabling secure quantum information exchange across continents.

Simultaneously, the development of quantum processors is undergoing a transformative shift towards greater qubit counts and enhanced stability, moving closer to practical fault-tolerant quantum computing. For instance, Google's Willow chip recently showcased pioneering results in quantum error correction, demonstrating performance below the critical threshold where increasing physical qubits lead to an exponential reduction in logical error rates (Bausch et al., 2024). Major industry players like IBM and Microsoft are also aggressively advancing their hardware roadmaps. IBM's roadmap anticipates the unveiling of processors such as "Flamingo" (1,386 qubits) and "Kookaburra" (4,158 qubits) by 2025, emphasizing modular architectures and inter-chip quantum communication to achieve unprecedented scalability (AbuGhanem, 2025). Concurrently, Microsoft's topological qubits, exemplified by their "Majorana 1" chip introduced in early 2025, represent a distinct approach. These qubits leverage exotic quasiparticles for inherent error resistance, offering a promising pathway towards achieving exceptional stability and the potential for integrating millions of qubits on a single chip, addressing one of the most formidable challenges in building robust quantum computers (Sarma et al., 2015).

## 2. Principal of Working

The traditional computers can be completely described and interpreted using the laws of classical physics and Newtonian physics (Crowell, 2001). This limits their capacity to simulate the quantum systems which show high variations in their parameters thereby, generating the need of a new technology.

The quantum computers which are based on the laws of quantum mechanics facilitate performing above stated tasks. The logic used in quantum computers is extremely different from that of classical computers. The probabilistic and nondeterministic behavior of quantum systems is handled wonderfully by quantum computers with the help of laws of quantum mechanics (Dirac, 1981; Giacomini et al., 2019). As the quantum computers allow processing in parallel, they provide an exponential increase in computation power and drastic decrease in time complexity.

At the quantum scale, the particles behave differently. Their properties do not remain distinct, instead are probabilistic. Many principles of quantum mechanics like coherence, decoherence, super positioning, entanglement (Haroche, 1998; Qiao et al., 2018) can be observed at these scales only. The quantum computers are designed to maximize these effects in order to incorporate the ability to deal with uncertainty and parallel state processing (Humble et al., 2021).

### 2.1 Superposition

Superposition is one of the special abilities of the quantum systems wherein the object exhibits more than one state simultaneously. This principle is observed in the most fundamental unit of quantum computers - qubits. The qubits can exhibit the states 0, 1 or a superposition of 0 and 1 (National Academies of Sciences, Engineering and Medicine, 2019; Rietsche et al., 2022). This ability to handle multiple states allows quantum computers to process tasks in parallel.

The concept of superposition can be interpreted in easy terms with the help of an example of a bulb. If the bulb is glowing, it is in ON state. When it is not glowing, it is in OFF state. However, if the bulb glows dimly it cannot be classified in either of the states. It is neither completely on nor completely off. Thus, one may declare this state as a superposition of ON and OFF. This property enables the quantum computers to solve a problem of $2^{N-1}$ states using $N$ qubits only in contrast with classical computers which would require both more memory and time. **Figure 2** presents a visual representation of the superposition principle in quantum computing.

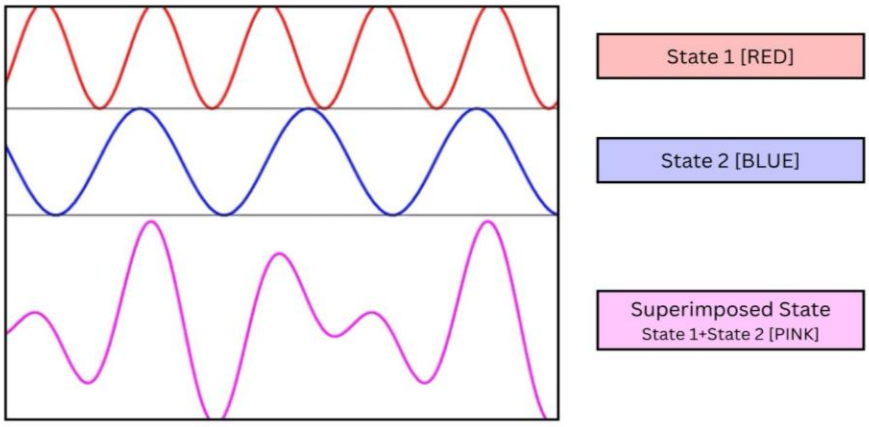


**Figure 2.** Superimposed state.

## 2.2 Entanglement

In the quantum systems, the particles sometimes exhibit the property of entanglement. The phenomenon of entanglement is an integral part of quantum mechanics. It suggests that whenever some particles of the system are interconnected due to their superposition state and exhibit inseparable wave function (Gühne & Tóth, 2009; Hassija et al., 2020; Horodecki et al., 2009). Then one can notice that if any particle is subject to change; correspondingly the effect can be noticed on all the particles no matter what their distance of separation is. This principle is also used highly at the time of processing in the quantum computers. Entanglement between qubits helps process the information faster. **Figure 3** illustrates the phenomenon of quantum entanglement between two qubits.

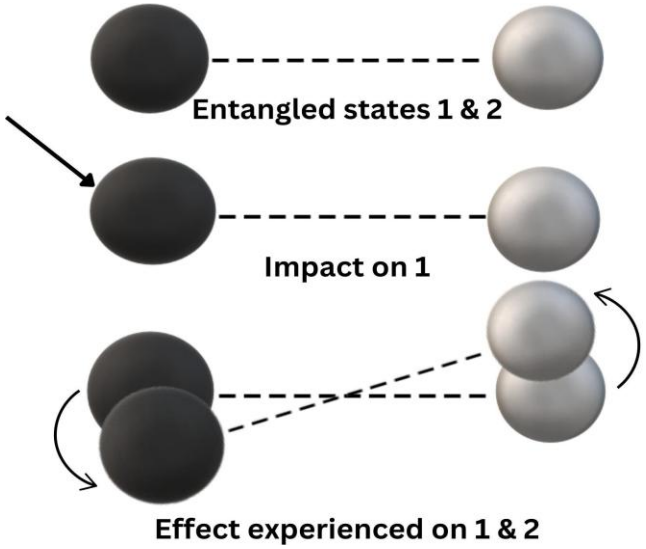


**Figure 3.** Entangled state.

## 2.3 Coherence

It is the most basic requirement for the quantum phenomenon like entanglement, super positioning, interference. A quantum system is said to be coherent when it's state can be described using a set of complex numbers, each number representing the different base states of the system (Chae et al., 2024; Douven & Meijs, 2007; Raz, 1992). It allows to maintain a fixed relationship that is the particles exhibiting coherence will demonstrate a specific behavior when exposed to the circumstances of the surroundings. The particles can be entangled or show super positioning only if they are coherent in nature.

## 2.4 Building Blocks

A quantum computer works using qubits instead of bits. These qubits (Hughes et al., 2021; James et al., 2001) can exhibit the principles of superposition, entanglement which allows us for higher parallelism and faster computation. The qubits have the potential to represent any number between zero and one and even complex numbers. These qubits are mostly represented using wave functions since the quantum computers obey the laws of schrödinger wave equations (Ziman & Bužek, 2005).

A general qubit is represented as:

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

where,

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

$|0\rangle$ and $|1\rangle$ are basis vectors, which are orthogonal to each other and the square of magnitude of the coefficient corresponds to the probability of the corresponding state. To visualize qubits, we use the Bloch sphere. The Bloch sphere is a three-dimensional representation where each point on its surface corresponds to a possible state of a qubit. Unlike classical bits, which are limited to the states $|0\rangle$ or $|1\rangle$, a qubit can exist in a superposition of these two states, meaning it can be represented as any point on the surface of the Bloch sphere. The north pole of the Bloch sphere represents the classical $|0\rangle$ while the south pole represents the classical state $|1\rangle$. The points between the poles represent superpositions of these two states. The position of a qubit on the surface of the Bloch sphere is determined by two parameters: θ, the polar angle (latitude), which ranges from 0 to π and ϕ, the azimuthal angle (longitude), which ranges from 0 to 2π. The general state of a qubit on the Bloch sphere (Liao et al., 2022; Wie, 2014; Wie, 2020) can be mathematically represented as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1.$$

Here,

$\cos\left(\frac{\theta}{2}\right)$ is the amplitude of the $|0$ state.

