Quantum Applications in Cryptography, Simulation, and Optimization: A Comprehensive Review

Afreen Jamshed Kara[1], Alka Roy[2]
[1]Institute of Science, Bengaluru, India
[2]DAV University, Jalandhar, India
AfreenJamshed@hotmail.com[1],Alka.Roy09@protonmail.com[2]

Abstract

Quantum computing is rapidly transitioning from a theoretical construct to a practical technology with the potential to revolutionize computation across numerous domains. Among the most transformative applications are cryptography, simulation, and optimization fields where quantum algorithms promise significant advantages over classical methods. This review offers a comprehensive exploration of the current state and future trajectory of quantum technologies in these key areas. We begin by examining foundational quantum algorithms such as Shor's algorithm, which threatens the security of widely used cryptographic protocols through efficient integer factorization, and Grover's algorithm, which accelerates unstructured search problems. These breakthroughs have far-reaching implications for cybersecurity, necessitating the development of post-quantum cryptographic systems. In the realm of simulation, quantum computing enables the modeling of complex quantum systems with exponential efficiency, offering profound applications in chemistry, condensed matter physics**,** and materials science. Simulating molecular interactions, electronic structures, and reaction pathways with high accuracy holds promise for drug discovery, catalyst design, and quantum material development. For optimization, quantum techniques such as quantum annealing**,** quantum approximate optimization algorithms (QAOA)**,** and variational quantum eigensolvers (VQE**)** are being investigated for solving combinatorial and high-dimensional optimization problems that are computationally intensive for classical computers. These applications span logistics, finance, machine learning, and operations research. Despite this progress, significant challenges remain in realizing the full potential of quantum computing. Issues such as qubit decoherence**,** error correction**,** hardware scalability, and algorithm robustness must be addressed to achieve reliable and scalable quantum systems. This review also discusses current technological limitations and surveys emerging approaches to mitigate them. Finally, we outline future research directions, including hybrid quantum-classical systems, improved quantum architectures, and novel algorithm development. Together, these advances will be crucial in bridging the gap between theoretical potential and real-world impact, marking the next frontier in the evolution of computing.

Keywords: Quantum Computing, Quantum Simulation, Quantum Cryptography, Quantum Algorithms

Article Number: SCHORES-JPSE-01-005
SchoRes Journal of Physical Sciences and Engineering
Volume 1, Issue 1, December 2025
Date Published: 1 December 2025

www.schores.org

1. Introduction

Over the past few decades, quantum computing has transitioned from a theoretical curiosity to a strategic technology poised to transform science, industry, and national security. Rooted in the counterintuitive principles of quantum mechanics, including *superposition*, *entanglement*, and *quantum interference*, quantum computing allows for computational paradigms fundamentally different from classical systems. These principles enable quantum processors to perform calculations on multiple inputs simultaneously, promising exponential or quadratic speedups for specific problem classes.

Among the most promising domains for quantum applications are cryptography**,** simulation, and optimization areas where classical algorithms face severe computational bottlenecks. In cryptography**,** algorithms such as Shor's algorithm can factor large integers in polynomial time, undermining the security assumptions behind widely used public-key cryptosystems like RSA and Elliptic Curve Cryptography [11]. This has accelerated the global push toward post-quantum cryptography, with organizations like National Institute of Standards and Technology (NIST) and ETSI working to establish quantum-resilient standards [2].

In quantum simulation**,** first proposed by Richard [5], quantum computers are employed to simulate complex quantum systems that are prohibitively expensive or even impossible to model with classical resources. Applications span molecular chemistry, condensed matter physics, and quantum field theory, offering pathways to design novel materials**,** superconductors, and drug molecules [1][3].

The third domain, optimization, includes a vast set of problems in logistics, supply chain management, portfolio optimization, neural network training, and beyond. These problems often require searching through exponentially large solution spaces, making them ideal candidates for quantum acceleration through algorithms such as Grover's search [6], QAOA [4], and quantum annealing using hardware like D-Wave systems [7].

This paper aims to offer a comprehensive review of quantum computing applications in these three key areas. We analyze the underlying quantum algorithms, evaluate their current implementations and limitations**,** and explore ongoing research efforts aimed at overcoming technical challenges such as noise, decoherence, and scalability. We also assess the hybrid quantum-classical architectures that bridge today's Noisy Intermediate-Scale Quantum (NISQ) era and the fault-tolerant quantum future. Ultimately, this review seeks to inform researchers, engineers, and policy-makers about the state-of-the-art developments, identify critical bottlenecks, and suggest strategic directions for future research and development in quantum-enhanced cryptography, simulation, and optimization.

