11

Post-Quantum Blockchain–Enabled Services in Scalable Smart Cities

Kumar Prateek* **and Soumyadev Maity**

Department of Information Technology, Indian Institute of Information Technology Allahabad, Prayagraj, India

Abstract

The mass migration of rural citizens toward urban areas in search of better employment opportunities, better education erupts a new threat for urban citizens. The increased population due to migration contributes in increasing traffic jams, green house gas emissions, waste disposal. To provide better day-to-day services to citizens, common issues such as fair broadband distribution and connectivity, digital and knowledge inclusion needs to be respected with possible integration and smooth management of various social, physical, and business infrastructure. Furthermore, the rapid development of digital society opens up vast of opportunities in smart cities thus implementing goals of education and healthcare for all, green society, green city. However, the continued adoption of new technologies such as internet of things (IoT) and cloud technologies for various applications in smart cities suffers from issues such as high latency, bandwidth bottlenecks, scalability, security, and privacy. The smart cities are usually autonomous in nature, which relies on distributed infrastructure and features applications such as intelligent information processing, heterogeneous network infrastructure, ubiquitous sensing, and intelligent control systems implemented in areas such as public safety, healthcare, and diagnosis. Besides, the blockchain-enabled applications such as data platform for sharing valuable data between non-trusted organizations, blockchain-based financial systems, online games, online education system, and identity management system improve reliability and democratization of cities by eliminating centralization. However, majority of applications depends on either digital signature or public key cryptography-based schemes which, in turn, depend on the premise that

**Corresponding author*: pcl2017003@iiita.ac.in

Rajesh Kumar Dhanaraj, Vani Rajasekar, SK Hafizul Islam, Balamurugan Balusamy and
Ching-Hsien Hsu (eds.) Quantum Blockchain: An Emerging Cryptographic Paradigm, (263–292)

computation of private key from public key is computationally hard. But with advent of quantum computer, the time complexity of all hard problems such as discrete log problem and integer factorization has reduced from millions of years to few seconds, thus endangering traditional cryptographic mechanism, which includes public key, secret key, and digital signature–based protocols used in blockchain technology–based services in smart cities. The quantum computing which uses law of physics for communication does not depend on mathematically hard problems. In addition, convergence of quantum computing with blockchain technology provides us with amicable solutions for smart cities. This chapter discusses overview of quantum computing, key characteristics, and quantum key distribution and presents an architecture enabling post-quantum blockchain–based applications within smart cities. In addition, the need of various services relying on quantum blockchain in smart cities is presented. Moreover, to enable conceptual architecture for post-quantum blockchain–enabled services in smart cities, smart contracts are designed for implementing transportation application.

Keywords**:** Blockchain, quantum blind signature, quantum computing, quantum key distribution, security, smart cities

11.1 Introduction

Distributed ledger has become an alternative to cloud computing. The flexibility provided by distributed ledger to store database in local proximity and allowing modification of records only after achieving mutual consensus among peers makes this technology extremely popular in market. In addition, each peer within network possesses synchronized copy of records. Although various work related to smart city application utilizing blockchain is present [1–4], huge scope of improvement in different verticals of society within any smart city still exists. Initially, with aim to store financial transaction history, distributed ledger is proposed in cryptocurrency, namely, Bitcoin. However, the secure implementation of blockchain-based application within any smart city demands combination of consensus and cryptographic techniques. Few popular consensus mechanisms which are widely used in blockchain-based applications are practical Byzantine fault tolerance [5], delegated proof of stake [6], proof of work [7], and proof of stake (PoS) [8], while hash-based and public key cryptography-based techniques are used to achieve security. However, with availability of quantum computer, all cryptographic mechanism using public key techniques becomes vulnerable. In addition, quantum computer capabilities to break mathematically hard problems such as integer factorization have only threatened the existing infrastructure. Quantum computer can easily attack on consensus and cryptographic mechanism in blockchain-based applications. Also, quantum computer has ability to phenomenally reduce complexity of SHA256 hash function used in Bitcoin for mutual consensus [9]. In addition, ECDSA scheme used in Bitcoin has become vulnerable due to advent of quantum computer. The centralized structure of smart city has only fabricated unauthorized data manipulation by powerful groups. Sometimes, with focus to fulfill their malicious agendas, huge accumulation of private data of individuals, transfer of illegitimate message in form of fake news, etc., are performed, thus endangering basic rights of privacy of individuals. Besides, illegitimate sell of retrieve data from centralized application has only boosting dark markets, thereby generating chances of increased crime. Although, decentralized mechanism can alone solve the mentioned issue but coordinated targeting by few industries can be performed with the private information achieved through quantum attacks. A classic example could be need of transportation pattern, vehicle-related information of individuals by few manufacturing companies to sell their specific products.

11.1.1 Motivation and Contribution

Because of the ever increasing population within smart cities, tremendous challenges have been emerged, thus requires quick redressal. One such problem is validation of driver records while driving vehicles to accomplish any journey within smart cities. In addition, government used to charge toll fees, etc., from drivers through toll collection point installed around particular road. Besides, penalties are also charged to vehicle's driver for reckless driving, wrong lane driving, breaking traffic rules, and safety measures. The non-possession of valid driving license, pollution certificate, etc., can lead to generation of penalty for individual vehicle. Also, because of multiple toll points, many junction and crossroads within smart cities, handling of vehicle records and managing penalty related records are tiresome. In addition, transfer of records through different organization is complex. Besides, there does not exist any standard benchmark approach which provides solution to such issue. However, a decentralized network, namely, blockchain network could become fruitful in envisioning solution. In literature, the smart road pricing (SRP) system using blockchain is subsequently introduced guaranteeing enhanced security as data stored in blockchain network is protected from tampering but arrival of quantum computer will also make standard encryption technique vulnerable. Therefore, we proposed a quantum blockchain–enabled SRP system to be used within smart cities. The specific contribution of this chapter is as follows:

- In addition to discussion on the need of post-quantum blockchain–enabled services within any smart city, we have proposed an architecture for post-quantum blockchain–enabled application for transportation application within any smart city.
- We have used distributed ledger to build blockchain network and stored records of each registered vehicle such as owner details, vehicle number, and license detail of driver in the blockchain network with aim to protect the transportation application from single point of failure within smart cities. The proposed work incorporates different roles, namely, vehicle, toll point, district transport agency, and network admin. All roles require permission for accessing data already stored in blockchain network. Besides, different smart contract has been designed to enable the whole SRP system (transportation application) within smart cities. The proposed system incorporates quantum blind signature within smart contract to enable automation of SRP system achieving unconditional communication security within smart cities.