$e^{i\phi}$ is a complex phase factor applied to the state.

$\sin\left(\frac{\theta}{2}\right)$ is the amplitude of the $|1$ state.

**Figure 4** displays the Blosch Sphere of a single qubit allowing us to understand various basic concepts and help visualise the state of qubit.

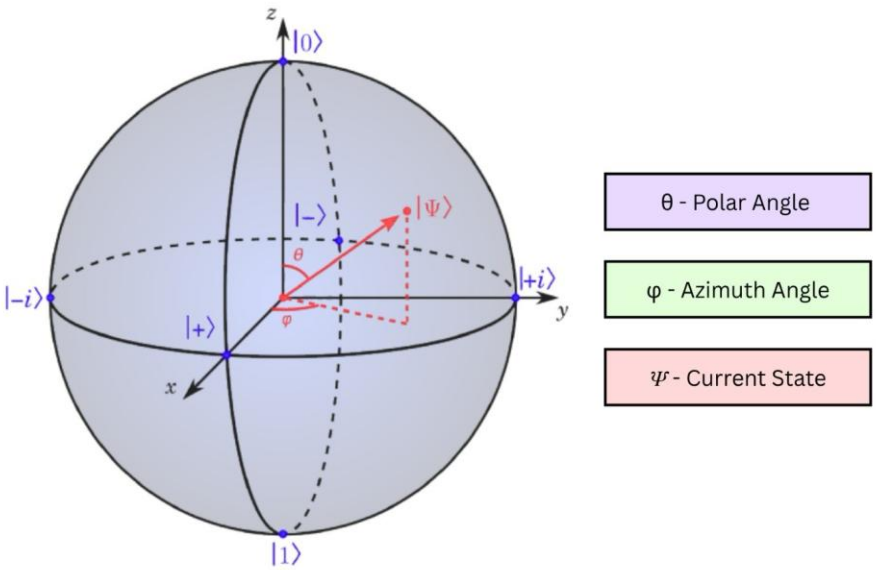


**Figure 4.** Blosch sphere.

These qubits are conceptualised in various forms like photons in optics-based quantum computers which use polarisation and beam splitters for phase shifting and entanglement, electron pairs - where their spin tells the state of qubit usually used in superconducting type quantum computers.

Along with qubits, we require gates for their manipulation. Some popular quantum gates are Hadamard (Shepherd, 2006; Tipsmark et al., 2011), Pauli-X, Pauli-Y, Pauli-Z (Just, 2023) and C-Not (Li et al., 2008). These gates help in manipulating the qubits by performing certain operations on them thereby helping in attaining superposition states, entangled qubits and performing phase shifts. All these operations allow us to build quantum circuits capable of doing tasks like quantum teleportation (Zeilinger, 2000), superdense coding (Harrow et al., 2004; Pati et al., 2005), fast database search, factoring large numbers using Shor's algorithm etc.

The quantum gates are supposed to perform unitary evolutions (Williams, 2011) to the qubit states and process the information accordingly. Similar to the logic gates, quantum gates act as the backbone in quantum computing (Bhat et al., 2022) by allowing us to make circuits which tailor to our needs and allow us to perform qubit manipulation. After manipulation of the qubits, measurement is performed which leads to collapse of the qubit state to the eigenvector corresponding to the eigenvalue which was recorded in the measurement (Korotkov & Jordan, 2006).

## 3. Popular Algorithms

Since the advent of quantum computing, numerous innovative algorithms have been introduced by scientists to tackle complex problems such as factoring large numbers and classifying functions into balanced or constant categories (Shor, 2002). These algorithms enable significant speed improvements over traditional methods. For instance, Lov Grover's algorithm for fast database search allows for quicker identification of a data item in an unstructured dataset, achieving a quadratic speedup by reducing time complexity to $O(\sqrt{n})$. Shor's algorithm presents a substantial advancement in factoring large numbers, offering an exponential speedup compared to classical computing techniques. Additionally, the Deutsch-Josza algorithm efficiently determines whether a function is balanced or constant, with a time complexity of O(1), thus delivering an exponential speedup over traditional algorithms that require O(2^N) time.

### 3.1 Shor's Algorithm

Shor's algorithm (Shor, 1994), introduced by Peter Shor in 1994, revolutionized the field of quantum computing by providing a groundbreaking solution to the problem of integer factorization. This computational challenge, particularly for large numbers, has long been considered unsolvable by classical computers. However, Shor's algorithm offers exponential speedup, enabling quantum computers to factorize large numbers in polynomial time, a significant improvement over the best-known classical algorithms that require exponential time (Willsch et al., 2023).

The heart of Shor's algorithm lies in quantum period finding, a process that harnesses quantum parallelism to identify the period "r" of a function $f(x) = a^x \bmod N$, where "N" is the integer to be factored and "a" is a randomly chosen integer (Kumar & Mondal, 2024; Shor, 1999). Quantum superposition allows the quantum computer to perform multiple calculations simultaneously, efficiently determining the period. This critical step is essential for breaking down the large number into its prime factors.

Once the period "r" is discovered, the classical portion of the algorithm employs the Greatest Common Divisor (GCD) to calculate potential factors of "N." If "*r*" is valid, the algorithm effectively factors "N" by

calculating two factors using the GCD of "$a^{\frac{r}{2}} - 1$" and "$a^{\frac{r}{2}} + 1$".This process reduces the large number into its prime factors. If the period is invalid, the algorithm repeats with a different random integer "a".

Shor's algorithm stands as a pivotal moment in quantum computing, marking the first instance where quantum computers demonstrated their ability to outperform classical machines in solving specific computational problems. Its success in factoring large numbers has profound implications for cryptography, particularly for encryption schemes like RSA (Gerjuoy, 2005; Kulkarni & Thakar, 2024; Singh & Sakk, 2024). This highlights the potential of quantum computing to challenge current security protocols and revolutionize the field of digital security. **Figure 5** depicts the flow chart of working of Shor's algorithm which is used for factorisation of numbers.