2. Foundations of Quantum Computing

Quantum computers manipulate quantum bits, or qubits, which differ fundamentally from classical bits. Unlike classical bits that exist strictly as either 0 or 1, qubits can exist in a superposition of states, meaning they can represent both 0 and 1 simultaneously. Another key property is entanglement, where qubits become correlated such that the state of one qubit directly influences the state of another, even when separated by significant distances. Additionally, quantum interference plays a critical role, enabling constructive and destructive interference to amplify or diminish specific probability amplitudes, thereby allowing precise control over computational outcomes.

Quantum algorithms are designed to exploit these unique properties to deliver significant computational advantages over classical algorithms. Notable foundational examples include Shor's algorithm, which allows efficient integer factorization and thus poses a threat to RSA encryption [11], and Grover's algorithm, which provides a quadratic speedup for solving unstructured search problems [6].

Several models of quantum computing have been developed, each with distinct computational paradigms and application domains. Gate-based quantum computers, such as those developed by IBM Q and Google's Sycamore, rely on quantum logic gates to perform computations in a circuit-based manner. Quantum annealers, exemplified by D-Wave systems, are particularly suited for optimization problems and use energy minimization techniques to find solutions. Measurement-based quantum computing, on the other hand, involves computation through sequences of entangled qubit measurements and is conceptually distinct from the other two models.

These models and algorithms collectively illustrate the potential of quantum computing to revolutionize fields such as cryptography, optimization, and data analysis by leveraging phenomena beyond the capabilities of classical systems.

3. Quantum Cryptography

Quantum Cryptography is a field that leverages principles of quantum mechanics to secure communication systems against both classical and quantum attacks. Unlike classical cryptographic methods, which rely on computational hardness assumptions, quantum cryptography offers security rooted in the laws of physics. A key application is Quantum Key Distribution (QKD), such as the BB84 protocol, which allows two parties to share encryption keys with provable security. Any attempt at eavesdropping introduces detectable disturbances, enabling the detection of interception. As quantum computers advance, quantum cryptography is expected to become essential for safeguarding sensitive data against future threats, especially those posed by algorithms like Shor's, which can break widely-used encryption schemes.

3.1. Threats to Classical Cryptosystems

Classical cryptography underpins the security of most modern communication systems, relying heavily on mathematical problems that are computationally infeasible to solve using classical algorithms within a reasonable time frame. Prominent examples include the factoring of large composite integers, which secures the RSA cryptosystem, and the discrete logarithm problem, which forms the basis of protocols such as Diffie-Hellman key exchange and the Digital Signature Algorithm (DSA). These cryptosystems assume that no efficient algorithm exists to solve these problems in polynomial time, thereby ensuring security through computational hardness.

However, the advent of quantum computing fundamentally challenges this assumption. Shor's seminal algorithm, introduced in 1994, demonstrated that a sufficiently large and fault-tolerant quantum computer could solve both integer factorization and discrete logarithms efficiently in polynomial time [11]. This breakthrough implies that widely used cryptographic protocols like RSA, Diffie Hellman, and ECC would become vulnerable to quantum attacks, potentially rendering current public-key infrastructures insecure.

The implications are profound: encrypted data protected under these classical schemes could be decrypted retroactively if stored and later exposed to quantum decryption, posing a significant threat to long-term data confidentiality. This has accelerated the field of post-quantum cryptography, which aims to develop new cryptographic algorithms resistant to attacks by quantum computers while remaining efficient on classical hardware.

Beyond Shor's algorithm, Grover's algorithm provides a quadratic speedup for searching unstructured databases, affecting the security parameters of symmetric-key cryptosystems like AES and hash functions by effectively halving their security level [6]. Although this is less catastrophic than Shor's exponential speedup, it still necessitates doubling key sizes to maintain equivalent security levels against quantum adversaries.

While practical quantum computers capable of executing these algorithms at scale do not yet exist, ongoing advances in quantum hardware make it imperative for the cryptographic community and

industry stakeholders to prepare for a quantum-secure future [9]. The transition involves not only the development and standardization of quantum-resistant algorithms but also the upgrading of existing infrastructures to accommodate these new protocols, a process that is both complex and time-sensitive given the long lifespans of cryptographic keys and the critical nature of digital security.