The organization of rest of the chapter includes preliminaries section where quantum computing and blockchain are described. Various recent literature utilizing quantum techniques in different application areas such as healthcare and cloud computing have been explored in Section 11.3. Section 11.4 describes background details of proposed work detailing design goals. Later, the proposed SRP system with detailed system architecture and vehicle records utilizing BB84 protocol along with designed smart contracts are described in Section 11.5. Finally, Section 11.6 concludes the work.

11.2 Preliminaries

This section gives insights about building blocks of proposed protocol, i.e., quantum computing, quantum key distribution (QKD), and blockchain. Besides, the need for amalgamation of quantum computing and blockchain is presented.

11.2.1 Quantum Computing

This section includes overview on quantum computing in addition to specifying details of key characteristic as well as quantum platform and software development kit (SDK) available in market where quantum algorithm can be simulated or executed on real quantum computer. The quantum computer will be made up of quantum chips contrary to silicon-based chips installed in classical computers. Moreover, the potential of quantum computer to break mathematically hard problems such as integer factorization (IF) problem and discrete log (DL) problem made it extremely popular, meanwhile, endangering all existing protocols whose security depends on mathematically hard problems. In addition, exponential increase of curiosity by major multi-national companies (MNCs) in building quantum computer that has not only created the hype rather availability of quantum computer in market is assured. Recently, IBM's roadmap predicts the arrival of 1,000 qubit quantum computer within few years. The announcement by several scientist indicates intense planning for cryptographic agility term used to upgrade existing protocols before they become vulnerable or outdated. In addition, quantum computing is also expected to turn around computationally difficult task such as training of neural network, which are known to be building blocks of several machine learning algorithm. The need of optimization for various deep learning algorithms only fosters the need of availability of quantum processing units (QPUs) to researchers and industry through cloud. It is expected that, similar to graphic processing units (GPUs), QPUs will be available to any individual for deploying their algorithm very soon. Now, what follows are basics of quantum system.

11.2.1.1 Basics of Quantum System

Quantum system depends heavily on quantum mechanics which uses complex number contrary to real numbers. In addition, contrary to bit, which is described with set of states, i.e., either 0 or 1, quantum bits are used by quantum system which could be narrated through 2D system $[c_0, c_1]^T$ where

$$|c_0^2| + |c_1^2| = 1. \tag{11.1}$$

where c_0^2 and c_1^2 signify the probabilities obtained after measuring the qubits in state |0 > and state |1 >. A real world implementation of quantum bit in day-to-day life will make switch of a bulb in ON and OFF state at the same time. In fact, the presence of electron in two different orbits around nucleus and existence of photon in any one out of two polarized states established the implementation of quantum bits. Therefore, existence of quantum indeterminancy and superposition effects within all system lies in universe.

11.2.1.2 Architecture of Quantum System

The quantum system possess reversibility property thereby action performed on quantum system must allowed to be reversed. The assurance of reversibility property within architecture of quantum system brought up the need of reversible gates. Reversible gates constitute all operations which are represented by unitary matrices and are not measurement. Example of reversible gate includes identity gate, NOT gate, CNOT gate, Toffoli gate, and Fredkin gate. The widely used AND gate in classical computing is not reversible as with output of |0 > from AND gate in hand, no one can determine whether input was |00 >, |01 >, or |10 > contrary to NOT gate and identity gates which are reversible.

$$NOT * NOT = I_2 \tag{11.2}$$

$$I_n * I_n = I_n \tag{11.3}$$

Therefore, an operator which acts on qubits and represented by unitary matrices is known as quantum gates. In addition, it may be noted that Toffoli and Fredkin gates are not only reversible but also is universal and unitary. However, all mentioned quantum gates are limited by no-cloning theorem for imitating fanout operation but transportation of quantum states is still feasible between two systems.

11.2.1.3 Key Characteristics of Quantum Computing

The key characteristics of quantum computing include superposition, measurement, and entanglement. Superposition enables quantum system to be in more than one state with some probability at the same time. The quantum state interferes with each other in superposition. Constructive interference enables addition of probability amplitudes of quantum states, while destructive interference cancels out probability amplitudes of each quantum state. Besides, entanglement is achieved due to superposition of quantum states. Because of entanglement of quantum particles a single system is formed thus generating correlation between entangled particles. This generated correlation is so strong that interconnection between particles remains unchanged even separated over light-year distance. Besides, measurement of quantum particle collapses the superposition state of particles producing binary state either state 0 or state 1.

11.2.1.4 Available Quantum Platform

The major corporation of world is investing huge amount of money for research and development of quantum computing applications. Similar to cloud computing as a service, major corporations of world are planning to provide quantum computing as a service. Recently, Microsoft has announced public preview of one product related to quantum computing, namely, Azure Quantum. It will enable developers and researchers to run newly designed applications or algorithm on real quantum computer (upto 40 bit quantum computer) through cloud. They have partnership with companies like Riggeti and Honeywell to make quantum computer accessible through cloud. In addition, Azure quantum SDK is also available which will allow developers to test their newly designed algorithms testing or simulation locally. Similarly, IBM offers open source SDK, namely, Qiskit. It also allows developers to run and test their quantum algorithm either locally or through cloud to real quantum computer. Google also offers a python library, namely, Cirq, to be used while writing quantum algorithm before running them on real quantum computer or simulator. In addition, an open source library, namely, TensorFlow quantum, is available to run quantum classical machine learning applications.

11.2.2 Quantum Key Distribution

QKD is implemented by utilizing non-orthogonal single quantum states. The existing QKD protocols can be classified on the basis of dimensions of source code into discrete variable and continuous variable protocol, whereas, if entanglement of light source is taken into account, then it is classified into prepare and measure as well as entanglement based protocols. The following subsections discuss the classified QKD in detail.

11.2.2.1 Discrete Variable QKD

While encoding and decoding these types of protocol includes finite-dimensional quantum states while, for key distribution, examples include all protocols which use certain number of relative phases of photon. Discrete variable QKD protocol incorporates prepare-and-measure as well as entanglement-based protocol in addition to distributed phase reference (DPR) protocol. With view to practical implementation of discrete variable QKD, first experiment results are revealed by Charles Bennett and Gilles Brassard. Later, extreme interest is shown by industry and governments with aim to improve the experimental results and extended the covered distance of QKD. Till date, discrete variable QKD can cover distance of 200–300 km.

