International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

Quantum Computing: A Review Of Current Trends And Future Directions

Harini P[1], Kiran Kumar G S[2], Mohammad Sadiq[3], Harsha B[4], Altaf Ahmed[5], Dr. Gurunath R[6]
[1, 2, 3, 4, 5]PG-MCA, Dept. of MCA, Dayananda Sagar College of Arts, Science and Commerce, Bangalore, India.
[6]Associate Professor, Dept. of MCA, Dayananda Sagar College of Arts, Science and Commerce, Bangalore, India.
EmailID: *haripartheeban27@gmail.com[1],kirankumargs02@gmail.com[2], mohammadsadiqmaniyar786@gmail.com[3], harshashiva33@gmail.com[4], meeraltaf123456@gmail.com[5], gurunath@dayanandasagar.edu[6]*

Abstract
Quantum computing is a paradigm shift in computational science, where computational tasks that cannot be computationally tackled with binary computing systems can be tackled using quantum mechanics principles, including superposition, entanglement, and quantum interference. The present paper gives a comprehensive summary of the present condition of quantum computing, including the most advanced hardware systems, such as topological qubits, photonics processors, trapped-ion systems and superconducting qubits, and their corresponding advantages and technical challenges. Also, quantum algorithms, including the Quantum Approximate Optimization Algorithm (QAOA) and the variational quantum eigen solvers (VQE), include a summary of the first algorithm, Shor's factorization method, and the second algorithm, Grover's search algorithm. Applications of such algorithms are evaluated in such areas as financial modeling, machine learning, material science, drug discovery, and cryptography. Taking into account the information provided by large research facilities and technology firms, the conditions under which quantum systems can outperform conventional technology, such a concept as quantum advantage is given specific focus in this review. Moreover, this paper pays particular attention to the key barriers to effective implementation, such as qubit decoherence, large error rates, scalability issues, and the lack of fault-tolerant quantum devices that can be sold commercially. Regarding the noisy intermediate-scale quantum (NISQ) devices that are expected to be available in the near future, we discuss novel approaches to quantum error correction, especially surface code and concatenated code. The quantum software industry, such as IBM Qiskit, Google Cirq, and Microsoft Q, and an evaluation of quantum workforce and research facility readiness across the globe is also discussed. In the end, this work highlights essential potential future paths, such as standards for post-quantum cryptography, hybrid quantum-classical computation, quantum networking and the quantum internet, and the long-term aims for universal fault- tolerant quantum computers. The review should provide researchers, graduate students, and practitioners with a systematic and up-to-date base to understand the fast-growing discipline of quantum computing and its extensive implications on science and business.

Keywords: *Examples of quantum technology include Quantum Computing, Qubits, Superposition, Quantum Entanglement, NISQ Devices, Quantum Algorithms, Quantum Error Correction, Superconducting Qubits, Quantum Advantage, Post- Quantum Cryptography, Hybrid Quantum-Classical Computing and Quantum Machine Learning.*

1. Introduction

The constraints of conventional computing have driven scholars towards the consideration of entirely new paradigms of information processing. The development of modern day processors has been incredible since the invention of Turing Machine, and the density of transistors has doubled every two years, as part of the Moore Law[1]. This traditional growth, however, has been faced with some basic

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

physical constraints especially with the problem of quantum tunneling as transistors are reduced to atomic scales[2]. The introduction of quantum computing is an important move out of binary logic and into systems operating in the spirit of probabilistic and nonlocal ideas of quantum mechanics. Quantum computers make use of quantum bits, or "qubits" as compared to current computers, which manipulate information with bits, which are represented by distinct states of 0 or 1. Computationally, this difference might not be very important, but has far reaching mathematical consequences, as it opens up exponentially growing computational possibilities with each added qubit, rather than linearly growing ones[3].

1.1. Historical Context: From Feynman To Modern Hardware

In 1981, physicist Richard Feynman delivered a landmark speech at MIT, in which he wrote: The nature of things is not classical, and in order to make a simulation of nature, it must be quantum mechanical. This may be regarded as the beginning of quantum computing. Meanwhile, Yuri Manin and Paul Benioff suggested theoretical models that showed that computers could be able to run using quantum phenomena[5]. This was followed shortly, in 1985, by David Deutsch suggesting the concept of the Universal Quantum Turing Machine, which states that a quantum computer can effectively simulate any physical process. In 1994, when Peter Shor published an algorithm proving that quantum computing may undermine the cryptographic underpinnings of the internet, this theoretical interest turned into a question of national security. Structured so that the amplitudes of the correct responses are constructively interfering, and the amplitudes of the incorrect responses are destructively interfering[4].

2. Hardware Architecture Designs

Arguably, the greatest technological difficulty of our day is putting quantum theory into practice. The DiVincenzo Criteria is a strict set of criteria created by David DiVincenzo that must be fulfilled by a practical qubit. Having a solid backing of both government and commercial enterprises, a myriad of competing architectures has emerged[6].

