Quantum computing: Overview and applications

Ittipong Khemapech [1*] Manachai Toahchoodee [2] Watsawee Sansrimahachai [3] and Tiwa Pensook [4]

Received: 21 June 2025; Revised: 23 November 2025; Accepted: 06 January 2026

Abstract

Advancements in computer technologies have been evolving in order to provide new services or to improve recent computing performance. Applications of computer technologies to several real-world domains are becoming more realistic and efficient. Two challenges are taken into consideration when applying such technologies including more complicated user requirements and exponential growth of data. In the real world, which is driven by business, achieving user requirements is one promising way of yielding competitive advantages. Moreover, time constraints are also crucial for corporate users. Apart from structured data, unstructured data have been significantly generated via several platforms. Such aspects make data processing more demanding. Quantum technology, which is instantiated in physics, has been utilized in various fields including computer science. Even the real quantum computer is still in its early development, but other concepts such as quantum information and quantum computing are making progress. Furthermore, some quantum-based algorithms have been analytically proven to have higher performance compared to the traditional ones. According to such important milestones, quantum computing has been regarded as one of the key infrastructures of future computing. This paper aims to focus on the main aspects of quantum computing including its backgrounds and recent advancement to provide a clearer picture. Its recent applications to intelligent system enhancement, cybersecurity and cryptography empowerment, and finance are addressed. Several key ideas, and opportunities of quantum computing utilization are also outlined based upon systematic reviews of existing works and case studies. Moreover, comparative analysis between classical and quantum computing in terms of core principles, computational efficiency, and practical feasibility is given. Better understanding and proper preparation of applying quantum computing are thus achieved.

Keywords: Application of Quantum Computing, Future Computation, Quantum Computing, Quantum Technology, Quantum-based Development

[*] *E-mail Address (Corresponding Author): ittipong_khe@utcc.ac.th*
[1,2,3,4] *School of Science and Technology, University of the Thai Chamber of Commerce*

1. Introduction

Several technologies have been continuously emerging to fulfill various requirements of society to improve people's quality of lives. In the 1940s, the first computer technologies were developed to facilitate computational tasks, especially in scientific and academic environments (Fernbach, 1985). The first generation of computer was vacuum tube-based and required significant space. To prove the concept, computer was developed to perform specific tasks which were basic numerical calculations and did not accept a variety of input. The first generation can thus be categorized as specific-purpose machines. From such starting point, several ideas and associated technologies have evolved to achieve smaller and cheaper machines for commercial purposes. Moreover, later generations of the computer were transformed from specific purpose to general purpose machines by means of high-level programming language development and storing instructions in memory (GetupLearn, 2021). Based on input and underlying algorithms, computer executes a variety of software or programs and produces various results. According to general aspect, later generations of the computer are more useful and applicable. Applications of computer technologies to several real-world domains are thus becoming more realistic and efficient. User requirements are getting more detailed and complicated to reach competitive advantage by offering better services and products (IEEE, 2020; Salesforce, 2021; & Shailesh, 2025). Moreover, the rise of the Internet and social media generated a large amount of both structured and unstructured data at an exponential rate. Such issues require more powerful computation which in the future goes beyond recent classical computer technologies (Business Wire, 2021).

Quantum technologies are initiated by the subject of physics (Regazzoni, Fowler, & Polian, 2018) where several properties in quantum state can be utilized in various domains such as quantum computer (IBM, 2021; The Verge, 2021; IEEE Spectrum, 2021; Physicsworld, 1998), quantum information (Symmetry, 2022) and quantum computing (Rieffel, & Polak, 2000; Kumar et al, 2015; Gill et al, 2022). Unlike classical computer where the system was started with hardware development, each of main components of quantum system has evolved simultaneously. Several algorithms associated with quantum computing have been proved to be much faster than the traditional ones (Shor, 1994) while quantum computer is still at its early stage. However, quantum computer is not replacing the classical but enhance or apply some specific problems which require complex computation or with time constraints. Quantum computing is regarded as one of the latest revolutions in computer science and better understanding should be made by considering its key characteristics, feasible applications, challenges and opportunities.

This article aims to provide big picture of quantum computing. Several mechanisms behind quantum computation differ significantly from the classical ones. This is mainly because of key properties of quantum state. Quantum computing is generally more powerful and can be applied to various domains of applications. However, utilization of quantum computing has several awareness which should be taken into consideration. Development of quantum computing algorithms has been in progress whereas full-scale quantum computers yet exist. The remaining parts of this article is organized as follows: Section 2 addresses key characteristics of quantum computing. Instead of having only 2 states which are 0 and 1, there are infinite states by implementing qubits or quantum bits. Several ideas or real-world scenarios which benefit from quantum computing application are provided in Section 3. Powerful quantum machine learning, post-quantum cryptography, and quantum-based algorithms for finance are becoming feasible. Section 4 outlines comparative analysis between classical and quantum computing approaches in terms of core principles, computational efficiency, and practical feasibility. Finally, the conclusion is given in Section 5.

2. Quantum computing overview

Quantum technology has been applied to several academic disciplines including computer science. In classical computer systems, three key components are hardware, software and data. This article focuses on quantum computing by means of its overview, and applications. Quantum computer or hardware is beyond scope of this article.

Even an era of quantum theory was recognized by Max Planck's paper published in 1900 (Carson, 2000), its application to other domains such as quantum computing is a novel and exciting phenomenon to the public, especially to computer scientists. Several survey articles focusing on key details of quantum computing are developed (Rieffel, & Polak, 2000; Kumar et al, 2015; Gill et al, 2022; Marella & Paris, 2020). This section aims to outline several key aspects of quantum computing and its differences from classical computing.