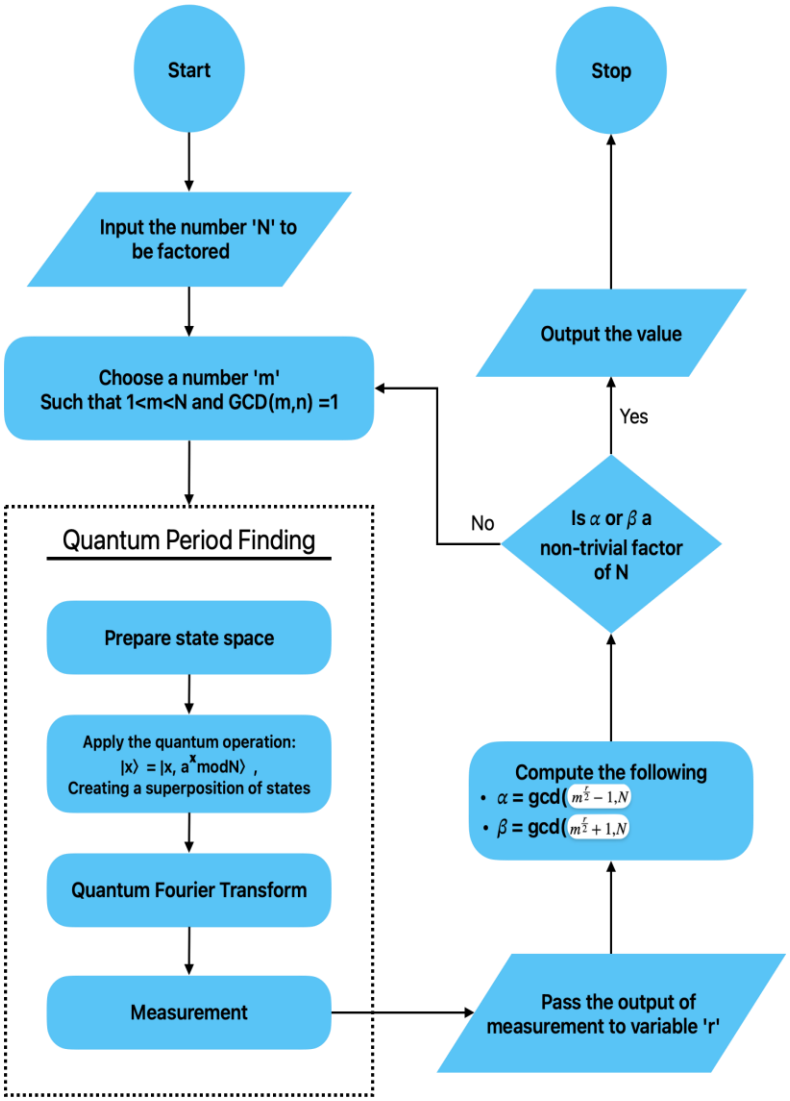


**Figure 5.** Algorithm of peter Shor.

### 3.2 Lov Grover Fast Database Search

Grover's algorithm (Grover, 1996), introduced by Lov Grover in 1996, revolutionized searching unsorted databases. In classical computing, finding a specific item in an N-item database required sequential checks, taking O(N) time. However, Grover's algorithm enables quantum computers to achieve this search in O(N) time, providing a quadratic speedup over classical algorithms.

At the heart of Grover's algorithm lies the oracle—a black-box function that identifies the desired solution. Quantum parallelism (Peruš, 1996) allows the quantum computer to explore multiple possibilities simultaneously. The algorithm iteratively amplifies the probability of the correct solution through amplitude amplification, increasing the likelihood of measuring the correct item while reducing the chances of measuring incorrect ones.

The algorithm commences by preparing an equal superposition of all possible solutions. The oracle is then applied to mark the correct solution by flipping its phase. Subsequently, a Grover diffusion operator is employed to invert the amplitude of all states relative to the average amplitude. This combination of oracle and diffusion operator is repeated approximately N times, progressively increasing the amplitude of the correct solution. After the iterative process, a measurement is made, with high probability yielding the correct solution.

Grover's algorithm showcases the potential of quantum computing to solve problems more efficiently than classical counterparts. While it doesn't provide exponential speedup like Shor's algorithm, it offers a substantial quadratic improvement for unstructured search problems. Consequently, it holds significant importance as a quantum algorithm for applications such as database search, optimization, and cryptanalysis.

### 3.3 Deutsch-Jozsa Algorithm

The Deutsch-Jozsa algorithm (Hooyberghs, 2022), introduced by David and Jozsa in 1992, is a quantum algorithm designed to solve a specific problem faster than any classical algorithm. It addresses the problem of determining whether a given function $f:\{0,1\}n \rightarrow\{0,1\}$ is constant (produces the same output for all inputs) or balanced (produces an equal number of 0s and 1s). For classical computers, solving this problem requires $O(2^n)$ evaluations of the function, since each input must be checked to determine the function's behavior. However, the Deutsch-Jozsa algorithm solves this problem in just one query to the oracle, providing an exponential speedup.

The key to the algorithm's efficiency lies in quantum parallelism and the use of superposition. The quantum algorithm initializes a superposition of all possible inputs using a quantum register, allowing the quantum computer to evaluate the function at all inputs simultaneously. The function is encoded in a quantum oracle, which operates on the superposition and marks the output. The algorithm then applies a quantum Fourier transform to the resulting quantum state, and a final measurement reveals whether the function is constant or balanced.

Unlike classical algorithms, which require multiple queries to determine the nature of the function, Deutsch Jozsa's algorithm uses quantum entanglement and superposition to efficiently check all possible inputs in parallel. After applying the quantum oracle and the Fourier transform, the measurement yields the correct answer with certainty.

The Deutsch-Jozsa algorithm represents one of the earliest examples of quantum algorithms that outperform classical counterparts. While it may not have practical applications in real-world scenarios due to its specific

problem domain, it serves as a foundational result in quantum computing, demonstrating the potential of quantum algorithms to solve problems exponentially faster than classical approaches. **Figure 6** displays a general circuit diagram for Deustch-Josza algorithm.

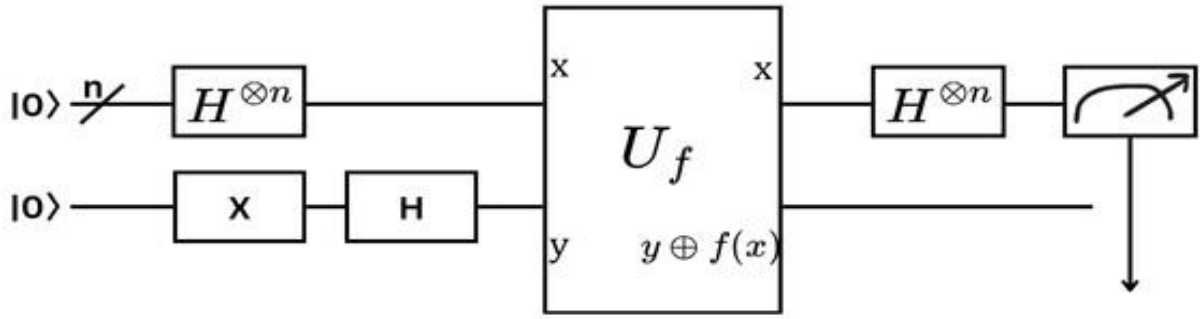


**Figure 6.** Generalised circuit diagram for Deustch-Josza algorithm.

## 4. Applications

The concept of quantum computing was introduced in 1982 by Richard Feynmenn, which was further developed by David and Jozsa between 1984 and 1985. However, significant progress was not made until 1994 when Peter Shor created an algorithm for integer factorization, a complex number theory problem, that could be solved in polynomial time using quantum computers. In 1996, Lov Grover developed a fast database search algorithm, known as Grover's algorithm. These advancements led to the development of Qubit Correction techniques, Quantum Complexity Classes, and Quantum Turing Machine. The proposals were tested on quantum computers in Bell labs and IBM, leading to the invention of three qubit quantum machine in 1999 and seven qubit quantum machines in 2000. **Figure 7** illustrates various applications of quantum computing across different industries.

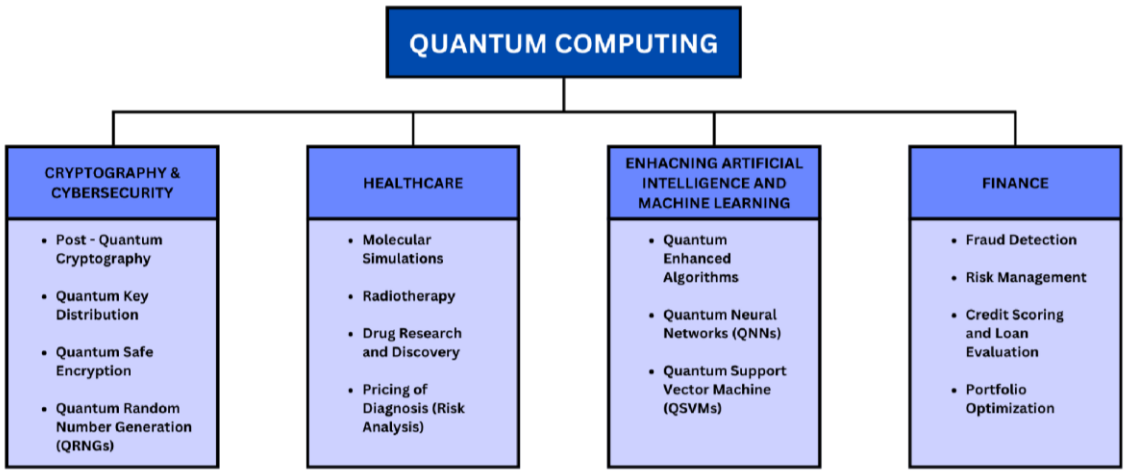


**Figure 7.** Applications of quantum computing.

The true potential of quantum computers is yet to be fully realized; quantum simulations continue to be a major area of research due to their wide-ranging possibilities. Quantum algorithms have shown potential as subroutines for large machine learning algorithms (Giang, 2023). However, the physical realization of a quantum computer remains a major challenge. Despite these challenges, the field of quantum computations and its applications is an exciting area of research, and it's are applications summarized below:

## 4.1 Healthcare

Quantum computing creates interest in upcoming technologies and more powerful computational techniques and capabilities. However, despite quantum computing being a very powerful technology, its potential in the field of healthcare and medicine is still undiscovered. Quantum computing can enhance the healthcare system through various healthcare operations like molecular simulations (Manby et al., 2019), drug research (Cao et al., 2018) and recovery, precision medicine (Bertl et al., 2025), radiology (Hilt et al., 2000), risk analysis (Woerner & Egger, 2019), diagnosis assistance and analysis, DNA sequencing (Ugya & Meguellati, 2022), and many more.

