American Journal of Engineering and Applied Sciences

Review

Quantum Technology: Advances and Trends

[1]Lidong Wang and [2]Cheryl Ann Alexander

[1]*Institute for Systems Engineering Research, Mississippi State University, Vicksburg, Mississippi, USA*
[2]*Institute for IT innovation and Smart Health, Vicksburg, Mississippi, USA*

Article history
Received: 30-03-2020
Revised: 23-04-2020
Accepted: 13-05-2020

Corresponding Author:
Cheryl Ann Alexander
Institute for IT innovation and
Smart Health, Vicksburg,
Mississippi, USA
Email: cheryl@techhealthsolutions.org

Abstract: Quantum science and quantum technology have become significant areas that have the potential to bring up revolutions in various branches or applications including aeronautics and astronautics, military and defense, meteorology, brain science, healthcare, advanced manufacturing, cybersecurity, artificial intelligence, etc. In this study, we present the advances and trends of quantum technology. Specifically, the advances and trends cover quantum computers and Quantum Processing Units (QPUs), quantum computation and quantum machine learning, quantum network, Quantum Key Distribution (QKD), quantum teleportation and quantum satellites, quantum measurement and quantum sensing, and post-quantum blockchain and quantum blockchain. Some challenges are also introduced.

Keywords: Quantum Computer, Quantum Machine Learning, Quantum Network, Quantum Key Distribution, Quantum Teleportation, Quantum Satellite, Quantum Blockchain

Introduction

The Tokyo QKD metropolitan area network was established in Japan in 2015 through intercontinental cooperation. A 650 km QKD network was established between Washington and Ohio in the USA in 2016; a plan of a 10000 km QKD backbone network was launched in the country. A quantum metropolitan area network was estAablished in the UK in 2016 and a practical national network for QKD and an international QKD network was planned. The Phase I network with a total length of about 256 kilometers was established in South Korea in 2016. The Beijing-Shanghai Trunk Line of QKD was created in China in 2017 and applications in electric power, finance and government administration were demonstrated (Liu *et al*., 2018).

The Personal Identifiable Information (PII) leak from big consumer databases, including social security numbers, financial status and additional private information have become a major concern and increased the interest in reliable methods of sensitive information processing. A growing requirement of online applications in healthcare and financial areas highlights worries about information sharing and privacy. Quantum technology has the potential to handle the privacy worries or concerns using quantum cryptographic methods such as super dense coding, quantum seals and QKD, which help protect information during the information transmission. Progress in quantum computing has offered some techniques of obscuring stored information and the computation that is executed throughout a transaction (Humble, 2018).

There have been advances in developing quantum equipment, which has been indicated by the number of successful QKD demonstrations. However, many problems still need to be fixed though achievements of QKD have been showcased. Main features of QKD technology lie in: (1) Communication is generally fulfilled on a hop-by-hop basis due to a main characteristic of the QKD network—no available quantum router or quantum repeater in practice; (2) QKD links are at all times performed in a point-to-point manner, thus leading to a restricted distance and a key rate that is inversely proportional to the limited distance. Furthermore, QKD links are possibly unavailable if the public channel is congested or there is not enough key material (Shahid *et al*., 2020).

Twin-field QKD was developed to obtain a remote key distribution with a maximum distance of secure transmission. However, there were still some problems in the source part though the security of the twin-field QKD was ensured in its detection part. The source of light had been regarded to be a very good coherent state though this assumption was not met in an actual QKD system, which led to secure problems in practice. A protocol called Sending-or-Not-Sending (SNS) was put forward for fixing the security problems. A condition was discussed that the Photon Number Distribution (PND) of the source is unknown for the SNS protocol. It was demonstrated a security analysis is still valid for a

Science Publications

source with an unknown PND. It was shown that the SNS protocol performance in the light source monitoring enables to keep nearly unchanged (Gao *et al*., 2019).

Standard quantum field theory has been thought to govern all the processes of human consciousness such as emotions, personality, beliefs, psychology, thoughts, etc. The brain-based consciousness has been considered as a dynamic self-awareness concept, constructed by the brain's cortical neurons as a quantum information field that continuously receives information/energy from the brain, evaluates and processes the information and initiates responses. External sensory information that is modelled as quantized electromagnetic waves has been regarded to feed cortical neurons and ultimately build the brain-based consciousness Hamiltonian. Any external information or energy, instantly reaching to the brain-based consciousness Hamiltonian, has been considered as a perturbation (Erol, 2019).

The main purpose of this paper is to deal with the advances and trends of quantum technology. Some challenges of quantum technology will also be presented. The following is the arrangement of the rest of the paper: section 2 presents quantum computers and QPUs; section 3 introduces quantum computation and quantum machine learning; section 4 describes quantum network; section 5 introduces QKD; section 6 presents quantum teleportation and quantum satellites; section 7 describes quantum measurement and quantum sensing; section 8 deals with post-quantum blockchain and quantum blockchain; and section 9 is the conclusion.

Quantum Computers and Quantum Processing Units

Superconductors, quantum dots, ion traps, linear optics, donor systems, distributed and monolithic diamonds and topological quantum computing help to develop quantum computers. The 4th-generation quantum computer utilizes the technology of topological quantum computing (also called anionic quantum computing) (Gyongyosi and Imre, 2019). Trapped atomic ions provide one of primary physical platforms for realizing a completely functional quantum computer, a programmable quantum computer prototype was displayed, and its performance was compared with that of a superconducting quantum computer with a similar size. Among all of qubit technologies, trapped ion qubits demonstrate the highest gate quality. Despite promises, further technical innovation is necessary to increase the number of qubits in a quantum computer module, enhance logic gates quality, and realize scalable increase using multiple modules (Maslov *et al.*, 2019).