2.1 End of classical computers?

Classical computers are becoming smaller, cheaper and more powerful compared to the previous generations. Significant improvement results from an advancement of components development. Key components include hardware and software. One of the main hardware components is processing unit which is regarded as brain of the computer. It was first implemented using vacuum tube in the first generation. This later evolved to maximize the number of transistors and to minimize the size of the electronic circuits which are currently the main component of processing unit (Rieffel, & Polak, 2000). With lowered cost of circuit development, recent computers are thus cheaper (Marella, & Paris, 2020).

The rate at which the number of transistors on a microprocessor chip increase was observed and analyzed by Gordon Moore. He found that the number of transistors would double, and the price of computer would halve very year. Such observation is known as Moore's Law. Smaller transistors have progressed to a point where an essential question arises – How small can the transistor become? If the transistor is reduced to an atomic scale, its characteristics and properties will not be the same due to being in "quantum state" where regular architecture will no longer apply (Rieffel, & Polak, 2000).

2.2 From bit to qubit

In order to simulate various phenomena in continuous or analog form for further processing in computer system, classical computer employs two digital states – ON and OFF or 1 and 0 corresponding to electric signals. The smallest unit that holds a definite binary state (1 or 0) at a time is called "binary digit" or "bit". All data – both data and instruction or computer program; is firstly transformed into binary format to be understood and executed by the computer system. Obtained results are also in binary format and it is then converted to a human readable format.

Quantum computers can be regarded as a new system which is different from the traditional one. Instead of being in 1 or 0, quantum information is capable of representing 1, 0, or other. Such characteristic is named superposition where a feature exists in several separate quantum states at the same time. A bit is therefore not applicable in the classical system and "quantum bit" or "qubit" is then used to demonstrate quantum information [18]. Two main states of a qubit include $|0\rangle$ and $|1\rangle$ compared to 0 and 1 in classical computing. The key difference between bit and qubit is that the qubit can be in superposition where its state can be a linear combination of $|0\rangle$ and $|1\rangle$ (Nielsen & Chuang, 2011). One of the key advantages is that, by applying qubit, quantum computers are thus able to employ an exponentially large Hilbert space which is a complete inner product space regarding the norms defined by the inner product. It is also the mathematical formulation of quantum mechanics which is fundamental of the quantum computing (Quantiki, 2015).

Pure single-qubit states can be represented as a point on a unit sphere called "Bloch" sphere as shown in Figure 1 (Nielsen & Chuang, 2011). A qubit as a unit of quantum information is processed like traditional bit in the classical system. Bloch sphere is used to geometrically represent several operations on single qubits. In Figure 1, the black dot represents a qubit $|\psi\rangle$ on the sphere. The north and the south poles labelled as z axis demonstrate orthonormal computational basis states $|0\rangle$ and $|1\rangle$, respectively. Moreover, the x and y axes point to the other two directions which are orthogonal to each other. A straight line drawn from the origin to the qubit $|\psi\rangle$ deviates θ degree from the z axis whereas its projection on the $x-y$ plane inclines φ degree from the x axis. Hence, the $|\psi\rangle$ is generally written in terms of θ and φ which relates to the combination of $|0\rangle$ and $|1\rangle$ states (Nielsen, & Chuang, 2011; Wie, 2020). Since such factors have infinite values, it can be stated that qubit is able to represent infinite states which makes quantum computing more powerful than the traditional system that relies on bit.

2.3 Key principles of quantum mechanics

Quantum mechanics is regarded as background of quantum computing. Interested particle behaves differently at its smallest scale. In order to understand quantum computing, four key principles of quantum mechanics should be addressed (Schneider & Smalley, 2025).

- Superposition: Quantum bits (qubits) hold quantum information. It can exist in multiple states simultaneously, unlike classical bits which are either 0 or 1. A qubit can be in a combination of both states at once. Superposition allows quantum computers to process many possibilities in parallel that make the quantum computers more powerful than the classical systems.

- Entanglement: Qubits can be correlated in ways where measuring one instantly affects the others, regardless of distance. Entanglement results in powerful connections between qubits that classical systems cannot replicate. Such phenomenal enables complex quantum algorithms.
- Interference: Regarded as engine of quantum computing, quantum states can amplify correct answers and cancel out wrong ones through constructive and destructive interference. This allows quantum algorithms to guide computations towards the right solutions while suppressing incorrect paths.
- Decoherence: Quantum states are extremely sensitive to environmental factors like heat, electromagnetic fields, and vibrations. The quantum states can thus collapse into non-quantum ones. This fragility causes quantum information to decay rapidly, requiring sophisticated error correction and isolation techniques to maintain quantum computations.

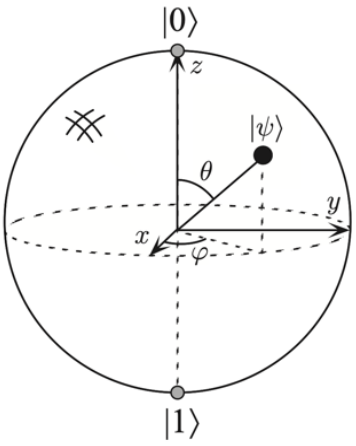


Figure 1 Bloch sphere representation of a qubit (Nielsen & Chuang, 2011)

3. Applications of quantum computing

Computing is an automated process which is performed by computing devices such as computers or smartphones. Initial objective of computing was to facilitate routine tasks to provide faster operations and more accurate results. With technological advancements, key objective has been transformed into providing an intelligent environment to improve quality of life. Higher computing power has been recently required for two reasons. First, more convenient and more personalized products or services are required by people, and businesses or industries are keen to achieve competitive advantages. Second, growth of structured and unstructured data exponentially increased during social media era. Thus, more powerful computing approaches such as quantum computing play a major role in the future of computation.

