J Inf Process Syst, Vol.16, No.6, pp.1459~1478, December 2020
https://doi.org/10.3745/JIPS.03.0154

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Quantum Communication Technology for Future ICT – Review

Sushil Kumar Singh*, Abir El Azzaoui*, Mikail Mohammed Salim*, and Jong Hyuk Park*

Abstract

In the last few years, quantum communication technology and services have been developing in various advanced applications to secure the sharing of information from one device to another. It is a classical commercial medium, where several Internet of Things (IoT) devices are connected to information communication technology (ICT) and can communicate the information through quantum systems. Digital communications for future networks face various challenges, including data traffic, low latency, deployment of high-broadband, security, and privacy. Quantum communication, quantum sensors, quantum computing are the solutions to address these issues, as mentioned above. The secure transaction of data is the foremost essential needs for smart advanced applications in the future. In this paper, we proposed a quantum communication model system for future ICT and methodological flow. We show how to use blockchain in quantum computing and quantum cryptography to provide security and privacy in recent information sharing. We also discuss the latest global research trends for quantum communication technology in several countries, including the United States, Canada, the United Kingdom, Korea, and others. Finally, we discuss some open research challenges for quantum communication technology in various areas, including quantum internet and quantum computing.

Keywords

Computing Security and Privacy, Quantum, Communication, Sensor, Smart Applications

1. Introduction

Werner Heisenberg, in 1925, described quantum physics as a physics theory presenting a mathematical description of matter and energy communication. Quantum mechanics, a subset of quantum physics, defines the foundational subatomic behavior, where the unknown location of a subatomic particle is observed. It details how the universe functions at a scale smaller than an atom, whereas classical physics describes nature elements at a more macroscopic level. Particles possess wavelike properties, and their behavior is observed using the wave equation and Schrodinger equation. Several new and distinct foundations in quantum technology have been derived, such as quantum chemistry, field theory, information science, and technology.

Quantum information theory (QIT) is an amalgamation of several concepts from computer science, classical information theory, and quantum mechanics, which include mathematical physics, quantum statistical physics, and probability theory. The study's primary purpose in QIT is to accomplish tasks

Manuscript received October 20, 2020; first revision November 24, 2020; accepted November 24, 2020.

Corresponding Author: Jong Hyuk Park (e-mail: jhpark1@seoultech.ac.kr)

* Dept. of Computer Science and Engineering, Seoul National University of Science & Technology (SeoulTech), Seoul, Korea (sushil.sngh001007@seoultech.ac.kr, abir.el@seoultech.ac.kr, mikail@seoultech.ac.kr, jhpark1@seoultech.ac.kr)

using quantum mechanical systems to achieve efficient storage and transmission of information using physical systems' quantum mechanical properties [1]. Information theory relies on probability theory to understand the mathematical limitations of communication and security. It utilizes quantum mechanics to determine information processing limits such as secret key agreement and quantum states' preservation.

Quantum information theory is the central pillar of quantum computers. Recently, quantum computers are being developed at a rapid pace [2]. As one of the prominent research institutions on the quantum computers area, Google has reached quantum supremacy with its "Sycamore" quantum computer that, reportedly, encloses 53 qubits and was able to solve complex computations in 200 seconds. The same mathematic puzzles will take over 10,000 years to solve using today's most influential classical computer. IBM also created a global community for researchers and companies called "IBM Q Network" to work all together for the advancement and development of quantum information-related areas. Other high-tech companies are developing their services and preparing their classical models to shift to a quantum model as soon as quantum computers are available.

The future information communication technology (ICT) will surely rely on quantum communication technologies (QCT) which is built over quntum physics laws to secure data communication; thus, preparing for this new upcoming area is significant. In the future ICT, computers are not the only benefits from quantum technology, but our communication will also shift to quantum. Instead of the classical Internet, quantum Internet is viewed as the new channel of communication. Recent studies are currently focusing more on quantum Internet and quantum teleportation as it is the most appropriate technologies now. The most utilized quantum Internet application is quantum key distribution (QKD), which is used to secure communication between the sender and receiver as it is based on quantum mechanics' law. QKD's security guarantees the high privacy of future quantum Internet, where not only data can be shared securely, but also multiple quantum devices can be grouped in the cloud and share huge computational power.

Quantum Internet, however, cannot get rid of the classical internet yet. To send data in quantum Internet, we send photons encoded into the qubits' status containing the data. These photons travel via a fiber-optic channel, albeit the distance they can cross is very limited (under 300 km). If a photon traveled for more than this distance, it risked being lost, and it could take us the billions of years to recover it. A photon as well as risk being destroyed while measured, which leads to a data loss. The fragile characteristics of photons are what make QKD and quantum Internet very secure. It is, however, the same reason that creates a burden on integrating quantum communication in today's ICT scenarios.

To fix this dilemma, researchers proposed to utilize a Quantum Repeater, which plays as a middle point between the sender and receiver. The Quantum Repeater entangled with the sender and receiver at the same time and store their qubit status in its memory, it receives from the sender the photon with the original information status, measure it, and send it to the final receiver. This method has been used for years now; however, it is not the perfect solution. The Quantum Repeater requires a huge quantum memory to store qubit's states; it obligates a big power consumption and executes all these steps. Moreover, the Quantum Repeater must be a very trusted node as we send it to all the messages or data at once.

To this end, we propose in this paper the use of Quantum machines with a single qubit as quantum chain repeaters. We divide the data into multiple qubit and send every qubit of information via different quantum machine in the quantum machine chain (QMC) at other time slots. Every quantum machine in QMC has to deal with a single qubit and register only the time-stamp and not the whole qubit state into

its memory, which will consume less time and demand less memory size and computational power. These quantum machines can be any device in the future ICT; the devices connected to a Quantum cloud can benefit from a Quantum computer-alike power without creating a complex system.

The main contribution of our paper is as follows:

- Discuss quantum technologies for future ICT, such as QKD and Blockchain-based quantum cryptography.
- We explain the main concepts and features of QIT, quantum computers, and quantum Internet in detail.
- We depict some of the recent state-of-the-art research and project trends and areas worldwide about quantum computers and quantum Internet.
- We explain our proposition overview of a QMC in future ICT and discuss its phases.
- Describe some of the main open research challenges in the area of quantum Internet and quantum computing as quantum communication technology.

The rest of the paper is organized as follows: in Section 2, we define the main foundation of quantum computer and quantum Internet and depict the related technologies for future ICT. Section 3 presents the recent research advances in the area of quantum Internet around the globe. In Section 4, we demonstrate our proposition of QMC and discuss the main components of our model; we clarify some and the leading open research challenges of the area. And we conclude our work with the fifth section.

2. Quantum Technologies for Future ICT

In this section, we discuss quantum technologies for future ICT. It is categorized into three subsections, including the foundation of quantum computers and quantum physics, quantum cryptography, and blockchain-based quantum computing.