There have been several superconducting quantum computing platforms with a big qubit number such as IBM and Rigetti. A powerful programmable quantum computer has been constructed that is an 11-qubit fully connected quantum computer in a trapped ion system and has demonstrated algorithms with successful rates above the Bounded-error Quantum Polynomial (BQP) threshold. The Hidden Shift (HS) and Bernstein-Vazirani (BV) algorithms have been compiled into native gates and executed on the hardware. The trapped ion quantum computer has been used to accomplish the quantum implementation of the HS and BV algorithms (Wright *et al.*, 2019).

A framework for hybrid quantum-classical algorithms was presented that uses a quantum computer (substantially smaller compared with the problem size). Given a randomly small ratio of the quantum computer to the problem size, a polynomial speedup for classical divide-and-conquer algorithms was achieved. A trade-off between the problem size and the speedup can be achieved. A small quantum computer can considerably speed up the solving process of a small-size problem. Also, it enables to obtain a more modest speedup of a larger instance (Ge and Dunjko, 2020).

A quantum computer can offer substantial speedup in machine learning. Algorithms that require quantum speedup in runtime rely on an efficient Quantum Random Access Memory (QRAM) (a critical component) in addition to a quantum computer. In a QRAM, the number of required quantum routing operations scales up exponentially with the number of qubits in the algorithms (Gao *et al*., 2018). Quantum memories are a cornerstone of quantum computers as well as a global-scale quantum Internet with high performances. Low retrieval efficiency is a main problem of quantum memories. A High-Retrieval-Efficiency (HRE) quantum memory was defined for a near-term quantum device. A unit of the HRE quantum memory was integrated with local unitary operations on its hardware level and utilized cutting-edge technologies in quantum machine learning. It was proven the local unitary of the HRE quantum memory achieves an optimized and unsupervised readout procedure. It was shown that the readout procedure of the HRE quantum memory was accomplished without any information regarding an input quantum system or an unknown quantum operation of a quantum register. The retrieval efficiency of the HRE quantum memory and the output of the Signal-to-Noise Ratio (SNR) was evaluated. The HRE quantum memory is an especially convenient unit for a gate-model quantum computer and the quantum Internet (Gyongyosi and Imre, 2020).

IBM launched the IBM Q Experience, which made universal quantum computers accessible to the public through the cloud service. IBM Q Experience offers an online platform for experimental testing of quantum physics fundamentals and various applications in quantum information theory. Qiskit (developed by IBM) provides tools for users who are required to run their quantum programs on prototype quantum simulators and devices. IBM has developed 20-qubit and 50-qubit quantum processors (Huang *et al.*, 2020a).

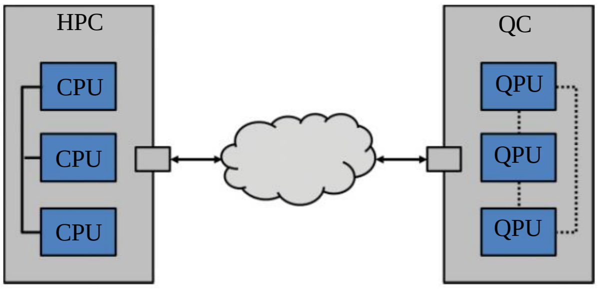

Fig. 1: An asymmetric multiprocessor model using a QC server, for instance, a type of cloud-based QC

How Quantum Processing Units (QPUs) integrate with a current or future High-Performance Computing (HPC) system architecture was investigated through considering the functional and physical design requirement. Integration pathways were examined that are differentiated by use cases expected for an HPC system and infrastructure constraints on QPUs. In a loose integration path, QPUs are isolated operational elements that need to interact with a host HPC system through a network interface. This is an effective client-server model illustrated in Fig. 1 (Britt and Humble, 2017). The concept of Quantum Computing (QC) as a service provides ease of use and more flexibility at the price of communication latency.

Quantum Computation and Quantum Machine Learning

A field that has been made remarkable progress is quantum computation with different physical platforms among which superconducting quantum circuits and trapped ions are the most prospective. Various quantum algorithms have been performed to show scaling issues, machine learning, the concepts of error correction, spin systems, many-body localization, the simulation of light-matter systems, the modeling spectra of molecules and other fermionic systems, etc., (Zhukov *et al*., 2019).

There are two major approaches to achieving practical QC in the industry: Quantum Annealing (QA) and the gate model (also called the circuit model). QA is a method of employing the physics of quantum phase transitions to conduct computation. A phase transition is a discrete change in some macroscopic properties of a physical system. A QPU of a D-Wave quantum computer has completed the annealing process. Among all QC platforms under development, Annealing-based QC provides the most viable way forward for connecting quantum hardware to a practical application (McGeoch *et al*., 2019).

ProjectQ is an open source software framework of QC. A high-level quantum language has been implemented as a domain-specific language embedded in Python language. The framework permits quantum algorithms testing through simulations and enables to run them on quantum hardware utilizing a back-end connection to the cloud service of IBM Quantum Experience (Steiger *et al*., 2018). Industry interest has brough two major products: Quantum programming language Q# (Python-compatible) of Microsoft and Python package qiskit of IBM. Each of them provides a user with tools to compute or manipulate with the qubit logic that interfaces with classical programming. The code written with quantum algorithms can be executed (Keplinger, 2018).

Quantum technology, particularly quantum computing, has the potential to bring a great boost to Machine Learning (ML). Many conceptual connections exist between quantum computing and machine learning. Some quantum algorithms can provide an exponential speed increase for significant tasks. One algorithm called the HHL algorithm is the foundation of the existing Quantum Machine Learning (QML) minirevolution. Many other quantum ML algorithms either extend HHL or use it as a subroutine. Additional intriguing algorithms, e.g., Quantum Support Vector Machines (QuSVMs) and quantum Principal Component Analysis (PCA) also have the potential of great speed-up. Furthermore, an algorithm of quantum-inspired tensor-network for ML has been proposed and begun to show intriguing merits. However, a unified theory of quantum learning has not been developed for quantum-enhanced ML (Sarma *et al*., 2019).