Realizing the feasible potential of the quantum computing, several applications and commercialization which require complex computation and have time constraints are outlined, such as artificial intelligence, cybersecurity, material science, finance, optimization and modeling (Dargan, 2024; Gossett, 2024; Analyticsindiamag, 2020; Harvard Business School, 2021; Bova, Goldfarb, & Melko, 2021). Several key applications of quantum computing are described in this section.

3.1 Intelligence enhancement

Artificial Intelligence (AI) has been recently of interest to the society. Apart from conducting traditional computing tasks, computer systems have recently become capable of learning and improving its performance based upon training data, received feedback and surrounding environments. Some of the key AI-based disciplines include machine learning, deep learning, natural language processing and computer vision. Due to various applications that can apply AI, various formats or patterns of data are essential. For example, simple text data and those in a 2-dimensional matrix are required for machine learning and computer vision, respectively. In order to gain better performances, such as more accurate predictions, higher amount and quality of data is required. Hence, quantum computing can be utilized in such cases (Analyticsindiamag, 2020 & Harvard Business School, 2021).

Several attempts to build quantum-based artificial intelligence have been realized. Due to recent limitations of quantum systems relying on initial state of quantum computer development, proposed algorithms are mainly analyzed by means of simulations. A quantum-based approach for modeling deep neural networks was proposed which two quantum mechanics related phenomena and one concept was employed including quantum entanglement, quantum teleportation and tensor networks, respectively. Quantum entanglement and quantum teleportation were used to transform classical algorithms into quantum equivalents. Tensor networks were employed for implementing the Convolutional Neural Networks (CNN) model. Moreover, an existing quantum logic circuit demonstrating forward and backward execution of a neural network was adopted for training proposed CNN model (Andreev, & Lazarova, 2020).

Classical machine learning theory and quantum approaches have been integrated to obtain higher system performance. Such integration result in quantum machine learning where quantum approaches were used to analyze quantum state instead of using the classical data. Quantum approaches were applied to both basic machine learning and complicated algorithms or techniques such as k-nearest neighbor algorithm, k-means algorithm and variational autoencoders. Furthermore, multiclass tree tensor network algorithm which is a quantum classification circuit together with its application were demonstrated on an IBM quantum processor (Fastovets, Bogdanov, Bantysh, & Lukichev, 2019).

Quantum machine learning is recently one of interesting research topics. Several algorithms have been developed to tackle the problems that are beyond classical systems' performances. However, quantum-related algorithms are required on quantum computers or their simulated environment. Unlike quantum computing algorithms, development of quantum computers is still in their early stage. Current progress demonstrates highly sensitive to environmental disturbances such as noises. This possibly results in incorrect outputs. Noisy Intermediate Scale Quantum (NISQ) technologies have thus been proposed for implementing quantum circuits. Moreover, NISQ algorithms enable a hybrid quantum-classical approach. Challenge tasks will be offloaded to a quantum computer whereas normal tasked will be operated on classical system (Preskill, 2018; Wang, & Liu, 2024).

Computer vision is one of the AI application domains which requires significant computing power. Deep learning has been utilized for processing image or video input. However, applying deep learning struggles from high resource utilization. Feasibility study on applying quantum machine learning to computer vision is therefore explored. Hybrid quantum-classical algorithms on small-scale quantum devices were used. Results show that image classifier outperforms traditional classical architectures (Mandadapu, 2024). Hybrid algorithm development is one of feasible research tracks. According to Mebtouhe, & Sahnoune (2024), several research possibilities are suggested including quantum feature extraction, quantum activation functions, hybrid quantum-classical models, quantum feature selection and dimensionality reduction, quantum model interpretability, and quantum computing hardware optimization.

Quantum computing has been also applied to Natural Language Processing (NLP) for sentiment analysis. Proposed approach is based upon complex-valued embedding and quantum long short-term memory neural network (Chu, Wang, Jin, Zang, Gao, & Shao, 2024). In order to improve ability to utilize context information, a complex-valued embedding to incorporate more semantic information has been used. It utilizes the Complex-valued Quantum-enhanced Long Short-term Memory Neural Network for feature extraction. Feasible interactions between words are obtained by complex-valued neural network based on density matrix. In terms of leveraging quantum computing, quantum-enhanced scheme motivated by quantum measurement theory and quantum long short-term memory neural network, is developed to learn interactions between sentences.

On the other hand, AI can be employed to empower the quantum computer development including quantum computer development and design, processing, device control and optimization, quantum error correction, and post processing (Alexeev et al, 2024). Main reason of applying AI in such scenario is its data-driven learning capabilities. However, quantum computer development has been in its starting phases which consist of many research challenges and opportunities.

3.2 Cybersecurity and cryptography empowerment

Cybersecurity has been one of major concerns as the numbers of online activities are increasing drastically in the digital era. Instead of conducting several transactions offline, people are using web or mobile applications to fulfill their needs. Cryptography has thus been invented to protect secret data by means of encryption and decryption processes. The more complex cryptography yields more secure data transmission and processing. However, higher computing power is required to yield the target security level. Quantum cryptography

or quantum encryption is referred to such approaches which employ quantum mechanics to achieve secure data encryption and transmission (IBM, 2023). The need for quantum-resistant algorithm has been inspired by Shor's algorithm which theoretically demonstrates the Las Vegas algorithms based upon the power of a quantum computer at the scale of 1,000 physical qubits per-error-corrected qubit on finding the prime factors of integers which could not be solved by a classical computer (Harvard Kennedy School Belfer Center for Science and International Affairs, 2021; Shor, 1994).