3.2. Post-Quantum Cryptography

The NIST has recognized the urgent need to develop and standardize cryptographic algorithms that can withstand attacks from quantum computers. In response, NIST launched the Post-Quantum Cryptography (PQC) Standardization Project in 2016, a multi-year global effort to evaluate and endorse quantum-resistant cryptographic schemes suitable for widespread adoption. This initiative aims to ensure the security and integrity of digital communications and data well into the quantum era.

Among the various candidates under consideration, lattice-based cryptography has emerged as a leading approach due to its strong security proofs and efficiency. These systems rely on the hardness of problems such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), which are believed to be resistant to both classical and quantum attacks [2]. Lattice-based schemes have the additional advantage of supporting advanced functionalities like homomorphic encryption and digital signatures, making them versatile for diverse applications.

Other promising categories include code-based cryptography, which is based on the hardness of decoding random linear codes, a problem that has resisted quantum algorithmic breakthroughs for decades. This approach, exemplified by the McEliece cryptosystem, offers high security margins but often suffers from large key sizes. Meanwhile, hash-based cryptographic schemes provide secure digital signature methods that rely solely on the security of underlying hash functions, making them conceptually simple and robust against quantum threats.

NIST's PQC process involves rigorous public evaluation, cryptanalysis, and implementation testing of these algorithms, with the goal of finalizing standards that balance security, performance, and practical deployability. The standardization of quantum-resistant cryptography is critical not only for securing future communications but also for safeguarding existing sensitive data that could be vulnerable to "harvest now, decrypt later" attacks. As the PQC field evolves, collaboration between researchers, industry, and government agencies remains essential to ensure a smooth transition to a quantum-safe digital infrastructure.

3.3. Quantum Key Distribution (QKD)

Unlike classical key exchange protocols that rely on computational assumptions for security, QKD offers unconditional security grounded in the fundamental principles of quantum mechanics. This security arises from the fact that any attempt at eavesdropping on the quantum channel necessarily disturbs the quantum states being transmitted, introducing detectable anomalies. The seminal BB84 protocol, introduced by Bennett and Brassard in 1984, was the first practical scheme to exploit this property. In BB84, two parties commonly called Alice and Bob exchange quantum bits encoded in non-orthogonal bases, allowing them to establish a shared secret key while monitoring for potential interception by an adversary.

Since its inception, QKD has evolved considerably with various improved protocols such as E91, B92, and continuous-variable QKD, each designed to enhance robustness, key rates, and transmission distances. Commercial implementations of QKD now exist, with companies offering solutions for secure key exchange over metropolitan fiber-optic networks. Experimental satellite-based QKD, exemplified by China's Micius satellite mission, has demonstrated quantum communication over thousands of kilometers, proving the feasibility of global-scale quantum-secure networks.

Despite these successes, scalability remains a significant challenge for widespread QKD deployment. Limitations arise from photon loss in optical fibers, distance constraints without trusted nodes or quantum repeaters, and the cost and complexity of integrating QKD hardware into existing communication infrastructures. Quantum repeaters devices that can extend quantum states over long distances without destroying their quantum nature are still in the early stages of development, representing a critical technological hurdle.

Moreover, practical QKD systems must address vulnerabilities such as side-channel attacks, imperfect devices, and implementation loopholes. To counter these risks, device-independent QKD protocols and measurement-device-independent QKD have been proposed, enhancing security guarantees even in less-than-ideal operational conditions.

Overall, QKD represents a promising avenue for future-proof secure communications, especially for governmental, military, and financial institutions where the highest levels of security are mandatory. Continued research into improving key rates, extending transmission distances, reducing costs, and integrating with classical cryptographic infrastructures will be essential to realize the full potential of QKD as part of a comprehensive quantum-safe security framework. Table 1 presents a summary of key quantum algorithms and their primary application domains**.** It highlights the specific problems each algorithm addresses and the computational advantages they offer over classical methods, emphasizing their transformative potential in cryptography, optimization, and quantum simulation.

