NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 0000-0000 PRINT ISSN: 0000-0000
CyberSystem Journal (CSJ)

CyberSystem Journal *Original Article*

Exploring Quantum Computing: Potential Applications and Current Challenges in Algorithm Design

Amjed A. Ahmed[1,2*], and Mohammad K. Hasan[1]

[1] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600, Bangi, Malaysia
[2] Department of Computer Techniques Engineering, College of Imam Al-Kadhum (IKC), University of Imam Al-Kadhum, 10011, Baghdad, Iraq

***** Corresponding Author: Amjed A. Ahmed, Email: amjedabbas@alkadhum-col.edu.iq.

Abstract: Quantum supremacy refers to the experimental demonstration that a quantum computing device performs a calculation that no classical computer can match in a reasonable time. Such machines would not be useful for solving problems of practical interest, but they would provide a proof of principle that larger and more useful machines could be built. The gap between classical and quantum computing is potentially enormous, and the apparent ease with which quantum states can be prepared, manipulated, and measured has led many to believe that quantum devices might one day outperform classical hardware at solving a broad range of computational tasks. The most immediate goal of progress in quantum engineering is the construction of a device that passes the proofs of principle of quantum supremacy experiments. They would transform a state that can be initialized neutrally, evolve it under a controlled Hamiltonian, then sample from the output distribution. Such devices must possess sufficient connectivity and low noise but can be cared for by classical software. Their demonstration would mark a historic milestone in the development of quantum technology, providing intrigue and awe but little societal benefit. However, if they can be produced with sufficient fidelity and scale, there is hope that more generally applicable quantum engines might be constructed that could exploit the exponential speedup to outperform classical computers for problems of deep societal importance.

Access this article online

Keywords: Classical Algorithms, Quantum Computing, Quantum Cryptography

1. Introduction

Quantum computing is often perceived as an extremely abstract yet fascinating field of knowledge. This article aims to elucidate some of the broad strokes regarding quantum computing, its success, and its downside. It shall try to provide the audience with basic familiarity with quantum computing, which is composed of two components: quantum mechanics and, inspired by that, quantum algorithms [1]. For the sake of brevity, mathematical rigorousness and technical details would be omitted; this is an essay about the big picture of Quantum Computing.

It began by providing an introduction to quantum mechanics as it pertains to information. Some basic concepts such as quantum states, basis states, density matrices, entangled states, no-cloning theorem, Bell states, etc. were elucidated. Some interesting consequences of quantum mechanics with regard to information were highlighted, Figure 1 is illustrated as an example of quantum cryptography. After a discussion of quantum gates, circuits, universal quantum computation, and Hamiltonian

Received February 27, 2024; Revised March 29, 2024; Accepted April 10, 2024; Published June 30, 2024
https://doi.org/10.57238/4srf6b63

simulation with a remark on their physical realizations, Shor’s algorithm was described.

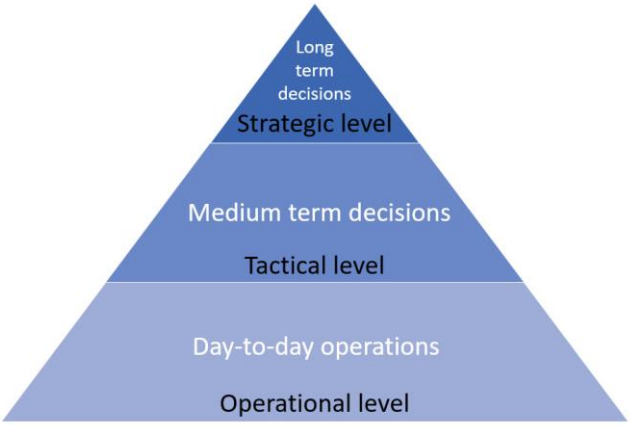


Figure 1. Quantum computing in logistics and supply chain management [2]

1.1 Background and Overview

Quantum computers operate on quantum mechanical phenomena such as wave-function interference, superposition (the ability to be in two or more states at once), and entanglement (the ability of two quantum mechanically coupled systems to be related in a way that does not disappear when the systems are separated). For the sake of simplicity, qubits, quantum registers, quantum gates, and quantum circuits will be defined now 2. Quantum registers are memory units that store the information of a quantum algorithm. A quantum register consisting of n qubits can be in any state $|\Psi\rangle = \sum 2n-1\ i=0\ \alpha i\ |i\rangle$, where $|i\rangle$ are the computational basis states or states of the computational basis of size 2n and the αi’s are complex amplitudes with $\sum 2n-1\ i=0\ |\alpha i|2 = 1$. A quantum register can be in a linear combination of two states, but when measuring it, it takes on one of the states $|i\rangle$ with probability $|\alpha i|$ [2].

Quantum gates are analogous to classical logic gates, as showed in Figure 2. They are reversible unitary operations U that can be defined in matrix form. Quantum gates act on the quantum registers such that a k-qubit gate takes a 2k × 2k matrix operator U and transforms the state $|\Psi\rangle$ of the quantum register into the state U $|\Psi$. Classical gates take a k-bit string and transform it into a k-bit string. A k-bit classical gate can be expressed as a non-unitary matrix of 2k rows and 2k columns. Quantum circuits are composed of quantum registers, classical registers that work as input and output for the algorithm, quantum gates, and measurement operations that ask for the value of a quantum register [1], as shown in Tabel 1.

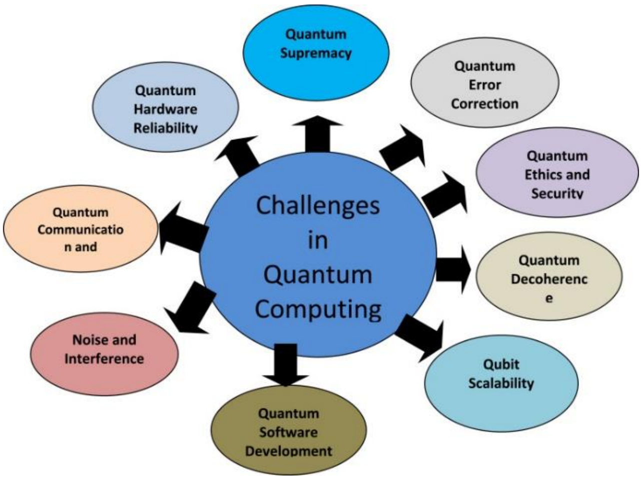

Challenges in Quantum Computing
Quantum Supremacy
Quantum Error Correction
Quantum Ethics and Security
Quantum Decoherence
Qubit Scalability
Quantum Software Development
Noise and Interference
Quantum Communication and
Quantum Hardware Reliability