- **Single-Photon Protocols:** A type of quantum protocol which utilizes single photon's different quantum states for encoding and decoding while distributing the keys. Various single-photon protocols includes protocol designed by Bennet and Brassard, namely, BB84 in the year 1984 [10], two-state protocol, namely, B92 [11], and six-state protocol by Bruß [12].
- **Entangled Photon:** A type of quantum protocol which utilizes pair of mutual entangled photon for key distribution. These photons contrary to single photon utilizes entangled states for communication. The few popular protocols under this category are protocols proposed by Bennett *et al.*, namely, BBM92 [13], and by Ekert in 1991 [14].
- **Other Discrete Variable protocols:** Various researchers tried to explore the field and proposed different one way discrete variable protocols such as protocol by Inoue *et al.* in year 2002 [15], "fast and simple one way quantum key

distribution" by Stucki *et al.* [16] in year 2005. Besides, two-way discrete variable QKD protocol are well described through Bostrom and Felbinger [17] and by Lucamarini and Mancini, namely, LM05 protocol [18].

11.2.2.2 Continuous Variable QKD

It is type of QKD where infinite-dimensional quantum states are used while distributing keys. Further classification of continuous variable QKD leads us to squeezed state, entangled state, and coherent state schemes. Examples of squeezed protocols and coherent protocols are [19–21]. Besides, experimental results of continuous variable QKD reveals transmission distance of 25 km. Later, major breakthrough is achieved in year 2013 when Jouguet *et al.* demonstrated successful implementation of QKD covering distance of 80 km [22].

11.2.2.3 Measurement Device-Independent QKD

Under the strict assumption of perfect single photon and photon detector, QKD is proved to be secure but QKD becomes vulnerable under loose assumption. Considering vulnerability under loose assumption, various researchers designed device-independent protocols such as protocol by Acin *et al.* [23]. However, inefficiency of loophole free bell test (LFBT) on which measurement device-independent protocols are based turns out to be serious issue. Later, protocols such as one side independent [24] and semidevice-independent [25] are proposed. In addition, various attacks such as wavelength dependent, faked state, and detector time shift attack are prevented using measurement device-independent QKD. The security proof and experimental analysis of these types of protocol is well described in [26].

11.2.3 Blockchain

It may be defined as list of linked records with properties such as data traceability and tamper-resistance. The list of linked records is known as blocks with each block connecting to previous block. Blockchain employs consensus algorithms for providing guarantee related to consistency of records. The privilege related to read-and-update the ledger leads us to classification of blockchain as public blockchain where strong autonomous

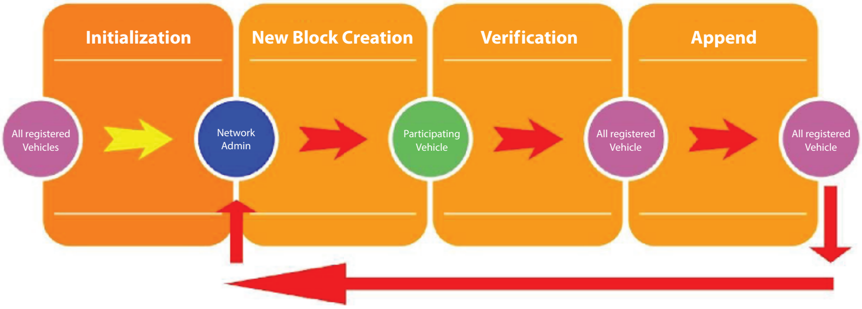


Figure 11.1 Life cycle of transportation application in blockchain.

facilities exist by achieving pure decentralization settings and private blockchain which incorporates control over network up to some extent. Blocks used in blockchain utilize cryptographic hash function to create a chain. However, scalability and efficiency always remain a critical issue during blockchain implementation. Smart contract enables automation of blockchain-based applications in addition to ensuring few popular properties such as atomicity, synchronicity, provenance, availability, immutability, and immortability (no records can be removed) in blockchain, thus opening up scope for designing various application in different industries ranging from healthcare industry, energy industry, robotics energy, agriculture and food industry, and manufacturing industry. In addition, blockchain as a service is expected to completely revolutionize the existing centralized ecosystem. Figure 11.1, shows life cycle of transportation application in blockchain.

11.2.4 Reason for Blend of Blockchain and Quantum-Based Security in Applications Within Smart Cities

All existing applications designed and implemented in smart cities utilize public-key cryptographic techniques to provide security. All public key cryptography-based protocol utilizes the assumption of mathematical hard problems, i.e., the security of existing applications within smart cities depends on mathematically hard problems such as integer factorization (IF). However, the arrival of a few bits quantum chips has indicated the availability of full-fledged quantum computers in the market much sooner than anticipated. The arrival of a full-fledged quantum computer will make existing classical public key-based protocols vulnerable to such an extent that attackers do not require to work very hard to break any system. Besides, utilizing blockchain technology direct access will be provided to every vehicle creating transactions in blockchain network related to vehicle's activities on road. In addition, with use of different available application programming interfaces (APIs) along with smart contract, transmission of data and execution of transaction within blockchain network will be enabled. Also, with vehicle's public identity, all transaction related to vehicle will be entertained, thereby enabling unique identification of all committed transaction in blockchain network. Later, vehicle can verify his records to toll point and district transportation agency whenever asked to verify while moving on road by sharing his secret key. Use of quantum secret based authentication and data sharing will provide unconditional security. Therefore, a decentralized quantum-based security will allow applications within smart cities to become more secure when compared to traditional security techniques.

