American Journal of Electrical and Electronic Engineering, 2020, Vol. 8, No. 2, 43-50
Available online at http://pubs.sciepub.com/ajeee/8/2/1
Published by Science and Education Publishing
DOI:10.12691/ajeee-8-2-1

Quantum Science and Quantum Technology: Progress and Challenges

Lidong Wang[1,*], Cheryl Ann Alexander[2]

[1]Institute for Systems Engineering Research, Mississippi State University, Vicksburg, Mississippi, USA
[2]Institute for IT innovation and Smart Health, Vicksburg, Mississippi, USA
*Corresponding author: lidong@iser.msstate.edu

Received February 11, 2020; Revised March 20, 2020; Accepted March 27, 2020

Abstract Quantum computing has the potential to offer new capabilities and quantum computers will achieve breakthroughs in finance, cybersecurity, medical science and healthcare, defense and military missions, etc. Progress in quantum science and quantum technology are introduced in this paper that specifically include quantum computers, quantum devices, quantum processing units (QPU), quantum artificial intelligence (QAI), quantum machine learning (QML), quantum cloud computing, quantum network and communication, quantum teleportation, quantum experiment satellite, quantum cryptography, and quantum key distribution (QKD). Some challenges are also presented.

Keywords: *quantum computer, quantum processing unit, quantum artificial intelligence, quantum machine learning, quantum cloud computing, quantum network, quantum communication, quantum teleportation, quantum experiment satellite, quantum key distribution, quantum blockchain*

Cite This Article: Lidong Wang, and Cheryl Ann Alexander, “Quantum Science and Quantum Technology: Progress and Challenges.” *American Journal of Electrical and Electronic Engineering*, vol. 8, no. 2 (2020): 43-50. doi: 10.12691/ajeee-8-2-1.

1. Introduction

Quantum computing offers new capabilities in health services, finance, logistics, etc. Cloud-based access to quantum-enabled data servers and centers will probably be approaches soon. Cloud-based quantum search methods help support various consumer devices and facilities such as autonomous vehicles, personal electronics, and smart homes. The devices interact with quantum computers, submit requests, and wait for computational results. Although an unstructured search is a difficult task, a quantum solution to an unstructured search problem was first studied by Grover who demonstrated quantum computing achieves a quadratic speed-up in the number of queries needed to search a database. In applications, for example, a quantum search can be adapted to planning and logistics [1].

Quantum annealing can be used in planning and scheduling. Automated planning and scheduling have various applications: from industrial automation, air traffic control, and logistics to general military tasks, disaster recovery, and the allocation of resources. Planning and scheduling issues are sometimes very challenging. The number of possible solutions grows exponentially with the growth of the number of events that will be planned or scheduled. These problems are generally handled using classical heuristic algorithms. Quantum annealing hardware helps the exploration of quantum heuristic methods for the problems, which aims to achieve significant improvement in efficiency [2].

Quantum probability fields have been used in the process of human perception and cognition with a wave function. Each person has a unique mind within his/her correspondent context; therefore, his/her own wave function needs to be described as a complex-valued probability amplitude. A quantum statistical approach has been used in elucidating the quantum mechanical feature—the context dependent dynamics of human’s cognitive conceptual processing. Quantum mechanics has peculiar features including its foundation in the analysis of mental entities, especially pertaining to perception and cognition [3].

Quantum computers have the potential to achieve breakthroughs: Internet encryption could be replaced by more secure approaches; discoveries in materials science and engineering could be revolutionized based on quantum process simulations; more lives could be saved due to effective and efficient drug design [4].

The purpose of this paper is to present progress, emerging technologies, and some challenges in quantum science and quantum technology.

2. Quantum Computers, Quantum Devices, and Quantum Processing Units

Quantum computer components operated at a room temperature unavoidably get errors from the thermal motion of atoms in the computer structure. These errors must be removed through quantum error correction [5]. A quantum system is susceptible to noise. The noise in a quantum computer means some qubits may end up in an ambiguous superposition state [6]. Theoretically, the capability of a quantum computer is based on its register of qubits with properties such as superposition and entanglement. But omnipotent quantum computation resources are weak when noise exists; therefore, it is difficult to control. The challenge of making quantum computing practical is to build quantum hardware that is robust enough to errors and possesses enough control fidelity to outperform most powerful classical computers [4].

Quantum entanglement discloses non-classical correlations between various subsystems. It has been regarded as an effective approach to handling information processing. The simplest entanglement (EPR pairs) enables tasks such as entanglement swapping, quantum cryptography, teleportation, and super-dense coding. The ability to prepare sizeable multi-qubit entangled states with a complete qubit control is significant for a physical platform upon which a quantum computer is built. The extent to which entanglement is found within a prepared graph state on *IBM Q Poughkeepsie* (a 20-qubit superconducting quantum computer) was investigated. A graph state along a path that consists of all the twenty qubits within the device was prepared and full quantum state tomography on all groups of four connected qubits along this path was performed [7].