Table 1: Key Quantum Algorithms and Their Applications

Quantum Algorithm	Domain	Problem Solved	Complexity Advantage
Shor's Algorithm	Cryptography	Integer factorization, discrete logarithms	Exponential over classical (RSA break)
Grover's Algorithm	Optimization	Unstructured search	Quadratic speedup
Quantum Phase Estimation	Simulation	Eigenvalue estimation	Exponential in some cases
Variational Quantum Eigensolver (VQE)	Simulation	Ground state energy calculation	Efficient for NISQ devices
Quantum Approximate Optimization (QAOA)	Optimization	Combinatorial optimization problems	Near-optimal under certain conditions
BB84 Protocol	Cryptography	Quantum key distribution	Unconditional security (ideal case)

4. Quantum Simulation

Quantum simulation is a powerful use case of quantum computing, aiming to tackle problems intractable for classical computers. It offers a transformative tool for understanding and predicting the behavior of complex quantum systems in physics, chemistry, and materials science.

4.1. Simulation of Quantum Systems

Quantum simulation was one of the earliest proposed applications [5]. Quantum computers can efficiently simulate quantum many-body systems, enabling breakthroughs in:

- Molecular dynamics and chemical reactions [1]
- High-temperature superconductivity
- Quantum phase transitions

4.2. Algorithms and Techniques

Key approaches include:

- **Variational Quantum Eigensolver (VQE)**: Hybrid algorithm to find ground states of molecules.
- **Quantum Phase Estimation (QPE)**: Precise energy eigenvalue computation.
- **Trotterization and Hamiltonian simulation**: Discrete time evolution modeling.

4.3. Applications in Materials Science and Chemistry

Quantum simulation allows accurate modeling of catalysts, drugs, and novel materials. Recent studies on small molecules (e.g., hydrogen, lithium hydride) have validated quantum approaches using near-term quantum hardware [8].

5. Quantum Optimization

5.1. Classical Optimization Problems

Optimization is central to disciplines such as operations research, machine learning, and network design. Many such problems are NP-hard and computationally intensive.

5.2. Quantum Approaches

Quantum algorithms offer significant speedups or provide alternative heuristic approaches for solving complex computational problems. One such method is quantum annealing, which is particularly well-suited for combinatorial optimization problems and is implemented in hardware systems such as those developed by D-Wave. Unlike gate-based approaches, quantum annealing leverages the principles of quantum tunneling and energy minimization to find near-optimal solutions in high-dimensional search spaces.

Another prominent algorithm is the Quantum Approximate Optimization Algorithm (QAOA), introduced by [4]. QAOA is a hybrid quantum-classical algorithm designed to run efficiently on current noisy intermediate-scale quantum (NISQ) devices. It balances quantum evolution with classical parameter optimization, making it a practical candidate for near-term applications in optimization. In addition, Grover's algorithm provides a quadratic speedup for unstructured search problems by reducing the number of required queries from O(N)O(N)O(N) to O(N)O(\sqrt{N}) O(N), demonstrating a fundamental advantage of quantum computation in exhaustive search scenarios. Collectively, these algorithms exemplify how quantum computing can outperform classical approaches, particularly in optimization, search, and approximation tasks, even under the hardware constraints of current quantum systems.

5.3. Industrial Applications

Quantum computing offers promising applications in solving complex optimization problems across various domains. In finance, quantum algorithms have been explored for portfolio optimization, where they can efficiently evaluate large sets of investment options to maximize returns and minimize risk [10]. In transportation and logistics, quantum-based approaches to traffic routing enable more efficient navigation and congestion management by evaluating numerous routing possibilities simultaneously. Job-shop scheduling, a critical problem in manufacturing and operations research, can also benefit from quantum techniques by optimizing task assignments and resource allocation to improve productivity and reduce downtime. Furthermore, quantum computing contributes to advancements in machine learning, particularly through quantum-enhanced gradient descent algorithms, which have the potential to accelerate the training of complex models by finding optimal solutions in high-dimensional parameter spaces more efficiently than classical methods. Table 2 outlines application-specific use cases of quantum computing across domains like cryptography, simulation, and optimization**.** It details the potential impact of these use cases and their current level of development, ranging from theoretical research to experimental and early-stage implementations.