### 4.1.1 Molecular Simulations

Compared to normal computing, quantum computers process data in a new manner using qubits, where the processing speed is governed by the combined circuits. Quantum computing uses quantum entanglement to store critical data, whereas in classical computing, the data is stored in the form of bits (0 or 1). In the field of healthcare and medicine, quantum computing can utilize artificial intelligence, data science, and machine learning to perform complicated tasks and compute programs.

In healthcare, things are often connected in complicated ways, where there are relations and structures between molecules and electrons. The processing requirement for performing operations and tasks in the domain of medicine is very big concerning the problem. Time is one of the largest limiting factors. Therefore, quantum computing is far more superior and efficient than classical computing because of its various methods and techniques.

### 4.1.2 Radiotherapy

Radiotherapy is one of the most common techniques to treat cancer patients, but this method has many disadvantages. In radiotherapy, the radiation beam is used to destroy the affected cancer cells and prevent them from increasing. During that process, the radiation beam also damages healthy cells and tissues, so it is essential to make an effective plan to reduce the impact of radiation. Radiology is a very complicated method; therefore, it requires highly specific and advanced computers to perform operations accurately. This involves executing various operations to achieve the optimal outcome.

Quantum computing can perform many operations or simulations in a short period and find the optimal outcome quickly, which determines new possibilities for using quantum computing in that domain. Companies like Qubit Pharmaceuticals are also applying quantum physics and AI to molecular design for life-changing treatments, including oncology and inflammation.

### 4.1.3 Drug Research and Discovery

Quantum computing helps medical field experts and scientists' study tiny particles that react with enzymes and proteins of the human body, which is crucial for medical research. That helps in diagnosing specific illnesses, discovering new drugs, analysis, and providing insights and hidden patterns in the medical data. The fundamental focus of medical experts and chemists is to discover the molecular and chemical structures that can be evolved into drugs with the help of science and technologies to treat or heal diseases. In the modern period, it is difficult to develop new forms of medicine and drugs due to various factors like climate

change, pollution, food contamination, and allergies.

Quantum computers are far superior compared to normal computers because of quantum entanglement, and quantum computing is highly accurate; therefore, it can calculate the quantum behavior of electrons in a very short period. IBM, in partnership with Cleveland Clinic and Moderna, is utilizing quantum systems to accelerate molecular simulations for new drug candidates and vaccine research.

### 4.1.4 Pricing of Diagnosis (Risk Analysis)

One of the main challenges is to develop a pricing scheme in the domain of healthcare and medicine, which will cause hurdles in the medicine industry. Quantum computing can estimate the health state of the patients and the likelihood that the attendee is vulnerable to a particular illness. The risk analysis over a large number of subjects and aligning the data with the help of the quantum analysis model could be used in financial risk assessment.

Quantum computing provides insights and hidden patterns that can detect performance, and that analysis could help in fraud detection in medical insurance and reveal the behavior of fraudulent claims.

## 4.2 Finance

Quantum computing even though being in its early stages of development still holds immense potential to revolutionize the finance sector by providing effective and efficient solutions to complex solutions. There is evident potential in direct correlation between key financial issues and principles of quantum mechanics. It thus also brings about notable risks related to cybersecurity that could endanger blockchain systems. The evolution of quantum computing necessitates a major shift in focus towards its less popular yet highly desirable applications that are anticipated to make a significant impact (Egger et al., 2020; Guo, 2023; Naik et al., 2025; Silverman, 2022).

### 4.2.1 Fraud Detection

Fraud detection is a critical function for banks to maintain trust with their customers and to protect their assets. However, traditional methods rely on rules-based systems and statistical analysis thus limiting their ability to detect sophisticated fraud schemes.

Quantum computing can provide significant advantages in fraud detection by processing vast amounts of data and detecting patterns that were impossible to detect with classical computers (Guo, 2023). It can also be used in banks to provide stronger encryption for sensitive data, ensuring no financial loss due to cyberattacks.

The utilization of machine learning has seen a growing application in the identification of fraudulent transactions but majority of the existing systems are only capable of detecting deceitful activities after they have taken place, rather than in real-time. This calls for an alternative approach to address the issue beyond conventional methods. One method to establish quantum-enhanced feature space is called the variational quantum classification (VQC), which finds the best hyperplane that is able to linearly separate the embedded data. In VQC, the data x, belonging to Rd, undergoes a mapping process known as the feature map circuit UΦ(x), which implements the function Φ(x). The binary decision is made by measuring the quantum state in the computational basis, resulting in $z \in \{0,1\}n$, and then combining the measurement results linearly. m=∑z∈{0,1}x^ nm(z)|z⟩⟨z|, noticed that m(·)∈{−1,1}. Organizations like PayPal and HSBC are collaborating with quantum firms to enhance fraud detection and cybersecurity.

### 4.2.2 Risk Management

Financial risk management encompasses the protection of a company's financial value by managing various forms of financial risks effectively. These risks include credit risk, market risk, operational risk, among other related categories. The primary objective is to mitigate potential hazards and safeguard a company's economic value.

To estimate the financial risk, contemporary methods involve the use of models and simulations. The level of accuracy can have a direct impact on the profits that companies or individuals yield. One common risk metric that is extensively utilized to measure the magnitude of potential financial losses within a company, is "Value at Risk" or VaR. However, it has a limitation where it fails to adequately capture the impact of extreme losses in the tail of the distribution. To address this shortfall, the Conditional Value at Risk (CvaR) is often used as an additional risk measure. CVaR subscript alpha represents the average value of all losses up to the Value at Risk at the alpha level.

Estimating Value at Risk is typically a computationally demanding task that involves classic Monte Carlo simulation. However, quantum Amplitude Estimation provides a quadratic speedup to achieve the same outcome (Egger et al., 2020). Therefore, to extend this approach to other financial simulation tasks, it is necessary to design task-specific quantum circuits to implement operators. Companies like JPMorgan Chase and Goldman Sachs are exploring quantum algorithms (e.g., QAOA (Quantum Approximate Optimization Algorithm), Quantum Monte Carlo) for portfolio optimization and complex risk analysis, aiming for faster and more accurate financial modeling.

### 4.2.3 Credit Risk Score

Quantum computing promises to revolutionize credit risk score management by tackling complex computations exponentially faster (Silverman, 2022). Its ability to analyze vast datasets and simulate various scenarios enables more accurate risk assessment, reducing financial institutions' exposure to defaults. Quantum algorithms can enhance predictive models, offering deeper insights into borrower behavior and market dynamic (Silverman, 2022). However, practical implementation remains in infancy due to hardware constraints and algorithmic development challenges. As quantum technology matures, it holds immense potential to reshape credit risk management, paving the way for more robust and adaptive financial systems (Silverman, 2022).

## 4.3 Cryptography and Cybersecurity

One of the most significant implications of quantum computing lies in cryptography (Naik et al., 2025). Shor's algorithm, a quantum algorithm capable of factoring large prime numbers exponentially faster than classical algorithms, poses a serious threat to current encryption systems such as RSA and ECC (Nielsen & Chuang, 2010). This could potentially render traditional cryptographic protocols obsolete, necessitating the development of post-quantum cryptographic (PQC) methods. Governments and organizations worldwide are investing in quantum-safe encryption, such as lattice-based and hash-based cryptography, to counteract potential quantum threats. Additionally, quantum key distribution (QKD) is emerging as a method to enable secure communication channels resistant to eavesdropping, further enhancing cybersecurity in the quantum era (Naik et al., 2025).