2.1. Superconducting Qubits

The foundation of the quantum programs started by titans like IBM, Google, and Rigetti are superconducting qubits, which are mostly made up of specialized electrical circuits that have been cooled to very low temperatures[7].

Mechanism: These circuits rely on the Josephson effect. An anharmonic oscillator consisting of a capacitor and a nonlinear inductor (a Josephson junction) is a typical superconducting qubit. The state of the qubit is controlled by the researchers using carefully tuned microwave pulses targeting this circuit[8].

Key Advantages: Superconducting qubits are lithographically printed on the existing CMOS manufacturing platform, using established semiconductor manufacturing technologies during the last few decades[10]. They have macroscopic dimensions and therefore can operate on a short time scale of gates, typically in the nanosecond range (10−9 seconds)[9].

Technical Hurdles: The functionality of such chips should be sustained in huge cryogenic dilution refrigerators at temperatures approximately 10 millikelvin (colder than deep interstellar space). Their coherence times can be as low as the microsecond range, which restricts the amount of instructions that can be completed[11].

2.2. Trapped-Ion Instruments

In trapped-ion computers, qubits are made out of the fundamental building blocks of nature: individual atoms. IonQ and Quantinuum companies are the leaders in this strategy[12].

Mechanism: A trapped-ion processor is based on using the changing electromagnetic fields to trap isolated individual ionized atoms. Maps of data are placed to constant electronic energy levels in each atom. The ions are lit up with laser beams that are precisely concentrated to carry out the operations[13].

Key Advantages: Trapped-ion systems are not sensitive to the production flaws that afflict synthetic circuits due to the fact that all atoms of a given isotope are exactly the same. This leads to tremendously long coherence times that can span minutes at a time. Issues in Engineering: Laser gate

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

rates are infamously slow, with tens to hundreds of microseconds per gate, although fidelity is excellent.

2.3. Photonic Processors

Quantum photonic computers do not use fixed materials to store information, but instead use the light particles. This design is leading in innovation by PsiQuantum and Xanadu[14].

Underlying Mechanism: The physical characteristics of single photons are used to represent qubits. Logical operations are implemented by manipulating photons by directing them through a complex interferometer, phase shifter, and beam splitter arrangement[15].

Principal Benefits: Photons have a natural resistance to electromagnetic interference and can, theoretically, be operated at room temperature. They are fully compatible with fiber optic systems and the process of transition to distributed quantum computing is simplified[16].

Difficulties in Engineering: It is nearly impossible to realize deterministic two-qubit entangling gates without the help of complex nonlinearities since photons do not interact efficiently with each other.

2.4. Topological Qubits

The extraordinary states of matter topological framework are highly supported by Microsoft Station Q.

Mechanism: Non-Abelian anyons are quantum data that are coded topologically in quasi-particles[17].

Major Benefits: They are physically hardened to fault tolerance at the level of physical hardware. Decoherence cannot be brought on by environmental disruptions unless the anyons are physically un-braided since the data is stored non-locally[18].

Engineering Issues: The definitive demonstration and isolation of non-Abelian anyons in the laboratory has become an unmatched challenge in physics[19].

2.5. Neutral Atoms And Silicon Spin Qubits

Novel approaches have lately drawn a lot of interest, presenting a threat to the traditional top designs:

Silicon Spin Qubits: Intel and UNSW academics are after these qubits, which store the information in the spins of single electrons trapped in solid silicon. It could be billions of them on a standard computer chip since their size is the same as actual electrons, they can be scaled up with standard lithography to very large sizes.

Neutral Atoms: Firms such as QuEra and Pasqal are trapping neutral atoms of Rubidium or Strontium in three-dimensional arrays with highly focused optical tweezers. The interaction between these atoms is through the Rydberg blockade mechanism, which has excellent potential to be applied to specialized analog quantum simulators capable of working with hundreds of qubits without a large cabling infrastructure. Neutral atoms have been established as extremely programmable logical processing units due to recent advancements in dynamic circuits[23].

2.6. Nitrogen-Vacancy (Nv) Centers In Diamond

One well-known hardware platform is the Nitrogen-Vacancy (NV) center. It is a flaw in a diamond lattice, in which a carbon atom is replaced by a nitrogen atom next to a lattice vacancy.

Underlying Process: Optical initialization and microwave pulses can be used to manipulate qubits by isolating the electron spin of the NV center, and the nuclear spins of surrounding carbon-13 atoms[22].

Main Benefits: NV centers have room temperature stability as a characteristic property. The imperfection can be trapped within the diamond lattice with remarkable coherence times (milliseconds to seconds) and the defect does not require the expensive cryogenic dilution refrigerators (costing a million dollars)[21].