D-Wave systems have been claimed to be the first commercially available quantum computers since 2011, but they are specifically developed for annealing computation, not being common circuit-model quantum computers [8]. A quantum annealer is advanced quantum computational hardware. Quantum annealing is a kind of metaheuristic optimization algorithm employing quantum effects (e.g., quantum tunneling and interference). A quantum annealer is a quantum computational device for a special purpose and only enables to run the quantum annealing metaheuristic. NASA in the USA hosted a 509-qubit D-Wave II machine that is one of the earliest quantum annealer prototypes and it was later upgraded to a 1097-qubit D-Wave 2X system later. Quantum annealers such as the D-Wave 2X are made of superconduct materials and run at a temperature of tens of milli-Kelvin [2]. A quantum simulator is a quantum device for specific application, for example, studying a model in quantum many-body physics [9].

The Quantum Exact Simulation Toolkit (QuEST) was introduced that is a new high-performance open-source framework for simulating a universal quantum computer. Compared with ProjectQ, qHipster, and a distributed implementation of Quantum++, QuEST demonstrates excellent scaling (both strong and weak) on multicore and distributed architectures. It demonstrates good strong scaling over OpenMP threads, competitive performance with a state-of-the-art single-node simulator ProjectQ when conducting multithreaded simulations of random circuits. Its communication strategy leads to similar performance to qHipster's and much better jobs than the distributed adaptation of Quantum++. Some simulators are listed and compared in Table 1 [10]. It should be noted that qHipster is not actively maintained anymore and has been renamed as Intel Quantum Simulator. Density matrices means the ability to accurately represent mixed states.

Algorithmic advantages of quantum computing require hardware devices that enable to encode quantum information, perform quantum logic, and finish sequences of complicated calculations based on the theory of quantum mechanics. Silicon spins, trapped ions, and superconducting transmons are three major approaches to quantum computing. Various qubit technologies are summarized in Table 2 [11].

Trapped-ion technologies and quantum processing units (QPUs) based on superconducting have emerged to be promising technologies of delivering quantum processors to market [1]. The integration of QPUs and high-performance computing (HPC) systems has been investigated. It has been found that the integration performance probably depends on the quantum interconnect that helps entangle multiple QPUs. QPU performance can be measured. Features that need to be tracked have been suggested and are listed in Table 3 [12]. FTQEC in the table stands for fault-tolerant quantum error correction and ISA stands for instruction set architecture.

Table 1. A Comparison of Some Simulators

Simulator	Stand-alone	Distributed	Multithreaded	GPU accelerated	Density matrices
ProjectQ			X		
QuantumSim				X	X
QuEST	X	X	X	X	X
Qrack	X		X	X	
qHipster	X	X	X		

Table 2. Comparison of Qubit Implementations

Features	Transmon Qubits	Trapped-Ion Qubits	Silicon Qubits
Qubit	Charge states in superconducting islands	Electron energy levels of ions in vacuum	Electron/nuclear spin states
Advantages	Solid-state, fast operation	Reproducible, long coherence times	Compact, solid-state, long coherence times
Control	Microwave fields	Optical fields	Microwave fields
Coupling	Resonator	Trap vibrational modes	Exchange-interaction
Readout	Resonator	Optical pumping	Spin-charge conversion
Qubit energy splitting	~ 5 GHz	~ 12 GHz (^{171}Yb^{+}), ~ 411 THz (^{40} Ca^{+})	Tens of gigahertz (electron spin), tens of megahertz (nuclear spin)

Table 3. Performance Metrics for a QPU

Metrics	Significance
Number of Qubits	Problem size capabilities
Number of Gates	Number of gates for completing a circuit
Clock Cycles Per Gate	Basis for determining quantum computation time
Entanglement Rate	Time required for refreshing or reestablishing entanglement between a set of qubits
Entanglement Latency	Time required for initially entangling a set of qubits
ISA Complexity	The diversity of gates that can be executed
Teleportation Rate	The rate at which quantum data can be exchanged
Inter-QPU Connectivity	Number of qubits with which a single qubit can entangle indirectly or at a remote site
Intra-QPU Connectivity	Number of qubits a single qubit can entangle with directly
FTQEC Latency	Additional computation time needed to incorporate FTQEC
FTQEC Gate Overhead	Number of extra gates needed to perform FTQEC
FTQEC Qubit Overhead	Number of extra qubits needed to perform FTQEC
Sample Rate	The lifecycle frequency for getting a result and resetting a circuit for getting an extra result