Figure 2. Quantum computing basics applications [1]

Table 1. Differences between quantum computing and classical computing

Quantum Computing	Classical Computing
• Calculates with Qubits, that can have values 0 or both simultaneously • Power increases exponentially in proportion to the number of Qubits • Have high error rates • Operates at close to absolute zero • Temperature • Much secured to work with • Suited for big/complex tasks, such as- optimization problems, data analysis and simulations	• Calculates with transistors, that can have values either 0 or 1 • Power increases linearly with the number of transistors • Have lower error rates • Operates at room temperature • Less secured to work with • Suited for processing tasks everyday

2. Foundations of Quantum Computing

This section lays the foundation for understanding the principles behind quantum computing systems. In the last two decades, there has been much interest in using quantum mechanics to perform computations on a computer, since it was believed that natural quantum systems were unsuitable for digital computers [2]. The main objective is to review the theoretical principles behind the achievements claimed by a quantum computing strategy. A few promising and widely cited quantum algorithms are presented, along with some current barriers to their implementation [3]. All that is required is a cursory knowledge of linear algebra and some familiarity with information theory. In addition, a simple implementation of some of the algorithms discussed on a contemporary quantum computer is provided, using the

Qiskit software package. A high-level overview of this package is also included.

Quantum computing is profoundly regulated by the principles of quantum mechanics, as show in Figure 3. In contrast to superpositions simply between the two orthogonal states representing "0" and "1" of classical bits, quantum bits or qubits may be in states that are linear combinations of such states. For example, a qubit's state could be $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. Thus, there are generally infinite possible orthogonal states for a qubit. A system of n qubits would have 2n orthogonal states and its state could be represented as a linear combination of the form $|\psi\rangle = \sum$i=0n-1 ci $|i\rangle$, where $|i\rangle$ could be a 2n-bit binary number. The linear coefficients must satisfy $\sum$i=0n-1 $|ci|^2 = 1$, meaning that a system of n qubits may represent an exponential amount of information, generally being 2n bits of information, with respect to classical bits. This quantum parallelism is further exploited when applying quantum gates, which are unitary transformations that manipulate the state of quantum systems [4]. As such, n qubits can process exponentially more information than a classical computer with n bits.

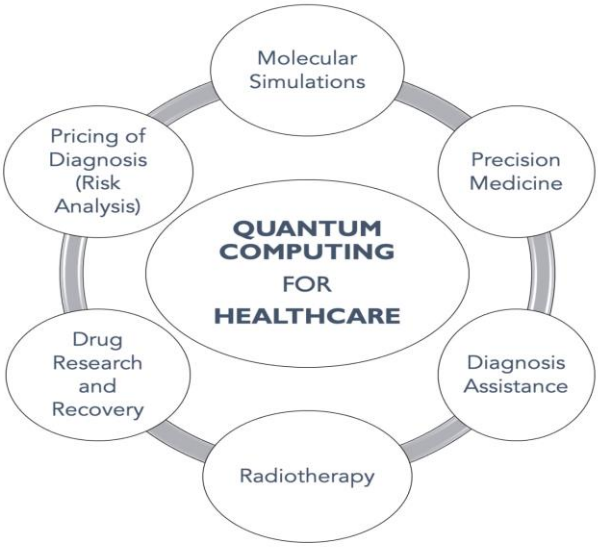

Molecular Simulations
Precision Medicine
Diagnosis Assistance
Radiotherapy
Drug Research and Recovery
Pricing of Diagnosis (Risk Analysis)
QUANTUM COMPUTING FOR HEALTHCARE

Figure 3. Quantum mechanics fundamentals

Pure states may evolve over time only because of 1-Hamiltonians. Under such Hamiltonians, all changes in any quantum system are unitary transformations. This property preserves bit-string orthogonality and means that the action of any Hamiltonian on a quantum system produces no noise. However, when a quantum system interacts with its environment, this result can no longer be guaranteed and unitarity is only valid for the whole system, which includes the environment. The interaction between a quantum system and the environment may be described by 2-Hamiltonians, one that describes the quantum system and the environment and the other that describes the quantum system-environment interaction. The interaction Hamiltonian is generally a time-varying Hamiltonian that may take the quantum system out of its subspace of interest and consequently cause noise. Appliable Hamiltonians of this sort are typically local in nature and correlation between quantum systems in a neighborhood evolves through a process known as decoherence. Therefore, any quantum system that interacts with the environment races to decay in a short time-scale into the well-known classical world measured by classical devices.

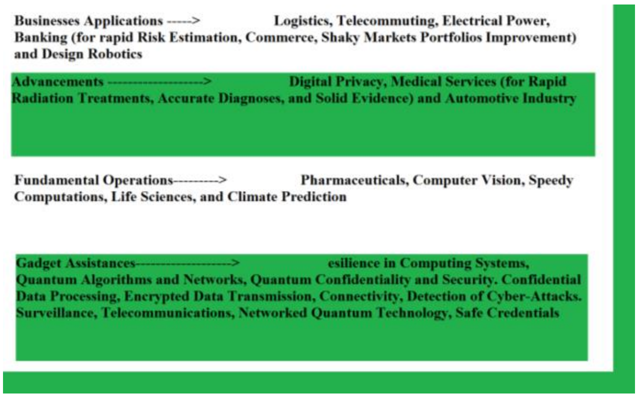
3. Quantum Computing Architectures

Quantum computing systems - both hardware and software - rely on the principles of quantum physics to operate. These systems are capable of performing computationally challenging tasks intractable with conventional computers exponentially faster and thus unlock an entirely new set of computational capabilities. Gate-based quantum computing systems are one of the architectures that can accommodate the development and deployment of quantum applications [5]. In such architectures, qubits are the fundamental unit of information encoded in the property of a physical system, e.g., a superconducting circuit, trapped ions, etc., supporting superposition and entanglement. Quantum gates are well-defined and repeatable operations that manipulate one or more qubits. A quantum circuit consists of a finite number of qubits and quantum gates described using quantum assembly languages like Qiskit or Q#.