11.3 Related Work

A blockchain-based architecture to provide security in maintaining electronic health records is presented in [27]. This paper discusses incentive mechanism in detail with frequency of addition of new blocks while giving overview on access control techniques. In addition, a scheme by Yue *et al.* reveals different architecture utilizing blockchain to store health data records securely [28]. This work includes design of application using blockchain where patient health records can be shared with doctors, clinician, etc., through access control mechanism. Also, in the scheme by Zhang *et al.* [29], two new protocols are presented, which enables formation of secure connection and sharing of data between different nodes in blockchain network. A scheme by Xia *et al.* [30] utilizes blockchain to share medical records. The work presents new data sharing scheme which is used by cloud infrastructure providers within blockchain network. In addition, a scheme by Liang *et al.* [31] discusses medical record sharing implementing blockchain in mobile healthcare applications. The work uses patient's wearable devices, medical inputs manually added by doctors, etc., to constitute medical data record then stores the generated data in cloud, thereby enabling sharing of medical data with healthcare companies as per agreement. Later, a scheme by Lin and Guo [32] discusses a system utilizing quantum blind signature in order to provide identity and message verification. The scheme generates secret keys for messages using quantum bits. Besides, in the scheme by Khodambashi and Zakerolhosseini [33], a smart contract is proposed utilizing quantum blind signature. This work just not only protects the system from quantum attacks but also eliminates the need of trusted third party. A scheme by Lin and Yanlin also uses quantum blind signature to propose quantum circuit which could become a perfect candidate to be used in development of electronic payment as well as electronic voting system [34]. A protocol by Minghui-Zhang *et al.* [35] uses entangled state for quantum blind signature in order to provide traceability, unforgeability, etc. Also, in [36], utilizing light weight quantum blind signature, a smart contract in blockchain network is presented by Cai *et al.*

The availability of quantum computer will definitely boost up number of active applications utilizing quantum computing in various verticals of society. Quantum computing applications are used nowadays in ever growing industries that even blend quantum computing with popular machine learning applications. In addition, in field related to cloud computing, fog computing, and Internet of Things (IoT), vast opportunity is available to design applications that solve specific problems using quantum computing within any smart city. The potential of quantum computing is of extreme importance. Various researchers tried to uncover the hidden potential of quantum computing in different fields such as scheme by Sharma and Kalra [37] in field of cloud computing. The scheme utilizing QKD presented identity-based secure authentication for cloud infrastructure. The scheme ensures identity authentication with unconditional security. In cloud-related application areas, some notable works are also presented by research community such as in schemes [38–40] where properties of QKD are employed to authenticate the entities. The QKD is known to use polarization of photon to encode information. In the scheme by Lohachab and Karambir [41], QKD and payload-based techniques are presented for mutual authentication of IoT devices, employing elliptic curve cryptography (ECC) in application area related to IoT. Also, in applications related to vehicular ad hoc networks (VANETs), identity authentication scheme is introduced for participating vehicles using QKD [42]. In addition, in [43], quantum authentication and communication protocol is designed utilizing one-time pad, while, in the scheme by Mehic *et al.*, detailed discussion on performance of QKD network in widely used network simulator NS-3 is presented [44].

11.4 Background of Proposed Work

This section gives insights on design goals along with fundamental tenets of our work such as conversion mechanism of binary to quantum bit, decision sequence, measurement sequence, template, and encrypted key generation.

11.4.1 Design Goal of Proposed Work

The security and privacy issues play a critical role while envisioning design goal of any protocol. Nowadays, easy availability of high-performance computing infrastructure has enabled any adversary to attack on critical infrastructure very comfortably. In addition, announcement of huge prize money in form of cryptocurrency like Bitcoin on dark web with aim to manifest coordinated attack has threatened any infrastructure like never before. Therefore, with aim to ensure secure communication in the proposed SRP system within smart cities utilizing quantum-blockchain, precautions against the following are designed as goals.

11.4.1.1 Impersonation Attack

It is a form of attack where adversary after manifesting himself to be trusted entity of network shares sensitive information thus creating a confusion within the network. The adversary steals the legal parameters to carry out impersonation attack.

11.4.1.2 Sybil Attack

It is a form of attack where adversary operates multiple pseudonymous identities in order to influence the authority of network. The multiple pseudonymous identities enables adversary to broadcast multiple bogus message, thus allowing him to conduct illegal actions. Examples of Sybil attack include 51% attacks in the blockchain network and generation of multiple fake reviews to any products in e-commerce platform. In order to prevent Sybil attack, different powers to different members need to be assigned. In addition, payment of certain cost for each member who intends to connect in the network should be followed, i.e., cost to create an identity must be accompanied. Also, the direct and indirect validation mechanism should be carried out to members before joining the network.

11.4.1.3 Message Modification Attack

It is a form of active attack where adversary aims to alter, delay, or reorder some segment of message for purpose of fulfilling unintended effect. It involves modifying the packet header and usually performed when adversary wants to either disturb or gain insights about receiver. Whenever instead of altering or reordering the message adversary insert fake data within some section of message, then it leads to bogus information attack.

11.4.1.4 Message Replay Attack

It is the form of attack where adversary delays or resends the intercepted message with aim to generate the mirage of accidents of packet to legal receiver. With proper technique of encryption, timestamping of each message along with small window time, establishing a session with random key which can be utilized only once, could prevent the network from message replay attack.

11.4.1.5 Denial-of-Service Attack

It is the form of attack where adversary floods the network with traffic information, fake requests, or with information that is responsible for triggering a crash. The adversary performs denial-of-service attack with aim to overload the network so that legitimate message cannot be entertained, i.e., intended members are denied with access to network.

11.4.1.6 Source Authentication

The process of ensuring the legitimacy of sender is called as source authentication. It is one of the primary features, which prevents the network from outsider attack.

11.4.1.7 Message Integrity

The process of ensuring that message are not altered or tampered during communication within the network by any adversary. Message digest is widely used to check the message integrity. Message digest is obtained whenever message is passed through hash function. Receiver, after receiving message and digest pair from sender, computes new digest after passing the received message from hash function. In addition, comparison of new computed digest and received digest is performed by receiver to verify integrity of message.

11.4.1.8 Identity Privacy Preservation

The process of preserving real identities of members within the network is known as identity privacy preservation. It is achieved by anonymizing the real identities of members with the help of pseudo identities within the network.

11.4.2 Conversion of Bits From One State to Another

The proposed work uses QKD and thus requires participation of quantum bit. With use of polarization of photon and interconversion rule, conversion of binary bit to quantum bit and vice versa occurs. The proposed protocol denotes photon polarizer through decision sequence and measurement sequence. It may be noted that decision sequence and measurement sequence are alike but do not carry out same function.

11.4.3 Decision Sequence

Decision sequence enables conversion of binary bit into quantum bit. It consists of two types of polarizer, namely, circular and linear polarizer. Horizontal and vertical directions are used to denote linear polarizer, while diagonal direction denotes circular polarizer. In addition, circular and linear polarizer consists of two states which are orthogonal to each other. To be specific, circular and linear polarizer follows orthogonality property.