2.1 Foundation of Quantum Computers and Quantum Physics

The term quantum computing was first proposed in 1980 by the mathematician Yuri Manin [3], where he discussed the idea of quantum computation in his book. Subsequently, physicist Feynman [4] recorded an exponential slowdown of efficiency while simulating a quantum physical system of $\mathbb{R}$ particles using ordinary computers. Simulating a classical physical system in the same computer, however, can be done without polynomial slowdown. The rationalization of this phenomenon is that classical physics describes linearly the size of a particle system in $\mathbb{R}$, while it is described exponentially in quantum physics. Based on this observation, physicist Feynman [4] suggested to build a computer-based on quantum physics laws. Classical computers and quantum computers are based on different laws and designed to achieve different tasks. Using transistors, a classical computer is capable of processing information and calculation based on a finite combination of binary digits (bits) denoted as 0 and 1. A quantum computer, however, is based on quantum mechanical states of elementary particles such as the internal angular momentum denoted as the spin. Quantum computers have also different other features from the classical computer, we note those elements as follows:

- *Qubit:* The term of qubit was first introduced in 1995 by physicist Schumacher [5], the proposed theorem states that the von Neumann entropy S of the density operator to describe a quantum state

can be perfectly represented by the spin of particles, the spin serves as a signal and was denoted in the paper by quantum bit. To understand the qubit, we will denote them as mathematical objects with unique characteristics. Similar to a classical bit which has two states, 0 or 1, a qubit as well as a state denoted by $|\mathbf{0}\rangle \boldsymbol{and} \ |\mathbf{1}\rangle$ with " $|\ \rangle$" known as the Dirac Notion. While a classical bit can either be in state 0 or 1, qubit has, however, the possibility to the in states other than $|\mathbf{0}\rangle \boldsymbol{or} \ |\mathbf{1}\rangle$ simultaneously. It is as well possible to create a linear combination of states, which is known in quantum theory by superposition. A state in quantum information is denoted as $|\boldsymbol{\psi}\rangle$ and can be represented as the following formula:

$$|\boldsymbol{\psi}\rangle = \boldsymbol{\alpha}\,|\mathbf{0}\rangle + \boldsymbol{\beta}\,|\mathbf{1}\rangle$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are two complex numbers. The state of qubit can be represented as a unit vector in a two-dimensional complex vector space where the states $|\mathbf{0}\rangle \ \mathbf{and} \ |\mathbf{1}\rangle$ form the orthonormal basis. Unlike the classical bits, we cannot examine a qubit to measure its state, rather we determine it based on its coefficients $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. At the measurement, the state can be 0 with the probability $|\boldsymbol{\alpha}|^2$ or 1 with the probability $|\boldsymbol{\beta}|^2$ and $|\boldsymbol{\alpha}|^2 + |\boldsymbol{\beta}|^2 = \mathbf{1}$ based on probability law. In order to visualize the concept of qubits, the previous formula can be represented as follows:

$$|\boldsymbol{\psi}\rangle = \boldsymbol{cos}\ \frac{\boldsymbol{\theta}}{\mathbf{2}}\,|\mathbf{0}\rangle + \boldsymbol{e^{i\alpha}}\ \boldsymbol{sin}\ \frac{\boldsymbol{\theta}}{\mathbf{2}}\,|\mathbf{1}\rangle$$

where $\boldsymbol{\theta}$ and $\boldsymbol{\alpha}$ represent points on the unit three-dimensional sphere that provides a conceptual way of visualizing the state of a qubit as shown in Fig. 1.

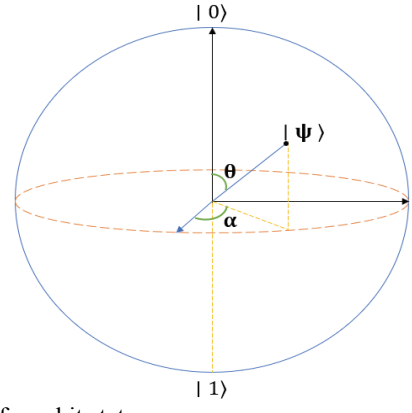

Fig. 1. Visuals representation of a qubit state.

- *Entanglement*: Einstein et al. [6] published a paper in 1935 stating that in a spatially separated Quantum system, a unique and nonclassical correlation was noticed. The authors called this action a "*spooky action at distance*". This action means that two spatially separated particles can be described with reference to each other and was called later as quantum entanglement or EPR paradox. Given this definition, if two particles are entangled and separated, the measurement of one particle spontaneously influences the other particle's state. Quantum entanglement serves as the main characteristic of quantum computers as is used to realize quantum teleportation.
- *Quantum Teleportation*: One famous demonstration of quantum entanglement is the quantum teleportation; it provides a solution of transmitting qubits without physically transferring the particle storing the qubit [7]. Using measurement-based of the Bell-State called BSM and an EPR pair shared

between source and destination, we can transmit a quantum state between two spatially separated quantum devices. As Fig. 2 depicted, to send information from Lab 1 to Lab 2, we must create two entangled particles (EPR pair) P1 and P2 each one is attributed to a Lab consecutively. In Lab 1, a BSM is performed upon the particle P1 and qubit state $|\psi\rangle$. The results of the measurement will be sent through a classical channel to Lab 2 in form of two Bits with four possibilities. Upon the reception, Lab 2 will start processing the results until it matches with the pre-entangled particle P2, and with that, they can retrieve the original status of P1 and the qubit $|\psi\rangle$ sent by Lab 1. We must note here that the original particles will both be destroyed upon measurement. Thus, in order to send other Qubit information, we need to re-construct a new EPR pair and distribute them between the sender and receiver.

- *Quantum Repeater*: Transferring qubit and quantum information over long distances require using fiber-optic networks [8]. Due to the fragile state of photons, however, they cannot be distributed over long distance channels without being lost. Moreover, it requires years to just detect a single photon, which will dismantle the concept and characteristics of quantum communication. As quantum approaches to this dilemma, a repeater can be used. A quantum repeater is a complex system with high-performance levels that store a quantum entanglement state, purify it, and swap it in a very organized architecture [9].

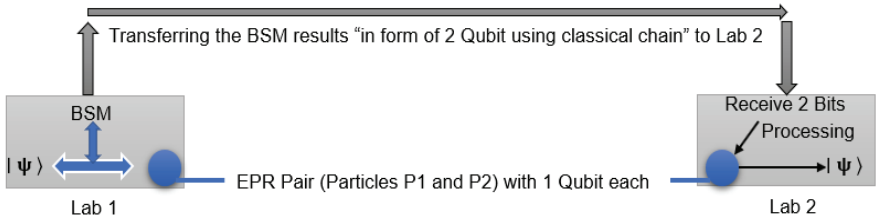

Fig. 2. Visual concept of quantum teleportation.

A quantum computer, using qubits, is potentially and theoretically capable of outstanding a classical computer in terms of capacity and computationally. Moreover, using the entanglement and transportation aspects, we can create a save and high-power quantum network sharing multiple quantum computers over a quantum Internet layer. The future of ICT is based on the development of quantum computers and the quantum Internet.

2.2 Quantum Cryptography

Cryptography is the method for preserving information by converting plain text data to unintelligible text data. It is a process of storing and sharing transaction data in a specific form so that only those for whom it is intended can read and process it. The enhancement of quantum technologies starts a new era for cryptography, and ICT with the latest possibilities are rapidly rising [10-12]. During the last three decades, quantum communication is the most developing field that combines quantum sensors, quantum computing, quantum physics, and information theory. The extension version of cryptography is known as quantum cryptography or quantum encryption. The basic quantum cryptography functionality is shown in Fig. 3. It applies quantum mechanics principles to encrypt messages and follows various security properties, including confidentiality, integrity, non-repudiation, and authentication [13-15]. Quantum cryptography is categorized into multiple sub-fields such as QKD, quantum random number generator

(QRNG), quantum digital signature (QDS), and quantum computation (QC) for better understanding the functionality of transmitting the transaction, which is the following:

***Quantum key distribution*:** According to the need for secure data communication, encryption and decryption are the part method because they protect from exposure to attacks or hackers. The integrity of data communication is dependent on symmetric cryptography; it has private and public keys. Thus, secure communication in the network is based on key distribution. It transfers the keys process between the sender and recipient to secure communication in the systems [16,17]. Traditional key distribution methods have various challenges, including security threatened by weak random number generators, needs high power CPU, unmanaged unknown attacks, and more. To effectively address these challenges, QKD is utilized, and it follows quantum properties for communicating the secret information. It facilitates the continuous generation and sharing of truly random one-time pad keys for the highest security requirements and follows the quantum mechanical properties. The working process of QKD have three points, which are the following:

- A quantum channel is free space or enabled fiber, send quantum light states between sender and recipient. This channel does not need to be secure.
- A public authenticated channel performs post-processing steps and uses a genuinely secrete key between the sender and receiver. Photons work as a private or secret key.
- Key distribution is the rules and regulations that utilize quantum characteristics to secure communication by identifying eavesdropping and estimating lost or appropriated information in the network system.