QML tasks such as quantum classification, boosting Quantum Computing (QC), quantum pattern recognition, adiabatic QC, and quantum process tomography and regression have been discussed. Quantum algorithms for outlier detection, neighborhood graph, and smart initialization of cluster center have been developed. In addition, the implementation of QuSVMs have been presented (Nawaz *et al*., 2019).

Quantum Fourier transform, quantum error-correction methods, quantum communication protocols, Quantum teleportation, and QKD play key roles in the implementation of distributed quantum computation. Their realization is essential for the development of the quantum Internet. The realization of some essential protocols for quantum reinforcement learning (utilizing superconducting quantum circuits) was studied. Superconducting quantum circuits help quantum information processing and quantum computation. A QuSVM for big data classification was defined. The Support Vector Machine (SVM) can be executed on a quantum computer. A quantum algorithm of association rules mining and an issue of the quantum mixing of Markov chains for unusual distributions were researched. The quantum Boltzmann machine was studied and a novel ML approach (based on the quantum Boltzmann distribution) was presented. The possibility of employing quantum annealing processors such as D-Wave to train a quantum Boltzmann machine was analyzed. The data discovery driven by a quantum annealer was studied in which a binary classifier uses a quantum annealer to generate a reliable class estimator. A classical- quantum Deep Learning (DL) framework for industrial data sets for near-term devices was also studied (Gyongyosi and Imre, 2019).

Outspreading fundamental the concepts of Artificial Neural Networks (ANNs) and quantum information processing, a Quantum Neural Networks (QNNs) concept was introduced. Advantages of QSVMs and QNNs over classical SVMs and ANNs according to reliability, scalability, processing speed, small scale and fast learning motivates the exploration of these methods in fixing diverse problems in wireless communication networks. The progress in ML and QC methods has opened new horizons of fulfilling Deep QML methods such as Deep QNNs. Quantum-assisted Deep Learning (DL) has been attracting a great attention for improving the performance metrics of communication networks. QC-based algorithms for DL are expected to influence ML greatly (Nawaz *et al*., 2019).

Quantum speedup for reinforcement learning has a great potential for an agent-environment paradigm. Progress in quantum-enhanced reinforcement learning has been presented. In the context of a communication system, methods of quantum-inspired reinforcement learning for optimal spectrum assignment have been studied (Nawaz *et al*., 2019). The advantage of quantum reinforcement learning lies in a specific part of the algorithm which interacts with a classical environment, produces results in a quantum environment and the process is reversible. The algorithm works in such a way and forecasts the output in an optimal manner. The processing and learning of the machine should be executed in parallel for a high implementation efficiency of the algorithm (Gupta *et al*., 2017).

The security of ML has become a significant issue. Classical ML algorithms, e.g., SVMs, clustering, Principal Component Analysis (PCA) are vulnerable to the changes of features, input data, and ultimate model parameters or hyper-parameters that are already learned. Attackers can have various purposes, e.g., an increase in false positive rate or false negative rate. The study of subverting an ML system by motivated attackers has been defined as adversarial ML. In adversarial quantum ML, some ways were discussed in which quantum information could be utilized for making quantum classifiers private as well as secure. A type of quantum PCA was demonstrated. It was shown that a quantum method could be employed to implement a private form of clustering with *k*-means. A quantum approach was introduced for boosting and bagging that used quantum superposition over classifiers or splits of a training dataset to aggregate many more models than classical methods (Wiebe and Kumar, 2018).

Searchable Encryption (SE) is an encouraging method for protecting users' sensitive data in cloud computing while maintaining search capability on the server side. For example, it permits a server to search for encrypted data without the leak of information in the plaintext data. A Full-Blind Quantum Computation (FBQC) model was developed that is multi-client and universal circuit-based. Various clients with limited quantum ability outsourced the key generation to a trusted key center and uploaded their encrypted data to a data center. A quantum searchable encryption scheme for the cloud data was then proposed through combining Grover searching algorithm and the multi-client FBQC model (Liu *et al*., 2019).

Quantum Network

A quantum network is composed of essential quantum hardware components including nodes, quantum repeaters, and the quantum channel. A node is a quantum processor connected to the quantum network. A quantum repeater extends a short distance and permits cubits to be arbitrarily transmitted over a large distance. The quantum channel supports quantum bits transmission. It can be a fiber optic channel. The development of quantum switch distribution device technologies has been growing fast. A switch is a device with a function of finding and transmitting data to the next receiver (Yaşar and Yilmaz, 2019). A quantum network structure is shown in Fig. 2 (Wehner *et al*., 2018).

A plug-and-play method that enables to synchronize building the blocks of a quantum network in an all-optical approach was implemented. It relied on robust classical telecommunication and nonlinear optical technology and could be performed in a general way with off-the-shelf components It was enabled to achieve a synchronization that is of high quality and compatible with a high network-operation rate. It was tested through synchronizing two distant photon pair sources. It paved a way to the synchronization of long-distance quantum networks based on a fiber, free-space, and hybrid solution. In addition, the synchronization approach permitted to add as many nodes (such as quantum memories and sources) to a quantum network as necessary. It could be regarded as a useful method of scaling up quantum networks (D'Auria *et al*., 2020).

Software Defined Networking (SDN) principles have been used to create a converged classical-quantum network that shares the logical and physical infrastructure among classical and quantum channels. A quantum enabled SDN structure has been proposed. It united under the same management as the classical and quantum communications, making network optimization better utilize all kinds of resources compared with a typical quantum network structure in which an ad hoc network is used to run in parallel to a usual one for qubit transmission (Aguado *et al*., 2019).