Quantum information is expressed by quantum states and with the exploitation of quantum effects such as quantum superposition, quantum entanglement, quantum interference, no-cloning theorem, decoherence, etc. In quantum computation, quantum operations are applied on quantum registers where quantum states express quantum superposition (while in a quantum circuit, quantum states are entangled). Quantum gates may be fulfilled through quantum dots, superconductors, diamonds, ion traps, donor-based systems, linear optic tools, or topological quantum computing elements. Quantum memristors are resistors with memory whose resistance relies on the crossing charges history. The model of quantum memristors may be used as a building block for neuromorphic quantum computation and quantum simulation of a non-Markovian system. Quantum CPUs use a quantum bus to communicate between the functional components of a quantum computer [13].

A quantum system tends to quickly lose its quantum nature (quantum coherence) and reverts to a classical description as the system becomes large and more complex primarily due to interactions with an environment that tends to destroy superposition and entanglement. Quantum logic gates manipulate complex coefficients of superposition states and any errors or noise in the gates can build up in an analog fashion. To deal with this problem, quantum error correcting codes (QECCs) have been developed that can be utilized to correct the errors [14].

A challenge of quantum computing is the characterization and reduction of various errors that are accumulated when an algorithm runs on large-scale processors. Cycle benchmarking (CB), a scalable protocol for characterizing global and local errors across multi-qubit quantum processors was developed. It was demonstrated that the CB was practicable based on experiments through quantifying the errors in non-entangling and entangling operations on an ion-trap quantum computer with up to 10 qubits. It was validated by CB data that the error rate per single-qubit gate and per two-qubit coupling does not go up with an increased system size. The CB can be easily executed on a general quantum computing architecture to evaluate the fidelity of multi-qubit processes [15].

3. Quantum Artificial Intelligence, Quantum Machine Learning, Quantum Cloud Computing, and Software for Quantum Computing

Quantum neural network is described as a system of blocks with a specific input and an output. This kind of neural structures is derived from biological neurons that are in our brain. A quantum network has various layers, for instance, the input layer, the output layer, the decision layer, etc. Quantum artificial neural networks (QuANNs) are very flexible in processing huge input data and complicated functions to predict the output. A main advantage of a quantum learning algorithm is the capability of reacting and adapting independently in a classical environment and a quantum environment [16]. QuANNs provide an approach to quantum machine learning based on networked quantum computation. In QuANNs, the networks' processing includes two stages: the learning stage (the networks converge to a specific quantum circuit) and the backpropagation stage (the networks effectively work as self-programing) [17]. One kind of quantum machine learning (ML) uses "quantum tunneling". The tunneling approach can be better or not than simulated annealing; however, using both the approaches may give a better solution than either of them [5].

A generative model tries to capture a full underlying probability distribution for observed data. Compared with discriminative models (e.g., feed-forward neural networks and support vector machines), generative models enable to describe much more complex relations among variables. Typical generative models include probabilistic graphical models (e.g., Markov random fields and Bayesian nets) and generative neural networks (e.g., deep belief nets, Boltzmann machines, and generative adversarial networks). A general quantum algorithm for machine learning was proposed based on a quantum generative model. It was proven the model can offer exponential enhancement in the representation capability over a commonly used classical generative model [18].

Metaheuristic refers to a set of methodologies that are conceptually positioned heuristics. Quantum metaheuristics are approximate algorithms developed to have an impact on running time, performance, and metrics because they will be implemented on quantum computers. But quantum-inspired metaheuristics have been developed to run on classical computers and simulating phenomena of quantum mechanics such as entanglement and superposition permit us to develop quantum programming to predict future results or behaviors. Implementing a metaheuristic on a quantum computer based on a circuit model requires a hybrid programming strategy that integrates a quantum computer (handling the quantum chromosome), quantum operators (modifying the register), and a classical computer (evaluating the fitness function and manipulating the algorithm flow) [19].

A mechanism of privacy-preserving quantum ML was presented. This mechanism was tested on the Wisconsin breast cancer dataset, which classified whether a tumor is benign or malignant. The dataset is sensitive and with features as well as target labels for the breast cancer prediction [20].