11.4.4 Interconversion Rule

Interconversion rule is widely used during conversion of bits. In accordance with interconversion rule, sender utilizes decision sequence to find out which polarized photon aligns to zero or one. In proposed work, interconversion rule is defined as follows: | →> ⇒ 0, and | ↑> ⇒1. Also, | ↗> ⇒ 0 and | ↖> ⇒ 1.

11.4.5 Measurement Sequence

Measurement sequence enables restoration of binary bit from quantum bit. It also consists of two types of polarizer, namely, rectilinear and diagonal polarizer similar to linear and circular polarizer of decision sequence.

In fact, the linear and rectilinear polarizer along with circular and diagonal polarizer correlate with each other. Moreover, in accordance with uncertainty principle, decision sequence and measurement sequence are conjugate bases with rectilinear (linear) and diagonal (circular) polarizer as conjugate states, i.e., receiver will only able to retrieve certain results if linear polarizer is measured by rectilinear and circular polarizer are measured by diagonal polarizer. On contrary, uncertain results are obtained. In addition, existence of non-orthogonality property between linear (rectilinear) and circular (diagonal) polarizer makes them indistinguishable. In the Table 11.1, L and R are used to denote linear and rectilinear polarizer, whereas C and D represent circular and diagonal polarizer.

11.4.6 Template and Encrypted Key Generation

Decision sequence and measurement sequence are randomly chosen by sender and receiver during communication. The generation of template occurs in accordance with decision sequence and measurement sequence. In addition, pre-master secret is generated as shown in Table 11.1. The pre-master secret comprises of accurate as well as inaccurate binary bits. Besides, 1/2k denotes selection probability of accurate measurement where k signifies length of bits. The accurate measurement sequence is shown in green color. Moreover, observing pre-master secret and template, encrypted key [0101] is produced as reported in Table 11.2.

11.5 Proposed Work

The proposed quantum blockchain–enabled SRP system includes four roles, namely, vehicles, road side units, network admin, and district

Table 11.1 Generation of pre-master secret.

Binary bit	0	1	1	0	1	0	1	1	1	0
Decision seq	C	L	C	C	L	C	L	L	C	L
Quantum bit	|↗>	|↑>	|↖>	|↗>	|↑>	|↗>	|↑>	|↑>	|↗>	|→>
Measurement seq	D	R	R	D	R	R	D	D	R	D
Pre-master secret	0	1	?	0	1	?	?	?	?	?

Table 11.2 Generation of encrypted key.

Decision seq	C	L	C	C	L	C	L	L	C	L
Measurement seq	D	R	R	D	R	R	D	D	R	D
Template	1	1	0	1	1	0	0	0	0	0
Pre-master secret	0	1	?	0	1	?	?	?	?	?
Encrypted Key	0	1	?	0	1	?	?	?	?	?

transportation agency. The proposed SRP system incorporates QKD and quantum blind signature along with blockchain to fulfill basic security and privacy goals. The implementation of network admin, vehicles, road side units, and district transportation agency is designed through Algorithm 11.1, Algorithm 11.2, Algorithm 11.3, and Algorithm 11.4, respectively.

```
Input    : Enrollment Certificate requested from TA
Output   : Access will be granted to Vehicle channel, Toll road,
           District Transportation agency channel

  Initialization: $N_{Admin}$ should be authentic
Procedure NetworkAdmin($V_{ID}$, $TP_{ID}$, $DTA_{ID}$) while TRUE do
      if $DTA_{ID}$ is authentic then
      Add DTA($B_{NET}$, $DTA_{ID}$); GrantAccess($DTA_{ID}$, Uname, $S_K$)
      else
      Invalid ($DTA_{ID}$);
      end
      if $V_{ID}$ is authentic then
      Add Vehicle($B_{NET}$, $V_{ID}$); GrantAccess($V_{ID}$, Uname, $S_K$)
      else
      Invalid ($V_{ID}$);
      end
       if $TP_{ID}$ is authentic then
      Add TollRoad(BNET, $TP_{ID}$); GrantAccess($TP_{ID}$, Uname, $S_K$)
      else
      Invalid ($TP_{ID}$);
      end

    if Trusted(N) then
            NotUpdate($DTA_{ID}$, $V_{ID}$, $TP_{ID}$)


    else
    end

```

Algorithm 11.1 Algorithm for network admin.

```
Input          : Enrollment ID Key requested from $N_{Admin}$
Output         : Access will be granted to District Transportation
                 Agency Transaction
Initialization: $DTA_{ID}$ should be authentic

Procedure DistrictTransportAgency($DTA_{ID}$) while TRUE
do
    if Access granted by $V_{ID}$ then
        if Granted $M_{VID} \varepsilon\ C$ then
            RecordsRead ($DTA_{ID}, V_{REC}, M_{VID}, B_{NET}$);
            RecordsUpdate ($DTA_{ID}, V_{REC}, M_{VID}, B_{NET}$);
        else
            RecordsWrite ($DTA_{ID}, M_{VID}, B_{NET}$);
            RecordsRead ($DTA_{ID}, M_{VID}, B_{NET}$);
        end
    else
        Invalid ($DTA_{ID}$);
    end
```