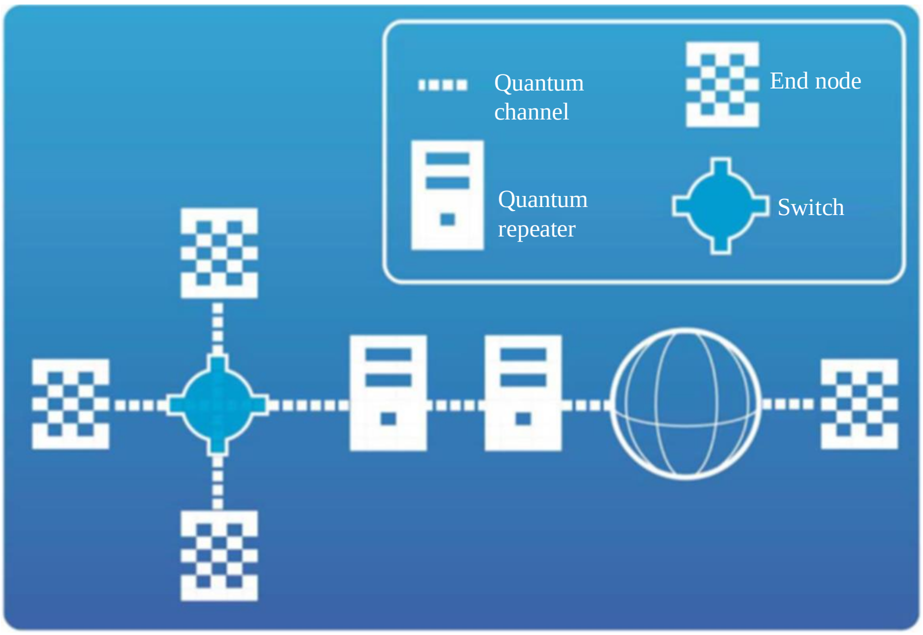

Fig. 2: A quantum network structure

The security of quantum communication over a network with the existence of a malicious adversary who eavesdrops and contaminates states was studied. The network is composed of noiseless quantum channels together with the unit capacity and nodes that apply noiseless quantum operations. An asymptotically secret as well as correctable quantum network code was presented as the quantum extension of classical network codes. The code was universal and structured without any knowledge of the topology of the network and specialized node operations. The quantum network code was executed through attaching a known communication protocol of a secure classical network. It could be regarded as the generalization of quantum secret sharing (Song and Hayashi, 2019).

Quantum Key Distribution

In quantum cryptography, QKD is very noticeable. It is a technology of the physical layer and the technology is immune to classical and quantum computational attacks or threats. It may be mathematically proven to be secure and independent of the resources of adversaries (Aguado *et al*., 2019). It is a technology for sharing encryption keys between two adjacent nodes. Because it enables to identify any eavesdropping based on the quantum theory, users can communicate securely while utilizing shared random numbers as encryption keys. A key management method was proposed for a QKD network with a high speed. The design, execution, and assessment of a key management method was presented (Takahashi *et al*., 2019).

Inspired by the substantial similarity between mobile ad-hoc networks and the QKD **t**echnology, researchers proposed a model of the Quality of Service (QoS) that includes metrics for deciding the states of quantum and public channels as well as the overall state of QKD links. They also proposed a routing protocol to minimize the consumption of cryptographic keys and obtain high-level scalability (Shahid *et al*., 2020).

In principle, QKD provides unconditional security through creating secret keys at a distance. For a standard QKD, two spatially separated parties (we often call them Alice and Bob) trust functions of their devices. However, this is a very strong assumption. A protocol is called one-Sided-Device-Independent (SDI) QKD if one of devices is not trusted; it is called Device-Independent (DI) QKD when both the devices are not trusted. The three QKD scenarios are in correspondence with the hierarchy of quantum correlations. The standard QKD requires that both Alice and Bob share entanglement or be connected by a channel that enables to keep entanglement. For SDI QKD, Alice and Bob are required to produce a secret key, which makes their systems violate a steering inequality. In DI-QKD, the systems of the two parties (Alice and Bob) violate a Bell inequality. Intrinsic non-locality and quantum intrinsic non-locality has been introduced as quantifiers for Bell non-locality. It has been proven they satisfy some desired properties, e.g., convexity, faithfulness, and monotonicity under shared randomness and local operations. Upper bounds on secret-key rates have been established that are attainable with SDI-QKD and DI-QKD. It has also been proven that restricted intrinsic steerability is an upper bound on secret-key rates in protocols of one-SDI secret-key-agreement (Bennet and Daryanoosh, 2019).

Quantum scissors were investigated as candidates for non-deterministic amplifiers in Continuous-Variable (CV) QKD. Such devices rely on single-photon sources for their operations. The rate of secret key generation for a protocol that used quantum scissors was bounded based on exact analytical modeling for system components. Such a protocol can reach a longer distance than the counterpart with no amplification for certain non-zero values of excess noise, which sheds light into the prospect of employing quantum scissors as an ingredient in CV quantum repeaters (Azhar *et al*., 2019).

Some researchers have focused on realizing more efficient and practical QKD systems. An urgent problem is a requirement for easy and efficient realization of reconciliation schemes for real-world QKD systems. Based on Low-Density Parity-Check (LDPC) codes, rate-adaptive schemes can accomplish an attractive execution of a key reconciliation process because they cover a full range of the channel parameter space with a limited set of pre-defined mother codes. Some rate-adaptive reconciliation schemes (based on the LDPC codes) were investigated, illustrating how their performance was compared with other set-ups in which fixed-rate non-adaptive LDPC codes (optimized for various channel conditions) were used. Especially, the impact of rate-adaptive codes on decoding complexity and subsequently overall secure key throughput was quantified by simulations of an entanglement-based version of a QKD protocol within the context of the entanglement source onboard a satellite (Ai *et al*., 2018).