A quantum algorithm, Figure 4 executed on a quantum computer to solve a problem, consists of a specific initial setup of qubits, a sequence of gates for manipulating qubits, and a readout operation that extracts and interprets the final measurement outcomes. Together these components represent a quantum program. The quantum compiler receives the quantum program written in a high-level quantum assembly language and optimizes it according to the desired target specifications. The compiler translates the quantum program into a circuit composed of a set of native gates implementable in a specific quantum computing system and optimizes the circuit to minimize the execution cost before it is sent for execution in a quantum processing unit. The quantum processing unit (QPU) executes the quantum circuit and carries out the physical operations in a quantum computing system. The quantum circuit is enacted through a control system that sends microwave pulses and voltage signals to drive the qubits and quantum gates. The readouts are sensitive operations requiring careful control that extracts information from qubits.

3.1 Gate-Based Quantum Computing

An approach that is often discussed in the context of large-scale quantum computing is gate-based quantum computing.



Businesses Applications -----> Logistics, Telecommuting, Electrical Power, Banking (for rapid Risk Estimation, Commerce, Shaky Markets Portfolios Improvement) and Design Robotics

Advancements -------------------> Digital Privacy, Medical Services (for Rapid Radiation Treatments, Accurate Diagnoses, and Solid Evidence) and Automotive Industry

Fundamental Operations---------> Pharmaceuticals, Computer Vision, Speedy Computations, Life Sciences, and Climate Prediction

Gadget Assistances--------------------> esilience in Computing Systems, Quantum Algorithms and Networks, Quantum Confidentiality and Security. Confidential Data Processing, Encrypted Data Transmission, Connectivity, Detection of Cyber-Attacks. Surveillance, Telecommunications, Networked Quantum Technology, Safe Credentials

Figure 4. Find solutions for complex problems quantum skills

Limitations like a prohibitive cost of preparation or measurement in many proven quantum speed-ups are avoided in the gate model as it opens our eye to interesting scenarios where the quantum dynamics is global and traverses many configurations of the states involved. Recently, areas such as quantum hardware and quantum algorithms have gained widespread interest. The fascinating computational power of quantum computers compared with their classical counterparts stems from remarkable phenomena in quantum mechanics, such as superposition and entanglement. The time-evolving Hamiltonians involved in quantum dynamics are typically chosen to preserve the number of particles and/or their resource states. Nevertheless, the global architecture of the quantum Hamiltonians generally allows particle number non-conserving processes.

Pioneering algorithmic proposals showed that quantum computers could leverage this capability to execute some tasks unattainable by classical ones: generating/mimicking global quantum dynamics not efficiently simulable on classical computers and creating a digital quantum simulator of hard-problems instances that efficiently digital quantum computers can tackle [6]. The core of these strategies is based on Europe’s first Quantum Computer Simulator (SimQP), which opens possibilities for observing essential features of quantum complexity investigation in Figure 5, not accessible in the state of the art of quantum hardware, where architectures are still being designed and optimized. It remains a significant challenge to design efficient algorithms for arbitrary many-body states in gate-based quantum computers.

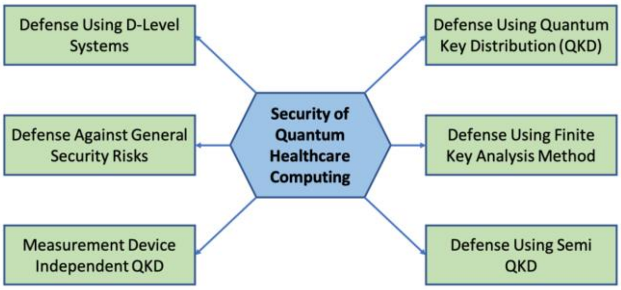

Defense Using D-Level Systems
Defense Using Quantum Key Distribution (QKD)
Security of Quantum Healthcare Computing
Defense Against General Security Risks
Defense Using Finite Key Analysis Method
Measurement Device Independent QKD
Defense Using Semi QKD

Figure 5. Quantum computing: vision and challenges

4. Quantum Algorithms

Quantum algorithms are different from classical algorithms in both their form and execution. Quantum algorithms must use specific processes to manipulate quantum states: linear superpositions and unitary transformations. However, using these fundamental processes often makes it more difficult to find the correct quantum states, since a desired output can frequently be represented by a very complex linear combination of the basic quantum states, i.e., the qubit states with 0 or 1 at each qubit. As a consequence, after any number of transformations (quantum gates), measurements on quantum states can only provide a probabilistic output. The more complex the desired output, the larger the number of transformations and measurements needed to extract a known and preferable output with high probability [6].

There exist quantum algorithms that have a clear computational advantage over the best-known classical algorithms. The most prominent of these is Shor’s polynomial-time algorithm for factoring integers. Shor’s algorithm takes as input a composite number N and a number x that is not a multiple of N. Its output is a non-trivial factor, p, of N. Classically, factoring integers is thought to require exponential time, or at least sub-polynomial time for general numbers. In comparison, Shor’s quantum factorization algorithm executes the correct periodic function in polynomial time and thus produces a good approximation of the desired output [7].

4.1 Shor's Algorithm

Shor’s quantum factoring algorithm is a well-known exponential speedup over classical computations for the integer factorization task, which is crucial to modern cryptographic protocols. A universal gate model based on the natural time evolution of quantum systems, rather than adiabatic evolution, is thought to be the simplest approach to building a scalable quantum processor, capable of implementing Shor’s algorithm. Shor’s algorithm is built upon the following steps: First, carry out the quantum part of the calculation, which on a quantum computer takes time O(n2 log n) from start to finish (for n-bit numbers), then the classical part (O(n2 log n log log n)), and finally, have some integer post-processing, classical within polynomial time, and simple to do by a computer of any kind, which together with the quantum part provides candidate factors of the integer to be factored.

Factoring a number N = pq, in the simplest case where N is the product of just two primes p and q, is a problem for which (1). A quantum computer can decide if a number is composite or probably prime in polynomial time; but, (2) If N has at least three prime factors, then classical computers can be used to discover these in polynomial time. If, on the other hand, N has an unknown p, which is approximately of order N^1/3, then both classical and quantum computers also can be used to discover candidates for p in a number of iterations log(N)/log(p) greater than 1 [7].