Quantum cryptography has been one of the research projects that are of interest. Applications and future prospects are addressed in Sahu, & Mazumdar, (2024). Unlike classical encryption which is based upon specific mathematical problems, quantum cryptography employs principles of physics to get its security. Among various proposed quantum cryptography schemes, Quantum Key Distribution (QKD) is the most well-known. It aims at sharing a secret key between two parties to be used for encrypting and decrypting communications. The information which is composed of a secret key is carried between both parties on qubits. Several challenges of widely deploying QKD include limited transmission rate and range, incompatibility of its point-to-point protocol with the packet-based, requirement of expensive special-purpose hardware and exclusion of authentication and integrity. However, the key advantages of QKD can be observed. Firstly, it is capable of establishing a secret key in a way that is secure against eavesdropping. It can also be integrated with the other encryptions to provide an additional layer of security. Secondly, QKD can be used to detect eavesdropping. Finally, QKD research plays a major role in building future technologies which are based upon quantum revolution. Furthermore, several aspects of QKD including real-world projects, protocol development, real-time key extraction, hardware, mechanisms, auxiliary systems and attacks are described in detail in (Moskovich, 2015).

QKD implementation consists of two setups including continuous-variable (CV-QKD) and discrete-variable (DV-QKD). CV-QKD encodes classical information whereas DV-QKD uses qubits to encode information. Moreover, DV-QKD employs single photon detectors to monitor and quantify eavesdropper in communication channel (Gill et al, 2025). Several QKD-based encryption protocols have been developed. Firstly, the BB84 protocol is the first and most well-known QKD protocol (Bennett, & Brassard, 1984). Two parties can securely exchange encryption keys by employing polarization states of photons. Processes begin with key generation in terms of random bit string. Each bit is then encoded as a photon where four possible polarization states are recognized including two of 45-degree components. The polarized photon is then transmitted to receiver through quantum channel to maintain the polarized state of the photon. Upon receiving the photons, the receiver randomly chooses the base to measure polarization of each incoming photon to make the eavesdropper hard to predict. Both sender and receiver then publicly compare the bases they used for encoding and measuring the photons over the classical channel. Shared string or raw key is thus obtained. Error correction and privacy amplification are also included in the processes. The study by Lee, Sohn, & Lee, (2022) utilizes Hoeffding's inequality to analyze upper bounds of false-positive ratio (FPR) and false-negative ratio (FNR) of eavesdropping detection. Analysis clarifies the trade-off between the accuracy of eavesdropping detection and the economy of utilized quantum resources. Moreover, an extensive simulation study was conducted where the grouped BB84 protocol with 300 qubits. Quantum channel conditions were varied rapidly. Results show that at least over 99% accuracy in eavesdropping detection was guaranteed.

Successive protocols have been proposed. Quantum entanglement is used by E91 protocol for exchanging encryption keys. Entangled photon pairs are generated by a source. One photon from each pair is then sent to sender and receiver to obtain link to the state of each other, regardless of distance between them. Security of the protocol is maintained via polarization management. The sender and receiver independently measure the polarization of their photons using randomly chosen bases. Similar processes to the BB84 protocol will be performed after secure key generation. SARG04 protocol has been extended from the BB84 protocol. Instead of four quantum states, total six quantum states are utilized in order to enhance key generation rates and security (Sahu, & Mazumdar, 2024).

As cryptography impacts the Internet and its services, some standards are outlined and followed for the post-quantum era. Governmental agencies play a major role in initiating, implementing and deploying such standards. Decades may be required to complete the whole process including replacement of the classical system by community (Barker, Polk, & Souppaya, 2021). Post-quantum cryptography standardization process has been initiated by NIST (National Institute of Standards and Technology) since December 2016. The process was started by determining several quantum-resistant cryptographic algorithms. Some of the algorithms were discarded and some have been under further study. Assessment has been conducted and enhanced to identify potential algorithms in terms of security proofs and performance metrics. Three drafts for three Federal Information Processing Standards (FIPS) for key-encapsulation mechanism, and digital signature standards were released in August 2023.

Such standards were open for public feedback and review. NIST has been recently working for a new FIPS (Dekkaki, Tasic, & Cano, 2024).

3.3 Finance

Quantum computing has been regarded as a paradigm shift in computational power. Financial landscape has been transforming into an integration of cutting-edge technologies such as blockchain, AI, and quantum computing. Finance is one of the key backbones which drive economy. Many technology-based financial services have been developed to respond the people's needs. As number and size of data exponentially grows, more computational power is required. Financial institutions struggle with computationally intensive problems, including forecasting, pricing, risk estimation, anomaly detection, and optimization. Traditional methods often strive against complexity and scale of such challenges, paving the way for quantum computing to provide the solutions. Quantum computing applications in finance primarily focus on three areas including stochastic modeling, optimization, and machine learning (Herman, et al, 2023).

Stochastic modeling plays a major role in pricing and risk management, especially for financial derivatives. In finance, stochastic modeling is used to make investment decisions. Value of a derivative, which is a contract whose value is derived from an underlying asset. It is typically calculated by simulating the dynamics of the underlying stochastic process and computing the payoff. Three cases of applying quantum computing in stochastic modeling are addressed. Firstly, Monte Carlo Integration (MCI) approach is used for simulating payoff stochastic process and estimating derivative price. Quantum MCI (QMCI) has been created to achieve more efficiently and accurately estimations compared to traditional MCI where significant risk modeling improvement can be yielded by producing an estimation error using fewer samples (Quantinuum, 2023). Secondly, Greeks (or sensitivities of derivative prices to model and market parameters) computation benefits from quantum computing. Quantum gradient methods can accelerate classical bump-and-reprices method for computing Greeks. Moreover, resource requirements are remarkably lowered (Stamatopoulos, Mazzola, Woerner, & Zeng, 2022). Finally, expected values of certain random variables governed by Stochastic Differential Equations (SDEs) can be expressed as solutions to parabolic Partial Differential Equations (PDEs). Quantum algorithms which utilize Quantum Linear Systems Algorithms (QLSAs) for solving multi-asset Black-Scholes PDEs hold the promise of exponentially reducing computational complexity with respect to dimensionality. Additionally, approaches like Variational Quantum Simulation (VQS) and Quantum Neural Networks (QNNs) are actively being investigated for their potential in addressing PDEs in financial applications (Herman, et al, 2023).