With the help of continuous error rectification and post-processing steps, we reduced information leakage and error bits. Traditional fiber-based QKD demonstrated for few 100 km distances, but recent QKD is distributing photons for 1,000 km distances with emerging latest technologies. These technologies employ powerful deterministic efficiencies light sources, high-speed data transmission, low-cost photon detection, more reliable quantum memories, and quantum repeaters.

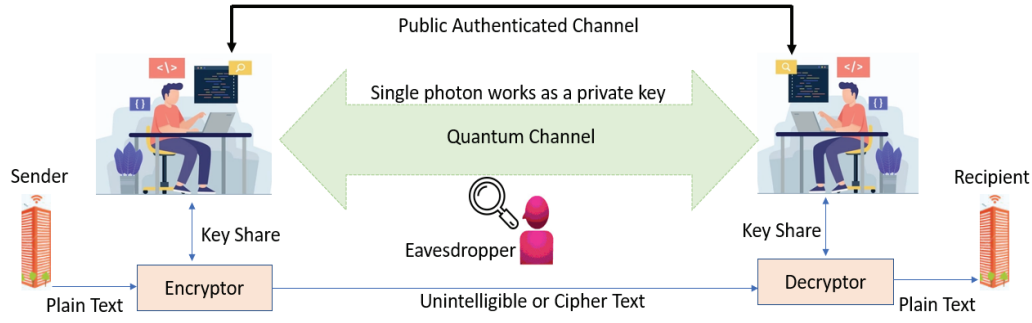

Fig. 3. Illustration of quantum cryptography functionality.

***Quantum random number generator*:** Random number generation is an essential security element for secure private information [18-20]; it has a vital role in various applications such as asymmetric cryptography and secret sharing. Generally, computer systems rely on deterministic methods like PRNG (pseudo random number generators). This process generates randomness, but it is not more secure

because it uses deterministic algorithms. QRNG is utilized for the address above issue and provides more security in advanced applications. QRNG is the quantum physics process that is radically probabilistic to construct true randomness. It is categorized based on the quantum channel's inner working method, modelized, and controlled to perform irregular randomness.

***Quantum digital signature*:** A digital signature is the mathematical techniques for modern sharing communication to validate authenticity and integrity by preventing masquerading. Traditional digital signature schemes (TDSS) need pairs of public and private keys for generating hashing functions in which signatures are based on the message bit and a secret or private key sign it, then verifies by the sender's public key. The hashing function for TDSS is only computational secure; it is easily hacked by the latest technological system, such as a quantum computer. Thus, nowadays, a QDS is deployed for mitigating this issue. It is based on quantum mechanics for providing secure communication. In this signature, the sender's signature is a message with quantum states and follow the properties of quantum function and multiport optical systems. Multiport optical systems are used to overcoming the quantum memory problem and utilized in asymmetric quantum cryptography.

***Quantum computation*:** As know that, numerous essential aspects of communication security rely on encryption and public-key cryptography, which are necessary for electronic business and protecting confidential automated information. Thus, the computation of messages is required for secure communication in advanced applications. QC is the process for calculation of message with a hash function and quantum-based computing devices. These devices follow quantum mechanics' properties and use qubits in which a single qubit can encode more than two states. We are showing the comparison of quantum cryptography and post-quantum cryptography in Table 1.

Table 1. Comparison table of quantum cryptography and post-quantum cryptography

Parameter	Quantum cryptography	Post-quantum cryptography
Channel requirement	Requires special channel such as fiber-based channel, line of the sight-based channel	No need a special channel
Algorithm needs	QKD has used a classical symmetrical algorithm such as AES, RSA, for bulk data sharing or communication.	Use larger keys than RSA and AES algorithm
Computational assumption	Computational assumption relies on the hardness factoring	Computational assumption relies on the test of time
Definition	It follows the properties of quantum mechanics, and optics for security is known as quantum cryptography	A new set of rules and regulations of classical algorithms is known as post-quantum cryptography

2.3 Blockchain-based Quantum Computing

Blockchain networks secure user records and data such as financial records stored in blocks as transactions using immutable ledgers supported by cryptographic methods such as digital signatures. Data stored in blocks require a considerable power to break the computationally complex mathematical problems protecting the network. Quantum computers pose a severe threat to the mining process of blocks, essential to growing the blockchain network. Attackers mine the blocks with a considerably higher computing power resulting in a much higher network hash rate than average users. Attacks such

as 51% attacks are simpler to execute using Quantum computers, allowing malicious attackers to steal and manipulate stored data.

QKD based authentication is essential to secure data in the quantum period. It requires the sender and receiver to share quantum states of light across fiber or free-space quantum channels. Kiktenko et al. [21] proposed a blockchain protocol combining Byzantine Fault Theorem without digital signatures and QKD for secure authentication. The protocol consists of two layers where the first layer is a QKD network permitting transmission of keys securely for each pair of nodes. The second layer transmits messages using a secure Toeplitz hashing using private keys received during the first layer. Blocks are created in a decentralized manner using the broadcast protocol [22], which allows managing paired-based grouped authentication assuming the number of dishonest users is below 3.

The protocol is applied to each unconfirmed transaction at a periodic interval of 10 minutes based on pairs to prevent data manipulation by a corrupted node. Forking in the blockchain network is prevented by approving authorized transactions based on timestamps and forming a common node. QKD is used only for generating the private keys while data is transmitted using the broadcast protocol. Experimental analysis using an urban fiber QKD network between three nodes (A, B, C) shows successful, legitimate transactions. An unauthorized block with illegitimate transactions attempting to perform a double-spending attack is successfully blocked.

Quantum computers have successfully broken the current security protocols of the blockchain network [23,24]. Several recent types of research have proposed modifications of blockchain technology [21,25] to secure against quantum attacks; however, they are not considered reliable due to new quantum algorithms proposed [26-28] that threaten these security measures. An ideal approach to secure blockchain against quantum attacks is to merge quantum entanglement with blockchain architecture. Rajan and Visser [29] proposed a quantum blockchain method where timestamped blocks and hash functions are linked with a temporal Greenberger–Horne–Zeilinger (GHZ) state of photons that do not correspond at the same time. Using superdense coding, quantum blockchain replaces the traditional structure with a spatially entangled Bell states.

$$| \beta_{xy} \rangle = \frac{1}{\sqrt{2}} (| 0 \rangle | y \rangle + (-1)^{x} | 1 \rangle | \bar{y} \rangle)$$

Here, $_{xy}$ represents two standard bits, 00, 01, 10. and 11. Every block in the traditional blockchain is transforming using temporal Bell state into a quantum block. The creation of the first block is represented as $t = 0$ and r represents each record:

$$| \beta_{r1r2} \rangle^{0,\tau} = \frac{1}{\sqrt{2}} (| 0^{0} \rangle | r_2^{\tau} \rangle + (-1)^{r_1} | 1^{0} \rangle | \overline{r_2^{\tau}} \rangle)$$

Entanglement between two quantum bits (qubits) exists initially as $t = \tau$. A new photon that did not exist earlier is created as a corresponding entangled qubit to the first qubit. The conversion of blockchain into temporal Bell state is as follows:

$$| \beta_{00} \rangle^{0,\tau}, | \beta_{10} \rangle^{\tau,2\,\tau}, | \beta_{11} \rangle^{2\tau,3\,\tau}$$

The response of the proposed new quantum blockchain to an attacker's attempt to modify a block's contents or tamper with photons results in the entire malicious block destroyed. In standard blockchain

technology, only the forward blocks are rejected. Since all previous photons are removed, an attacker cannot access the last photon.