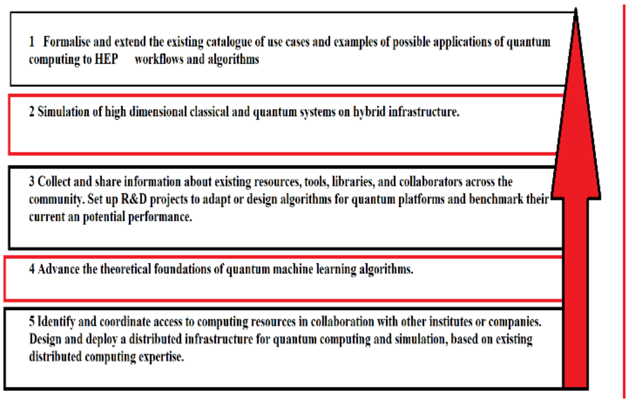
5. Quantum Machine Learning

One important topic at the intersection between quantum computing and AI is “quantum machine learning” (QML). QML is the application of quantum computing to “classical” (non-quantum) machine learning (ML) algorithms, often with the motivation to speed them up in some way. The hope is that by taking advantage of quantum computing, the power of ML algorithms could be harnessed to more efficiently analyze large datasets, recognition patterns, and make predictions based on them [8].

In addition to (and different than) QML, there is also the related topic of quantum neural networks (QNNs) [9]. A QNN is a particular kind of QML algorithm, as it usually is closely analogous to classical neural networks in their structure and function. Like classical neural networks, QNNs are an area of research with the hope of applications in many fields: analyzing data, making predictions, solving mathematical equations, frontal face recognition, texture mapping restoration, stock market modeling, etc. In theory, a well-trained QNN could be exponentially more efficient than any classical architecture of comparable size.

5.1 Quantum Neural Networks

Quantum neural networks, as an application of quantum machine learning, is a rapidly growing area of research. There is great interest in what quantum computers can bring to the field of machine learning. These computers, which could generate and manipulate quantum states to carry out mathematical operations, are fast and complex due to the special characteristics of quantum systems [10]. The most exciting promise of quantum computing is its capability to solve problems that current technological resources cannot hope to compute within useful time limits. For instance, simulating the behaviour of quantal systems, such as new materials or pharmaceuticals, could allow the rational design of molecules with desired properties [11]. Another potential advantage is to find patterns in highly dimensional datasets. Figure 6 could revolutionize industries like finance, telecommunication, health care, and others, which generate huge amounts of data and have difficulties in extracting useful information.



1 Formalise and extend the existing catalogue of use cases and examples of possible applications of quantum computing to HEP workflows and algorithms

2 Simulation of high dimensional classical and quantum systems on hybrid infrastructure.

3 Collect and share information about existing resources, tools, libraries, and collaborators across the community. Set up R&D projects to adapt or design algorithms for quantum platforms and benchmark their current an potential performance.

4 Advance the theoretical foundations of quantum machine learning algorithms.

5 Identify and coordinate access to computing resources in collaboration with other institutes or companies. Design and deploy a distributed infrastructure for quantum computing and simulation, based on existing distributed computing expertise.

Figure 6. Hybrid quantum computing infrastructures, algorithms

6. Quantum Cryptography

Quantum principles can be exploited to devise secure communication protocols. The best-known example is quantum key distribution, QKD. An important class of QKD protocols relies on the properties of quantum measurements. These protocols do not need entanglement to work. The simplest scheme, due to Bennett and Brassard in 1984, is often referred to as BB84, after the initials of the authors [12].

In the BB84 protocol, one of the parties (Alice) wants to send information to another party (Bob). Alice and Bob wish to establish a secret symmetric key that can be used to encrypt/decrypt subsequent messages. First, they agree on a method to encode classical bits as quantum states and to perform measurements on the quantum states. The encoding and measurement bases may be chosen from one of the four pairs of bases: (Z,|+|,|-|), (X,|0⟩,|1⟩), (C,|D⟩,|A⟩), and (C,|J⟩,|M⟩). The first two are the common computational (Z) and Hadamard (X) bases. The last two pairs are non-commuting bases. In order to generate a shared string of bits, Alice begins by randomly choosing a basis for each bit (from {Z,X}) that she wishes to send to Bob and preparing the corresponding states. She sends the states to Bob, who measures them and announces the basis he chose for each measurement (but not the results). Alice then reveals her basis choices and they discard the bits for which Alice and Bob used different bases. The remaining bits form a raw key. Alice and Bob now have correlated bits, but Eve, an eavesdropper, may have partial knowledge of the raw key since she can intercept the quantum states that Alice sends to Bob. To eliminate Eve’s information on the raw key, Alice and Bob must perform error correction and privacy amplification.

6.1 Quantum Key Distribution

Cryptography has been explored as an application of quantum mechanics since the early days of quantum computation. In particular, it has been proposed that certain properties of quantum information—properties that cannot be simulated classically—could be used to enhance the security of data protection measures that are currently at risk of being compromised by quantum computation. Bennett and Brassard first introduced quantum key distribution (QKD) in 1984, which enables a pair of parties to exchange a cryptographic key over a potentially insecure channel, using common sources of randomization [12]. The security of QKD protocols relies on the fundamental characteristics of quantum mechanics, which are immune to increasing power of computation. Over the years, much work has gone into refining theoretical protocols for QKD, analyzing their security, demonstrating them experimentally, and exploring their implications. Conversely, there is a growing realization of how little is known about the security of most classical cryptographic protocols and how, without further research, the world will face an insurmountable cryptographic crisis in the future. Furthermore, the problems of constructing well-founded classical cryptographic systems and of winning trust in practical quantum implementations share interesting similarities. Therefore, the topic of quantum cryptography may hold surprising insights for the classical world, which is of utmost importance for being able to cope with the new risks that quantum technologies confer [13].

Most QKD protocols fall into two families: prepare-and-measure (PM) protocols and entanglement-based (EB) protocols. PM protocols are relatively simple. They use the Heisenberg Uncertainty principle, which states that the measuring act of a quantum state changes that state in a certain way. This makes it very difficult for an attacker to eavesdrop on a communication channel: any attempt at intercepting information invariably changes it in a way that reveals that interception. If the channel was being eavesdropped on, the legitimate exchange parties are able to discard the information and calculate the amount of information that has been intercepted, using a two-step process called parameter estimation.