Difficulties in Engineering: A significant challenge to direct large-scale clustering remains to synthesize synthetic diamonds with specific locations of defects accurately, and to be able to entangle isolated NV centers over long distances physically via photonic links[20].

2.7. Hardware Performance Measurement

Benchmarks should be uniformed in various topologies in order to assess feasibility of current devices. The logic gate fidelities and coherence lifetimes are the two key indicators:

T1 and T2 times: Coherence limits of superconducting chips, including the Google Sycamore or IBM Condor architectures, are typically 100 to 300 microseconds. Captured-ion systems, such as those offered by Quantinuum and IonQ, on the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

other hand, have very long T2 times, in the range of seconds or even minutes[24].

Fidelity of the Gates: In order to offer useful fault-tolerance, logic gates fidelity should always exceed 99.9% which is the standard of most surface code algorithms. At present, single-qubit gates used in superconducting technologies typically achieve approximately 99.9% and two-qubit entangling gates, such as the CZ or CNOT gates, can drop to between 98% and 99.5%. This presents important issues to the achievable circuit depth of complete state decoherence because of cross-talk. The popular target of hardware manufacturing companies worldwide is the 5 nines (99.999) target[25.

3. Quantum Algorithms

To develop quantum algorithms, data has to be regarded as a wavefunction. Mathematical base on which creators base is much different and it deals with unitary matrices and manipulation of complex vector space[26].

3.1. Basic Algorithms

Several important algorithms that defined the BQP (Bounded-error Quantum Polynomial-time) computational classification greatly aided in the theoretical development of quantum computing[27].

Shor Algorithm (1994): Shor algorithm applies Quantum Fourier Transform (QFT) to determine the period of a modular exponential function and thus is used to factor complex numbers into their prime factors exponentially, resulting in exponential improvements. This advancement is a major threat to RSA and ECC cryptographic systems[28].

Grover Search Algorithm (1996): The algorithm of Grover searches and finds the solution in O(N) operations, and, in a sense, provides a quadratic speedup to breaking hashes or searching symmetric keys, in an unstructured dataset[29].

Quantum Phase Estimation (QPE): QPE is a crucial subroutine, which is basically included in the HHL and the Shor sub-algorithm. It can effectively measure the eigenvalue (phase) of a unitary operator on a quantum eigenvector. It is known as one of the key processes in quantum science as the Inverse Quantum Fourier Transform in QPE transforms it into a highly accurate binary fractional readout[30].

HHL Algorithm for Linear Systems: An exponential improvement in solving large linear equation systems (solving Ax = b) is offered by the HHL Algorithm of Linear Systems that was developed by Harrow, Hassidim, and Lloyd in 2009. With the underlying physics simulations, machine learning, and engineering relying on huge linear algebra matrices, the ability of HHL to invert an exponentially large matrix fundamentally changes the constraints of algorithms in practical applications.

3.2. Heuristic And Near-Term (Nisq) Algorithms

The advanced fault-tolerant algorithms are reducing to noise in the present Noisy Intermediate-Scale Quantum (NISQ) regime. Consequently, the field is moving towards the direction of heuristic hybrid quantum-classical methods[31].

Variational Quantum Eigensolver (VQE): VQE is a method that uses a classical optimizer to update the parameters of a parameterized quantum state (Ansatz). With VQE converging to the last ground state calculations in molecular chemistry, the environmental noise is significantly reduced since the quantum circuit only requires short-term evaluations at the beginning of each iteration[32].

Quantum Approximate Optimization Algorithm (QAOA): QAOA is an algorithm, which entails a series of exchanges between quantum and classical processors to approximate solutions to NP-hard optimization problems. Such issues are crucial to the industries such as logistics, network design, and finance[33].

4. Applications

Quantum computing is a highly disruptive technology, and could change various areas of the world economy and science due to the theoretical benefits offered by algorithms like Shor, Grover, VQE, and QAOA[34].

4.1. Cryptography And The Post-Quantum Era

Due to the difficulty of modern public key infrastructure (PKI) being based on the computational challenge of factorizing numbers (RSA) or solving discrete logarithmic equations (ECC), a quantum computer sufficiently advanced to execute the algorithm suggested by Shor could break nearly all secure digital online communications. An

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

entirely new area, called Post-Quantum Cryptography (PQC), or sometimes Y2Q or the Cryptopocalypse, is a response to this imminent reality. PQC is based on fundamentally different mathematical concepts, and is theoretically resistant to both classical and quantum cryptography attacks, unlike RSA and ECC. The following salient options have been the main concern of organizations such as the US National Institute of Standards and Technology (NIST):

Lattice-Based Cryptography: is used to create structures such as CRYSTALS-Kyber using the Shortest Vector Problem (SVP) in high-dimensional lattices[35].