## 4.4 Enhancing Artificial Intelligence and Machine Learning

Quantum computing has the potential to significantly advance artificial intelligence (AI) and machine learning (ML) applications (Egger et al., 2020; Naik et al., 2025). Quantum enhanced algorithms can process vast amounts of data more efficiently than classical counterparts, leading to improvements in optimization, pattern recognition, and decision-making models. For example, quantum neural networks

(QNNs) and quantum support vector machines (QSVMs) are being explored for enhancing deep learning applications. Additionally, hybrid quantum-classical AI models could bridge the gap between current computational capabilities and the future of fully quantum-powered AI, paving the way for advancements in natural language processing, autonomous systems, and robotics.

### 4.5 Material Science

Quantum computing is emerging as a transformative force in material sciences, with the potential to drastically improve the way we simulate, design, and understand materials at the atomic and molecular levels. This potential is rooted in quantum computing's unique ability to naturally model quantum systems—something classical computing struggles to do efficiently. Quantum computing is redefining the future of materials science. It offers the tools to simulate complex quantum behavior more naturally and accurately than classical methods, especially when combined with machine learning techniques.

Simultaneously, material science is key to improving the performance and scalability of quantum hardware. Together, these disciplines form a feedback loop—each pushing the other forward—toward groundbreaking advances in the understanding and design of materials (Schuhmacher et al., 2022).

#### 4.5.1 Advanced Simulation Techniques

One of the key applications of quantum computing in material science is solving electronic structure problems. These problems involve calculating the energy and behavior of electrons in molecules and materials, which are critical to understanding properties such as conductivity, magnetism, and chemical reactivity. Current quantum algorithms, like the Variational Quantum Eigensolver (VQE) and Quantum Phase Estimation (QPE), are designed to approximate the ground state energies of quantum systems (McClean et al., 2016, Tilly et al., 2022). While classical algorithms become computationally expensive for large systems due to exponential scaling, quantum computers are inherently better suited for such calculations—even when limited by today's hardware-constraints.

Given the current hardware limitations of quantum computers, especially in terms of noise and circuit depth, researchers are turning to hybrid strategies. One such approach combines quantum-computed data with machine learning potentials (MLPs). Instead of running full quantum simulations for every step in a molecular dynamics experiment, data from quantum computers is used to train neural network models. These trained models can then predict the behavior of materials across many configurations efficiently and with high accuracy. This method not only bridges the performance gap between current quantum and classical methods but also enables simulations over longer timescales and larger system sizes.

Conventional techniques in electronic structure calculations, such as Density Functional Theory (DFT) or Quantum Monte Carlo (QMC), have proven effective but are still constrained in their ability to scale to large systems or capture highly correlated quantum behavior. Quantum computing offers the prospect of overcoming these bottlenecks by providing more efficient scaling for certain material problems. As quantum hardware continues to improve, it may be able to tackle simulations that are currently out of reach for even the most powerful classical supercomputers (Arute et al., 2020).

#### 4.5.2 Development of Materials for Development of Quantum

Material science itself plays a crucial role in the advancement of quantum computing technology. Quantum bits (qubits), the foundational units of quantum computers, are extremely sensitive to environmental disturbances. Their performance is affected by material imperfections, noise, and fabrication quality. Enhancing material properties—through the creation of purer semiconductors, improved fabrication methods, and engineered interfaces—can significantly improve qubit coherence times and reliability,

allowing for more scalable quantum architectures. In tandem, the rise of Noisy Intermediate-Scale Quantum (NISQ) devices is opening new pathways for experimental research. While these devices do not yet support error correction or massive computation, they are already being used for specialized tasks in materials science, such as simulating small systems or testing emerging quantum algorithms. These early explorations provide critical insights that drive progress in both quantum computing hardware and materials research.

## 5. Quantum Networking

Quantum networking, a rapidly developing field, aims to interconnect quantum devices and distribute quantum information. This infrastructure promises capabilities far beyond classical networks, including ultra-secure communication, distributed quantum computing, and enhanced sensing. Recent breakthroughs in long-distance entanglement and specialised quantum components are accelerating progress towards a global quantum internet.

### 5.1 Quantum Key Distribution (QKD)

QKD uses quantum mechanics to establish unbreakable cryptographic keys, ensuring secure communication. Recent advancements include China's intercontinental QKD via the Micius satellite and the development of metropolitan fibre-optic quantum networks. Hybrid satellite-terrestrial QKD systems are also being explored for robust and widespread secure communication (Ecker et al., 2023). The fundamental No-Cloning Theorem states that an arbitrary unknown quantum state cannot be perfectly copied. This principle underpins the security of Quantum Key Distribution (QKD), as any eavesdropping attempt inevitably disturbs the quantum state, alerting legitimate users. It also necessitates novel quantum error correction techniques, distinct from classical redundancy.

### 5.2 Quantum Internet

The quantum internet aims to connect quantum processors and distribute entangled states globally, enabling truly distributed quantum computing. Progress involves developing quantum repeaters to overcome photon loss over long distances in optical fibres. Initiatives like EuroQCI and the US National Quantum Initiative are establishing testbeds and roadmaps for future quantum internet infrastructure. Quantum teleportation enables the transfer of a quantum state between locations using entanglement and classical communication, without physically transmitting the qubit itself (Boone et al., 2015). Recent breakthroughs include record setting long-distance teleportation via satellites and high-fidelity demonstrations over terrestrial networks, which are crucial for interconnecting quantum nodes and processors.

## 6. Limitations and Challenges

Quantum Computing possesses the potential to revolutionize fields like cryptography, drug discovery, and optimization by leveraging principles like superposition, entanglement, and quantum parallelism. However, in spite of recent advancements, large-scale, fault-tolerant quantum computers still remain a distant goal due to several significant challenges. These challenges include qubit stability, scalability, error correction, algorithmic development and hardware limitations. This section focuses on the critical obstacles that hinder the widespread adoption of quantum computing.

### 6.1 Qubit Stability and Decoherence

Qubits, the building blocks of quantum computers, are very sensitive to noise in the environment which can be in the form of temperature variations, electromagnetic noise, and mechanical vibrations. Noise causes the fragile quantum state to collapse, and qubits lose their coherence, a process referred to as decoherence. Even a small noise is sufficient to reduce a quantum state to a classical state, making computation useless.

Currently qubits like superconducting and trapped-ion qubits exhibit coherence for only milliseconds to microseconds. This short time frame significantly restricts the complexity and length of computation before errors start to build up, rendering long computations heavily error-prone.

To maintain qubit coherence, quantum systems need extremely controlled environments, generally temperatures near absolute zero (millikelvin range) and advanced shielding is required. It is hard and costly to maintain, so it is an additional aspect of operational complexity.

### 6.2 Scalability and System Complexity

For practical applications, quantum computers require millions of quality qubits. However, scaling quantum systems introduces numerous complicating factors. With more qubits, maintaining coherence is exponentially more challenging and cross-talk among qubits is exponentially more challenging to reduce.

Construction of large-scale quantum systems necessitates the creation of structures that can maintain high qubit connectivity without compromising on noise. High performance over a vast array of qubits is a significant engineering challenge. Scaling also demands greater physical space, complex cooling infrastructure, and complex control electronics, making the infrastructure even more sophisticated. **Figure 8** highlights the key challenges and limitations faced by quantum computing technologies.