Quantum computing can be used in optimization problems which are prevalent in finance. Both classes including continuous and discrete optimizations are observed. Firstly, continuous optimization problems deal with variables which are continuous values. Key goal is to find values of decision variables which minimize or maximize objective function. This function maps a set of decision variables to a scalar value which represents the problem's objective (Symons, et al, 2023). Several quantum computing approaches to these problems such as linear and semidefinite programs offer potential computational advantages through quantum basic linear algebra subroutines that can improve the worst-case complexity scaling with problem size. Various applications in financial domains including capital allocation, liquidity management, and investment portfolio construction benefit from such schemes. The goal is to optimize asset selection to balance return maximization against risk exposure (Herman, et al, 2023). On the other hand, discrete optimization problems involve decision variables which focus on discrete or categorical values. These problems deal with searching for a finite set of possible solutions which can be very large (Symons, et al, 2023). Numerous financial optimization problems such as portfolio optimization which involve discrete aspects like assets quantities require combinatorial solutions. Quantum algorithms such as quantum walk search (QWS) have demonstrated potential quadratic improvement in tree search procedures which can be utilized to solve complex mixed-integer programs (MIPs). In addition, quantum walk (QW) is beneficial for simulated annealing which is a probabilistic technique for approximating the global optimum of a given function. For example, Markov Chain Monte Carlo (MCMC) technique for tackling combinatorial optimization has demonstrated improved convergence rates using QW (Herman, et al, 2023).

Quantum machine learning (QML) algorithms have been investigated for various financial applications including portfolio optimization, market prediction and trading, pricing, and risk management. Several quantum machine learning algorithms have been developed for supervised, unsupervised, and reinforcement learning tasks which encompass quantum versions of, for example, support vector machines, nearest-neighbor classifiers, and k-means clustering techniques (Mironowicz, et al, 2024). Current research also discovers quantum implementations of expectation-maximization (EM) algorithms for Gaussian mixture models and quantum approaches to spectral clustering paradigms. Quantum computing has also been investigated for enhancing

boosting algorithms which combine weak learners to form strong predictors. In addition, quantum-inspired classical algorithms have been applied to the development of recommendation systems (Herman, et al, 2023).

4. Comparative analysis between classical and quantum computing approaches

Quantum computing has been regarded as a new approach of computing that provides more computational power. It is thus suitable for solving complex problems which are beyond computing power of the classical scheme. Unlike traditional approach, quantum computing is governed by quantum mechanics which benefits from superposition, entanglement and interference. Underlying technologies and concepts make quantum computing perform differently and serve specific requirement in terms of computing power. This section focuses on addressing comparative analysis between classical and quantum computing approaches. Three issues including core principles, computational efficiency, and practical feasibility are determined.

Regarding core principles, units of information used in classical and quantum computing are bit and qubit, respectively. Unlike bit, qubit can be simultaneously represented in 0 and 1 by means of superposition. Classical computing is governed by classical physics whereas quantum computing benefits from quantum mechanics including superposition, entanglement, and interference. As a result, exponential scaling in terms of computational power is feasible in quantum computing. Quantum logic gates such as Pauli-X, Hadamard, and CNOT gates are developed to enable data processing in quantum computing. They can be regarded as building blocks of quantum circuits. Boolean algebra is fundamental in classical computing while linear algebra is used in quantum computing (Arel, 2025).

Both classical and quantum computing approaches are developed for performing computation. Due to several differences, their computational efficiency should be compared. In case of classical computing, it serves general purpose computing tasks which require straightforward algorithms and have linear complexity such as transaction processing, and running software. Efficiency of such scheme is highly reliable and extremely fast for sequential processing. Its algorithms are well-understood, and hardware is highly optimized and mature. On the contrary, quantum computing is developed for specialized, highly complex problems where the computational resources required for classical solutions scale exponentially. Some of the specific tasks include cryptography, simulation, and optimization (SPINQ, 2025). Quantum computing can provide exponential speedups for specific problems.

For example, Google's Sycamore processor completed creating quantum states on 53 qubits corresponding to a computational state-space of dimension 2^{53} in 200 seconds that was estimated to take a powerful classical supercomputer about 10,000 years to complete (Arute, et al, 2019). Regarding cryptography, performance of several classical and post-quantum cryptographic algorithms was empirically compared by means of operation latency, and memory and bandwidth requirements. Classical cryptographic algorithms included RSA-2048, and ECC-P256 while post-quantum cryptographic algorithms consisted of Kyber-512, Dilithium-II, and Falcon-512. Most of the post-quantum algorithms required average operation times on key generation less than the classical ones. Kyber-512 took key generation time 4-time and 1-time less than RSA-2048 and ECC-P256, respectively. However, insignificant differences between both schemes on encryption and decryption were observed. Larger key and cyphertext/signature were required for the post-quantum. Furthermore, all post-quantum algorithms were resistant to quantum vulnerabilities. Unfortunately, both classical algorithms were solved by Shor's algorithm (Scrivano, 2025). Finally, quantum computing integration to classical machine learning has been one of interesting research works. Quantum Support Vector Classifier (QSVC) algorithms were employed to detecting buggy software commits. Their performance was analyzed alongside classical Support Vector Machine (SVC) algorithms. Application of QSVC to large datasets demonstrated significant challenge in terms of exponential runtime requirements of quantum feature mapping. QSVC can be used under specific conditions and the difference between its performance compared to that of classical SVC was insignificant (Nadim, et al, 2025). Similar observation was detected in the comparative study of classical-to-quantum mapping techniques and their impact on machine learning accuracy. An integration of quantum data embedding techniques into classical machine learning algorithms was conducted. Various evaluation metrics were used to address the impacts. The performance of both quantum-integrated and classical approaches was tinily different. However, the results can be used to explore the new way of empowering machine learning by quantum computing (Rath, & Date, 2024).