Table2: Application-Specific Use Cases

Domain	Quantum Use Case	Impact	Current Status
Cryptography	RSA/elliptic curve breaking with Shor's	Compromises classical public-key systems	Theoretical + simulations
Cryptography	Quantum Key Distribution (QKD)	Secure communications resistant to eavesdropping	Experimental deployments

Simulation	Protein folding and drug discovery (VQE)	Faster and more accurate molecular modeling	Pilot applications
Simulation	Superconductor and catalyst modeling	Advanced material design	Academic and industrial R&D
Optimization	Portfolio and supply chain optimization	Cost and time savings	Early-stage hybrid systems
Optimization	Traffic flow and scheduling (QAOA/annealing)	Real-time dynamic optimization	Proof-of-concept trials

6. Comparative Analysis of Quantum Applications

Quantum computing is impacting cryptography, simulation, and optimization in distinct yet overlapping ways. Each domain presents unique computational challenges and opportunities for quantum advantage, and their comparison reveals the varying levels of algorithmic maturity, hardware demands, and practical deployment readiness.

In cryptography, quantum computing acts as both a threat and a tool. Algorithms like Shor's and Grover's demonstrate that classical public-key systems are vulnerable to quantum attacks, prompting the development of quantum-resistant cryptographic standards. However, practical implementation of these attacks remains far off due to hardware limitations. Conversely, QKD already demonstrates practical, albeit limited, security applications. Among the three domains, cryptography is the most theoretically mature but requires significant scalability for real-world quantum attacks.

In contrast, quantum simulation is one of the most promising near-term applications of quantum computing. Unlike cryptographic attacks that require large-scale fault-tolerant devices, many quantum simulation tasks can benefit from hybrid quantum-classical algorithms on current NISQ devices. Fields such as molecular chemistry**,** material science**,** and drug discovery are seeing early progress using algorithms like VQE and Quantum Phase Estimation, with ongoing collaborations between academia and industry accelerating this trend.

Quantum optimization, while less mature algorithmically, shows considerable potential through approaches such as QAOA and quantum annealing. These techniques target problems in logistics**,** scheduling, and machine learning, offering approximate solutions that are potentially faster than classical heuristics. However, unlike simulation and cryptography, the optimization domain still lacks clear benchmarks for quantum advantage, and existing hardware like D-Wave's annealers are limited by their problem encoding and lack of universality.

Cryptography leads in theoretical maturity but lags in experimental feasibility for quantum attacks. Simulation stands out as a near-term use case with real-world traction, while optimization offers long-term promise but remains exploratory. Each domain is at a different stage of quantum readiness, emphasizing the need for tailored development strategies and interdisciplinary efforts.

7. Challenges and Limitations

Despite significant advancements, quantum computing continues to face several critical challenges that hinder its widespread practical adoption. One of the foremost issues is qubit decoherence and noise, where quantum bits rapidly lose their quantum state due to interactions with the environment, leading to errors in computation. To address this, quantum error correction is essential; however, it imposes a substantial overhead in terms of additional qubits and computational resources, making scalable implementations particularly demanding. The scalability of qubit architectures remains another significant barrier, as current hardware technologies struggle to reliably maintain and control large numbers of qubits with high fidelity. Moreover, algorithmic limitations restrict the capabilities of existing NISQ devices, which are unable to run fully error-corrected algorithms and are limited to approximate or hybrid computations. Additionally, resource estimation for practical, real-world

quantum applications often remains uncertain, with unclear thresholds for when quantum advantage will be realized. These limitations underscore the need for continued innovation in hardware, error mitigation, and algorithm design to fully harness the transformative potential of quantum computing. Table 3 provides a comparison of major quantum hardware platforms, focusing on their underlying technologies, qubit capacities as of 2025, and operational fidelities. It also highlights each platform's target applications, showcasing the diversity of hardware approaches tailored to specific quantum computing tasks.

Table 3: Quantum Hardware Platforms and Capabilities

Platform	Technology	Qubit Count (2025)	Fidelity	Target Applications
IBM Quantum	Superconducting qubits	127–1121 (roadmap)	~99.9%	General-purpose, simulation, QAOA
Google Sycamore	Superconducting qubits	53–100+	~99.9%	Quantum supremacy, benchmarking
IonQ	Trapped ions	29–64	~99.99%	VQE, cryptography, optimization
Rigetti	Superconducting qubits	80+	~98%	Hybrid computing
D-Wave Advantage	Quantum annealing	5000+	NA (annealing)	Combinatorial optimization