Quantum Teleportation and Quantum Satellites

Quantum teleportation offers a method of transporting unknown quantum states between remote systems based on shared quantum entanglement and quantum measurement; therefore, it establishes an essential element in making large-scale quantum processors with a modular quantum structure and fulfilling various quantum information processing and quantum computation tasks over the quantum network. Two protocols were proposed to teleport qubits over an *N*-node quantum network in a chain-type cluster state or highly entangled box-cluster state. The protocols were applicable to any size of modules and systematically scalable to any finite number *N*. The protocol that was based on a box-cluster state was employed on a 14-qubit quantum computer of IBM and *N* was up to 12. A toolbox was provided that was composed of networking teleportation protocols and criteria to identify faithful teleportation for general quantum computers with modular structures and improve the reliability of quantum information processing (Huang *et al*., 2020b).

Micius is a quantum experiment science satellite designed to conduct quantum experiment at the scale of space. One of objectives was to perform ground-satellite quantum teleportation that was of a main interest. This kind of teleportation was the first application of spaceborne and low-noise Single-Photon Detectors (SPDs), received uplink configurations and placed a complex multiphoton setup on the ground (Yang *et al*., 2019).

A high-fidelity transmission of polarization with encoded qubits plays a critical role in the quantum communication of a long distance. The polarization encoding of photons has been the first choice for the quantum communication with a long distance and over a free space, including satellite-based quantum entanglement distribution. Transmission antennas with polarization maintenance were designed and a polarization compensation scheme used for satellite motions was presented. In addition, entangled photons were distributed from the ground to a satellite. This research has provided support for other work, for example, ground-to-satellite teleportation and the testing of the model of gravitationally induced quantum decoherence (Han *et al*., 2020).

Creating a global quantum communication network depends on the integration of fiber-based networks and satellite-based links. A universal and basic model was provided for the modelling and simulation of the loss resulted from a satellite-based optical link. It has confirmed by simulations that quantum communication over a long distance could be realized not only employing medium-sized satellites (such as Micius of China), but also employing nano-satellites that permit to save costs of a global space-based quantum network substantially. A performance analysis of various QKD realizations was conducted, covering finite-key effects (with a focus on various interesting application scenarios) (Liorni *et al*., 2019).

QKD on satellite networks enables to overcome shortcomings of terrestrial optical networks, e.g., difficulty of intercontinental domain communication and attenuation over a fiber channel with a long distance. A single satellite cannot fulfil QKD at ground stations on a full day using existing schemes. In addition, research is a challenge due to the limitation of the satellite coverage such as the limited cover time of Low Earth Orbit (LEO) satellites and high channel losses of Geostationary Earth Orbit (GEO) satellites. An architecture of trusted-repeater-based double-layer Quantum Satellite Networks (QSNs) that consist of

LEO and GEO satellites was proposed to overcome the limitations. The problem regarding Routing and Key Allocation (RKA) for key-relay services over QSNs was addressed (Huang *et al*., 2020b).

Using Terahertz (THz) frequencies was explored as an approach to realizing quantum communication within a constellation of micro-satellites in LEO. Quantum communication between high-altitude terrestrial stations and the micro-satellite constellation was investigated too. It was demonstrated that THz QKD and THz quantum entanglement distribution are viable deployment options for micro-satellites. There is a possibility for a simple integration of global quantum and wireless networks. Such an integration has been regarded as a significant step for global quantum communication in the future. The possibility of employing THz frequencies for quantum radar applications in the LEO deployment context was discussed. Quantum radars show how entangled quantum states bring up better detection of remote objects via reflection (Wang *et al*., 2019).

SPDs play a significant role in a highly sensitive detection application, e.g., quantum communication, deep space optical communication and remote sensing and ranging. But adverse conditions in the space, e.g., increased radiation flux and thermal vacuum harshly restrict their noise performances, lifetime, and reliability. An example of spaceborne SPDs with high reliability and low noise was presented. The SPDs helped to establish a practicable satellite-based up-link quantum communication that was validated on the platform of a quantum experiment science satellite. The SPDs also offered a choice for weak optical signal reception in the space applications, e.g., laser time transfer, deep-space optical communication, and satellite-based quantum application (Yang *et al.*, 2019).

Quantum Measurement and Quantum Sensing

In quantum teleportation, quantum entanglement has been exploited twice. First, entanglement is a "quantum teleportation channel" (entanglement between various systems in a distance). Second, entanglement is in the eigenvectors of a joint measurement. Entanglement facilitates entirely new types of quantum measurement. After the discovery of quantum teleportation, there have been many advances on quantum steering, Bell-locality and more general quantum information theory. Similarly, great progress has taken place in experimental investigation, applied engineering, and even the industrial development of quantum technology. However, little progress happened in improving the understanding of joint measurements (Gisin, 2019).

In the quantum communication where states are sent via a noisy channel, an optimal measurement can identify which state has been sent via the channel though the state may not be fully secured. A scheme of preserving an optimal measurement over a channel has been called "channel coding of a quantum measurement". Approaches to preserving states have been called "channel coding of states". A framework of preserving a measurement on quantum systems interacting with an environment was formulated and presented. Channel coding of qubit measurement was presented. It was shown that the measurement can be preserved for any channel for both pairs of qubit states and ensembles of equally possible states. The protocol that preserves a quantum measurement was demonstrated with quantum computers of IBM (Kechrimparis *et al*., 2020).

The quantum measurement incompatibility is a typical feature in quantum mechanics. The existence of incompatible measurements also means the no-cloning theory. The measurement incompatibility was classified for a given set of measurements and a hierarchy of quantum measurement incompatibilities was presented. The transition between various kinds of incompatible measurements was studied utilizing the semidefinite program. A criterion for judging the incompatibility of a given multiple measurement was presented. Examples regarding unbiased qubit measurements were given in details. The incompatibility of quantum measurements is a very useful tool in quantum information theory (Sun *et al*., 2020).