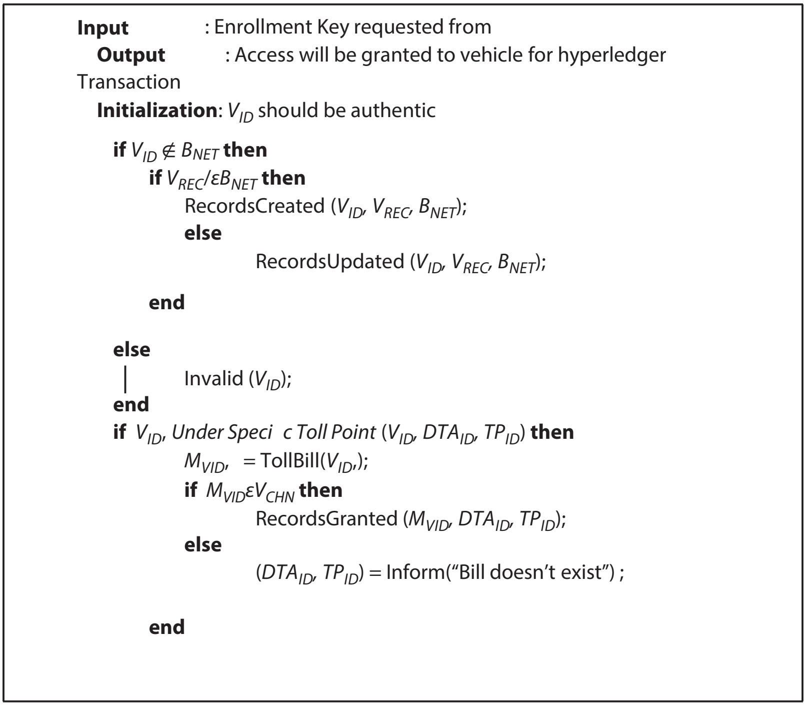
Algorithm 11.2 Algorithm for district transport agency.

```
Input          : Enrollment ID Key requested from
Output         : Access will be granted to Toll Road hyperledger
Transaction
Initialization: $TR_{ID}$ should be authentic

    if Access granted by $V_{ID}$
    then if Granted $M_{VID} \varepsilon C$
      then
            RecordsRead ($TP_{ID}, V_{REC}, M_{VID}, B_{NET}$ );

            RecordsUpdate ($TP_{ID}, V_{REC}, M_{VID}, B_{NET\ i.e.,}$ ($TP_{ID}, V_{REC}, M_{VID}, B_{NET}$);

        else
            RecordsRead ($DTA_{ID}, M_{VID}, B_{NET}$);
  end
```

Algorithm 11.3 Algorithm for toll road.

11.5.1 System Architecture

Figure 11.2 illustrates the network model of the transportation application within any smart city that includes the district transportation agency consisting of various toll points. Each toll point covers various roadside units (RSUs). All RSUs are connected to trusted authorities through optical fiber cables for faster connectivity in the real world. The system architecture of the proposed



```
Input           : Enrollment Key requested from
  Output          : Access will be granted to vehicle for hyperledger
Transaction
  Initialization: $V_{ID}$ should be authentic
    if $V_{ID} \notin B_{NET}$ then
        if $V_{REC}/\varepsilon B_{NET}$ then
            RecordsCreated ($V_{ID}$, $V_{REC}$, $B_{NET}$);
            else
                RecordsUpdated ($V_{ID}$, $V_{REC}$, $B_{NET}$);
        end
    else
    |       Invalid ($V_{ID}$);
    end
    if $V_{ID}$, Under Specific Toll Point ($V_{ID}$, $DTA_{ID}$, $TP_{ID}$) then
            $M_{VID}$,  = TollBill($V_{ID}$,);
            if $M_{VID} \varepsilon V_{CHN}$ then
                RecordsGranted ($M_{VID}$, $DTA_{ID}$, $TP_{ID}$);
            else
                ($DTA_{ID}$, $TP_{ID}$) = Inform("Bill doesn't exist") ;
        end
```

Algorithm 11.4 Algorithm for vehicle.

SRP system gets illustrated in Figure 11.3. There is one district transportation agency within any smart city responsible for maintaining records of all registered vehicles within any city. The district transportation agency handles the collection of money in penalties or taxes by deploying different infrastructures such as toll points. In addition, the generation of driving licenses, pollution certificates, documents related to the vehicle, etc., is also managed by the district transportation agency. In addition, to stop the unlawful driving activities by young drivers, members of the district transportation agency perform strict auditing at any junction or crossroads within the city. The uninformed and instant auditing by members of the district transportation agency leads to an exponential decrement in lane speed violations and hazardous accidents, creating safe and secure transport facilities within the city.

11.5.2 Quantum Information Transmission

QKD is used to exchange keys securely between participating parties. The QKD possesses unconditional security utilizing laws of physics such as superposition, interference, and entanglement. In the proposed protocol,

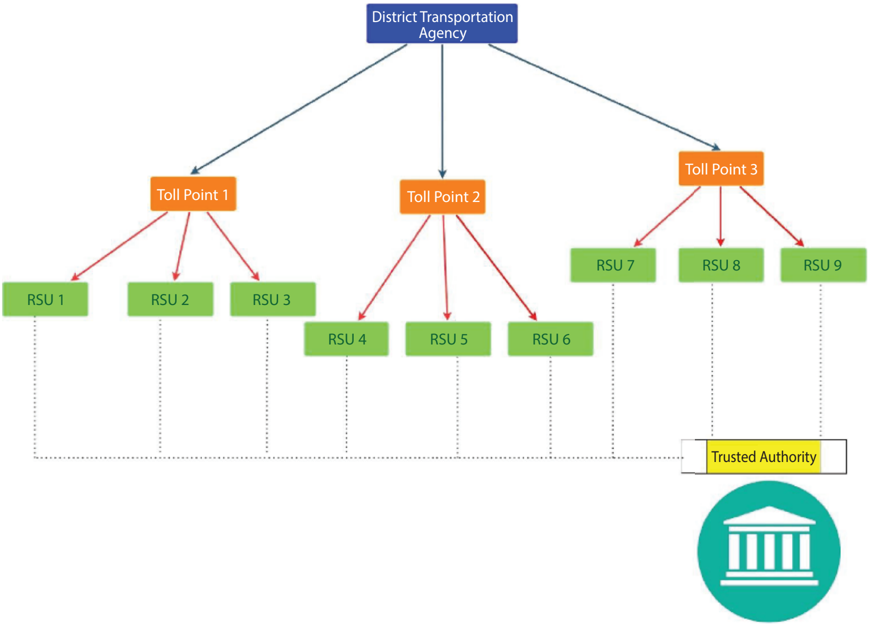


Figure 11.2 Network model of transportation application in smart cities.