Classical computing is currently practical technology whereas quantum computing is in its early stage. Various technical hurdles limit quantum computing's current utility. Classical computing is robust and reliable technology with massive global infrastructure. Its relatively low cost for general-purpose machines makes classical computing easily accessible and it does not require special environment. Moreover, error correction mechanisms are well established and efficient. Quantum computing, on the contrary, requires quantum computers

which are not practical for most real-world applications. Current generation of quantum computers is referred to as Noisy Intermediate Scale Quantum (NISQ). They are prone to considerable error rates, and the number of logical qubits is limited. As a result, quantum computers are unreliable to conduct general computation (Dargan, 2025). Most quantum computers require highly controlled and expensive environments such as ultra-low temperatures. Moreover, they are often available only through cloud services or are owned by major research institutions.

Table 1 summarizes comparative analysis between classical and quantum computing approaches which include core principles, computational efficiency, and practical feasibility.

Table 1 Comparative analysis between classical and quantum computing approaches

Issues / Tasks	Classical computing	Quantum computing	References
Core principles			
Unit of information	Bit	Qubit	Nielsen & Chuang, 2011
Circuit behavior	Classical physics	Quantum mechanics (Superposition, entanglement, and interference)	Arel, 2025
Data processing	Binary logic	Quantum logic	Nielsen & Chuang, 2011
Operation	Boolean algebra	Linear algebra	Nielsen & Chuang, 2011
Computational efficiency			
Creating quantum states on 53 qubits	10,000 years	200 seconds	Arute, et al, 2019
Cryptographic algorithms (key generation time)	-	4-time to 1-time less	Scrivano, 2025
Cryptographic algorithms (encryption and decryption)	No significant difference		Scrivano, 2025
Cryptographic algorithms (sizes of key and cyphertext/signature)	-	Larger	Scrivano, 2025
Machine learning			
Quantum Support Vector Classifier	No significant difference		Nadim, et al, 2025
Quantum data embedding	No significant difference		Rath, & Date, 2024
Practical feasibility			
Current utility	Worldwide	Early stage (NISQ)	Dargan, 2025
Accessibility	Easy	Limited	IBM, 2021
Operating environment	Normal	Complex	Arel, 2025

5. Conclusion

During a digital disruption era where more powerful computation is required, quantum computing has been regarded as one of the new frontiers of computing. A new way of computing is introduced by integrating several characteristics and properties of atomic-sized particles or quantum state. Quantum computing can be used in specific tasks which process large amounts of data with time constraints.

This article discusses several important features of quantum computing, including an overview, and some key applications in the real world. As the size of transistor has been becoming smaller and approaching an atomic size, its characteristics and associated properties are changing. Several theories used for traditional systems will

no longer apply and will be replaced by the quantum related scheme. Like classical system, quantum systems mainly consist of hardware, software and data. Quantum computers are in its early development and created by innovative companies. Proposed quantum algorithms corresponding to specific requirements, on the other hand, are built by academia, research institutes and industries. Testing such algorithms is therefore limited to simulation or modified classical computers. Qubit is implemented to hold quantum information. It represents state 0 or 1 or both at the same time. Such capability, superposition, is one of the unique phenomena that makes the quantum system more powerful than the traditional system.

Several domains which apply quantum computing include artificial intelligence, cybersecurity and cryptography, and finance. Comparative study between classical and quantum computing demonstrates an early stage of applying quantum computing to the real-world. The key challenge is that quantum computer is still NISQ which result in limited current utility. Access to quantum computer or quantum platform is limited and expensive due to their early stage of development. Only big companies and large institutions are capable of developing quantum technologies. In order to make quantum computing based applications become reality, collaborations among governmental, academic, research, and industrial parties are crucial. Key challenges of utilizing quantum computing are steep a learning curve, new computing system, limitations on testing and support and collaboration. Several opportunities include empowering computational power, better quality of life and scientific advancement. Finally, it should be noted that quantum computing is not proposed to replace the traditional system. It has been developed to overcome several specific problems that desire higher computing power and performance. Feasible future works include in-depth study on how quantum computing is being used in real businesses and industries. Successful cases can be used as a roadmap of applying quantum computing in real environments.

References

Alexeev, Y., Farag, M. H., Patti, T. L., Wolf, M. E., Ares, N., Aspuru-Guzik, A., Benjamin, S. C., Cai, Z., Chandani, Z., Fedele, F., Harrigan, N., Kim, J.-S., Kyoseva, E., Lietz, J. G., Lubowe, T., McCaskey, A., Melko, R. G., Nakaji, K., Peruzzo, A., Stanwyck, S., Tubman, N. M., Wang, H., & Costa, T. (2024). **Artificial intelligence for quantum computing**. Retrieved 19 June 2025 from https://arxiv.org/abs/2411.09131.

Analyticsindiamag. (2020). **Top applications of quantum computing everyone should know about in 2024.** Retrieved 24 May 2025 from https://analyticsindiamag.com/top-applications-of-quantum-computing-everyone-should-know-about/?fbclid=IwAR2RcF4c_u6YuloMaT8RPSNhfwauuwZYEEoVFkuJZWVTDQh3t5En93g_ND0.

Andreev, D., & Lazarova, M. (2020). **Quantum entanglement-based deep convolutional neural networks**. In CompSysTech'20, 66-73.