Hash-Based Signatures: Digital claims in both stateful and stateless forms using massive Merkle Trees, like SPHINCS+. The international initiative to adopt PQC systems is now being implemented with an understanding of the so-called Store Now, Decrypt Later threat model whereby the attackers are currently amassing encrypted information that will be decrypted in the future by quantum computer[36].

4.2. Quantum Chemistry, Pharmaceutical Discovery

Nature is not classical, but quantum in its very essence, and this is what the great physicist Richard Feynman said in the 1980s. The depiction of a molecule needs a quantum computer to be done accurately. Variational Quantum Eigensolver (VQE) is a method scientists hope to use to simulate the correct ground state energies of reaction paths. By accurately simulating the activity of a target protein in the presence of thousands of diverse ligand structures, pharmaceutical companies can potentially vastly speed up the production of targeted treatments, innovative vaccinations and highly personalized medicine, without wasting time in unproductive biochemical production. The large approximation errors that are often found in traditional Density Functional Theory (DFT) calculations are eliminated by this method[37].

4.3. High Materials Science

It is now possible to select special materials with special physical properties by designing materials scientists with special physical properties by precisely simulating atomic and subatomic interactions, as in the drug discovery field. The quantum consortiums are currently engaged in working on projects that involve:

Enhancing Battery Life Chemistry: Simulating cathode decay and studying constant lithium-sulfur densities.

High-Temperature Superconductors: Discovering the rules of superconductivity at room temperature to allow the transfer of electricity losslessly around the globe.

The Haber-Bosch Process and Nitrogen Fixation: Theoretically bypassing the highly carbon-intensive industrial Haber-Bosch process by naturally reproducing the exact catalytic reaction that takes place in nitrogenase enzymes[38].

4.4. Non-Cryptographic National Security Implications

The development of quantum sensing poses a significant challenge to international security infrastructure, despite the concern of decryption being the most significant popular issue. Theoretically, quantum radar technology, utilizing entangled microwave particles, reduces the effectiveness of current stealth camouflage techniques by identifying the small, radar-absorbing shapes of the technology employed in aerospace systems today with ease. Also, very sensitive quantum accelerometers and magnetometers also offer navigation systems which do not rely on the satellite GPS systems, which means that submarines can move through the deep water without necessarily having to surface up strategically to determine their location[39].

5. Quantum Advantage

An important technological breakthrough is called quantum advantage (or quantum supremacy), a point at which a quantum machine can perform a computational task that no conventional supercomputer is likely to be able to perform in a reasonable time. With its 53-qubit superconducting processor, dubbed "Sycamore," Google achieved a well-publicized milestone in 2019. Sycamore was given the task of producing samples of a random quantum circuit. This quantum processor, according to Google, made the sampling task in 200 seconds. They estimated that they would require over 10,000

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

years to run the same simulation on the most powerful classical supercomputer, the Oak Ridge Summit system. This claim was subsequently validated by experiments using photonic networks, including the Jiuzhang quantum computer by Chinese scholars, capable of accomplishing Gaussian boson sampling tasks in a minute or two, compared to billions of years on classical computers. The caveat to the acceptance of random circuit sampling as a real advantage, however, must be made. Though these demonstrations of concept confirm the mathematics of quantum amplitude manipulation over large matrices, they work on problems, which are essentially impossible to solve in practice. The present aim is to prove a viable quantum advantage, which would entail proving a situation where a quantum system performs better than classical techniques in a commercially significant problem, say finding out the specific binding energy of an essential pharmaceutical enzyme[40].

6. Implementation Difficulties

Even with the blistering advancement, physical challenges that make modern prototypes commercially feasible computers are still numerous. Nowadays, we are in the Noisy Intermediate-Scale Quantum (NISQ) era, where a computer contains enough qubits, but lacks any active fault tolerance[41].

Qubit Decoherence (Short T1 and T2 times): Qubits are extremely fragile and are therefore easily broken. The uncontrollable interaction with the environment, even a single photon strike or thermal noise or a noisy electromagnetic field can cause the quantum state to collapse to classical determinism at any particular point in time. Two variables, T1 (relaxation time) and T2 (dephasing time, at which the phase relationship between superposed states is disrupted), are used to measure decoherence[42].

High Gate Error Rates and Cross-Talk: Small variations in computation are due to the tiny inconsistencies in control equipment that arise when a qubit is interacted with by a microwave pulse or laser. Quantum amplitudes are continuous, as opposed to conventional digital computing, where voltage variations might happen without changing a defined 0 or 1. Errors are introduced by each operation, crippling circuit depth. Moreover, in a dense configuration, the condition of altering a single qubit can accidentally cause disturbance to adjacent qubits, a condition referred to as crosstalk.