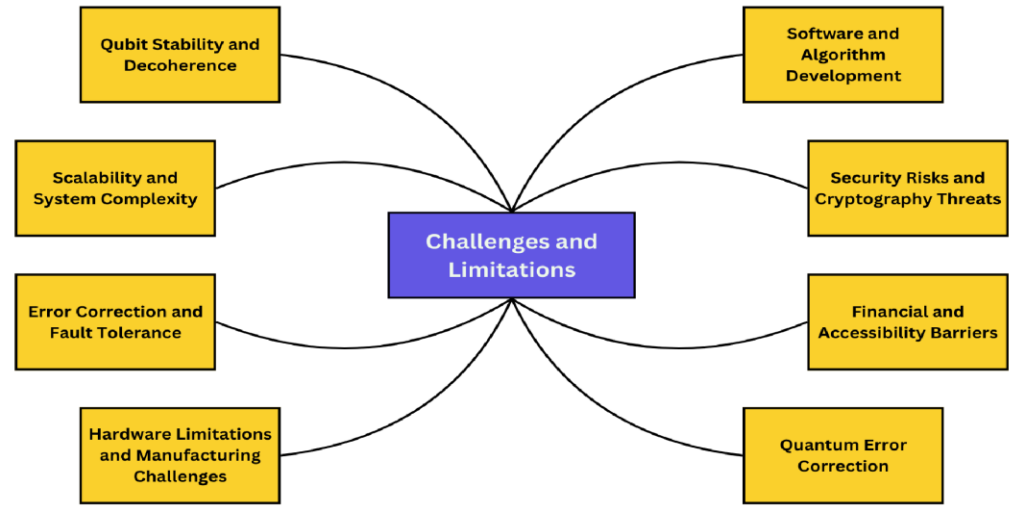


**Figure 8.** Challenges and limitations of quantum computing.

### 6.3 Error Correction and Fault Tolerance

Quantum gates, which act to manipulate qubits, introduce errors due to limitations in hardware and external noise. The errors build up over time and contribute to the decay of quantum computational results. Because error rates in quantum systems are much larger than those of classical systems, the assurance of trustworthy results is a major challenge.

Quantum error correction is exponentially more difficult in quantum systems than in classical computation. Because of the no-cloning theorem, which forbids the copying of quantum states, redundancy cannot be implemented by straightforward duplication. Rather, QEC stores one logical qubit with a multitude of

physical qubits in order to detect and correct errors. This imposes a humongous resource overhead, which means thousands of physical qubits to keep one stable logical qubit.

For a fault-tolerant quantum system, the error rates should be driven below some kind of critical level (generally $10^{-3}$ to $10^{-4}$ per gate operation). Maintaining error rates as low as these while also scaling the system is a standing problem. In the absence of satisfactory error correction, quantum computations become unreliable through a growing system.

### 6.3.1 Error Correction Techniques

The states of qubit are very sensitive nature and get affected in the presence of low noise environments also. In quantum computing, we mainly face two types of errors: bit flip and phase flip. These flips cause error in the net computation and processing of the qubit. In order to deal with these errors, error mitigation and error correction strategies have been developed. A bit flip is a type of error wherein the state undergoes a change similar to not operation (like application of X-gate) i.e- |0> becomes |1> and vice-versa. On the other hand, a phase flip is an error wherein the state of the qubit gets modified by a 180° rotation about Zaxis of blosch sphere or a change in $\phi$ by pi radians (like application of Z-gate). A bit flip results in incorrect measurement and processing while phase flip only results in incorrect processing and does not affect measurement.

Classical computers ensure correctness of data by performing error detection and correction by following the series of steps: duplication of bits, detection of error by analysing the pattern and finally correcting the error by performing a not operation on the detected incorrect bit. In a quantum computer, the no cloning theorem prevents the duplication of the state of an arbitrary qubit. Due to this, we cannot implement the same strategy for error detection and correction as in classical computers. To perform quantum error correction, we require ancilla qubits; these qubits help in encoding the information regarding which qubit state got modified due to noise or gate errors. Finally, an error syndrome is present, which detects which qubit has undergone phase flip or bit flip and then rectifies that error of qubit by applying Z-gate or X-gate respectively

## 6.4 Hardware Limitations and Manufacturing Challenges

***Specialized and Expensive Equipment***

Quantum computers need very advanced hardware, such as:

- Cryogenic Cooling Systems: Many qubit technologies such as superconducting qubits require temperatures near absolute zero to preserve coherence.
- Ultra-High Vacuum Chambers: Trapped-ion and photonic qubits will probably need vacuum conditions to minimize decoherence.
- Precision Control Electronics: Advanced laser technologies and microwave control systems are needed for accurate control of qubits.

***Manufacturing Challenges***

Creating stable and durable qubits at scale requires cutting-edge materials and manufacturing techniques still in the process of being explored. Qubit consistency across a large quantum system remains a powerful barrier.

***Diverse Qubit Technologies***

There are several competing qubit technologies, such as superconducting qubits, trapped ions, and photonic qubits. Each has its strengths and weaknesses, and there has not yet been agreement on which technology will eventually permit large-scale, fault-tolerant quantum computing.

### 6.5 Software and Algorithm Development

Although certain algorithms such as Shor's algorithm (for factorizing integers) and Grover's algorithm (for database searching) are remarkable advancements in computational efficiency, discovering practical quantum algorithms for significant problems remains an active field of research. There are numerous computational problems to be successfully restated in terms of quantum models.

Quantum programming languages and tools are still in their nascent stage of development. Quantum device programming requires deep familiarity with quantum mechanics, linear algebra, and advanced error handling. Most quantum algorithms, so far, are being programmed using low-level programming languages that speak directly to quantum hardware, leading to issues in creating and optimizing them for broader applications.

Because of the probabilistic nature of quantum mechanics, correctness and reliability verification of quantum computations can be problematic. Developing reliable methods for quantum software verification is an open problem in research.

### 6.6 Security Risks and Cryptography Threats

Quantum computers of large size are a grave threat to today's cryptography. RSA and ECC algorithms would become easy to crack with Shor's algorithm, which could break global data security. This pending threat requires developing and implementing post-quantum cryptography that resists attacks by high powered quantum computers.

### 6.7 Financial and Accessibility Barriers

Quantum computer systems involve large amounts of financial investment due to specialized hardware, cryogenic gear, and infrastructure needs. It involves constant monitoring, advanced materials, and very specialized expertise, making it prohibitively expensive for most organizations.

Today, access to quantum computing platforms is largely reserved for large research institutions, governments, and select top technology companies. Although cloud-based quantum services have started democratizing access, the platforms are still providing relatively small numbers of qubits, stability, and computing power.

### 6.8 The Central Challenge of Quantum Error Correction

The central obstacle to realizing useful quantum computation is the achievement of fault-tolerant quantum systems through sound quantum error correction (QEC) (Lidar & Brun, 2013; Devitt et al., 2013; Roffe, 2019). Current quantum hardware contains error rates too great for large-scale computation, and error correction requires encoding logical qubits in tens of thousands of physical qubits. This will require a massive resource overhead, and the achievement of large-scale error-corrected systems is currently not a practical prospect using current technology. Without efficient error correction, making quantum systems useful is an unrealizable dream. These issues will need to be addressed through continuing innovation in hardware design, reduction of noise, error correction technique, and quantum algorithm design.

## 7. Conclusion

Quantum computing, grounded in principles such as superposition, entanglement, and coherence, has emerged as a transformative paradigm with the potential to outperform classical systems in solving complex computational problems. Literature across disciplines highlights its wide-ranging applications—from molecular modeling and drug discovery in healthcare, to fraud detection, risk analysis, and market

forecasting in finance. In artificial intelligence, quantum algorithms are expected to enhance data analysis and decision-making, while in cybersecurity, they drive both disruption and innovation, with quantum-safe protocols becoming increasingly vital.

Despite its promise, significant technical and practical challenges remain. Qubit instability, decoherence, and the overhead of error correction impede the development of fault-tolerant quantum systems. Current methods often require thousands of physical qubits per logical qubit, posing major scalability and engineering difficulties. Furthermore, high development costs, specialised hardware requirements, and manufacturing constraints limit broad accessibility, concentrating progress within elite research institutions and industry leaders. The threat quantum computing poses to classical encryption also underscores the urgency for global migration to post-quantum cryptographic standards.

Nonetheless, recent advances in quantum hardware, algorithm design, and cloud-based quantum platforms indicate steady progress toward practical deployment. The integration of quantum computing with existing digital infrastructures offers a promising pathway for broader adoption. As research continues and interdisciplinary collaboration expands, quantum computing is increasingly positioned to reshape computational science, unlock new forms of secure communication, and drive innovation across a range of critical fields.