Traditional blockchain technology implements the elliptic curve cryptography or the Rivest–Shamir–Adleman (RSA) to create digital signatures and secure blocks from attackers that rely on mathematical complexity [25]. Factoring of large composite numbers into two prime factors increases the complexity in RSA; however, quantum computers possess the computational capacity to solve difficult problems, which take hundreds of years on a standard computer. Quantum powered computers, due to high speedups in computation, can break RSA, DSA, and elliptic curve cryptography. One of the two popular quantum algorithms, Shor's algorithm, breaks the RSA encryption due to its high efficiency in factoring large numbers. The Shor's algorithm's high execution speed compared to other existing algorithms is due to its input length being polynomial. To determine an odd integer *N*'s prime factors, we choose a co-prime of *N*, x. The order r relates x to N according to:

$$x^r mod\ N = 1$$

r determines the factors provided by the greatest common divisor [30] and this is made possible only by using quantum computers resulting in a 4096-bit RSA key, breakable.

$$gcd\left(x^{\frac{r}{2}} \pm 1, N\right)$$

The Grover's algorithm attacks the Blockchain security using two methods, locate hash collisions and replace blocks without affecting the integrity of the blockchain network. The second method is to influence the chain's integrity by increasing the creation of nonces to the level where chains of records are recreated using modified hashes. The speed of Grover's algorithm is given by $O\sqrt{N}$ compared to $O(n)$ used by classical algorithms. The increase in speed allows the algorithm to break a hashing function and insert a modified block in the blockchain network. An attacker can potentially create multiple blocks in negligible times allowing them to take control of the entire network. The faster-growing chain in the network is decided to be the main chain, effectively allowing the attacker to rewrite transactions and initiate double-spending in cryptocurrency-based blockchain networks.

Quantum computing has grown in strides in recent years with organizations such as Google and IBM developing their quantum systems. Google's Sycamore system computes complex mathematical problems in 200 seconds using 53 qbits, whereas today's supercomputer requires a minimum of 10,000 years. IBM's Q Network allows various companies and academic institutions to improve and advance the quantum algorithms using an open-source Qiskit programming framework. Recent advances in quantum technology have prompted researchers to develop new algorithms to secure blockchain networks and counter any future quantum based attacks. Some of the proven algorithms that secure Blockchain networks against quantum based attacks include quantum entanglement, lattice-based cryptography, and QKD. We discussed earlier quantum entanglement in blockchain networks to secure stored data in blocks by Rajan and Visser [29] and now present lattice-based cryptography and QDK to secure blockchain networks.

The general lattice definition is described as a collection of points in n-dimensional space with a cyclic composition. The foundation of the lattice L is $B = (b_1, b_2, \dots, b_n)$ and different lattices could represent the same lattice. For a group of independent vectors b, the lattice formed by them is as follows:

$$\mathcal{L}(b_1, \quad b_2, \ldots, b_n) = \sum_{i=1}^{n} [\mathrm{x}_i b_i : x_i \epsilon\, \mathbb{Z}, b_n \epsilon\, \mathbb{R}^m]$$

Lattice-based algorithms are cited and suggested by several recent kinds of research due to their resistance to attacks against elliptic curve cryptography in blockchain networks. Torres et al. [31] proposed a one-time linkable ring signature (L2RS) relying on lattice-based cryptography, enabling verification of multiple signatures created by an identical signatory. The L2RS assures a privacy-preserving protocol for cryptocurrencies and presents a foundation for block building and homomorphic assurance fundamental to secure the post-quantum confidential transactions. Gao et al. [32] proposed a signature scheme relying on the lattice algorithm to produce secret keys using stochastic values. A post-quantum blockchain is designed by first signing the message using a preimage sampling algorithm, and secondly, a double signature reduces the relationship between the message and the signature. The analysis of the signature scheme showed resistance to quantum computing attacks.

To secure keys, QDK relies on exchanging cryptographic keys using individual photons where each photon contains a single bit of data as either 0 or 1. The theory of quantum physics states that each photon's value is based on the spin and the polarization, i.e., the photon's state. QKD destroys the block in the blockchain network if an attacker attempts to modify or read block contents. A laser at the sender's end produces a range of single photons where each photon is in a defined state of polarization, i.e., vertical, or horizontal. Additionally, the sender cannot create the same photon using the same state of polarization. The photon receiver measures the state of photons to assure the sender is a secure and authorized user. Using the Heisenberg uncertainty principle, QDK prevents an attacker from determining quantum particles' position and velocity.

3. Global Research Trends for QCT

This section discusses the recent global research trends with QCT for various advanced fields, including electronic market, semiconductor testing, energy storage, internet, and others for multiple countries such as the United States, the United Kingdom, Korea, Canada, and China. These countries are using various projects based on quantum cryptography and providing secure communication in the advanced industries.

In North America, the United States has allocated US$1.2 billion for quantum research as part of the National Quantum Initiative Act. The focus of the Act is to build development research centers to be developed. The research centers aim to collaborate with academia, industry, and the government to accelerate the quantum research progress. The focus of research is on developing quantum processors that enable further computing applications, quantum clocks for precise timekeeping and maintaining communications during warfare incidents in GPS denied conditions, and research on gravity using the quantum information theory. Research on quantum-resistant cryptography for the post-quantum era, such as new optimizations using novel algorithms and cybersecurity systems [33].

Canada has invested more than US$1 billion in the past decade for research and development in quantum computing technology. It ranks 5th in the world for patents filed in the field of quantum computing. The focus of research is on quantum information processing, metrology, communications, cryptography, and networks. In collaboration with the Canadian Space Agency, Canada's government,

with a funding of US$80.9 million, is actively researching quantum key distribution to enhance secure and encrypted communication in space and protect digital communication. Quantum sensors are recognized as an important research area to help the country extract oil in an environmentally friendly manner [34].

Germany has pledged €2 billion, the highest in Europe, to promote quantum computing research from its COVID recovery fund to catch up with other countries such as the United States and China, which have filed 500 and 200 patents, respectively [35]. The increase in quantum technology investment comes after a government decision in 2018 to invest €650 million. The German research minister, Anja Karliczek, announced the building of an experimental Q System One quantum computer in collaboration with IBM near Stuttgart by 2021. The Fraunhofer Gesellschaft, Europe's leading applied research institute, works with IBM to develop new quantum technology, application scenarios, and new algorithms [36]. As part of its National Quantum Technologies Programme in the United Kingdom, the UK Research and Innovation (UKRI) aims to establish the National Quantum Computing Centre (NQCC) at the Harwell Campus in Oxfordshire by 2025. The NQCC will invest £95 million in working on multiple workstreams. The research projects include 100+ qubit Noisy Intermediate-Scale Quantum hardware platform, Quantum software, algorithm, applications development, and high performing and scalable qubit technology. Participants include multiple stakeholders from the government, business organizations, and academic researchers [37]. On March 24, 2020, the National Cyber Security Center released a whitepaper on quantum-safe cryptography, highlighting the best mitigation methods against quantum computers and suggests reducing reliance on asymmetric cryptography due to their vulnerability against quantum computers [38].