7. Quantum Simulation

All chemical processes can be viewed as operations on quantum mechanical systems consisting of electrons and nuclei governed by the rules of quantum mechanics [14]. Classical computations of chemical systems either neglect quantum mechanical effects or resort to a numerical solution of the full many-body Schrödinger equation. Because the number of degrees of freedom of a quantum mechanical system scales exponentially with the number of quantum particles, such computations scale poorly with system size. Consequently, systems of interest in chemistry, such as Photo-DNA, gold nanoparticles, and protein folding, are generally deemed “classically impossible” to compute. The exponentially large Hilbert space of quantum systems remains, however, amenable to computation by quantum mechanics itself. Hence, perfect quantum simulators can efficiently simulate any quantum many-body system Hamiltonian that they are initialized in, including those systems of interest to chemistry [15].

It is within the realm of quantum chemistry that quantum computers could have the most profound impact on the ability to model and simulate chemical systems. Although many-body systems are unavoidable in all branches of chemistry, they arise in particularly challenging form in fields such as catalysis, materials science, and biochemistry. Today’s most powerful classical computers readily simulate “complex” chemical systems of thousands of degrees of freedom in the classical limit. However they expeditiously become useless for systems exhibiting quantum phenomena – quantum phase transitions, ground state correlation, photosynthetic complexes, quantum computing with molecular qubits, etc. Anticipated quantum devices with just hundreds of qubits could begin to explore these fascinating quantum systems in ways beyond the capabilities of classical simulations.

7.1 Applications in Chemistry

Today’s powerful computers are able to solve problems of great economic and social importance, while basic scientific understanding of complicated systems is often still lagging behind. One reason for this discrepancy is the exponentially increasing complexity of the system as more constituents are added. Consequently, properties such as the ground states of strongly correlated systems become inaccessible to classical calculations. Such a limit to computation also exists for certain problems, a demonstration of which would be of great theoretical importance. The basic result of this argument is known as ‘quantum supremacy’ [15].

8. Quantum Error Correction

A quantum computer is a powerful computation device. At a fundamental level, at the smallest available size, it is a collection of highly controllable systems. All computations operate on states of these systems, and typically, the states change with time according to a mathematical object called the Hamiltonian [16]. The challenge is that these states are quantum states, and without great care and complex technology, these states will be highly affected by the environment, losing their quantum character and being misinterpreted by the computation device as one of the possible classical states. Once the quantum state is misinterpreted as a classical one, recovering the quantum information is impossible. The loss of the quantum state is called a quantum error. Further, due to the inherent nature of a quantum process operating on Quantum Electric chambers (QEC), there are important characteristics of the quantum states that give rise to additional error possibilities that are absent in classical computation.

Because of the chance of loss of the quantum state due to interaction with the environment, or due to the nature of the operations on the quantum system, which may add errors, there is a need for safeguards to secure the quantum computation [17]. Quantum error correction codes are devices that are capable of recovering a quantum state after it has suffered a limited number of errors, what the classical error correction codes can do. This is done by spreading the quantum information, by acting on the quantum states transformations that have a redundancy against the action of quantum operations that can be considered noiseless. In a quantum circuit, such redundancy would mean performing a projective measurement on an auxiliary register of qubits that are in a certain fixed state, usually called the ancilla qubits.

8.1 Stabilizer Codes

A stabilizer code is a quantum error-correcting code characterized by a special set of operators known as stabilizer operators. These operators are products of Pauli operators whose simultaneous eigenstates form the code space. Stabilizer codes can be understood in terms of group theory and have a collection of useful properties that make them favorable for demonstration in a quantum computing system 18. Error detection and correction processes can be derived by investigating the action of the stabilizer on single-qubit errors.

There are many aspects of stabilizer codes that can be of interest. First, the code may be described in terms of logical operators. For a distance-3 code, a single bit-flip error is unable to corrupt the code, but two bit-flip errors will do so. An important result is the Knill–Laflamme condition, which derives necessary and sufficient conditions for encoding states such that an error will not corrupt a logical qubit. Next, the code may be described using parity checks. A code can be viewed as a collection of parity checks acting on its raw qubits, and the possible corrections can be described as the error syndrome detected by the parity checks. Alternatively, the net operation of the stabilizer can be described using the so-called weight of the operator. If stabilizers are normed Gaussians, weight is defined as the number of qubits that information is spread across, and alternatively the norm of quadratic stabilizers quantifies how strongly a measurement limits freedom [18].

9. Quantum Supremacy

9.1 Experiments and Implications

20 argue that a programmable quantum system consisting of 50 to 100 qubits will allow unprecedented simulations of quantum many body dynamics, exploring the real time evolution of systems Hamiltonians taking the form of tranverse field Ising and similar models. These simulations could revolutionize scientific research, enabling the modeling of devices with technologies expected to outpace current computational approximations. A key milestone towards realizing these applications will be the demonstration of an algorithm which exceeds the capabilities of any classical computer, a demonstration tantamount to achieving quantum supremacy. Sampling problems, such as those described here, are an example of algorithms designed specifically for this purpose. Several implementations of, or proposals for, circuits relevant to such sampling problems have been presented. A successful demonstration of quantum supremacy would be momentous, proving that engineered quantum systems are in fact capable of performing calculations beyond the reach of the most advanced classical computers [19]. Furthermore, this would refocus the community's attention on exploring the capabilities of quantum devices. Nevertheless, before any experimental implementation is undertaken, it is important to comprehend the conditions under which supremacy could be claimed and to characterize these challenges. achieved would be unambiguous evidence of quantum supremacy. To understand the implications of achieving quantum supremacy, it is useful to analyze the evolution of a quantum many-body system under a simple local Hamiltonian. The complexity of simulating this evolution on a classical computer is easy to understand and to quantify. The complexity is then simply given by asking how much classical memory does it take to store the state-vector [20]. Storing the state of a 46-qubit system takes nearly a petabyte of memory and is at the limit of the most powerful computers. Sampling from the output probabilities of such a system, therefore, would constitute a clear demonstration of quantum supremacy.

10. Challenges in Quantum Algorithm Design

Novel quantum algorithms have been designed to run on large-scale quantum systems. Unfortunately, many of them suffered from a serious problem: they were either too noisy or required too regular or deep architectures. Hence, only few of them were recommended by their designers. Moreover, understanding what is still possible on near-term quantum devices raises prosperous open questions, both on a theoretical and an experimental basis.

One important aspect when designing quantum algorithms is to keep noise in mind. On the one hand, one wants to incorporate as much noise reduction as possible, as for example in quantum error correction. On the other hand, there are a number of ideas on how to make quantum algorithms more robust against noise, which could be understood under the aspect of coping with noise [21]. While there is still some understanding of how to design quantum algorithms when noise is taken into account, there is a considerable gap of knowledge when it comes to continuous noise or the more abstract classes of quantum noise, e.g. stochastic quantum maps: these could model an open quantum system that is exposed to an environment yielding some non-unitary effects. Such classes of noise would be important to specify quantum systems that are really scalable towards quantum gravity regimes, fault-tolerant computation, and other fundamental questions in high energy physics and general relativity.