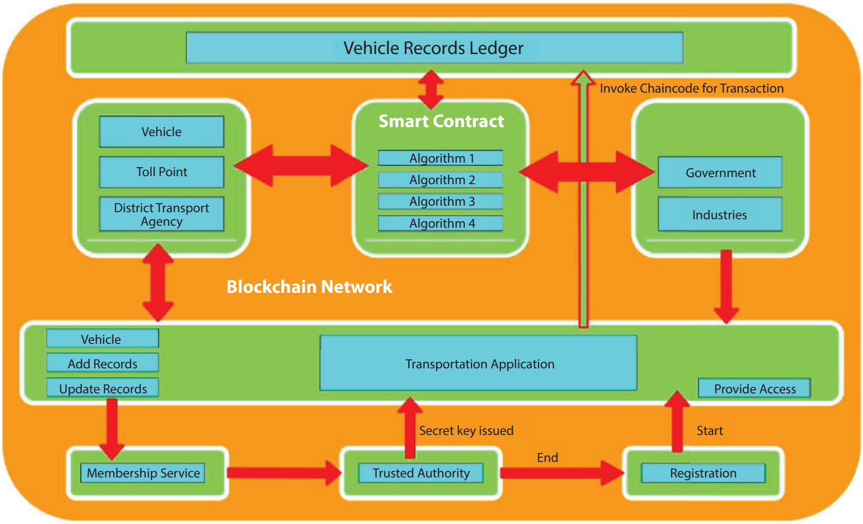


Figure 11.3 Smart road pricing application.

QKD is used within smart contract. Specifically, a quantum communication protocol, namely, BB84, which is proposed by Bennett and Brassard is used. The BB84 allows unconditionally secure exchange of keys between parties as well as enables intrusion detection by prohibiting copying of quantum states in accordance with no-cloning theorem. The implementation of BB84 protocol utilizes polarization photons (linear and circularly polarized photons) in order to encode information. These polarization photons are well known for encoding one bit string to q bit and can retrieve q bit string to traditional binary bits. The high-level description and basics of proposed protocol is already discussed in Section 11.4. Besides, Table 11.3 summaries the notations which are used in the proposed work whereas Table 11.4 reports the time complexity of proposed algorithms. The security of BB84 protocol is well discussed in [45].

11.5.3 Life Cycle of Smart Contract

The proposed quantum blockchain–enabled SRP system for smart cities incorporates smart contracts utilizing quantum blind signature. The quantum blind signature is well discussed in [46]. The post-quantum blockchain–enabled application within any smart city utilizes quantum blind signature to provide unconditional security, which includes three stages, namely, contract development stage, contract release stage, and contract execution stage, as illustrated in Figure 11.4. As the name suggests, contract development

Table 11.3 Notations used in the chapter.

Uname	Username
S_K	Secret key
V_{ID}	Vehicle identity
V_{CHN}	Vehicle channel
TP_{ID}	Toll point identity
TP_{CHN}	Toll point channel
B_{NET}	Blockchain network
DTA_{ID}	District transport agency identity
DTA_{CHN}	District transport agency channel

Table 11.4 Time complexity of proposed algorithm.

Algorithm	Smart contract	Time complexity
Algorithm 1	Implementation of N_{ADMIN}	O(N)
Algorithm 2	Implementation of district transportation agency	$O(DTA_{ID})$
Algorithm 3	Implementation of toll point	$O(TP_{ID})$
Algorithm 4	Implementation of vehicle	$O(V_{ID})$

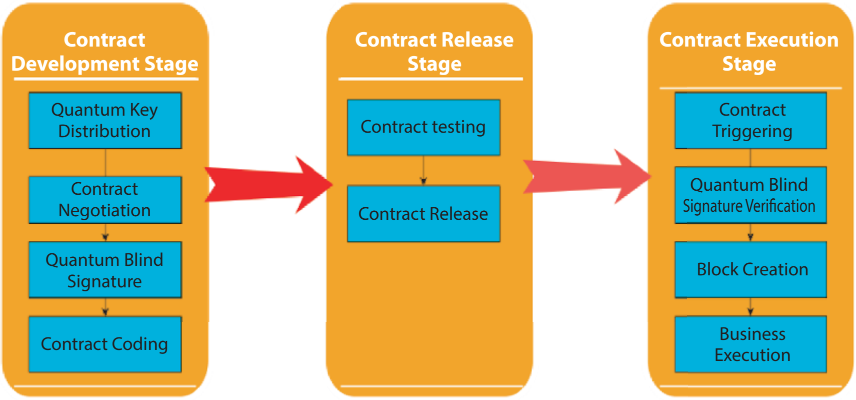


Figure 11.4 Life cycle of smart contract.

stage revolves around development of smart contract. It primarily includes exchange of keys using QKD, contract negotiation, contract coding, and quantum blind signature. The second stage, namely, contract release stage, includes process to perform contract testing thereby performing release of contract. Execution of contract testing will allow transfer of smart contract to each node within the network. As soon as each node receives smart contract due to implementation of contract testing, it performs packing of received smart contract into a set known as contract set. Contract set contains hash value of contract in set and then transfer to different nodes in the blockchain network for further processing. The other nodes, after receiving this contract set, compare the hash with its own contract, leading to decision by all nodes in network regarding release of contract. The third stage, namely, contract execution stage activities, just not only includes triggering of contract and creation of block but also verification of quantum blind signature and execution of protocol. In fact, contract execution is performed using event-based trigger mechanism. As soon as smart contract, which requires verification of quantum blind signature, is received to any node within the network, then verification of quantum blind signature is carried out by respective node. Successful verification will result in creation of new block otherwise not only creation of block gets failed but prohibition of contract execution also takes place.

11.5.4 Algorithm Design and Flow

The QKD occurs between trader and block creator. As soon as utilizing negotiated key, a signed transaction message is received to block creator, utilizing shared key K, the decryption process of signature is performed by block creator, thus producing business request R. It may be noted that since there is chance of collapsing a block creator in any stages of life cycle of smart contract therefore block creator by performing recovery techniques can recover from that particular stage. In addition, automatic execution of contract is enabled in case where business request R and specific signature state b is found to be same otherwise leading to failure of block creation. The steps for execution of smart contract is illustrated through Figure 11.5.