8. Future Directions

To achieve practical quantum advantage in cryptography, simulation, and optimization, several key strategies must be pursued. First, significant advancements in quantum hardware are required, particularly in the scalability and coherence of qubit technologies such as superconducting circuits, trapped ions, and photonic systems. These improvements are foundational to achieving stable and large-scale quantum processors. Second, the development of more efficient hybrid algorithms is essential. Enhancing the interplay between classical and quantum components in algorithms like the VQE**,** QAOA, and quantum machine learning models will be critical in leveraging current NISQ devices. Third, robust quantum error correction mechanisms must be implemented to mitigate decoherence and gate errors. Approaches like surface codes and color codes offer promising pathways toward fault-tolerant quantum computing. Additionally, for quantum cryptography to scale globally, efforts should focus on integrating QKD with existing infrastructure, including satellite-based systems and fiber-optic communication networks. Lastly, the inherently interdisciplinary nature of quantum technologies necessitates stronger collaboration among physicists, computer scientists, chemists**,** and industry leaders to translate theoretical breakthroughs into deployable solutions. These coordinated efforts will be vital to unlock the full transformative potential of quantum computing across critical application domains.

9. Conclusion

Quantum computing holds transformative potential across the critical domains of cryptography, simulation, and optimization, each poised to benefit from fundamentally new computational paradigms. The theoretical foundations underlying quantum algorithms such as Shor's algorithm for cryptography, variational methods for quantum simulation, and optimization protocols like QAOA are now well-established, providing clear evidence of quantum advantage in principle. However, translating these theoretical breakthroughs into practical, large-scale applications remains a formidable challenge due to limitations in current quantum hardware, including qubit coherence times, gate fidelities, and error correction capabilities. Significant progress has been made in recent years in both algorithm development and quantum hardware platforms. The emergence of NISQ devices has enabled the first experimental demonstrations of quantum simulation and approximate optimization, validating the potential for near-term applications even without full fault tolerance.

QKD systems have reached commercial viability in certain contexts, marking the beginning of secure quantum communication networks. Despite these advances, several obstacles must be overcome before quantum computing can achieve widespread impact. Scalable and fault-tolerant quantum architectures remain a key engineering hurdle, while improving hybrid quantum-classical algorithms is crucial to fully leverage existing hardware. Moreover, the integration of quantum technologies into classical infrastructures, especially for cryptographic applications, demands new standards and collaborative efforts across disciplines. Looking forward, sustained interdisciplinary research, combined with strategic investments in hardware, algorithm design, and error mitigation, will be essential to unlock the full promise of quantum computing. As these technologies mature, they are expected to revolutionize scientific discovery, enhance cybersecurity, and optimize complex systems across industries, thereby ushering in a new era of computation that fundamentally reshapes our technological landscape.

References

[1] Aspuru-Guzik, A., Dutoi, A. D., Love, P. J., & Head-Gordon, M. Simulated quantum computation of molecular energies. *Science*, 309(5741), 1704-1707, 2005.

[2] Chen, L., Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R.A. and Smith-Tone, D. *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.

[3] Cao, Y., Romero, J., Olson, J.P., Degroote, M., Johnson, P.D., Kieferová, M., Kivlichan, I.D., Menke, T., Peropadre, B., Sawaya, N.P.D. and Sim, S. Quantum chemistry in the age of quantum computing. *Chemical Reviews*, 119(19), pp.10856-10915, 2019.

[4] Farhi, E., Goldstone, J., & Gutmann, S. A quantum approximate optimization algorithm. *arXiv preprint* arXiv:1411.4028, 2014.

[5] Feynman, R. P. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7), 467–488, 1982.

[6] Grover, L. K. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219, 1996.

[7] Johnson, M.W., Amin, M.H., Gildert, S., Lanting, T., Hamze, F., Dickson, N., Harris, R., Berkley, A.J., Johansson, J., Bunyk, P. and Chapple, E.M. Quantum annealing with manufactured spins. *Nature*, 473(7346), pp.194-198, 2011.

[8] Kandala, A., Mezzacapo, A., Temme, K., Takita, M., Brink, M., Chow, J. M., & Gambetta, J. M. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature*, 549(7671), 242–246, 2017.

[9] Nielsen, M.A. and Chuang, I.L. Quantum computation and quantum information, 1991.

[10] Rosenberg, G., Haghnegahdar, P., Goddard, P., Carr, P., Wu, K. and De Prado, M.L. Solving the optimal trading trajectory problem using a quantum annealer. In *Proceedings of the 8th workshop on high performance computational finance* (pp. 1-7), 2015.

[11] Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124–134, 1994.

[12] Terhal, B.M. Quantum error correction for quantum memories. *Reviews of Modern Physics*, *87*(2), pp.307-346, 2015.