Cryogenic Thermal Loads and Scalability Limits: A significant technical difficulty in developing a processor with a million qubits is to make it cryogenic. Each qubit in superconducting designs typically has a dedicated coaxial communication line that passes through room temperature generators, through a cryogenic dilution refrigerator stage. This direct point-to-point technology, scalable to millions of qubits, causes unnecessary thermal loads (heat leakage of large copper wiring) that puts the 10-millikelvin environment perilously near boiling.

7. Quantum Error Correction (Qec)

The error-free transmission in traditional computing requires redundancy, which involves the creation of a copy. Yet, quantum mechanics has a strong No-Cloning Theorem that forbids the cloning of any unknown quantum state. Quantum Error Correction (QEC) overcomes this restriction by distributing the quantum information of one "logical qubit" throughout a vast structure composed of many very flawed "physical qubits."

The Surface Code Algorithm: The main design concept is the topological surface code. Physical qubits are organized in a checkerboard pattern in two dimensions. In this setup, the qubits of data and the qubits of measure/syndrome switch. At this time, the system uses parity stabilizer tests on the surrounding syndrome qubits instead of necessarily testing the sensitive data qubits. The software can observe the correction process and find out the position of the phase or bit flip using classical decoders such as Minimum Weight Perfect Matching algorithms to identify which syndrome qubits indicate errors. The Surface Code has a major drawback in that it requires a large amount of resources. The latest estimation is that the balancing of 1,000 to 10,000 imperfect physical qubits is required to generate a perfect logical qubit, which can survive trillions of operations. For this reason, millions of actual processor arrays are required to operate a Shor's architecture.

Concatenated Codes and Classical Parallels: In the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

pre- topological era, concatenated codes used recursively with error-correction logic. Two good examples are the seven- qubit code of Steane and the nine-qubit code of Peter Shor, which could be connected with the classical Hamming codes. Without these related codes, the Threshold Theorem, which says that massive calculations can be done as long as the physical noise is kept below some tolerance threshold cannot be proven. However, in the scaling techniques of solid-state systems, topological structures like Surface and Color codes are favored because they only need nearest- neighbor connections inside of big 2D grids.

8. Software And Ecosystem

Hardware development is only the initial step; to use it successfully requires retraining the world workforce and state-of-the-art algorithmic compilers. The Hybrid Cloud Software Stack: With quantum accelerators being provided to major technology firms (e.g., AWS Braket, IBM Quantum, and Microsoft Azure Quantum) through the integration of quantum accelerators with existing cloud systems, they have been able to succeed in making them available.

IBM Qiskit: This popular open-source Python platform enables algorithms written in traditional imperative programming to be translated into accurate microwave QASM (Quantum Assembly) pulses which can be executed in upstate New York.

Google Cirq: The exact physical calibration which NISQ (Noisy Intermediate-Scale Quantum) hardware architectures need is the main focus of this platform.

Microsoft Q# and QDK: This is a special programming language that is used to write only to translate complex unitary matrices and phase operations into current Visual Studio syntax.

The Looming Quantum Talent Bottleneck: The growing engineering practice is soon to face a quantum bottleneck in the human resources sector with billions of dollars being invested in new companies and research centers. One needs a good background in theoretical condensed matter physics and must be able to work and innovate in this area, but requires a background in low level electrical engineering and computer science compilers. Changing undergraduate programs is now the focus of major international grants.

9. Future Directions

The future development of quantum computing will be determined by three different convergence areas with the traditional networking in the next two decades:

Modular Supercomputing Interconnects: In the state- of-the-art computing systems, quantum units will not be used to execute traditional CPU logic, but instead implement specialized deep circuit accelerators in place of more conventional GPUs.

Quantum Networking and the Entangled Internet: On fiber-optic channels (with protocols such as BB84), the entanglement networks are used by definition to thwart any attempts of eavesdropping: because the measurement of a quantum state is irreversible. The photon's condition is immediately destroyed by any attempt by a possible interceptor to see the results, which alerts the receiver. The main engineering objective is to create sophisticated "Quantum Repeaters" that are necessary to combat optical "Quantum Repeaters" that are necessary to combat optical absorption over huge ocean distances, hence laying the groundwork for a Quantum Internet that is impenetrable worldwide.

3. The Road to FTQC: The overall ambition is to transcend the heuristic NISQ models and design Universal Fault- Tolerant Quantum Computers (FTQC). These state-of-the- art devices will revolutionize the frameworks of algorithms that we can currently not understand through logic error rates between 10−15 in multiple logical qubits.