The study of subverting ML systems through motivated attackers is called adversarial ML. Adversaries can replicate the underlying model, reduce the confidence of prediction, recover training data, backdoor models to fail on specific examples, and even reprogram a model to a totally different task. A main objective of adversarial ML is to address and characterize problems through making a classifier more robust to attacks or providing a better tool to find when an attack occurs. The most important classes of attacks are the exploratory attack and the causative attack. An exploratory attack is not designed to explicitly influence a classifier but is intended to provide adversary information about the classifier. Such an attack works by an adversary feeding test examples to the classifier and then inferring information about it from returned classes (or meta data). A causative attack tries to change a model by providing it with training examples. Blind quantum computing may secure quantum ML algorithms and blind underlying datasets from any adversary. Quantum technologies have the potential to boost privacy and security, which helps implement quantum enhanced privacy and security for artificial intelligence and ML (such as clustering medical data) [21].

The human brain may be regarded as a dynamical graph with electrical signals (frequency, amplitude, and phase). A neuron has two basic states that are expressed as |0> (for a ground state) and |1> (for an excited state). The whole state of an area of neurons is a linear combination of the two states with complex coefficients that represent the signals (with the three parameters: frequency, amplitude, and phase) along neurons. A simple model was presented to express the neural network through creating sub-graphs of the whole network with same or similar states. Areas of neurons with the same state (a ground state or an excited state) was formed. Interactions between the areas were described with closed loops and feedback loops. A change of a graph was given using the deformation of the loops. It was shown that there were many common properties in the model of the neural network and quantum circuits. A formal link between neural networks and quantum computing was discussed. It was also discussed whether the brain (or neural networks) can be simulated using a quantum computer with small resources [22].

The human mind is constituted by subjective, inner, private, first-person conscious experiences. Both the quantum state and the inner world of consciousness are unobservable. The origin of the inner privacy of consciousness can be regarded as unobservable and incommunicable quantum information with quantum states of a human brain. Identifying consciousness with unobservable quantum information (with quantum states of a physical brain) permits us to use quantum information principles to resolve possible paradoxes (resulted from the inner privacy of conscious experience) and elucidate how a brain is constructed by accessible bits of classical information and extracted from the physical quantum brain upon measurement with devices. Quantum mechanics plays a significant role in human's consciousness and thinking [23].

Privacy-preserving database query permits a user to retrieve data-items from a cloud database without disclosing the information of the data-items, while limiting the user's access to other ones. A quantum-based database query scheme for privacy protection in a cloud environment was established. Specifically, all the data-items of the database were firstly encrypted with various keys to protect a server's privacy and the server was needed to transmit all the encrypted data-items to a client with an oblivious transfer strategy to ensure the client's privacy [24].

A security model of quantum cryptography in mobile cloud computing was presented for highly secure data and privacy cryptography. Quantum keys were distributed to users' phones in two phases in this model. First, the classical optical network was transformed as quantum distribution network conveniently using the multiplexing technology and the BB84 quantum key distribution protocol (performed based on decoy state) was adopted; Second, a security authentication protocol based on quantum keys and distance-bounding HKQ was provided; quantum keys were transmitted into a security storage area of users' phone in the trusted area using the near field communication (NFC) technology; and mobile users could access the data on the cloud using quantum secret keys, guaranteeing users' data security and privacy [25].

There has been some open source software used for quantum computing. As for adiabatic quantum computation, quantum annealing devices exploit this model. It uses a phenomenon from quantum physics that is known as the adiabatic theorem to seek a global optimum of a discrete optimization problem. For quantum computing simulators, Quantum++ is a simulator with high performance that was written in C++. Qrack is another simulator based on C++ and is of extra support for graphics processing units (GPUs). Developers of Qrack emphasized on performance through a parallelization support over multiple CPU or GPU cores. Quirk is a quantum computer simulator that is less performance-oriented and more educational. It is JavaScript-based and enables to simulate up to 16 qubits in a modern web browser. Rigetti Computing is a hardware startup that focuses on superconducting circuits for a discrete gate model. In quantum annealing, there have been open source projects and most of the projects are supported by D-Wave Systems such as Qbsolv together with other simulators of quantum computer. The package dimod is an API based on Python to solve QUBO problems with different backends (including D-Wave's quantum processors) [9].

4. Quantum Network and Communication

Large-scale quantum computations should be conducted in a manner of distributed topologies. Quantum computers communicate with each other via a quantum bus (fulfilled by wireless quantum channels, optical fibers, etc.). Quantum algorithms and error-correction processes are performed in a distributed manner. Distributed quantum control and measurement are required. It is necessary to create quantum metropolitan area networks (Q-MAN) or quantum wide area networks (Q-WAN) for a large distance [13].

A quantum network basically consists of terminals, connections, switches, and protocols. A terminal is an interface in a network that is used for transmitting and receiving data by a user. It can be a node (a destination node for data acquisition or a source node for data transmission). A connection is a data communication medium between terminals. A switch is a device used to find and transmit data to the next receiver. A protocol defines rules that guarantee proper operations in the network. A quantum network mainly has the routing protocol and the packet protocol [26].