Arel, B. (2025). **Classical vs. quantum computing: what are the differences?** Retrieved 22 November 2025 from https://www.techtarget.com/searchdatacenter/tip/Classical-vs-quantum-computing-What-are-the-differences#:~:text=of%20classical%20vs.-,quantum%20computers,is%20the%20number%20of%20qubits.

Arute, F. et al. (2019). **Quantum supremacy using a programmable superconducting processor**. Retrieved 22 November 2025 from https://www.nature.com/articles/s41586-019-1666-5.

Barker, W., Polk, W., & Souppaya, M. (2021). **Getting ready for post-quantum cryptography: exploring challenges associated with adopting and using post-quantum cryptographic algorithms**. Retrieved 15 June 2025 from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf?fbclid=IwAR17bGs3bebuyqKaxzCm8qqbvFMK8oiXa_yumv6sPYLp5ZrdwL5vlf3TiO4.

Bennett, C. H., & Brassard, G. (1984). **Quantum cryptography: Public key distribution and coin tossing**. In IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

Bova, F., Goldfarb, A., & Melko, R. G. (2021). Commercial applications of quantum computing. **EPJ Quantum Technology**. 8, 2. https://doi.org/10.1140/epjqt/s40507-021-00091-1

Business Wire. (2021). **Data creation and replication will grow at a faster rate than installed storage capacity, according to the IDC Global DataSphere and StorageSphere forecasts**. Retrieved 9 May 2025 https://www.businesswire.com/news/home/20210324005175/en/Data-Creation-and-Replication-Will-Grow-at-a-Faster-Rate-Than-Installed-Storage-Capacity-According-to-the-IDC-Global-DataSphere-and-StorageSphere-Forecasts /.

Carson, C. (2000). **The origins of the quantum theory**. Retrieved 20 May 2025 from https://www.slac.stanford.edu/pubs/beamline/30/2/30-2-carson.pdf.

Chu, Z., Wang, X., Jin, M., Zang, N., Gao, Q. & Shao, L. (2024). **An effective strategy for sentiment analysis based on complex-valued embedding and quantum long short-term memory neural network**. Retrieved 19 June 2025 from https://www.mdpi.com/2075-1680/13/3/207.

Dargan, J. (2025). **What is NISQ quantum computing?** Retrieved 22 November 2025 from https://thequantuminsider.com/2023/03/13/what-is-nisq-quantum-computing/

Dargan, J. (2024). **5 crucial quantum computing applications & examples.** Retrieved 21 May 2025 from https://thequantuminsider.com/2023/05/24/quantum-computing-applications/.

Dekkaki, K. C., Tasic, I., & Cano, M. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. **Technologies**. 12, 12. https://doi.org/10.3390/technologies1212024.

Fastovets, D. V., Bogdanov, Y. I., Bantysh, B. I., & Lukichev, V. F. (2019). **Machine learning methods in quantum computing theory**. Retrieved 30 May 2025 from https://arxiv.org/abs/1906.10175.

Fernbach, S. (1985). Computers: The first six generations. **IEEE Transactions on Nuclear Science**. 32, 1. https://doi.org/10.1109/TNS.1985.4336815

GetupLearn. (2021). **Generations of computer first to fifth, classification, characteristics, features, examples**. Retrieved 10 May 2025 from https://getuplearn.com/blog/generations-of-computer-first-to-fifth/.

Gill, S. S., Cetinkaya, O., Marrone, S., Claudino, D., Haunschild, D., Schlote, L., Wu, H., Ottaviani, C., Liu, X., Machupalli, S. P., Kaur, K., Arora, P., Liu, J., Farouk, A., Song, H. H., Uhlig, S., & Ramamohanarao, K. (2025). **Quantum computing: Vision and challenges**. Retrieved 18 June 2025 from https://arxiv.org/pdf/2403.02240.

Gill, S. S., Kumar, A., Singh., H., Sing, M., Kaur, K., Usman, M., et al (2022). Quantum computing: a taxonomy, systematic review and future directions. **Software: Practice and Experience**. 52, 1. https://doi.org/10.1002/spe.3039

Gossett, S. (2024). **10 quantum computing applications and examples.** Retrieved 26 May 2025 from https://builtin.com/hardware/quantum-computing-applications?fbclid=IwAR2P-wqU9wWdcMiP3yJWQZobdbRtAtioMjDDjvSPbiTitix9hKGjYKOhM-Y.

Harvard Business Review. (2021). **Quantum computing is coming. What can it do?** Retrieved 24 May 2025 from https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do?fbclid=IwAR2J0BW_zqcwO8uh1S1VUGHndzjMPM1u-vBjImryOzTAwe7SVdR9y1wyWm4.

Harvard Kennedy School Belfer Center for Science and International Affairs. (2021). **Quantum computing and cybersecurity**. Retrieved 30 May 2025 from https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity?fbclid=IwAR0ny-VruO9zI4lRapYHZ709VTBBnZYGLiRuGNJS2U51BzuA5CJyTTLc1AM.

Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., Pista, M., & Alexeev, Y. (2023). **Quantum computing for finance.** Retrieved 20 June 2025 from https://arxiv.org/pdf/2307.11230.

IBM. (2023). **What is quantum cryptography?**. Retrieved 17 June 2025 from https://www.ibm.com/think/topics/quantum-cryptography.

IBM. (2021). **IBM unveils breakthrough 127-qubit quantum processor**. Retrieved 9 May 2025 from https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.

IEEE. (2020). **Real-life use cases for edge computing**. Retrieved 8 May 2025 from https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/.

IEEE Spectrum. (2021). **Two of world's biggest quantum computers made in China**. Retrieved 10 May 2025 from https://spectrum.ieee.org/quantum-computing-china.

Kumar, K., Sharma, N. A., Prasad, R., Deo, A., Khorshed, M. D. T., Prasad, M., et al (2015). **A survey on quantum computing with main focus on the methods of implementation and commercialization gaps**. In 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), 1-7.