Concluding Remarks

The most frenzied and strategically salient multidisciplinary engineering competition in the twenty-first century is surely beginning with the emergence of quantum computing out of the theoretical physics realm. The quantum structures provide incomparable abilities to solve complicated molecular, optimisation, and cryptographic issues by the special manipulation of the multi-dimensional wave functions, and conventional systems remain the primary tool of ordinary structural processes. Globally, the trend is towards a gradual and progressive progress, despite the challenges of

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

engineering roadblocks such as thermodynamic cabling constraints, limited coherence times, and the prohibitive cost of surface code infrastructure, which now manifests as a gap between current NISQ technologies and groundbreaking fault- tolerant designs. The strategic adjustments to implement a fully scalable infrastructure are urgent: a post-quantum cryptography must be introduced as a conceptual part of the infrastructure to address the possible "Decrypt Later" risks, a new layer of quantum software development tools should be created, and much money must be invested in the adaptation of hybrid hardware systems. There are three major shifts in the overall scientific approaches, which are required to be prepared to the quantum era.

Appendix A

Quantum logic gates should be analyzed in detail so that we can fully understand the process of executing such algorithms like the Shor Algorithm and VQE. These gates are unitary matrices which operate on state vectors of Hilbert space.

The Pauli Matrices: The single-qubit Pauli gates model rotations along the axes of the Bloch sphere which geometrically models the state space of a qubit.

Pauli-X (Bit-Flip): It flips the probability amplitudes of $|0\rangle$ and $|1\rangle$, much like the traditional NOT gate.

$$X = [0 \;\; 1 \; 1 \;\; 0]$$

Pauli-Y: In conjunction with a bit flip, it introduces a phase shift.

$$Y = [0 \;\; -i \; i \;\; 0]$$

Pauli-Z (Phase-Flip): Flips the phase of leaves state of computational basis $|0\rangle$ fixed.

$$Z = [1 \;\; 0 \; 0 \;\; -1]$$

The Hadamard Gate (H): The Hadamard Gate, which is required to implement the superposition, transforms the basic basis states into equal superposition. It generates a uniform superposition of all 2n possible states when used on a qubit register that is initialized to $|0\rangle$.

$$H = \frac{1}{\sqrt{2}}[1 \;\; 1 \; 1 \;\; -1]$$

Controlled-NOT (CNOT): This is the basic component of quantum entanglement, the Controlled-NOT (CNOT). The CNOT gate consists of two qubits: one of them is the control qubit and the other is the target qubit. Only when the control qubit is in the state $|1\rangle$ does it change the target qubit's state (implement Pauli-X).

$$CNOT = (1 \;\; 0 \;\; 0 \;\; 00 \;\; 1 \;\; 0 \;\; 00 \;\; 0 \;\; 0 \;\; 10 \;\; 0 \;\; 1 \;\; 0)$$

12. APPENDIX B

Any suggested hardware design should comply with the five criteria that David DiVincenzo proposed in his seminal article of 2000, to qualify as a full-fledged universal quantum computer. Physical requirements: The following need to be satisfied:

- **A Scalable Physical System with Well-Defined Qubits:** The system should be scalable to increase the number of qubits without greatly increasing the error rates or the physical architecture. It's also essential to have a thorough understanding of the qubit's internal Hamiltonian.
- **The Capacity to Prepare the State of the Qubits:** Each time a calculation is to be done, the entire register should always be brought into a clean state, especially to the $|000...0\rangle$ state.
- **Long Relevant Decoherence Times (T1 and T2):** The duration of time a qubit can be run without becoming vulnerable to environmental noise must be much longer than the duration of time needed to run a logic gate. To create successful fault-tolerant error correction, ideally the coherence times must be 104 or 105 times slower than the speed of gate operations.
- **Quantum Gate Collection that is Universal:** The design must be capable of actually implementing a collection of gates which can simulate any random unitary transformation. This can be best achieved when the system can produce the Hadamard, Phase, $\pi/8$ (T-gate) and CNOT gates in a way that is consistent.
- A Measurement Capacity Unique to Qubits: The system should have the ability to measure certain qubits to classical states with very high precision at the output of the algorithm, without affecting the other unmeasured qubits nearby.

Case Studies

Some corporate projects which exhibit quantum utility are discussed in a manner that further brings out the industrial implications that are discussed in

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

Section 4.

Case Study 1: JPMorgan Chase and Quantum Risk Analysis

To explore the possibility of using the Quantum Approximate Optimization Algorithm (QAOA) in quantitative finance, JPMorgan Chase has been collaborating with IBM Quantum. The researchers have shown that the quantum amplitude estimation had the potential to analyze financial derivatives with a quadratic enhancement over traditional Monte Carlo techniques by encoding the European Option pricing models into quantum circuits. This fundamental study, although currently limited by the depth capabilities of NISQ devices, indicates that the incorporation of quantum computing into the infrastructure of high-frequency trading and full-risk assessment is more than an idea, but is systematically implemented into the banking process.

Case Study 2: Mercedes-Benz and Quantum Battery Design

Mercedes-Benz, the market leader in the automotive industry, applied quantum simulations in a very close partnership with IBM to investigate the dipole moment of lithium-sulfur battery interactions. The number of electrons involved in the interaction is astronomically large, thus making the analysis of the interactions of so many electrons such enormous combinatorial problems that a standard computer cannot adequately simulate the exact molecular binding energy of these systems. Mercedes-Benz used the supply chain management, as well as in dynamic urban transportation.