In Asia, China is leading the research in quantum technology to build computers outperforming the computational power of existing systems, and sensors that can view through smog and corners [39]. The research area of focus in developing QKD's industrial applications was initiated by the National Development and Reform Commission and the China Academy of Science between 2011–2015, with an investment of US$490 million. The focus of research pushed by both the central and local governments since 2016 has centered on quantum communication, computation, and metrology. In 2017, the study's direction was on building a national standard of quantum cryptography [40]. The research for satellite-based quantum communication proved to be a success with the launch of satellite Micius. Quantum cryptographic keys were distributed between Vienna and Beijing's ground stations, facilitating a secure virtual meeting between academics from Austria and China [41].

Quantum research in Japan in quantum information processing, metrology, and sensing is funded by the Japan Science and Technology (JST) and the Japan Society for the Promotion of Science (JSPS). Quantum communication and cryptography are funded by the National Institute of Information and Communications Technology (NICT). Between the years 2001–2015, the research focus in QKD in collaboration between industries and universities resulted in designing high-speed QKD systems performing at a 1-GHz repetition rate known as the Tokyo QKD network. The research focus has expanded to secure cryptographic applications such as TV conferencing, IP routers, and smartphone systems. The JST has funded numerous projects between 2003–2010 in quantum information processing with photonic qubits, superconducting qubits, quantum information processing by entangled photons, optical lattice clock, and quantum simulation tools [42].

Several mobile companies, including SKT, KT, Samsung, and LG, provide telecommunication services and electronic business for industries and humans in Korea. KT and Samsung electronics companies,

however, already started developing technologies for quantum-based communication with quantum computers [43]. So, Korea's e-market is jumping into the quantum industries, followed by SKT. KT telecommunication company is going to discover a quantum information research center, known as Korea Advanced Nano Fab Center, with the Korea Institute of Science and Technology (KIST). KIST, KT operate this research center, and it has planning to concentrate their capabilities in secure communication with quantum computers. Already, SAIT (Samsung Advanced Institute Of Technology) completed one project, Global Research Outreach (GRO), which is dependent on quantum computers. In Korea, now Samsung aims to develop quantum error-free, highly effective, more secure, recent qubit equipment, and algorithms. In 2014, quantum information communication medium and long-term promotion strategies were established by the South Korean Government.

The government joined the race of the next generation of ICT developments field, including quantum computing. It is investing 44.5 billion Korean won over the next 5 years, which will enhance computational performance with secure sharing information worldwide with quantum computers and quantum mechanics [44]. By developing key technologies for quantum computing, the government plans to complete a presentation of the effective five-qubit quantum computer system with more than 90% security by 2023. Market Research Media in Korea estimates that global markets for quantum cryptography communication and quantum computers will be worth more than US$23.2 billion (26 trillion Korean won) in 2025 [44]. The Korean government will provide an investment of 13.4 billion Korean won for next-generation ICT technology, including ultra-high-computing data, computer software, intelligence systems, and human-computer interaction, and quantum computing.

4. A Quantum Communication Model

Based on the current research trends, researchers are focusing on QKD as it is one of the most applicable techniques nowadays. The leading application for quantum Internet [45] enables secure remote communication between two or more parties based on quantum mechanic's laws. This section will propose QMC; a model that uses small, relatively restricted devices compared to the normal quantum repeater to send a message through the quantum Internet, between two quantum computers separated by at least 300 km.

4.1 Proposed Quantum Communication Model System

Quantum Internet, unlike classical internet, will theatrically support and develop several applications, including secure access to quantum computers from relatively restricted devices, clock synchronization, and other scientific applications in physics, medicine, and astronomy. Transferring qubit between quantum computers in the quantum Internet layer, however, is not a straightforward nor simple task to do. Due to photons and particles' physical nature, they cannot be entangled perfectly in a distance over 300 km. The progress has been significant in recent years. Researchers in China have successfully managed to measure for 900 times two entangled particles destined over 1,400 km from each other using a satellite as a Quantum Repeater. This is a huge step toward quantum Internet in future ICT. Nonetheless, the quintessential architecture and design for quantum computers are quite complex. Relying on quantum entanglement distribution, quantum repeaters

require two-way communication between the sender and receiver. To apply the BSM, and a large quantum memory to save the particles' state [46], not to mention that the quantum information needs to be sent all through the same repeater that must be a trusted node; otherwise, security and privacy concerns arise.

To this end, we propose in this paper a one-way single qubit transmission to send quantum information from a quantum computer to another, as discussed in Fig. 4. To understand the proposal, we take the case-example where a quantum computer wants to send a message to another quantum computer located at a distance of over 300 km. The first quantum computer named QC1 will generate the message and encode it into qubits; every single qubit should be sent through the QMC. QMC is a group of quantum machines will only at least 1 qubit. Unlike Quantum Repeaters, those machine does not require large quantum memory and computational power. QMCs are distributed around the future smart city; it could be phones, base stations, and personal computers connected to quantum computers in the cloud. The QC1 encode each qubit of the message into a Bell measurement and send it through signals to the first quantum machine in the QMC based on the proximity with a time-stamp to memorize the time slot of each message.

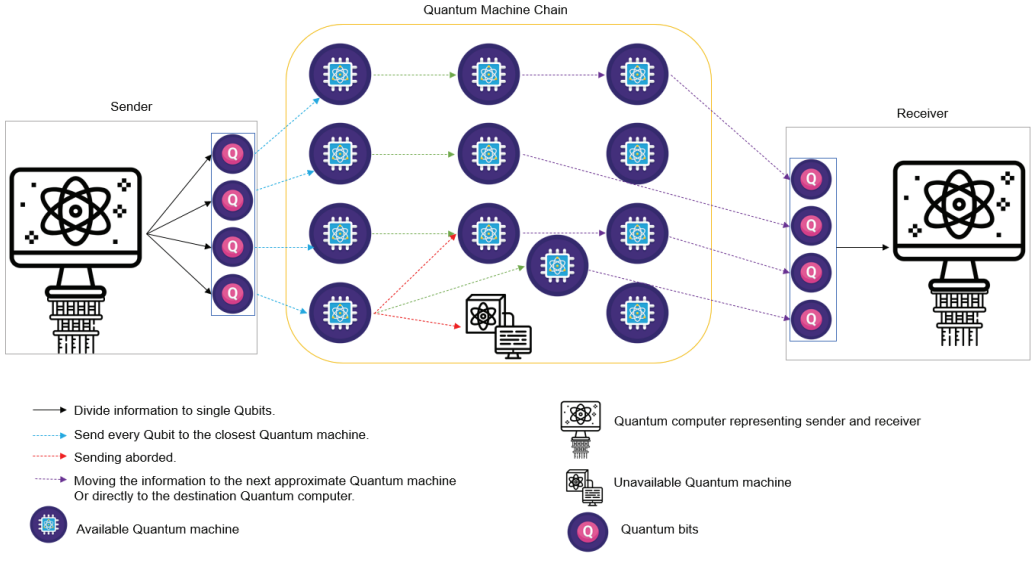

Fig. 4. Model overview of quantum machine chain.