Software defined networking (SDN) principles have been used to create a converged quantum-classical network that shares the logical and physical infrastructure among classical and quantum channels. Compared with typical quantum network architectures that employ an ad hoc network running in parallel to a conventional one for qubit transmission, the quantum enabled SDN architecture unites quantum and classical communications, leading to network optimization for better utilization of all resources [27].

A framework for 6G communication networks was proposed in which quantum ML (QML) and quantum-assisted ML are core technologies. QML and quantum-assisted ML can be regarded as key technologies for solving massive-objectives optimization tasks of the massive and complex communication networks in the future such as massive-objectives routing in Massive-IoT (M-IoT) for a smart world [28].

5. Quantum Teleportation and Quantum Experiment Satellite

Quantum teleportation allows for transmitting quantum data to a preferred distance without any communication channel, which guarantees data cannot be listened to because no channels is used for listening. Quantum teleportation is based on the physical theory of entanglement, acts as a significant principle of quantum information tasks, and embodies a major building block of quantum technology [26].

Satellite-based quantum communication enables long distance and even global quantum networking of quantum optical signals. Quantum communication facilitates various applications such as high communication density and highly secure cryptography beyond the capabilities of classical channels. Optical signals that are sent between ground and a satellite enable to cover a much larger distance than that on a similar terrestrial link due to low transmission loss in an empty space (no atmospheric scattering). So, the only current method of establishing global-range quantum communication for single optical photons is using an Earth-orbiting satellite [29].

The first quantum science satellite (called Micius) in the world was launched in 2016. It was on a sun-synchronous orbit around 500 km above the Earth to create a platform for long-distance quantum science experiment, perform space-scale quantum science experiment, and facilitate wide-area or even global quantum communication. Specifically, tasks cover space-to-ground quantum entanglement distribution, wide-area quantum key network experiment, space-to-ground high-speed quantum key distribution, ground-to-space experiment of quantum teleportation, etc. Two years later, a satellite-based entanglement distribution to two locations separated by 1,200 km on the earth and the Bell test were finished, which demonstrated quantum entanglement exists in a so long distance. Afterwards, the decoy-state quantum key distribution (QKD) of satellite-to-ground and the quantum teleportation of ground-to-satellite were fulfilled. Entanglement-based QKD with a satellite is practicable. These experiments with the Micius quantum satellite are the first step toward a global and space-based quantum network [30].

An example of low-noise, spaceborne, and high reliability single-photon detectors (SPDs) was presented based on COTS (commercial off-the-shelf) silicon APD (avalanche photodiodes). Multistage cooling technologies, configurable driver electronics, and special shielding structures were developed based on the high noise-radiation sensitivity of silicon APD, which greatly mitigated the SPD noise-radiation sensitivity and improved the COTS APD reliability. The low-noise and spaceborne SPDs helped to develop a practicable satellite-based up-link quantum communication. It was tested and demonstrated on the platform of the quantum science satellite [31].

Research on quantum communication in a free space and in the daytime has fostered efficient operations of a "quantum satellite constellation". It is needed to create various optical links with low channel loss, including ground to satellite, satellite to ground, and satellite to satellite links for global networks of quantum communication in the future that is based on constellation. A transmission antenna with the point-ahead technique was designed and an easy-to-perform method for calibration was provided. The antenna helped to create an uplink to the quantum satellite Micius. A quantum optical transmitter for the uplink of ground-to-satellite was designed and implemented. A quantum optical link was created between ground and the quantum science satellite. A quantum teleportation experiment of ground-to-satellite was completed. Space-based quantum communication will be a significant step toward a global network of quantum communication [32].

A combined technology of satellite-ground for video transmission was presented. The QKD technology was employed in the satellite-ground combined video transmission tasks. The video transmission protection with a high security level via quantum key was fulfilled. Quantum relay technology and quantum signal rapid rectifying technique were employed to overcome technical difficulties, e.g., multi-relay node and hybrid network of buried optical cable and overhead optical cable [33].

6. Quantum Cryptography and Quantum Key Distribution

Quantum electronic signature is a method of signature generation based on quantum data processing that includes keys in the process from production to signature [26]. The property of entanglement in quantum communication has implication for quantum cryptography that is a highly secure brand of cryptography [6]. Many efforts have been made to explore post-quantum cryptography (PQC) techniques to prepare for the emergence of quantum computers and quantum computing. Most current PQC schemes can be divided into the following categories: hash-based, code-based, lattice-based, and multivariate. Isogeny-based cryptography was investigated that is a relatively young and promising post-quantum technique and has small key sizes and signature sizes [34].