Case Study 4: Biogen, Accenture, and Neurodegenerative Simulation

Biogen, a biotech company, partnered with Accenture in a major collaboration in the biomedical sector integrating quantum chemistry and healthcare, and specifically on the molecular biology of neurodegenerative diseases and, specifically, research on treatments of Alzheimer and Parkinson diseases. Combinatorial quantum methods were applied to understand the interactions between different ligand modifications with complex receptors in the brain, discovering molecules with an identical structure with varied isotopes. This approach performs better than traditional chemical discovery approaches by reducing the time, it takes to discover drugs, by years to months, and finds highly effective therapies to complex protein misfolding disorders.

Appendix C: Quantum Fourier Transform (Qft)

An essential subroutine that enables exponential speedups in computing is the Quantum Fourier Transform (QFT), which is required in key algorithms such as Quantum Phase Estimation and in the algorithm of Shor. Unlike the traditional Fast Fourier Transform (FFT), which operates on vectors with a complexity of O(N log N) and where N = 2n , the QFT performs the same transformation directly on the probability amplitudes of superimposed states with a much simpler circuit depth of just O(n2) quantum logic gates.

Mathematical Representation: The QFT acts on any given n-qubit basis state $|x\rangle$ in a transversal manner; that is, the following conventional formula is used:

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle$$

In this case, x and y are different states of computation in the framework of a system with 2n dimensions.

Circuit Application: Iteratively connecting two popular gate types throughout the quantum processor is essential in order to actually carry out the QFT:

Hadamard (H) Gates: This method is used to produce the fundamental, uniform superposition by applying this method systematically to the qubit register.

Controlled Phase Shift Rotations (Rk): Entangling operations that can perform precise complex fractional rotations. Particularly, an Rk gate causes a relative phase change of $e^{2\pi i/2k}$ which depends on the state of the control qubit. When configured symmetrically the final, unmeasured output is a reflection of the phase-encoded fourier basis representation of the original input matrix.

References

[1]. P. W. Shor, "Algorithms Operating in Polynomial Time on Prime Factorization and Discrete Logarithms," SIAM Journal on

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

Computing, vol. 26, no. 5, pp. 1484-1509, 1997.
[2]. L. K. Grover, "An Efficient Quantum Mechanical Method to search databases," in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96), pp. 212-219, 1996.
[3]. J. Preskill, "Quantum Computing in the NISQ Era and the Future," Quantum, vol. 2, p. 79, 2018.
[4]. F. Arute, K. Arya, R. Babbush, et al., "Demonstrating Quantum Supremacy with a Programmable Superconducting Processor," Nature, vol. 574, pp. 505-510, 2019.
[5]. A. Peruzzo, J. McClean, P. Shadbolt, et al., "A Variational Solver on a Quantum Photonic Processor to compute Eigenvalues," Nature Communications, vol. 5, p. 4213, 2014.
[6]. E. Farhi, J. Goldman, S. Gutmann, "A Quantum Approximate Optimization Method," arXiv:1411.4028 [quant-ph], 2014.
[7]. D. P. DiVincenzo, "The Realization of Quantum Computation," Fortschritte der Physik, vol. 48, no. 9-11, pp. 771-783, 2000.
[8]. A. G. Fowler, M. Mariantoni, J. M. Martinis, A. N. Cleland, "Surface Code: Progressing to Large-Scale Practical Quantum Computation," Physical Review A, vol. 86, no. 3, 032324, 2012.
[9]. P. W. Shor, "Method of reducing decoherence in quantum memory," Physical Review A, vol. 52, no. 4, pp. R2493-R2496, 1995.
[10]. A. M. Steane, "Quantum Theory Error Correction Codes," Physical Review Letters, vol. 77, no. 14, pp. 3252-3255, 1996.
[11]. H.-S. Zhong, H. Wang, Y.-H. Deng, et al., "Photon use in Quantum Computational Advantage," Science, vol. 370, no. 6523, pp. 1460-1463, 2020.
[12]. N. Moll, P. Barkoutsos, L. S. Bishop, et al., "Employing Variational Algorithms to Quantum Optimization on Near-term Quantum Devices," Quantum Science and Technology, vol. 3, no. 3, 030503, 2018.
[13]. M. H. Devoret and R. J. Schoelkopf, "An Outlook on Superconducting Circuits to Quantum Information," Science, vol. 339, no. 6124, pp. 1169-1174, 2013.
[14]. C. Monroe and J. Kim, "Expanding the Ion Trap Quantum Computer," Science, vol. 339, no. 6124, pp. 1164-1169, 2013.
[15]. J. L. O'Brien, A. Furusawa, J. Vučković, "Technologies for Quantum Photonics," Nature Photonics, vol. 3, no. 12, pp. 687-695, 2009.
[16]. J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd, "Exploring Quantum Machine Learning," Nature, vol. 549, no. 7671, pp. 195-202, 2017.
[17]. D. J. Egger, C. Gambella, J. Marecek, et al., "State-of-the-Art and Future Perspectives of Quantum Computing in Finance," IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-24, 2020.
[18]. C. Outeiral, M. Strahm, J. Shi, G. M. Morris, S. C. Benjamin, C. M. Deane, "Potential of Quantum Computing in Computational Molecular Biology," WIREs Computational Molecular Science, vol. 11, no. 1, e1481, 2021.
[19]. H. L. Nguyen, et al., "An easy-to-understand guide to quantum machine learning and optimization," Quantum Information Processing, vol. 19, no. 2, p. 57, 2020.
[20]. V. Havlíček, A. D. Córcoles, K. Temme, et al., "Supervised learning with quantum feature spaces," Nature, vol. 567, no. 7747, pp. 209-212, 2019.
[21]. C. H. Bennett and G. Brassard, "Quantum secure communication: Public-key distribution and coin flipping,"
[22]. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179, 1984.
[23]. S. J. Devitt, W. J. Munro, K. Nemoto, "Introduction to quantum error correction," Reports on Progress in Physics, vol. 76, no. 7, 076001, 2013.
[24]. A. W. Cross, L. S. Bishop, J. A. Smolin, J. M. Gambetta, "Quantum Assembly Language," arXiv:1707.03429 [quant- ph], 2017.
[25]. K. Svore, A. Geller, M. Troyer, et al., "Q# and NWQSim: A platform for quantum computing," Proceedings of the 2018 ACM