The quantum machine that received the signals will re-encode it and check if the destinated QC2 (receiver) is close by (less than 50 km). If yes, the signals, along with the time stamp, will be sent directly to the receiver. If not, they will be sent to the next quantum machine, and it keeps going until it reaches the receiver. Another case is if the quantum machine is busy and cannot receive the signals, in this condition, the next approximate available quantum machine will be a solicitation. Moreover, if the quantum machine has already carried a bit in the previous time slot for the same quantum computer, it cannot be solicited again, and we will move directly to the next quantum machine. After receiving all the signals, the receiver end (QC2) will start to decode them based on their timestamp and starting with the oldest signals to retrieve the original message.

4.2 Methodological Flow of Proposed Model System

To understand the flow of the proposed model, we refer to the Fig. 5. Here we use the notion of photonic tree clusters presented by Borregaard et al. [47]. The QC1 encodes his message into multiple qubits. Each qubit is encoded using BSM with the root spin qubit of the photonic tree cluster. The encoded qubit is sent to the next quantum machine, where it will be re-encoded using BSM. The re-encoding is done between the first-level photonic qubit and the next new photonic tree. Again, the photons will be sent either to the next quantum machine, and the same phases will be repeated, or directly to the QC2 (receiver). The receiver decodes the qubit by measuring the photon tree received. the tree-cluster scheme's overview is shown in Fig. 5.

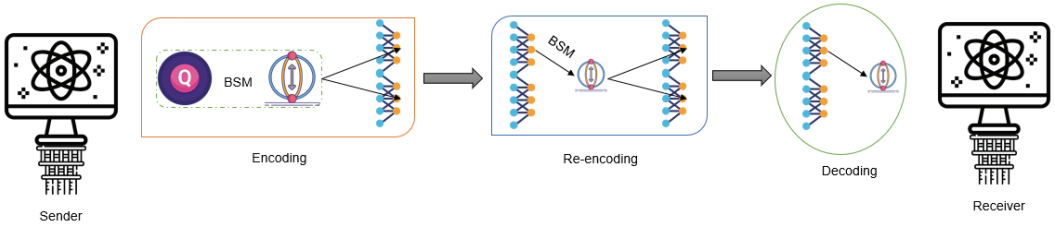

Fig. 5. Tree-cluster scheme's overview.

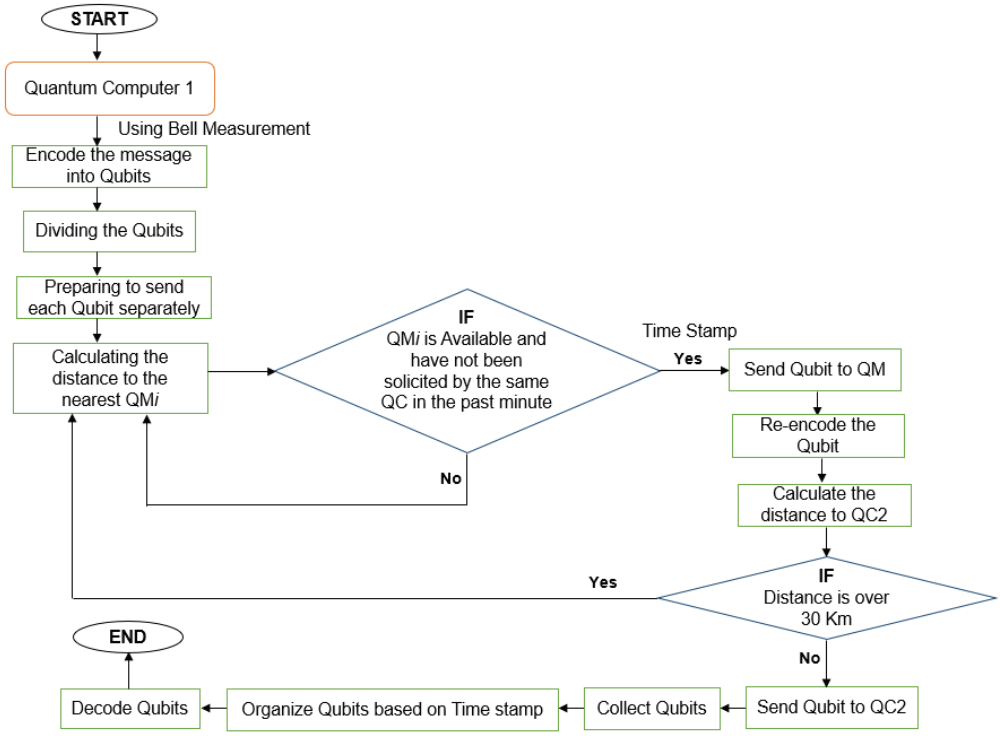

Fig. 6. Methodological flow of the proposed model system.

The timestamp is used every time the qubit is sent from a quantum machine to another to keep track of qubits order. The encoding, re-encoding, and decoding phases fell out of the scope of this study; however,

it will be covered in detail in our future work. After receiving the qubits, the quantum machine starts organizing them based on their history and time stamp from the oldest Qubit to the newly received ones and decoding them to retrieve the message. Fig. 6 depicts in detail the proposed model's phases as methodological flow.

4.3 Discussion and Open Research Challenges

Quantum computers and processors are very soon to become our daily reality and replace classical computers. This industry's advancement is speedy, especially with tech-giant companies such as Google and IBM's efforts to develop quantum computers. Moreover, hosting a quantum computer in the cloud can facilitate the task. In the future smart cities, quasi all IoT devices, and machines with only 1 qubit processor, will be able to use the full power and benefit from a highly developed quantum computer hosted in the cloud layer. To realize this, however, we will need a quantum network known as quantum Internet. Nowadays, countries worldwide are engaging in quantum communication research such as the United States, European countries, and China. Quantum Internet will enable high-private networks where devices and machines built upon quantum mechanics rules will be able to communicate and share information securely using QKD law. Moreover, based on quantum Internet, a quantum computer can be hosted on the cloud and used by several machines with a lower quantum processor's capability (at least 1 qubit).

Due to quantum state fragility, however, two qubits cannot be entangled throughout long distances. That was the reason behind the use of quantum repeaters. As explained previously, a quantum repeater can entangle the sender's state with the receiver's state; it acts as a middle-point to transfer the information. Nonetheless, quantum repeaters require large quantum memory and a powerful quantum processor to save the quantum state and re-encode it, which creates a serious dilemma. With this method, creating a scalable quantum network will upscale the cost and demand high requirements. To this end, we propose in this paper a QMC model that can replace the Quantum Repeaters. The main purpose is to lower the cost of creating quantum Internet and scalable communication for future ICT.

QMC relies on dividing the encoded message into several qubit, sent to multiple quantum machines with relatively smaller quantum processors compared with Quantum Repeaters. It does not require large quantum memory as it deals with only one qubit of information. The model uses time stamper to record the history of each qubit and organize the message later at the receiver side. Our future work will be focusing on the encoding, re-encoding, and decoding phases as we intend to explain them in detail and prove our proposal's performance compared to other related works.

The science and technology have achieved so much in the field of quantum computers and quantum Internet. In the future ICT and due to the heterogeneous nature of future smart cities [48-50]. Quantum computers will be stored in the cloud rather than local machines. They give access to relatively smaller and restricted devices into the quantum cloud, where they can benefit from the computational power to execute complex tasks. Quantum Internet and computers will improve and empower smart cities and be the main pillars for future ICT. It is still, however, not an easy task yet. Quantum computers and Quantum Internet still face multiple challenges, which is shown in Fig. 7.

***Limited Resource*:** Quantum repeaters require multiple systems available for widespread public usage with sufficient processing power to forward a single qubit to other devices. The most powerful Quantum computer built by IBM processes 65 qubits, but by 2023, IBM expects to make a quantum computer

capable of processing 1,000 qubits. Current classical systems operate well in room temperatures, whereas current quantum computers require near-zero temperatures using cooling systems, making them confined to laboratories.