Much work is being done in quantum-resilient or post-quantum cryptography. Lattice-based cryptography (LBC) is promising as a quantum-safe alternative to the available public-key cryptography. It has become the best fit according to the key size compactness and simplicity of application compared with other alternative schemes with quantum-safety. But the performance of the LBC scheme suffers from associated large public key size compared with traditional public key schemes, which is a challenge for a system in the real world [35].

One of applications of quantum information technology is QKD. QKD uses the property of quantum light to provide information–theoretic (unconditional) security for the storage and transmission of classical data. There has been noteworthy advance in experiment for giving point-to-point and long-distance QKD links and creating multi-site quantum networks. Simulations of proof-of-principle for two protocols were conducted using the superconducting quantum computers of IBM Quantum Experience. Especially, 5- and 16-qubit superconducting processors were used. The latter could be regarded as a complicated quantum network with physical qubits (network nodes). The super dense coding protocol and the famous quantum key distribution BB84 protocol were used. The capability of quantum devices to serve as quantum memory and store entangled states that were utilized in quantum communication was examined [36].

QKD offers an opportunity to provide unconditional security for communication. The most robust QKD is based on quantum entanglement. With the focus on discrete variable QKD and using a low data rate consistent with the measured entanglement distribution from space, benefits from state-of-the-art short-block length codes in the context of device independent QKD were quantified [37].

For quantum communication in a free space, especially with a satellite, if it is assumed that a man-in-the-middle attack could be detected by a classical channel monitoring technique, a simplified protocol and hardware system of quantum communication could be realized and deliver an improved key rate. A photon key distribution (PKD) protocol has a higher rate than a QKD protocol. The hardware categories and relating approaches of PKD and QKD are summarized in Table 4 [38].

Table 4. PKD and QKD Approaches Modelled for Various Hardware Implementation

Photon Source	PKD Encoding (Example)	QKD Protocol
Ideal single photon source	Left or Right-handed polarized photons	Single photon BB84
Weak coherent pulse	Pulse position modulation	Decoy state BB84
Spontaneous parametric down conversion pairs	Heralded Left or Right-handed polarized photons	BBM92 (entanglement-based BB84)

7. Quantum Blockchain

A simple voting protocol was proposed based on quantum blockchain. The protocol satisfies security requirements: anonymous, eligible, verifiable, non-reusable, binding, fair and self-tallying. Its structure is like the voting protocol of bitcoin blockchain and includes two phases: ballot commitment phase and ballot tallying phase [39].

Quantum bitcoin was the first distributed quantum currency. It was an application of quantum mechanics in which an ideally distributed and publicly verifiable payment system was created. The no-cloning principle lays the solid foundation of unforgeable items and a blockchain allows for making currency without trusting a central entity. Two parties can transfer the quantum bitcoin through transferring a quantum state over a quantum channel and reading off a publicly available blockchain. A transaction is completed immediately without a need of waiting for a confirmation from a miner. The system can be scaled to permit an unlimited rate of transactions with no transaction fee. Because a sender and a receiver need to share a quantum channel, conventional Internet infrastructure is not adequate to transact over a very long distance [40].

A quantum computing attack seriously threatens blockchain security. A secure cryptocurrency scheme was proposed based on post-quantum blockchain (PQB). It enables to fight a quantum computing attack. Firstly, a signature scheme was proposed based on lattice problem. The lattice basis delegation algorithm was used for the generation of secret keys with selecting a random value and signing message by preimage sampling algorithm. Furthermore, the first signature and the last signature were designed in the scheme, which was defined as double-signature. This reduces the correlation between the signature and the message. Secondly, a PQB was constructed and a cryptocurrency scheme was proposed through the combination of the proposed signature scheme and blockchain. Compared to conventional signature schemes, sizes of signature and secret keys in the proposed cryptocurrency scheme are shorter, which decreases computational complexity [41].

An architecture of a quantum-enabled blockchain based on a consortium of quantum servers was presented. The network is hybrid, using a digital system (for processing and sharing classical information) combined with a fiber-optic infrastructure as well as quantum devices (for processing and transmitting quantum information). An interactive mining protocol that is energy-efficient and enacted between servers and clients was delivered. It utilizes quantum information (encoded in light). The use of a quantum-secure authentication protocol was explored for physical addressing, tamper detection of devices, prevention against a Sybil attack, and various authentications (authenticating hardware, clients, and communication channels) [42].