Measurement-based Quantum Correlations (MbQCs) depend on how strongly an observer perturbs an unobserved system. This differentiates MbQCs from traditional quantum correlations such as entanglement and discord though entanglement and discord have been regarded as essential in quantum state discrimination and quantum computation tasks. MbQCs were used to clarify quantum information processing capabilities in quantum computation and quantum state discrimination. It was shown that MbQCs exist more generally than entanglement and discord in optimal assisted quantum state discrimination and deterministic quantum computation with a single qubit. An MbQC-based dimension witness was proposed and analyzed in various noisy and noiseless scenarios. MbQCs were recently discovered to be relatively more resourceful than quantum entanglement and super quantum discord in the field of mixed state quantum metrology (Khalid *et al*., 2020).

Quantum sensing (Q-sensing) utilizes nonclassical resources to enhance measurement precision. There have been many applications such as bio-sensing, quantum illumination, atomic clocks, quantum reading, and the laser interferometer gravitational-wave observatory. Entanglement can be extremely beneficial when a sensing task involves multiple parties. In principle, Continuous-Variable (CV) error correction codes can be employed to improve the reliability of a protocol that utilizes CV quantum information. Distributed quantum sensing that is improved by CV error correction was studied (Zhuang *et al*., 2020).

Quantum systems can be developed in the superposition of states and this particularity results in phenomena called quantum entanglement and coherence. Q-sensing exploits both the properties to implement enhanced sensors and measuring protocols. How to exploit the quantum features of molecular spins for Q-sensing was studied. Further particularity of molecular spins may be exploited for Q-sensing at the nanometer scale (Troiani *et al*., 2019).

Post-Quantum Blockchain and Quantum Blockchain

The vulnerabilities of modern blockchain networks and some potential post-quantum mitigation methods were introduced. A lattice-based signature scheme was presented that can be used for securing blockchain networks over existing classical channels. Moreover, a description of the Post-Quantum Blockchain (PQB) transaction was given in details. PQB is a quantum information vision system. It is a classical blockchain system equipped with the post-quantum cryptography or a storage structure of the classical blockchain with quantum communication (Li *et al*., 2018).

The influence of quantum-computing attacks on a blockchain was analyzed and how to employ a post-quantum cryptosystem to mitigate such attacks was studied. The most relevant post-quantum schemes were investigated and their applications to blockchains were studied. In addition, extensive comparison was presented regarding the performance and characteristics of the most promising post-quantum public-key encryption and digital-signature schemes for a blockchain (Fernández-Caramès and Fraga-Lamas, 2020).

Random sequences were generated as a tool to protect transactions completely based on Bitcoins under an assumption that the transition probability in quantum mechanics was observed as a full blockchain operation. An algorithm with integer-order Bessel functions was tested. A formalism based on quantum mechanics was presented that permitted the simulation of the dynamics of blockchain for an e-commerce transaction (Nieto-Chaupis, 2019).

QKD is a well-known method of quantum cryptography. The transparency and immunity of a blockchain-based crypto-currency system was investigated through the simulation of a six-state QKD protocol. The generation of key rate was observed to guarantee a path for producing a better crypto-currency system (Azhar *et al*., 2019).

Safeguard measures were proposed through creating a framework of a quantum-secured and permissioned blockchain that is named Logicontract (LC). LC uses a digital signature scheme based on a QKD mechanism and a vote-based consensus algorithm to get consensus on a blockchain. Main deliverables were developed, including a logic-based scripting language for writing smart contracts on LC, a scalable consensus protocol used by LC, an unconditionally secure signature scheme for LC that makes it immune to quantum computing attacks and a quantum-resistant lottery protocol that shows the utilization and power of LC (Sun *et al*., 2019).

Compared with conventional voting methods, e-voting has been used in various decision scenarios due to its convenience and low costs. An e-voting protocol with transparency in the voting process was proposed based on blockchain. It also enables to audit voters with incorrect operations and fight quantum attacks using the certificateless and code-based cryptography. Specifically, the code based Niederreiter algorithm was used to fight quantum attacks (Gao *et al*., 2019).

A smart contract based on light-weighted quantum blind signature was proposed to boost the security performance of blockchain smart contracts against quantum attacks. The structure of the smart contract was built by five main lays that is shown in Table 1 (Cai *et al*., 2019) and enables to deal with both quantum information and classic information.

Table 1: The structure of a smart contract of blockchain based on the quantum blind signature

User Layer	Data Layer	Management Layer	Verification Layer	Execution Layer
Authority management	Data collection	Contract management	Code generation	Virtual machine
Account management	Data cleansing	Protocol management	Formal description	Container
Security verification	Data processing	Parameter management	Formal verification	Application interface
Reputation management	Data storage	Business management	Conformance testing	Business application
User's quantum blind signature	Quantum information processing	Quantum key management	Quantum signature verification	Quantum state restoration

Conclusion

Quantum computers enable to offer considerable speedup in machine learning. Quantum memories are a foundation stone of quantum computers and the global quantum Internet with high performance. Quantum computing have the potential to boost ML greatly. However, a unified quantum learning theory has not been created for quantum-enhanced ML. Superconducting quantum circuits facilitate quantum computation and quantum information processing. In adversarial quantum ML, quantum information can be utilized to make quantum classifiers more private and secure.

QKD can be secure and independent of resources of the adversary. It provides security for establishing secret key at a distance. Quantum teleportation enables to transport unknown quantum states between remote systems. QKD over satellite networks overcomes the shortcomings of terrestrial optical networks. Quantum entanglement facilitates entirely new types of quantum measurement Q-sensing uses nonclassical resources to improve measurement precision. Quantum computing has the potential to protect information during the information transmission. Also, the influence of quantum-computing attacks on blockchain has become a major concern. Post-quantum cryptosystems can be used to mitigate such attacks. Progress has been made to enhance the security performance of blockchain against quantum attacks.