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0312
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2156 – 2166

International Conference on Supercomputing, pp. 417-428, 2018. National Institute of Standards and Technology (NIST), "Standardization of Post-Quantum Cryptography," NIST.gov, 2022. [Online].

[26]. Y. Cao, J. Romero, J. P. Olson, et al., "Quantum Chemistry in the Age of Quantum Computing," Chemical Reviews, vol. 119, no. 19, pp. 10856-10915, 2019.

[27]. V. V. Albert, K. Noh, K. Duivenvoorden, et al., "Characteristics and functionality of single-mode bosonic codes,"

[28]. Physical Review A, vol. 97, no. 3, 032346, 2018.

[29]. J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, "Challenges in training quantum neural networks: The problem of barren plateaus," Nature Communications, vol. 9, no. 1, p. 4812, 2018.

[30]. V. Havlíček, et al., "Supervised learning with quantum feature spaces," Nature, vol. 567, pp. 209-212, 2019.

[31]. S. K. Liao, W. Q. Cai, W. Y. Liu, et al., "Quantum key distribution of satellites to terrestrial stations," Nature, vol. 549, no. 7670, pp. 43-47, 2017.

[32]. A. K. Ekert, "Quantum secure communication based on the Bell theorem," Physical Review Letters, vol. 67, no. 6, pp. 661-663, 1991.

[33]. C. H. Bennett, G. Brassard, "Quantum secure communication: Distribution of public keys and coin flipping," Theoretical Computer Science, vol. 560, pp. 7-11, 2014.

[34]. D. J. Egger, et al., "Quantum computing applications in finance: Current advancements and future possibilities," IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-24, 2020.

[35]. F. Neukart, G. Compostella, C. Seidel, D. Von Dollen, S. Yarkoni, B. Parity, "Optimization of traffic flow with a quantum annealer," Frontiers in ICT, vol. 4, p. 29, 2017.

[36]. M. V. Kues, et al., "On-chip production of high-dimensional entangled quantum states and their precise control," Nature, vol. 546, pp. 622-626, 2017.

[37]. F. Arute, et al., "Achieving quantum supremacy with a programmable superconducting processor," Nature, vol. 574, pp. 505-510, 2019.

[38]. H. Levine, A. Keesling, A. Omran, et al., "Precise control and entanglement of qubits using Rydberg atoms," Physical Review Letters, vol. 121, 123603, 2018.

[39]. P. C. Maurer, et al., "Quantum bit storage at room temperature greater than one second," Science, vol. 336, pp. 1283- 1286, 2012.

[40]. S. B. Bravyi, A. Yu. Kitaev, "The lattice quantum codes with boundaries," quant-ph/9811052, 1998.

[41]. E. Dennis, A. Kitaev, A. Landahl, J. Preskill, "Memory in topological quantum states," Journal of Mathematical Physics, vol. 43, no. 9, pp. 4452-4505, 2002.

[42]. T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O'Brien, "Technology slots: quantum computers, Nature, vol. 464, pp. 45-53, 2010.