## 8. Future Scope

As researchers and industry leaders continue to invest in quantum technology, the future of quantum computing appears promising, with potential breakthroughs in various domains, including cryptography, artificial intelligence, material science, and optimization problems.

One of the primary challenges in quantum computing is achieving scalable and fault-tolerant systems. Current quantum processors, such as those developed by IBM, Google, and other research institutions, have demonstrated computational capabilities beyond classical systems for specific problems. However, these systems are still in their infancy, suffering from issues like qubit decoherence, error rates, and limited connectivity. Future research is focused on developing more stable qubits, whether through superconducting circuits, trapped ions, or topological qubits, to create scalable quantum processors. Advances in quantum error correction techniques, such as surface codes and cat qubits, are expected to play a crucial role in making quantum computing practical for real-world applications. Some of the applications that are going to be drastically affected by the upsurgence of quantum computing are listed as follows:

### 8.1 Optimization and Financial Modeling

Many industries rely on optimization problems, ranging from logistics and supply chain management to financial risk analysis. Quantum computing offers solutions to these challenges by leveraging quantum algorithms like the Quantum Approximate Optimization Algorithm (QAOA) and Variational Quantum Eigensolver (VQE) (Farhi et al., 2014). These algorithms can find optimal solutions for complex problems in record time, reducing costs and improving efficiency in real-world applications. In finance, quantum computers could enhance portfolio optimization, fraud detection, and market simulation, allowing organizations to manage risk more effectively and make data-driven investment decisions.

### 8.2 Climate Science and Energy Optimization

Quantum computing could play a critical role in tackling global challenges such as climate change and energy optimization. Complex climate models, which require enormous computational power, could be executed more efficiently using quantum simulations. This would enable scientists to better predict climate patterns, design sustainable solutions, and mitigate environmental risks. Additionally, quantum computing

has the potential to optimize energy grids, improve battery efficiency, and contribute to breakthroughs in nuclear fusion, ultimately supporting the transition to clean energy solutions.

### 8.3 Quantum Internet and Secure Communication

The development of a quantum internet is another exciting prospect for the future. Unlike traditional networks, a quantum internet would utilize quantum entanglement and teleportation to enable ultra-secure communication. Researchers are currently exploring ways to establish quantum communication networks that could enable instantaneous and unhackable data transmission over long distances (Kimble, 2008). If successfully implemented, quantum networking could revolutionize industries such as finance, defense, and national security by providing a fundamentally secure method for transmitting sensitive information (Pirandola et al., 2020).

#### Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

#### Acknowledgments

The authors are grateful for the support received from Vivekananda Institute of Professional Studies - Technical Campus (School of Engineering and Technology).

#### AI Disclosure

During the preparation of this work the author(s) used generative AI in order to improve the language of the article. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

## References

AbuGhanem, M. (2025). IBM quantum computers: evolution, performance, and future directions. *The Journal of Supercomputing*, *81*(5), 687.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., & Zalcman, A. (2020). Hartree-Fock on a superconducting qubit quantum computer. *Science*, *369*(6507), 1084-1089.

Bausch, J., Senior, A.W., Heras, F.J., Edlich, T., Davies, A., Newman, M., Jones, C., Satzinger, K., Niu, M.Y., Blackwell, S., & Holland, G. (2024). Learning high-accuracy error decoding for quantum processors. *Nature*, *635*(8040), 834-840. https://doi.org/10.1038/s41586-024-08148-8.

Bernstein, E., & Vazirani, U. (1993). Quantum complexity theory. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing* (pp. 11-20). Association for Computing Machinery. New York.

Bertl, M., Mott, A., Sinno, S., & Bhalgamiya, B. (2025). Quantum machine learning in precision medicine and drug discovery--a game changer for tailored Treatments?. *arXiv preprint arXiv:2502.18639*.

Bhat, H.A., Khanday, F.A., Kaushik, B.K., Bashir, F., & Shah, K.A. (2022). Quantum computing: fundamentals, implementations and applications. *IEEE Open Journal of Nanotechnology*, *3*, 61-77.

Boone, K., Bourgoin, J.P., Meyer-Scott, E., Heshami, K., Jennewein, T., & Simon, C. (2015). Entanglement over global distances via quantum repeaters with satellite links. *Physical Review A*, *91*(5), 052325.

Cao, Y., Romero, J., & Aspuru-Guzik, A. (2018). Potential of quantum computing for drug discovery. *IBM Journal of Research and Development, 62*(6), 6-20.

Chae, E., Choi, J., & Kim, J. (2024). An elementary review on basic principles and developments of qubits for quantum computing. *Nano Convergence*, *11*(1), 11. https://doi.org/10.1186/s40580-024-00418-5.

Crowell, B. (2001). *Newtonian physics* (Vol. 1). Light and Matter, California.

Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, *439*(1907), 553-558.

Devitt, S.J., Munro, W.J., & Nemoto, K. (2013). Quantum error correction for beginners. *Reports on Progress in Physics, 76*(7), 076001.

Dirac, P.A.M. (1981). *The principles of quantum mechanics* (No. 27). Oxford University Press, New York.

Douven, I., & Meijs, W. (2007). Measuring coherence. *Synthese, 156*(3), 405-425.

Ecker, S., Pseiner, J., Piris, J., & Bohmann, M. (2023). Advances in entanglement-based QKD for space applications. In *International Conference on Space Optics—ICSO 2022* (Vol. 12777, pp. 925-945). SPIE. https://doi.org/10.1117/12.2689972.

Egger, D.J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., & Yndurain, E. (2020). Quantum computing for finance: state-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering*, *1*, 1-24.

Farhi, E., Goldstone, J., & Gutmann, S. (2014). *A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem*. arXiv:1412.6062.

Feynman, R.P. (2018). Simulating physics with computers. In Hey, A.J.G. (ed) *Feynman and Computation* (pp. 133-153). CRC Press. Boca Raton, USA.

Gerjuoy, E. (2005). Shor's factoring algorithm and modern cryptography: an illustration of the capabilities inherent in quantum computers. *American Journal of Physics, 73*(6), 521-540.

Giacomini, F., Castro-Ruiz, E., & Brukner, Č. (2019). Quantum mechanics and the covariance of physical laws in quantum reference frames. *Nature Communications*, *10*(1), 494. https://doi.org/10.1038/s41467-018-08136-1.

Giang, V. (2023). Quantum computing and its applications in healthcare. *OUR Journal: ODU Undergraduate Research Journal, 10*(1), Article 5.

Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (pp. 212-219). Association for Computing Machinery. New York.

Gühne, O., & Tóth, G. (2009). Entanglement detection. *Physics Reports, 474*(1-6), 1-75.

Guo, S. (2023). Investigating essential technologies and applications of quantum computing in finance. In *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence* (Vol. 108, p. 329). Springer Nature. Netherlands.

Haroche, S. (1998). Entanglement, decoherence and the quantum/classical boundary. *Physics Today*, *51*(7), 36-42.

Harrow, A., Hayden, P., & Leung, D. (2004). Superdense coding of quantum states. *Physical Review Letters, 92*(18), 187901.

Hassija, V., Chamola, V., Goyal, A., Kanhere, S.S., & Guizani, N. (2020). Forthcoming applications of quantum computing: peeking into the future. *IET Quantum Communication, 1*(2), 35-41.

Hilt, B., Fessler, P., & Prévot, G. (2000). The quantum X-ray radiology apparatus. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 442*(1-3), 355-359.

Hooyberghs, J. (2022). Deutsch-Jozsa algorithm. In *Introducing Microsoft Quantum Computing for Developers*. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-7246-6_9.

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. *Reviews of Modern Physics*, *81*(2), 865-942.

Hughes, C., Isaacson, J., Perry, A., Sun, R.F., & Turner, J. (2021). What is a qubit?. In *Quantum Computing for the Quantum Curious* (pp. 7-16). Springer International Publishing. https://doi.org/10.1007/978-3-030-61601-4_2.

Humble, T.S., McCaskey, A., Lyakh, D.I., Gowrishankar, M., Frisch, A., & Monz, T. (2021). Quantum computers for high-performance computing. *IEEE Micro*, *41*(5), 15-23.