8. Conclusion

Quantum computers are based on their registers of qubits with properties such as superposition and entanglement. It is a challenge of quantum computing to characterize and reduce various errors as well as build quantum hardware that is robust enough to withstand errors. Quantum neural network is derived from biological neurons in a human brain. QuANNs are very flexible in processing huge input data and complex functions. Quantum technologies have the potential to boost quantum enhanced privacy and security for artificial intelligence and ML. A quantum-based database query in a cloud environment ensure privacy preservation.

It is significant to create Q-MAN and Q-WAN for a large distance. Space quantum communication is a major step toward a global quantum communication network. Quantum teleportation is based on quantum entanglement and enables to transmit quantum data (with security guarantee) to a desired distance without any communication channel. Satellite-based quantum communications facilitates global quantum networking of quantum optical signals. Entanglement-based QKD with a satellite is feasible. QKD enables to guarantee unconditional communication security. Quantum blockchain integrates the advantages of quantum technology and blockchain, which resists cyberattacks.

References

[1] Humble T. Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications. IEEE Consumer Electronics Magazine. 2018 Oct 5; 7(6): 8-14.

[2] Biswas R, Jiang Z, Kechezhi K, Knysh S, Mandrà S, O'Gorman B, Perdomo-Ortiz A, Petukhov A, Realpe-Gómez J, Rieffel E, Venturelli D. A NASA perspective on quantum computing: Opportunities and challenges. Parallel Computing. 2017 May 1; 64: 81-98.

[3] Conte E, Kaleagasioglu F, Norman R. The quantum statistical mechanics in the analysis of the context dependence in quantum cognition studies: may a quantum statistical analysis connect the science of complexity?. Chaos and Complexity Letters. 2017 May 1; 11(2): 203-18.

[4] McGeoch CC, Harris R, Reinhardt SP, Bunyk PI. Practical annealing-based quantum computing. Computer. 2019 Jun 3; 52(6): 38-46.

[5] DeBenedictis EP. A future with quantum machine learning. Computer. 2018 Feb 23; 51(2): 68-71.

[6] Keplinger K. Is quantum computing becoming relevant to cyber-security?. Network Security. 2018 Sep 1; 2018(9): 16-9.

[7] Mooney GJ, Hill CD, Hollenberg LC. Entanglement in a 20-qubit superconducting quantum computer. Scientific reports. 2019; 9.

[8] Hu S, Liu P, Chen CR, Pistoia M, Gambetta J. Reduction-Based Problem Mapping for Quantum Computing. Computer. 2019 Jun 4; 52(6): 47-57.

[9] Fingerhuth M, Babej T, Wittek P. Open source software in quantum computing. PloS one. 2018; 13(12).

[10] Jones T, Brown A, Bush I, Benjamin SC. Quest and high performance simulation of quantum computers. Scientific reports. 2019 Jul 24; 9(1): 1-1.

[11] Humble TS, Thapliyal H, Munoz-Coreas E, Mohiyaddin FA, Bennink RS. Quantum Computing Circuits and Devices. IEEE Design & Test. 2019 Apr 3;36(3):69-94.

[12] Britt KA, Humble TS. High-performance computing with quantum processing units. ACM Journal on Emerging Technologies in Computing Systems (JETC). 2017 Mar 17; 13(3): 1-3.

[13] Gyongyosi L, Imre S. A survey on quantum computing technology. Computer Science Review. 2019 Feb 1; 31: 51-71.

[14] Maslov D, Nam Y, Kim J. An Outlook for Quantum Computing [Point of View]. Proceedings of the IEEE. 2018 Dec 27; 107(1): 5-10.

[15] Erhard A, Wallman JJ, Postler L, Meth M, Stricker R, Martinez EA, Schindler P, Monz T, Emerson J, Blatt R. Characterizing large-scale quantum computers via cycle benchmarking. Nature communications. 2019 Nov 25; 10(1): 1-7.

[16] Gupta S, Mohanta S, Chakraborty M, Ghosh S. Quantum machine learning-using quantum computation in artificial intelligence and deep neural networks: Quantum computation and machine learning in artificial intelligence. In2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON) 2017 Aug 16 (pp. 268-274). IEEE.

[17] Gonçalves CP. Quantum Neural Machine Learning-Backpropagation and Dynamics. arXiv preprint arXiv:1609.06935. 2016 Sep 22.

[18] Gao X, Zhang ZY, Duan LM. A quantum machine learning algorithm based on generative models. Science advances. 2018 Dec 1; 4(12):eaat9004.

[19] Ross OH. A review of quantum-inspired metaheuristics: going from classical computers to real quantum computers. IEEE Access. 2019 Dec 25.

[20] Senekane M, Mafu M, Taele BM. Privacy-preserving quantum machine learning using differential privacy. In2017 IEEE AFRICON 2017 Sep 18 (pp. 1432-1435). IEEE.