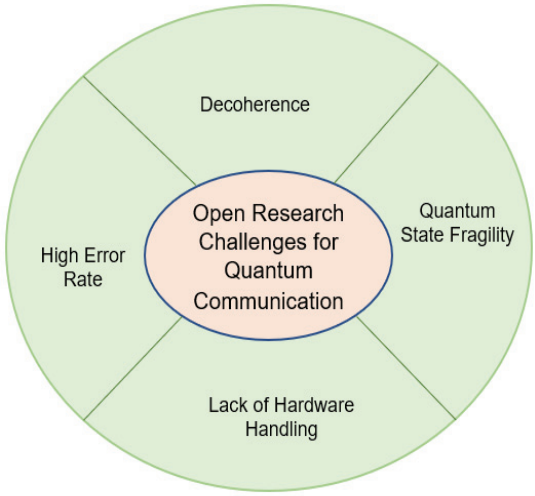

Fig. 7. Open research challenges for quantum communication.

***High Error Rate*:** Performance enhancement of ion trap computers requires improving the gates' laser intensity exposing qubits to environmental factors such as electromagnetic waves and temperature variations, result in decoherence, i.e., loss of data from the qubit to the environment. An error rate of 10^{-6} per gate can be avoided by placing ions in small holes or pits preventing unwanted transformations. Furthermore, fault tolerance schemes using error-correcting algorithms can tolerate error probability rates of 10^{-6}, which is adequately below the accuracy threshold.

***Decoherence*:** Quantum computers follow superposition, entanglement problems resolving by quantum principles, and these principles properties. These computers utilize quantum states. Decoherence is the next open research challenge for quantum communication technology for future ICT because quantum states are more vulnerable to error than the classical computer in communication. Decoherence is when the environment interacts with the qubits and changes their quantum states and loses or changes the information in the quantum computers. Various aspects generate decoherence, including radiation from warm objects, a collision between qubits, changing electric and magnetic fields, the collapse of wave functions in quantum mechanics. Thus, it represents an open issue for the practical implementation of quantum computers.

***Quantum State Fragility*:** It is another open challenge for quantum communication for future ICT. As already knows that, quantum computers use quantum states value (0 and 1 bunch) as qubits. Qubits states may be incredibly fragile, compared to bits because they use the outside environment, electric and magnetic fields, wave functions, and object radiations. Using these environments, quantum states may be changed, which means original pieces of information also change or lost in the quantum computers with quantum communications in future ICT. Thus, quantum state fragility is a very crucial open research issue for secure transmission in advanced applications.

5. Conclusion

This paper reviewed quantum communication technologies for future ICT and proposed a quantum communication model system based on quantum machines to create a scalable quantum Internet network. We discussed all phases of the quantum machine chain in futuristic communications. We showed how to use blockchain in quantum computing for providing the secret-sharing the data to each other with the help of the quantum computers. We also discuss the latest global research trends for quantum communication technology as several countries, including the United States, Canada, United Kingdom, Korea, and others. Finally, we discussed some open research challenges for quantum communication technology. We also provided a comparison table of quantum communication cryptography and post-quantum cryptography.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (No. NRF-2019R1A2B5B01070416).

References

[1] N. Datta, "Course 9 - Quantum entropy and quantum information," *Les Houches*, vol. 83, pp. 395-466, 2006.
[2] E. G. Rieffel and W. H. Polak, *Quantum Computing: A Gentle Introduction*. Cambridge, MA: MIT Press, 2011.
[3] Y. Manin, *Computable and Uncomputable*. Moscow, Russia: Sovetskoye Radio, 1980.
[4] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467-488, 1982.
[5] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, no. 4, pp. 2738-2747, 1995.
[6] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, no. 10, pp. 777-780, 1935.
[7] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Routing entanglement in the quantum internet," *npj Quantum Information*, vol. 5, article no. 25, 2019.
[8] Quantum Flagship, "Quantum Repeater," 2020 [Online]. Available: https://qt.eu/discover-quantum/underlying-principles/quantum-repeaters/.
[9] B. Zhao, M. Muller, K. Hammerer, and P. Zoller, "Efficient quantum repeater based on deterministic Rydberg gates," *Physical Review A*, vol. 81, no. 5, article no. 052329, 2010.
[10] Z. Dou, G. Xu, X. B. Chen, J. Li, and M. Naseri, "Rational non-hierarchical quantum state sharing protocol," *Computers, Materials & Continua*, vol. 58, no. 2, pp. 335-347, 2019.
[11] Y. Sun, Y. Chen, H. Ahmad, and Z. Wei, "An asymmetric controlled bidirectional quantum state transmission protocol," *Computers Materials & Continua*, vol. 59, no. 1, pp. 215-227, 2019.
[12] Y. Chang, S. Zhang, L. Yani, G. Han, H. Song, Y. Zhang, X. Li, and Q. Wang, "A quantum authorization management protocol based on EPR-pairs," *Computers Materials & Continua*, vol. 59, no. 3, pp. 1005-1014, 2019.
[13] W. Liu, Y. Xu, J. C. Yang, W. Yu, and L. Chi, "Privacy-preserving quantum two-party geometric intersection," *Computers Materials & Continua*, vol. 60, no. 3, pp. 1237-1250, 2019.

[14] C. Li, G. Xu, Y. Chen, H. Ahmad, and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things," *Computers Materials & Continua*, vol. 61, no. 2, pp. 711-726, 2019.

[15] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975-990, 2020.

[16] A. El Azzaoui, S. K. Singh, Y. Pan, and J. H. Park, "Block5gintell: blockchain for AI-enabled 5G networks," *IEEE Access*, vol. 8, pp. 145918-145935, 2020.

[17] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, J"A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, article no. 9, 2020.

[18] K. Gafurov and T. M. Chung, "Comprehensive survey on Internet of Things, architecture, security aspects, applications, related technologies, economic perspective, and future directions," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 797-819, 2019.

[19] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: a systematic literature review," *Human-centric Computing and Information Sciences*, vol. 9, article no. 21, 2019.

[20] Y. Kim, "Samsung Electronics and KT jump into Quantum Industries followed by SK Telecom," 2017 [Online]. Available: https://english.etnews.com/20170615200001.

[21] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, "Quantum-secured blockchain," *Quantum Science and Technology*, vol. 3, no. 3, article no. 035004, 2018.

[22] D. Malkhi, *Concurrency: The Works of Leslie Lamport*. San Rafael, CA: ACM, 2019.

[23] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on Bitcoin, and how to protect against them," 2017 [Online]. https://arxiv.org/abs/1710.10377.

[24] S. King and S. Nadal, "PPCoin: peer-to-peer crypto-currency with proof-of-stake," 2012 [Online]. Available: https://decred.org/research/king2012.pdf

[25] J. H. Witte, "The Blockchain: a gentle four page introduction," 2016 [Online]. Available: https://arxiv.org/abs/1612.06244.

[26] D. McMahon, *Quantum Computing Explained*. Hoboken, NJ: John Wiley & Sons, 2007.

[27] A. Montanaro, "Quantum algorithms: an overview," *npj Quantum Information*, vo. 2, no. 1, pp. 1-8, 2016.

[28] W. Zeng, B. Johnson, R. Smith, N. Rubin, M. Reagor, C. Ryan, and C. Rigetti, "First quantum computers need smart software," *Nature News*, vol. 549, no. 7671, pp. 149-151, 2017.