James, D.F., Kwiat, P.G., Munro, W.J., & White, A.G. (2001). Measurement of qubits. *Physical Review A*, *64*(5), 052312.

Just, B. (2023). Quantum gates on one qubit. In *Quantum Computing Compact: Spooky Action at a Distance and Teleportation Easy to Understand* (pp. 69-82). Springer, Berlin, Heidelberg.

Kimble, H.J. (2008). The quantum internet. *Nature, 453*(7198), 1023-1030.

Korotkov, A.N., & Jordan, A.N. (2006). Undoing a weak quantum measurement of a solid-state qubit. *Physical Review Letters, 97*(16), 166805.

Kulkarni, S.S., & Thakar, H.S. (2024). Quantum cryptanalysis: analyzing Shor's algorithm and its impact on RSA. In *Proceedings of 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications* (Vol. 1, p. 347). Springer Nature. Singapore.

Kumar, M., & Mondal, B. (2024). Study on implementation of Shor's factorization algorithm on quantum computer. *SN Computer Science, 5*(4), 413. https://doi.org/10.1007/s42979-024-03026-7.

Ladd, T.D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J.L. (2010). Quantum computers. *Nature*, *464*(7285), 45-53.

Li, H.J., Shun-Jin, W., & Jun, T. (2008). Physical realization of quantum C-Not gate. *Chinese Physics Letters*, *25*(3), 813.

Li, J., Jia, Q., Xue, K., Wei, D.S., & Yu, N. (2022). A connection-oriented entanglement distribution design in quantum networks. *IEEE Transactions on Quantum Engineering*, *3*, 1-13.

Liao, Y.P., Cheng, Y.L., Zhang, Y.T., Wu, H.X., & Lu, R.C. (2022). The interactive system of Bloch sphere for quantum computing education. In *2022 IEEE International Conference on Quantum Computing and Engineering* (pp. 718-723). IEEE. Broomfield, CO, USA.

Lidar, D.A., & Brun, T.A. (2013). *Quantum error correction*. Cambridge University Press, U.K.

Manby, F., Miller, T., Bygrave, P., Ding, F., Dresselhaus, T., Batista-Romero, F., & Williams, Z. (2019). entos: a quantum molecular simulation package. ChemRxiv. https://doi.org/10.26434/chemrxiv.7762646.v1.

McClean, J.R., Romero, J., Babbush, R., & Aspuru-Guzik, A. (2016). The theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*, *18*(2), 023023.

Naik, A.S., Yeniaras, E., Hellstern, G., Prasad, G., & Vishwakarma, S.K.L.P. (2025). From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance. *Financial Innovation*, *11*(1), 1-67.

National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum computing: Progress and prospects*. The National Academies Press. https://doi.org/10.17226/25196.

Nielsen, M., & Chuang, I. (2010). *Quantum computation and quantum information*. Cambridge University Press. UK.

Ozawa, L., & Itoh, M. (2003). Cathode ray tube phosphors. *Chemical Reviews, 103*(10), 3835-3856.

Pati, A.K., Parashar, P., & Agrawal, P. (2005). Probabilistic superdense coding. *Physical Review A—Atomic, Molecular, and Optical Physics*, *72*(1), 012329.

Peruš, M. (1996). Neuro-quantum parallelism in brain-mind and computers. *Informatica, 20*, 173-183.

Pirandola, R., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colangelo, P., & Braunstein, S.L. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 10121236.

Qiao, L.F., Streltsov, A., Gao, J., Rana, S., Ren, R.J., Jiao, Z.Q., & Jin, X.M. (2018). Entanglement activation from quantum coherence and superposition. *Physical Review A*, *98*(5), 052351. https://doi.org/10.1103/PhysRevA.98.052351.

Rajaraman, V. (2020). *Groundbreaking inventions in information and communication technology*. PHI Learning Pvt. Ltd. Delhi.

Raz, J. (1992). The relevance of coherence. *BUL Review, 72*, 273.

Rietsche, R., Dremel, C., & Bosch, S. (2022). Quantum computing. *Electronic Markets, 32*, 2525-2536. https://doi.org/10.1007/s12525-022-00608-y.

Roffe, J. (2019). Quantum error correction: an introductory guide. *Contemporary Physics, 60*(3), 226-245. https://doi.org/10.1080/00107514.2019.1667078.

Sarma, S.D., Freedman, M., & Nayak, C. (2015). Majorana zero modes and topological quantum computation. *NPJ Quantum Information*, *1*(1), 1-13.

Schuhmacher, J., Mazzola, G., Tacchino, F., Dmitriyeva, O., Bui, T., Huang, S., & Tavernelli, I. (2022). Extending the reach of quantum computing for materials science with machine learning potentials. *AIP Advances*, *12*(11), 115321. https://doi.org/10.1063/5.0099469.

Shepherd, D.J. (2006). On the role of Hadamard gates in quantum circuits. *Quantum Information Processing*, *5*, 161-177.

Shor, P.W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). IEEE. Santa Fe, NM, USA.

Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, *41*(2), 303-332.

Shor, P.W. (2002). Introduction to quantum algorithms. In Lomonaco, S.J. (ed) *Proceedings of Symposia in Applied Mathematics* (Vol. 58, pp. 143-160). American Mathematical Society, Washington.

Silverman, B.W. (2022). Quantum computing for credit risk management. *Journal of Financial Engineering*, *27*(3), 45-59.

Singh, S., & Sakk, E. (2024). *Implementation and analysis of Shor's algorithm to break RSA cryptosystem security*. Authorea Preprints. https://doi.org/10.22541/au.171073075.06143428

Tilly, J., Chen, H., Cao, S., Picozzi, D., Setia, K., Li, Y., & Tennyson, J. (2022). The variational quantum Eigensolver: a review of methods and best practices. *Physics Reports*, *986*, 1-128.

Tipsmark, A., Dong, R., Laghaout, A., Marek, P., Ježek, M., & Andersen, U.L. (2011). Experimental demonstration of a Hadamard gate for coherent state qubits. *Physical Review A— Atomic, Molecular, and Optical Physics*, *84*(5), 050301.

Ugya, A.Y., & Meguellati, K. (2022). Quantum technology a tool for sequencing of the ratio DSS/DNA modifications for the development of new DNA-binding proteins. *Egyptian Journal of Basic and Applied Sciences*, *9*(1), 308-323.

Vedral, V., & Plenio, M.B. (1998). Basics of quantum computation. *Progress in Quantum Electronics*, *22*(1), 1-39. https://doi.org/10.1016/S0079-6727(98)00004-4.

Wie, C.R. (2014). Bloch sphere model for two-qubit pure states. *arXiv preprint arXiv:1403.8069*.

Wie, C.R. (2020). Two-qubit Bloch sphere. *Physics, 2*(3), 383-396.

Williams, C.P. (2011). Quantum gates. In *Explorations in Quantum Computing* (pp. 51-122). Springer, London.

Willsch, D., Willsch, M., Jin, F., De Raedt, H., & Michielsen, K. (2023). Large-scale simulation of Shor's quantum factoring algorithm. *Mathematics, 11*(19), 4222. https://doi.org/10.3390/math11194222.

Woerner, S., & Egger, D.J. (2019). Quantum risk analysis. *npj Quantum Information*, *5*(1), 15. https://doi.org/10.1038/s41534-019-0130-6.

Yin, J., Cao, Y., Li, Y.H., Liao, S.K., Zhang, L., Ren, J.G., & Pan, J.W. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, *356*(6343), 1140-1144.

Zeilinger, A. (2000). Quantum teleportation. *Scientific American, 282*(4), 50-59.

Ziman, M., & Bužek, V. (2005). All (qubit) decoherences: complete characterization and physical implementation. *Physical Review A—Atomic, Molecular, and Optical Physics, 72*(2), 022110.

Zohuri, B. (2020). What is quantum computing and how it works. *Journal of Material Sciences & Manufacturing Research*, *1*(1), 1-5.



**Publisher's Note**- Ram Arti Publishers remains neutral regarding jurisdictional claims in published maps and institutional affiliations.