10.1 Noise and Decoherence

Noise and decoherence in quantum systems are the main concerns when designing quantum algorithms. They affect the performance of computations performed by quantum computers. Noise can be caused by environmental interactions, imperfections in experimental setups, or errors in classical post-processing of quantum measurement results. Decoherence is a specific type of noise that refers to the loss of quantum coherence due to the interaction of a quantum system with its environment [22]. That causes a transition from a quantum superposition between the states that are discarded, where the output cannot be determined with certainty, to a classical mixture of the states still in computation that can be post-processed classically.

In quantum mechanics, a quantum state to be measured can be mathematically represented as a vector (or point) in a high-dimensional complex vector space, called a Hilbert space. The physical state of the quantum variable described by that vector would be different for two different bases in that space. As per the principle of relativity, those two bases have to be the same for all observers. Thus, the noise and decoherence mechanisms that represent a change in quantum states must be described in an observer-independent manner [23].

11. Quantum Software Development

This section addresses the topic of software development for quantum computing systems, with a focus on quantum programming languages. There is an overview of the main quantum programming languages used in the development of quantum software. Moreover, a detailed discussion on the development of a quantum algorithm, including design, implementation, compilation, and execution of the quantum circuit is provided. In particular, the compilation and execution phases are described in detail, as they are critical steps for the successful execution of a quantum circuit on a quantum computing device. Furthermore, the challenges of quantum software development, which may have implications on the design and implementation of quantum algorithms, are illustrated [24].

Quantum software development focuses on the creation of programs that can be executed on quantum computing hardware or simulators. Quantum programming languages are software tools that enable developers to write, compile, and run quantum programs on a variety of quantum computing platforms. Similar to classical programming languages, these languages assist programmers in the translation of high-level algorithm specifications into a form that can be executed on quantum machines. However, the peculiarities of quantum mechanics impose significant differences to be considered as compared to classical programming languages [25].

11.1 Quantum Programming Languages

Independently of their physical implementation, all quantum computers offer a set of quantum gates, basis states, and a means to perform measurement. Based on this universal set of quantum gates, a formalism of quantum circuits has been developed. Quantum algorithms are written in terms of this formalism which is similar to Boolean circuits although it explicitly uses continuous unitary transformations [26]. Despite its conceptual simplicity, it seems that this formalism will be inadequate for quantum computers with more than a couple of qubits. The number of design choices grows enormously while the usefulness of qubits in representing the data is destroyed. More abstract and potentially more powerful methods will be required, at least for the design of large quantum circuits.

There are many well-established concepts of classical programming languages like subroutines, local variables or conditional branching. As the general principles of quantum mechanics directly imply probabilities, amplitudes, and non-locality, it is not clear a priori how well these concepts translate into the quantum domain. However, it can be shown explicitly that many of those concepts can be ported to the field of quantum computing [27]. A quantum programming language which semantically integrates those concepts into an existing formalism of quantum circuits will allow for a better and more intuitive understanding of non-classical algorithms, and also be crucial for developing more complex quantum circuits. Quantum subroutines can “accept” and “deliver” qubits, preserving the quantum states; conditional branching can be performed by pausing a computation until the result of a quantum measurement is made available, as there is a well-defined temporal order of operations before and after the measurement; and local variables can be realized by unitary transformations addressing the qubits in subunits.

12. Quantum Computing in Industry

Although still considered an emerging technology by many, quantum computing has taken more substantial steps toward applicability in industry sectors including finance, optimization and materials. Besides multi-million dollar investments in quantum hardware and software, as part of IT and R&D departments, companies and banks also participate in academic-industry collaborations for education, knowledge transfer, and public-private initiatives. Tech-giants like IBM and Google participate in both home-grown and external collaborations. Financial corporations like JP Morgan Chase and Barclays also partnered with academic institutions, including the academic-institution-initiated Qiskit Global Summer School in 2020, and London Institute of Physics in 2021-2023 [28]. Further, there are meaningful industry-consortium initiatives being led by IBM, as described below. Interest in quantum computing has also sparked many start-ups focused on quantum software and algorithms.

Notably, quantum computing is thought to be the first alternative computing model that would reach, and has arguably already reached the level of applicability that justifies its investment; this is so mainly by focusing on the optimization use-case 12. There are now opportunities for investment and collaboration in quantum computing offered to small and mid-sized companies by large tech firms, particularly in North America and Europe. The companies would like to build a true ‘quantum ecosystem’; software applications designed to be run on near-term devices. Products to be developed range from high-level programming languages to quantum applications for chemical simulation, finance, supply chain and logistics, AI and ML, advanced materials discovery, portfolio optimization, risk analysis and others.

12.1 Finance and Optimization

Quantum computing offers the possibility of executing algorithms whose performance cannot be matched on classical architectures, owing to the very different properties of quantum systems. Such algorithms can be classified as either exploiting naturally quantum processes or resulting from significant developments in theoretical physics, mathematics, and computer science. Quantum annealing is an effective strategy for the design of computational algorithms for optimization problems. The space of possible solutions is treated as a physical problem where parameters are manipulated so that the system has a unique minimum corresponding to the optimal solution. Nowadays nimble devices based on this quantum technology are available for demonstrating proof-of-principle implementations of quantum-inspired algorithms, models, and techniques. Industrial applications in finance and optimization can be anticipated, at the starting point in enhancing the discovery of materials, portfolio optimization, or machine learning.

Optimization problems are at the core of many financial problems. These problems traditionally comprise finding a set of values for the variables that minimize/maximize a cost function. A pertinent problem in finance is portfolio optimization, which consists of selecting a fraction of the total capital to invest in different financial assets. The first step is to minimally model the system by estimating the expected returns and correlation matrix of the assets. Given current investment strategies, the methodology used to analyze portfolios is based on distance functions in the space of probability distributions [29]. This modeling approach borders on computational intractability for classical computers as the number of investment opportunities to analyze N increases exponentially because the investment strategies are represented as binary strings of length N (once investment opportunities are selected, all combinations of investments $\gamma i = 0,1$ must be analyzed).