Lee, C., Sohn, I., & Lee, W. (2022). Eavesdropping detection in BB84 quantum key distribution protocols. **IEEE Transactions on Network and Service Management**. 19, 3. https://doi.org/ https://doi.org/10.1109/TNSM.2022.3165202

Mandadapu, P. (2024). **Exploring quantum-enhanced machine learning for computer vision: Applications and insights on noisy intermediate-scale quantum devices.** Retrieved 7 June 2025 from https://arxiv.org/pdf/2404.02177/.

Marella, S. T., & Paris, H. S. K., (2020). **Quantum computing and communications**. Retrieved 22 May 2025 from https://www.intechopen.com/chapters/73811.

Mebtouche, N. E., & Sahnoune, S. (2024). Quantum computing for computer vision: Applications, challenges, and research tracks. In Drias, H., & Yalaoui, F. (Ed.) **Quantum computing: Applications and challenges**. Springer Nature Link. https://doi.org/ http://dx.doi.org/10.1007/978-3-031-59318-5_12.

Mironowicz, P., Shenoy, A., Mandarino, A., Yilmaz, A. E., & Ankenbrand, T. (2024). **Applications of quantum machine learning for quantitative finance.** Retrieved 19 June 2025 from https://arxiv.org/html/2405.10119v1/.

Moskovich, D. (2015). **An overview of the state of the art for practical quantum key distribution**. Retrieved 24 May 2025 from https://arxiv.org/pdf/1504.05471.pdf.

Nadim, M., Hassan, M., Mandal, A. K., Roy, C. K., Roy, B., & Schneider, K. A. (2025). **Comparative analysis of quantum and classical support vector classifiers for software bug prediction: an exploratory study**. Retrieved 22 November 2025 from https://arxiv.org/pdf/2501.04690v1.

Nielsen, M. A., Chuang, I. L. (2011). Quantum computation and quantum information: 10th anniversary edition. Cambridge University Press.

Physicsworld. (1998). **Fundamentals of quantum information**. Retrieved 10 May 2025 from https://physicsworld.com/a/fundamentals-of-quantum-information/.

Preskill, J. (2018). **Quantum computing in the NISQ era and beyond.** Retrieved 7 June 2025 from https://arxiv.org/pdf/1801.00862/.

Quantiki. (2015). **Hilbert spaces.** Retrieved 26 May 2025 from https://www.quantiki.org/wiki/hilbert-spaces.

Quantinuum. (2023). **Unveiling the first fully integrated and complete Quantum Monte Carlo Integration Engine.** Retrieved 20 June 2025 from https://www.quantinuum.com/press-releases/unveiling-the-first-fully-integrated-and-complete-quantum-monte-carlo-integration-engine.

Rath, M., & Date, H. (2024). Quantum data encoding: a comparative analysis of classical-to-quantum mapping techniques and their impact on machine learning accuracy. **EPJ Quantum Technology**. 11, 72. https://doi.org/10.1140/epjqt/s40507-024-00285-3

Regazzoni, F., Fowler, A., & Polian, I. (2018). **Quantum era challenges for classical computers**. In 18th International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation, 173-178. Pythagorion, Greece.

Rieffel, W., & Polak., W. (2000). An introduction to quantum computing for non-physicists. **ACM Computing Surveys**. 32, 3. https://doi.org/10.1145/367701.367709

Sahu, S. K. & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. **Frontiers in Physics**. 12. https://doi.org/10.3389/fphy.2024.1456491

Salesforce. (2021). **Machine learning: 6 real-world examples**. Retrieved 8 May 2025 from https://www.salesforce.com/eu/blog/2020/06/real-world-examples-of-machine-learning.html/.

Schneider, J., & Smalley, I. (2025). **What is quantum computing?** Retrieved 20 June 2025 from https://www.ibm.com/think/topics/quantum-computing.

Scrivano, A. (2025). **A comparative study of classical and post-quantum cryptographic algorithms in the era of quantum computing**. Retrieved 22 November 2025 from https://arxiv.org/pdf/2508.00832.

Shailesh. (2025). **10 big data applications in real life**. Retrieved 8 May 2025 from https://intellipaat.com/blog/10-big-data-examples-application-of-big-data-in-real-life/.

Shor, P. W. (1994). **Algorithms for quantum computation: discrete logarithms and factoring**. In 35th Annual Symposium on Foundations of Computer Science, 124-134.

SPINQ. (2025). **Quantum computing vs classical computing: key differences**. Retrieved 22 November 2025 from https://www.spinquanta.com/news-detail/quantum-computing-vs-classical-computing-full-breakdown.

Stamatopoulos, N., Mazzola, G., Woerner, S., & Zeng, W. J. (2022). **Towards quantum advantage in financial market risk using quantum gradient algorithms.** Retrieved 20 June 2025 from https://quantum-journal.org/papers/q-2022-07-20-770/pdf/.

Symmetry. (2022). **What is quantum information?** Retrieved 10 May 2025 from https://www.symmetrymagazine.org/article/what-is-quantum-information.

Symons, B. C. B., Galvin, D., Sahin, E., Alexandrov, V., & Mensa, S. (2023). A practitioner's guide to quantum algorithms for optimisation problems. **Journal of Physics A: Mathematical and Theoretical**. 56.

The Verge. (2021). **Google wants to build a useful quantum computer by 2029**. Retrieved 9 May 2025 from https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor.

Wang, Y., & Liu, J. (2024). **A comprehensive review of Quantum Machine Learning: from NISQ to Fault Tolerance.** Retrieved 7 June 2025 from https://arxiv.org/pdf/2401.11351/.

Wie, C. R. (2020). Two-qubit bloch sphere. **Physics**. 2, 3. https://doi.org/10.3390/physics2030021