[21] Wiebe N, Kumar RS. Hardening quantum machine learning against adversaries. New Journal of Physics. 2018 Dec 21; 20(12): 123019.

[22] Asselmeyer-Maluga T. Quantum computing and the brain: quantum nets, dessins d'enfants and neural networks. arXiv preprint arXiv:1812.08338. 2018 Dec 18.

[23] Georgiev DD. Inner privacy of conscious experiences and quantum information. Biosystems. 2020 Jan 1;187:104051.

[24] Liu W, Gao P, Liu Z, Chen H, Zhang M. A quantum-based database query scheme for privacy preservation in cloud environment. Security and Communication Networks. 2019;2019.

[25] Han J, Liu Y, Sun X, Song L. Enhancing data and privacy security in mobile cloud computing through quantum cryptography. In 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS) 2016 Aug 26 (pp. 398-401).

[26] YAŞAR C, YILMAZ İ. Secure Distribution of Electronic Documents over Network in Quantum Information Management Systems. In2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2019 Oct 11 (pp. 1-8).

[27] Aguado A, Lopez V, Lopez D, Peev M, Poppe A, Pastor A, Folgueira J, Martin V. The engineering of software-defined quantum key distribution networks. IEEE Communications Magazine. 2019 Jul 19; 57(7): 20-6.

[28] Nawaz SJ, Sharma SK, Wyne S, Patwary MN, Asaduzzaman M. Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future. IEEE Access. 2019 Apr 4; 7: 46317-50.

[29] Jennewein T. Towards Quantum Communications with Satellites. In2018 IEEE Photonics Society Summer Topical Meeting Series (SUM) 2018 Jul 9 (pp. 217-218).

[30] Yin J, Ren JG, Liao SK, Cao Y, Cai WQ, Peng CZ, Pan JW. Quantum Science Experiments with Micius Satellite. InCLEO: Applications and Technology 2019 May 5 (pp. JTu3G-4). Optical Society of America.

[31] Yang M, Xu F, Ren JG, Yin J, Li Y, Cao Y, Shen Q, Yong HL, Zhang L, Liao SK, Pan JW. Spaceborne, low-noise, single-photon detection for satellite-based quantum communications. Optics Express. 2019 Dec 9; 27(25): 36114-28.

[32] Han X, Yong HL, Xu P, Wang WY, Yang KX, Xue HJ, Cai WQ, Ren JG, Peng CZ, Pan JW. Point-ahead demonstration of a transmitting antenna for satellite quantum communication. Optics express. 2018 Jun 25;26(13):17044-55.

[33] Liu Y, Yan L, Chen Z, Gao D, Shi R, Cao Y, Li L. Technology of Satellite-Ground Combined Video Transmission Based on Quantum Key Distribution. In2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2) 2018 Oct 20 (pp. 1-5).

[34] Peng C, Chen J, Zeadally S, He D. Isogeny-Based Cryptography: A Promising Post-Quantum Technique. IT Professional. 2019 Nov 11; 21(6): 27-32.

[35] Khalid A, McCarthy S, O'Neill M, Liu W. Lattice-based Cryptography for IoT in A Quantum World: Are We Ready?. In2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI) 2019 Jun 13 (pp. 194-199).

[36] Zhukov AA, Kiktenko EO, Elistratov AA, Pogosov WV, Lozovik YE. Quantum communication protocols as a benchmark for programmable quantum computers. Quantum Information Processing. 2019 Jan 1; 18(1): 31.

[37] Ai X, Malaney R, Ng SX, Hanzo L. Short Codes and Entanglement-based Quantum Key Distribution via Satellite. In2017 Sensor Signal Processing for Defence Conference (SSPD) 2017 Dec 6 (pp. 1-5).

[38] Vergoossen T, Bedington R, Grieve JA, Ling A. Satellite quantum communications when man-in-the-middle attacks are excluded. Entropy. 2019 Apr; 21(4): 387.

[39] Sun X, Wang Q, Kulicki P, Sopek M. A simple voting protocol on quantum blockchain. International Journal of Theoretical Physics. 2019 Jan 15; 58(1): 275-81.

[40] Jogenfors J. Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics. In2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2019 May 14 (pp. 245-252).

[41] Gao YL, Chen XB, Chen YL, Sun Y, Niu XX, Yang YX. A secure cryptocurrency scheme based on post-quantum blockchain. IEEE Access. 2018 Apr 18; 6: 27205-13.

[42] Bennet AJ, Daryanoosh S. Energy efficient mining on a quantum-enabled blockchain using light. arXiv preprint arXiv:1902.09520. 2019 Feb 25.