[29] D. Rajan and M. Visser, "Quantum Blockchain using entanglement in time," *Quantum Reports*, vol. 1, no. 1, pp. 3-11, 2019.

[30] A. E. Azzaoui and J. H. Park, "Post-quantum blockchain for a scalable smart city," *Journal of Internet Technology*, vol. 21, no. 4, pp. 1171-1178, 2020.

[31] W. A. A. Torres, R. Steinfeld, A. Sakzad, J. K. Liu, V. Kuchta, N. Bhattacharjee, M. H. Au, and J. Cheng, "Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (Lattice RingCT v1.0)," in *Information Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 558-576.

[32] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205-27213, 2018.

[33] National Science and Technology Council, "National strategic overview for quantum information science," 2018 [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf.

[34] B. Sussman, P. Corkum, A. Blais, D. Cory, and A. Damascelli, "Quantum Canada," *Quantum Science and Technology*, vol. 4, no. 2, article no. 020503, 2019.

[35] Inside Quantum Technology, "Germany's billions in funding for quantum computing reflects its push for technological sovereignty & European self-reliance," 2020 [Online]. Available: https://www.insidequantumtechnology.com/news/germanys-billions-in-funding-for-quantum-computing-reflects-its-push-for-technological-sovereignty-european-self-reliance/.

[36] J. Eitner, "IBM and Fraunhofer bring quantum computing to Germany," 2020 [Online]. Available: https://www.fraunhofer.de/en/press/research-news/2020/march/ibm-and-fraunhofer-bring-quantum-computin-to-germany.html.
[37] National Quantum Computing Centre [Online]. Available: https://www.ukri.org/about-us/nqcc/.
[38] National Cyber Security Center, "Quantum-safe cryptography," 2016 [Online]. Available: https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography.
[39] J. Whalen, "The quantum revolution is coming, and Chinese scientists are at the forefront," 2019 [Online]. Available: https://www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront/.
[40] Q. Zhang, F. Xu, L. Li, N. L. Liu, and J. W. Pan, "Quantum information research in China," *Quantum Science and Technology*, vol. 4, no. 4, article no. 040503, 2019.
[41] H. Siljak, "China's quantum satellite enables first totally secure long-range messages," 2020 [Online]. Available: https://theconversation.com/chinas-quantum-satellite-enables-first-totally-secure-long-range-messages-140803.
[42] Y. Yamamoto, M. Sasaki, and H. Takesue, "Quantum information science and technology in Japan," *Quantum Science and Technology*, vol. 4, no. 2, article no. 020502, 2019.
[43] Korea-EU Research Centre, "Korea starts five-year development program for quantum computing technology," 2019 [Online]. Available: https://k-erc.eu/korea-rd-research-trends-and-results/korea-starts-five-year-development-program-for-quantum-computing-technology/.
[44] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: networking challenges in distributed quantum computing," *IEEE Network*, vol. 34, no. 1, pp. 137-143, 2019.
[45] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: a vision for the road ahead," *Science*, vol. 362, no. 6412, 2018. http://doi.org/10.1126/science.aam9288
[46] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78-90, 2015.
[47] J. Borregaard, H. Pichler, T. Schroder, M. D. Lukin, P. Lodahl, and A. S. Sorensen, "One-way quantum repeater based on near-deterministic photon-emitter interfaces," *Physical Review X*, vol. 10, no. 2, article no. 021071, 2020.
[48] S. K. Singh and N. Rastogi, "Role of cyber cell to handle cyber crime within the public and private sector: an Indian case study," in *Proceedings of 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Bhimtal, India, 2018, pp. 1-6.
[49] S. K. Singh, Y. S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustainable Cities and Society*, vol. 60, article no. 102252, 2020.
[50] S. K. Singh, S. Rathore, and J. H. Park, "Blockiotintelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721-743, 2020.

Sushil Kumar Singh **https://orcid.org/0000-0003-2926-3931**

He received his M.Tech. degree in Computer Science and Engineering from Uttarakhand Technical University, Dehradun, India, in 2018. He also received an M.E. degree in Information Technology from Karnataka State University, Mysore, India, in 2011. Currently, he is pursuing his Ph.D. degree under the supervision of Prof. Jong Hyuk Park at the Ubiquitous Computing Security (UCS) Lab, Seoul National University of Science and Technology, Seoul, South Korea. He has more than 9-year experience of teaching in the field of computer science. His current research interests include blockchain, artificial intelligence, big data, and the Internet of Things. He is a reviewer of the *IEEE Systems Journal*, *FGCS*, *Computer Network*, *HCIS*, *JIPS*, and Others.

Abir El Azzaoui **https://orcid.org/0000-0002-9406-8932**

She received the B.S. degree in computer science from the University of Picardie Jules-Verne, Amiens, France. She graduated from the National School of Higher Education Hassan II in the Development of Information Systems, Marrakech, Morocco. She is currently pursuing a master's degree in computer science and engineering with the Ubiquitous Computing Security (UCS) Laboratory, Seoul National University of Science and Technology, Seoul, South Korea, under the supervision of Prof. Jong Hyuk Park. Her current research interests include blockchain, the Internet-of-Things (IoT) security, and post-quantum cryptography. She is also a reviewer of the *IEEE Access*. She has received the Quarterly Franklin Membership from the London Journal of Engineering Research (LJER), London, UK.

Mikail Mohammed Salim **https://orcid.org/0000-0001-7870-9368**

He received his bachelor's degree in Computer Applications from Bangalore University, Bangalore, India in May 2011. He also received his Post Graduate Diploma in Management from Integrated Learning in Management, Greater Noida, India in 2014. Currently he is pursuing his Master's combined Ph.D. degree under the supervision of Prof. Jong Hyuk Park at the UCS Lab, Seoul National University of Science and Technology, Seoul, South Korea. He has 5 years of experience working as a Marketing and Project Manager designing web services for clients. His research interests include IoT and 5G network security. He is the reviewer of the *Journal of Supercomputing*, and *Human-centric Computing and Information Science*.

James J. (Jong Hyuk) Park **https://orcid.org/0000-0003-1831-0309**

He received Ph.D. degrees from the Graduate School of Information Security, Korea University, Korea and the Graduate School of Human Sciences of Waseda University, Japan. Dr. Park served as a research scientist at the R&D Institute, Hanwha S&C Co. Ltd., Korea from December 2002 to July 2007, and as a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea from September 2007 to August 2009. He is currently employed as a professor at the Department of Computer Science and Engineering and the Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has also served as the chair, program committee chair or organizing committee chair at many international conferences and workshops. He is a founding steering chair of various international conferences including MUE, FutureTech, CSA, UCAWSN, etc. He is employed as editor-in-chief of *Human-centric Computing and Information Sciences* (HCIS) by Springer, *The Journal of Information Processing Systems* (JIPS) by KIPS, and the *Journal of Convergence* (JoC) by KIPS CSWRG. He is also the associate editor or editor of fourteen international journals, including eight journals indexed by SCI(E). In addition, he has been employed as a guest editor for various international journals by such publishers as Springer, Elsevier, Wiley, Oxford University Press, Hindawi, Emerald, and Inderscience. Dr. Park's research interests include security and digital forensics, human-centric ubiquitous computing, context awareness, and multimedia services. He has received "best paper" awards from the ISA-08 and ITCS-11 conferences and "outstanding leadership" awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, and PDCAT-11. Furthermore, he received an "outstanding research" award from SeoulTech in 2014. Also, Dr. Park's research interests include human-centric ubiquitous computing, vehicular cloud computing, information security, digital forensics, secure communications, multimedia computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.