Acknowledgement

Authors thank Technology and Healthcare Solutions, Mississippi, USA and the Institute for IT innovation and Smart Health, Mississippi, USA for great support.

Author’s Contributions

Authors made equal contribution to this paper.

Ethics

Ethical principles related to scientific and academic research articles are observed.

References

Aguado, A., V. Lopez, D. Lopez, M. Peev and A. Poppe *et al*., 2019. The engineering of software-defined quantum key distribution networks. IEEE Commun. Magazine, 57: 20-26. DOI: 10.1109/MCOM.2019.1800763

Ai, X., R. Malaney and S.X. Ng, 2018. Quantum key reconciliation for satellite-based communications. Proceedings of the Global Communications Conference, Dec. 9-13, IEEE Xplore Press, Abu Dhabi, UAE, pp: 1-6. DOI: 10.1109/GLOCOM.2018.8647658

Azhar, M.T., M.B. Khanand and A.U.R. Khan, 2019. Blockchain based secure crypto-currency system with quantum key distribution protocol. Proceedings of the 8th International Conference on Information and Communication Technologies, Nov. 16-17, IEEE Xplore Press, Karachi, Pakistan, pp: 31-35. DOI: 10.1109/ICICT47744.2019.9001979

Bennet, A.J. and S. Daryanoosh, 2019. Energy efficient mining on a quantum-enabled blockchain using light.

Britt, K.A. and T.S. Humble, 2017. High-performance computing with quantum processing units. ACM J. Emerg. Technol. Comput. Syst., 13: 1-13. DOI: 10.1145/3007651

Cai, Z., J. Qu, P. Liu and J. Yu, 2019. A blockchain smart contract based on light-weighted quantum blind signature. IEEE Access, 7: 138657-138668. DOI: 10.1109/ACCESS.2019.2941153

D’Auria, V., B. Fedrici, L.A. Ngah, F. Kaiser and L. Labonté *et al*., 2020. A universal, plug-and-play synchronisation scheme for practical quantum networks. NPJ Quantum Inform., 6: 1-6. DOI: 10.1038/s41534-020-0245-9

Erol, M., 2019. Resolution of brain-based consciousness as a quantum information field. BRAIN. Broad Res. Arti. Intell. Neurosci., 10: 41-60.

Fernández-Caramès, T.M. and P. Fraga-Lamas, 2020. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8: 21091-21116. DOI: 10.1109/ACCESS.2020.2968985

Gao, S., D. Zheng, R. Guo, C. Jing and C. Hu, 2019. An anti-quantum e-voting protocol in blockchain with audit function. IEEE Access, 7: 115304-115316. DOI: 10.1109/ACCESS.2019.2935895

Gao, X., Z.Y. Zhang and L.M. Duan, 2018. A quantum machine learning algorithm based on generative models. Sci. Adv., 4: eaat9004-eaat9004. DOI: 10.1126/sciadv.aat9004

Ge, Y. and V. Dunjko, 2020. A hybrid algorithm framework for small quantum computers with application to finding Hamiltonian cycles. J. Math. Phys., 61: 012201-012201. DOI: 10.1063/1.5119235

Gisin, N., 2019. Entanglement 25 years after quantum teleportation: Testing joint measurements in quantum networks. Entropy, 21: 325-325. DOI: 10.3390/e21030325

Gupta, S., S. Mohanta, M. Chakraborty and S. Ghosh, 2017. Quantum machine learning-using quantum computation in artificial intelligence and deep neural networks: Quantum computation and machine learning in artificial intelligence. Proceedings of the 8th Annual Industrial Automation and Electromechanical Engineering Conference, Aug. 16-18, IEEE Xplore Press, Bangkok, Thailand, pp: 268-274. DOI: 10.1109/IEMECON42627.2017

Gyongyosi, L. and S. Imre, 2019. A survey on quantum computing technology. Comput. Sci. Rev., 31: 51-71. DOI: 10.1016/j.cosrev.2018.11.002

Gyongyosi, L. and S. Imre, 2020. Optimizing high-efficiency quantum memory with quantum machine learning for near-term quantum devices. Sci. Rep., 10: 1-24. DOI: 10.1038/s41598-019-56689-0

Han, X., H.L. Yong, P. Xu, K.X. Yang and S.L. Li *et al*., 2020. Polarization design for ground-to-satellite quantum entanglement distribution. Opt. Exp., 28: 369-378. DOI: 10.1364/OE.28.000369

Huang, D., Y. Zhao, T. Yang, S. Rahman and X. Yu *et al*., 2020a. Quantum key distribution over double-layer quantum satellite networks. IEEE Access, 8: 16087-16098. DOI: 10.1109/ACCESS.2020.2966683

Huang, N.N., W.H. Huang and C.M. Li, 2020b. Identification of networking quantum teleportation on 14-qubit IBM universal quantum computer. Sci. Rep., 10: 1-12. DOI: 10.1038/s41598-020-60061-y

Humble, T., 2018. Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage and efficient applications. IEEE Consumer Electro. Magazine, 7: 8-14. DOI: 10.1109/MCE.2017.2755298

Kechrimparis, S., C.M. Kropf, F. Wudarski and J. Bae, 2020. Channel coding of a quantum measurement. IEEE J. Selected Areas Commun., 38: 439-448. DOI 10.1109/JSAC.2020.2969034

Keplinger, K., 2018. Is quantum computing becoming relevant to cyber-security? Network Security, 9: 16-19. DOI: 10.1016/S1353-4858(18)30090-4

Khalid, U., J. Ur Rehman and H. Shin, 2020. Measurement-based quantum correlations for quantum information processing. Sci. Rep., 10: 1-8. DOI: 10.1038/s41598-020-59220-y