There are several ways to implement algorithms on a quantum computer. The most prominent approach is based on quantum annealing and adiabatic quantum computation [30]. The mapping is performed in preparation for the implementation of a quantum device. The advantage of the approach selected is actually twofold. At the theoretical level, it opens the possibility for a more natural representation of discreet investment opportunities and the reduction in the cost of encoding complex constraints on observed data. At the practical side, the quantum device D-Wave readily implements this mapping at a higher logic level in comparison to the more physical Ising mapping. The architecture of the quantum hardware must be taken into account at the area of implementation of quantum-inspired algorithms in order to devise a coherent implementation and analysis of results.

13. Ethical and Security Considerations

The following discusses ethical and security considerations associated with quantum computing, particularly privacy. This includes considerations based on anticipated advances in quantum hardware and capabilities, as well as consideration of society and institutions more broadly, based on machine learning and advanced AI; the latter is in keeping with observations raised by the National Academy of Sciences (NAS). The anticipated progress of quantum computing is considered in the context of advances in quantum engineering, fabrication, and control that have led or will lead to quantum computing incursions in current mathematics and cryptography.

Privacy and data security in cyberspace “Society is so thoroughly dependent on cyberspace at almost every level that a catastrophic failure of the entire cyberspace institution is tantamount to the collapse of industrial civilization” [31]. The proposal to build quantum computers is, at least in part, based on concerns that the rapid increase in the number of integers used as digital keys, in combination with advances in algorithmic and therefore computational ability, will allow powerful organizations to decode messages. On the other hand, advances in the development of more secure keys can also be anticipated. The discussion herein is somewhat agnostic with respect to the effects on the broader social context due to computer codes and algorithms.

However, “sufficiently powerful artificial intelligence (AI) machines that can aggregate and mode current information-delivering social algorithms” may prefigure a quantum level of threat to human existence, which has been further explored elsewhere. In summary, further considerations of the social implications of new technologies seem to be warranted. Also, based on the recent states of affairs, the current balance between ethical considerations and prudence with respect to the use and development of extant technologies across multiple scientific domains, including intelligence and weaponry, can be seen to be clearly unbalanced. Given historical precedents and recent social trends, societal empowerment with respect to quantum computing seems altogether unlikely.

13.1 Privacy and Data Security

The advancements in quantum computing could have dire consequences for privacy and data security [32]. However, massive investments are being made globally in quantum hardware and software, which would guarantee the creation of so-called powerful quantum computers. Although at this point in time, no significant threat exists towards sensitive data and personal information, there is a strong incentive to prepare and make sensitive data resilient to potential future quantum attacks. This implies that all currently employed public key infrastructure (PKI) either be replaced completely with post-quantum cryptography (PQC) tested systems or data be encrypted and further aggregated before being transferred to potentially low-security environments. The latter is much easier to achieve and can be done within most existing systems.

At the time when quantum computers are mature enough to break encryption methods, a lot of sensitive info about grants, contracts, R&D, etc., will potentially be public information [33]. Data leaks that can allow reverse engineering of products will be very hard to withstand and detect. In the case of personal data leakage, possible breach of privacy might lead to discount credit histories, inflated insurance risks, or stalking. Mere ownership of a quantum computer could potentially allow turning of these negative sides into business opportunities.

14. Future Directions and Open Problems

14.1 Quantum Computing for Climate Change

In terms of specific physics capabilities, modular quantum error mitigation with non-stochastic post-processing schemes also may become possible when quantum clouds coexist with QG and high-fidelity deterministic processes. To realize quantum advantages in these processes, current endeavors are focused on the implementation of quantum memories and the establishment of a quantum cloud-computing networks that could be widely accessible.

Earth system dynamics applications of QG models such as low-latitude long waves, teleconnections, and the quasi-biennial oscillation can further inspire new coupled quantum classes [34]. Compatibility with classical modeling purposes and future satellite observing system developments highlights the synergy between quantum clouds and GCM development. Most importantly, the results further highlight that the added complexity of quantum clouds remains beneficial up to QBN comparable numbers of quantum states. In contrast to purely gravitational systems with QBN-qualitative classical-to-quantum transition, a gradual transition between quantum and classical behavior is revealed here for clouds [35]. Consistent quantum-to-classical dynamics at GCM model resolution is confirmed via laboratory QG and QH experiment studies. Furthermore, with respect to complexity and performances, the results suggest that stochastic GCMs could outpace deterministic GCMs in observational predictability experiments.

References

[1] S. Zhang and L. Li, "A brief introduction to quantum algorithms," *CCF Transactions on High Performance Computing*, vol. 4, pp. 53-62, 2022, doi: https://doi.org/10.1007/s42514-022-00090-3

[2] K. Malenko, "The consequences of quantum computing," BSc Thesis, University of Ljubljana, 2017.

[3] D. Koch, L. Wessing, and P. M. Alsing, "Introduction to coding quantum algorithms: A tutorial series using pyquil," *arXiv:1903.05195*, pp. 1-120, 2019, doi: https://doi.org/10.48550/arXiv.1903.05195

[4] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," *ACM Computing Surveys*, vol. 32, no. 3, pp. 300-335, 2000, doi: https://doi.org/10.1145/367701.367709

[5] A. A. Khan *et al.*, "Software architecture for quantum computing systems—A systematic review," *Journal of Systems and Software*, vol. 201, p. 111682, 2023, doi: https://doi.org/10.1016/j.jss.2023.111682

[6] T. S. Humble, H. Thapliyal, E. Munoz-Coreas, F. A. Mohiyaddin, and R. S. Bennink, "Quantum computing circuits and devices," *IEEE Design & Test*, vol. 36, no. 3, pp. 69-94, 2019, doi: https://doi.org/10.1109/MDAT.2019.2907130

[7] L. M. Baker and L. M. Ogren, "Quantum Algorithms from a Linear Algebra Perspective," 2017.

[8] D. Kopczyk, "Quantum machine learning for data scientists," *arXiv:1804.10068*, pp. 1-46, 2018, doi: https://doi.org/10.48550/arXiv.1804.10068

[9] C. Ciliberto *et al.*, "Quantum machine learning: a classical perspective," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 474, no. 2209, p. 20170551, 2018, doi: https://doi.org/10.1098/rspa.2017.0551

[10] M. Schuld, I. Sinayskiy, and F. Petruccione, "The quest for a quantum neural network," *Quantum Information Processing*, vol. 13, pp. 2567-2586, 2014, doi: https://doi.org/10.1007/s11128-014-0809-8

[11] F. Tacchino *et al.*, "Variational learning for quantum artificial neural networks," *IEEE Transactions on Quantum Engineering*, vol. 2, p. 3101110, 2021, doi: https://doi.org/10.1109/TQE.2021.3062494

[12] E. G. Rieffel, "An overview of quantum computing for technology managers," *arXiv preprint arXiv:0804.2264*, pp. 1-23, 2008, doi: https://doi.org/10.48550/arXiv.0804.2264

[13] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 405-414, 2018, doi: https://doi.org/10.14569/IJACSA.2018.090354

[14] I. Kassal, J. D. Whitfield, A. Perdomo-Ortiz, M.-H. Yung, and A. Aspuru-Guzik, "Simulating chemistry using quantum computers," *arXiv:1007.2648*, pp. 1-27, 2010, doi: https://doi.org/10.1146/annurev-physchem-032210-103512

[15] I. Kassal, J. D. Whitfield, A. Perdomo-Ortiz, M.-H. Yung, and A. Aspuru-Guzik, "Simulating chemistry using quantum computers," *Annual Review of Physical Chemistry*, vol. 62, pp. 185-207, 2011, doi: https://doi.org/10.1146/annurev-physchem-032210-103512

[16] J. Roffe, "Quantum error correction: an introductory guide," *Contemporary Physics*, vol. 60, no. 3, pp. 226-

245, 2019, doi: https://doi.org/10.1080/00107514.2019.1667078

[17] A. Chatterjee, K. Phalak, and S. Ghosh, "Quantum error correction for dummies," in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Bellevue, WA, USA, 2023: IEEE, pp. 70-81, doi: https://doi.org/10.1109/QCE57702.2023.00017

[18] . K. Sarvepalli, "Quantum stabilizer codes and beyond," PhD Thesis, Texas A&MUniversity, 2008.

[19] C. S. Calude and E. Calude, "The road to quantum computational supremacy," in *From Analysis to Visualization*, 2020: Springer, pp. 349–367, doi: https://doi.org/10.1007/978-3-030-36568-4_22

[20] C. Neill *et al.*, "A blueprint for demonstrating quantum supremacy with superconducting qubits," *Science*, vol. 360, no. 6385, pp. 195-199, 2018, doi: https://doi.org/10.1126/science.aao4309

[21] H.-L. Huang *et al.*, "Near-term quantum computing techniques: Variational quantum algorithms, error mitigation, circuit compilation, benchmarking and classical simulation," *Science China Physics, Mechanics & Astronomy*, vol. 66, p. 250302, 2023, doi: https://doi.org/10.1007/s11433-022-2057-y

[22] A. A. Saki, M. Alam, K. Phalak, A. Suresh, R. O. Topaloglu, and S. Ghosh, "A survey and tutorial on security and resilience of quantum computing," in *2021 IEEE European Test Symposium (ETS)*, Bruges, Belgium, 2021: IEEE, pp. 1-10, doi: https://doi.org/10.1109/ETS50041.2021.9465397

[23] S. Dasgupta, "Stability of Quantum Computers," *arXiv:2404.19082*, 2024, doi: https://doi.org/10.48550/arXiv.2404.19082

[24] M. De Stefano, F. Pecorelli, D. Di Nucci, F. Palomba, and A. De Lucia, "Software engineering for quantum programming: How far are we?," *Journal of Systems and Software*, vol. 190, p. 111326, 2022, doi: https://doi.org/10.1016/j.jss.2022.111326

[25] M. Haghparast, T. Mikkonen, J. K. Nurminen, and V. Stirbu, "Quantum Software Engineering Challenges from Developers' Perspective: Mapping Research Challenges to the Proposed Workflow Model," in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Bellevue, WA, USA, 2023, vol. 2: IEEE, pp. 173-176, doi: https://doi.org/10.1109/QCE57702.2023.10204

[26] B. Ömer, "Classical concepts in quantum programming," *International Journal of Theoretical Physics*, vol. 44, pp. 943-955, 2005, doi: https://doi.org/10.1007/s10773-005-7071-x

[27] K. Svore *et al.*, "Q# enabling scalable quantum computing and development with a high-level dsl," in *Proceedings of the real world domain specific languages workshop 2018*, Vienna, Austria, 2018: Association for Computing Machinery, pp. 1-10, doi: https://doi.org/10.1145/3183895.3183901

[28] M. Pistoia *et al.*, "Quantum machine learning for finance ICCAD special session paper," in *2021 IEEE/ACM international conference on computer aided design (ICCAD)*, Munich, Germany, 2021: IEEE, pp. 1-9, doi: https://doi.org/10.1109/ICCAD51958.2021.9643469

[29] R. Orús, S. Mugel, and E. Lizaso, "Quantum computing for finance: Overview and prospects," *Reviews in Physics*, vol. 4, p. 100028, 2019, doi: https://doi.org/10.1016/j.revip.2019.100028

[30] N. Bornman, "An introduction to financial option pricing on a qudit-based quantum computer," *arXiv:2311.05537*, pp. 1-22, 2023, doi: https://doi.org/10.48550/arXiv.2311.05537

[31] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure," *arXiv:2404.10659*, pp. 1-25, 2024, doi: https://doi.org/10.48550/arXiv.2404.10659

[32] M. Möller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethics and Information Technology*, vol. 19, pp. 253-269, 2017, doi: https://doi.org/10.1007/s10676-017-9438-0

[33] R. Au-Yeung, B. Camino, O. Rathore, and V. Kendon, "Quantum algorithms for scientific applications," *arXiv:2312.14904*, p. 71, 2023, doi: https://doi.org/10.48550/arXiv.2312.14904

[34] F. Tennie and T. Palmer, "Quantum computers for weather and climate prediction: The good, the bad, and the noisy," *Bulletin of the American Meteorological Society*, vol. 104, pp. E488-E500, 2023, doi: https://doi.org/10.1175/BAMS-D-22-0031.1

[35] K. Ueno and H. Miura, "Quantum Algorithm for a Stochastic Multicloud Model," *Geophysical Research Letters*, pp. 1-10, 2024, doi: https://doi.org/10.48550/arXiv.2406.11350

How to cite this article

A. A. Ahmed and M. K. Hasan, "Exploring quantum computing: Potential applications and current challenges in algorithm design," *CyberSystem J.*, vol. 1, no. 1, pp. 42-53, 2024. doi: 10.57238/4srf6b63

Access this article online