Li, C.Y., X.B. Chen, Y.L. Chen, Y.Y. Hou and J. Li, 2018. A new lattice-based signature scheme in post-quantum blockchain network. IEEE Access, 7: 2026-2033. DOI: 10.1109/ACCESS.2018.2886554

Liorni, C., H. Kampermann and D. Bruß, 2019. Satellite-based links for quantum key distribution: Beam effects and weather dependence. New J. Phys., 21: 093055-093055. DOI: 10.1088/1367-2630/ab41a2

Liu, W., Y. Xu, W. Liu, H. Wang and Z. Lei, 2019. Quantum searchable encryption for cloud data based on full-blind quantum computation. IEEE Access, 7: 186284-186295. DOI: 10.1109/ACCESS.2019.2960592

Liu, Y., L. Yan, Z. Chen, D. Gao and R. Shi *et al*., 2018. Technology of satellite-ground combined video transmission based on quantum key distribution. Proceedings of the 2nd IEEE Conference on Energy Internet and Energy System Integration, Oct. 20-22, IEEE Xplore Press, Beijing, China, pp: 1-5. DOI: 10.1109/EI2.2018.8582343

Maslov, D., Y. Nam and J. Kim, 2019. An outlook for quantum computing [Point of View]. Proc. IEEE, 107: 5-10. DOI: 10.1109/JPROC.2018.2884353

McGeoch, C.C., R. Harris, S.P. Reinhardt and P.I. Bunyk, 2019. Practical annealing-based quantum computing. Computer, 52: 38-46. DOI: 10.1109/MC.2019.2908836

Nawaz, S.J., S.K. Sharma, S. Wyne, M.N. Patwary and M. Asaduzzaman, 2019. Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future. IEEE Access, 7: 46317-46350. DOI: 10.1109/ACCESS.2019.2909490

Nieto-Chaupis, H., 2019. Description of processes of blockchain and cryptocurrency with quantum mechanics theory. Proceedings of the CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, Oct. 29-31, IEEE Xplore Press, Valparaíso, Chile, pp: 1-4. DOI: 10.1109/CHILECON47746.2019.8988006

Sarma, S.D., D.L. Deng and L.M. Duan, 2019. Machine learning meets quantum physics.

Shahid, F., I. Ahmad, M. Imran and M. Shoaib, 2020. Novel One Time Signatures (NOTS): A compact post-quantum digital signature scheme. IEEE Access, 8: 15895-15906. DOI: 10.1109/ACCESS.2020.2966259

Song, S. and M. Hayashi, 2019. Secure quantum network code without classical communication. IEEE Trans. Inform. Theory, 66: 1178-1192. DOI: 10.1109/TIT.2019.2933422

Steiger, D.S., T. Häner and M. Troyer, 2018. ProjectQ: An open source software framework for quantum computing. Quantum, 2: 49-49. DOI: 10.22331/q-2018-01-31-49

Sun, B.Z., Z.X. Wang, X. Li-Jost and S.M. Fei, 2020. A note on the hierarchy of quantum measurement incompatibilities. Entropy, 22: 161-161. DOI: 10.3390/e22020161

Sun, X., M. Sopek, Q. Wang and P. Kulicki, 2019. Towards quantum-secured permissioned blockchain: Signature, Consensus and Logic. Entropy, 21: 887-887. DOI: 10.3390/e21090887

Takahashi, R., Y. Tanizawa and A. Dixon, 2019. A high-speed key management method for quantum key distribution network. Proceedings of the 11th International Conference on Ubiquitous and Future Networks, July 2-5, IEEE Xplore Press, Split, Croatia, pp: 437-442. DOI: 10.1109/ICUFN.2019.8806052

Troiani, F., A. Ghirri, M.G.A. Paris, C. Bonizzoni and M. Affronte, 2019. Towards quantum sensing with molecular spins. J. Magnetism Magnetic Mater., 491: 165534-165534. DOI: 10.1016/j.jmmm.2019.165534

Wang, Z., R. Malaney and J. Green, 2019. Inter-satellite quantum key distribution at terahertz frequencies. Proceedings of the International Conference on Communications, May 20-24, IEEE Xplore Press, Shanghai, China, pp: 1-7. DOI: 10.1109/ICC.2019.8761168

Wehner, S., D. Elkouss and R. Hanson, 2018. Quantum internet: A vision for the road ahead. Science, 362: eaam9288-eaam9288. DOI: 10.1126/science.aam9288

Wiebe, N. and R.S.S. Kumar, 2018. Hardening quantum machine learning against adversaries. New J. Phys., 20: 123019-123019. DOI: 10.1088/1367-2630/aae71a

Wright, K., K.M. Beck, S. Debnath, J.M. Amini and Y. Nam *et al*., 2019. Benchmarking an 11-qubit quantum computer. Nature Commun., 10: 1-6. DOI: 10.1038/s41467-019-13534-2

Yang, M., F. Xu, J.G. Ren, J. Yin and Y. Li *et al*., 2019. Spaceborne, low-noise, single-photon detection for satellite-based quantum communications. Opt. Exp., 27: 36114-36128. DOI: 10.1364/OE.27.036114

Yaşar, C. and İ. Yilmaz, 2019. Secure distribution of electronic documents over network in quantum information management systems. Proceedings of the 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, Oct. 11-13, IEEE Xplore Press, Ankara, Turkey, pp: 1-8. DOI: 10.1109/ISMSIT.2019.8932951

Zhuang, Q., J. Preskill and L. Jiang, 2020. Distributed quantum sensing enhanced by continuous-variable error correction. New J. Phys., 22: 022001-022001. DOI: 10.1088/1367-2630/ab7257

Zhukov, A.A., E.O. Kiktenko, A.A. Elistratov, W.V. Pogosov and Y.E. Lozovik, 2019. Quantum communication protocols as a benchmark for programmable quantum computers. Quantum Inform. Proc., 18: 31-31. DOI: 10.1007/s11128-018-2144-y