11.5.4.1 Stage 1: Contract Development

The development phase of contract uses QKD for exchange of keys. QKD enables sharing of keys through quantum channel between block creator and trader. In addition, block creator prepares n pair entangled particles in superposition state. Then, negotiation of contract with respect to contract term and quantum keys is carried out. After that, block creator and trader analyze the feasibility of contract term, safety of channel and key. Henceforth, with aim to process business transaction request T_i, blinding factor t and transaction summary k are chosen randomly.

$$T_i = tkT_i'(mod\, n) \tag{11.4}$$

Now, result obtained after blind transformation of transaction request is forwarded to signer. After carefully selecting negotiation particles, signer generates quantum state T_i corresponding to each pair of particles.

$$T_i|(a) >= T_i|(a) >= \alpha|0 > + \beta|1 > where,\ |\alpha|^2 + |\beta|^2 = 1. \tag{11.5}$$

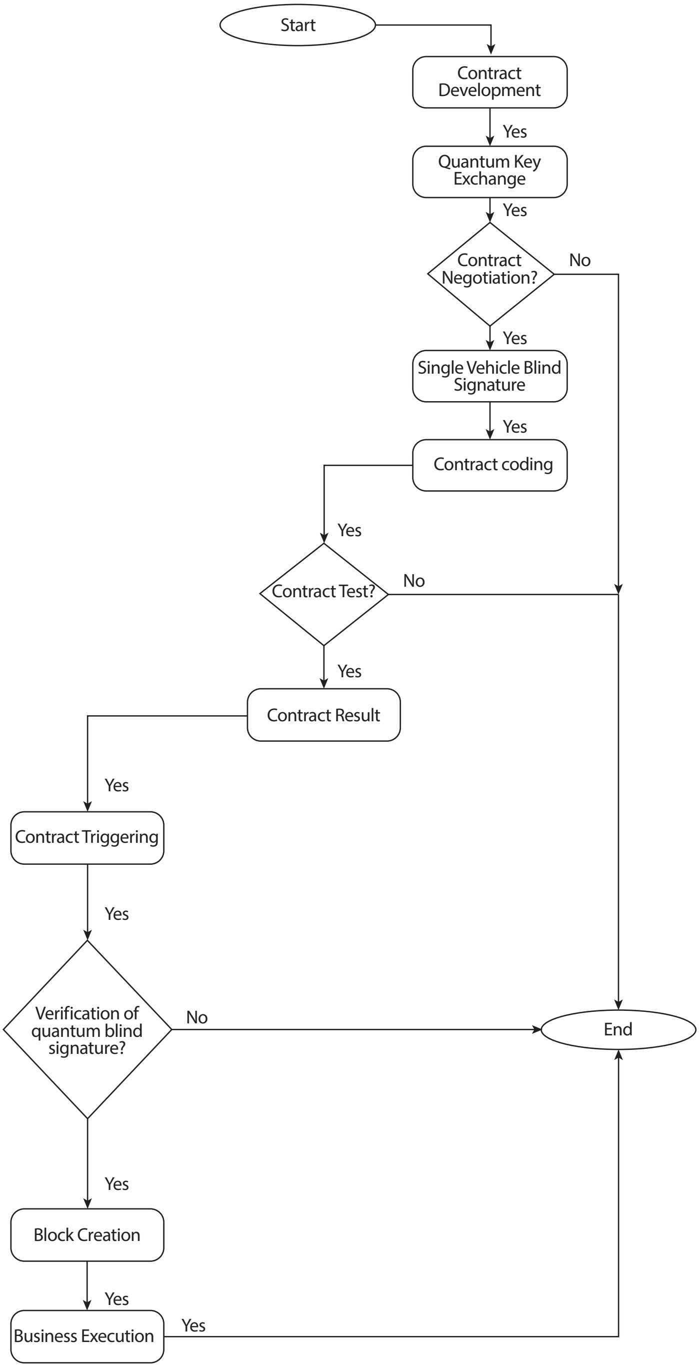


Figure 11.5 Execution of smart contract.

Next, business trader forwards quantum state $T_i(b)$ to block creator while retain $T_i(a)$ to itself. Block creator then verifies the validity of signed transaction request and communicates entangled pairs back to trader. As soon as trader listens back from block creator, calculates particle a_i, T_i, and obtains encrypted result, thereby utilizing bell measurement for generating quantum key corresponding to signature S.

$$S = E_k(T_i) \tag{11.6}$$

11.5.4.2 Stage 2: Contract Release

In this stage, contract testing is done. If testing results is found to be positive, then release of contract is performed.

11.5.4.3 Step 3: Contract Execution

In this stage, triggering of contract is performed after successful fulfillment of conditions. After triggering, the verification process of quantum blind signature is accomplished, leading to conduction of contract evaluation and contract execution. The successful verification will generate a transaction message T_i'. As soon as contract is executed, in addition to creation of a new block, broadcast of message revealing successful transaction to all nodes within the network is performed.

$$T_i' = t^{-}T_i(mod\, n) \tag{11.7}$$

11.6 Conclusion

The potential of quantum computing has threatened existing infrastructure, thus motivating research community to design new quantum resistant protocols.

Besides, use of blockchain enables complete transformation of various applications in any smart cities. Blockchain eliminates need of trusted third party, thus decentralizing the smart city application with automated secure data collection and sharing while ensuring protection against single point of failure. In addition, the amalgamation of quantum computing with blockchain can do the wonders for any smart cities applications. Therefore, this chapter just not only discusses in detail about quantum computing, blockchain, blend of blockchain, and quantum computing but also describes a post-quantum blockchain architecture for transportation application within any smart city. The description also includes design of a SRP system containing smart contracts with aim to store and share vehicle records securely among four roles, namely, vehicle, toll points, network administrator of network, and district transportation agency. The presented work will not only enable smooth management of vehicle records but also boost up the collaboration between different organization situated within the same city, thereby realizing vision of robust and inclusive smart city.

References

1. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W., PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.*, 88, 101653, 2020, https://doi.org/10.1016/j.cose.2019.101653.
2. Esposito, C., Ficco, M., Gupta, B.B., Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manage.*, 58, 2, 102468, 2021, ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2020.102468.
3. Kifokeris, D. and Koch, C., A conceptual digital business model for construction logistics consultants, featuring a sociomaterial blockchain solution for integrated economic, material and information flows. *J. Inf. Technol. Construct.*, 25, 500–521, 2020.
4. Khattak, H.A., Tehreem, K., Almogren, A., Ameer, Z., Din, I.U., Adnan, M., Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. *J. Inf. Secur. Appl.*, 55, 102615, 2020, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102615.
5. Castro, M. and Liskov, B., Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.*, 20, 4, 398–461, 2002.
6. Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., Zhou, M., Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 7, 118541–118555, 2019.
7. Kumar, D.R., Krishna, T.A., Wahi, A., Health monitoring framework for in time recognition of pulmonary embolism using internet of things. *J. Comput. Theor. Nanosci.*, 15, 5, 1598–1602, 2018.
8. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., Dutkiewicz, E., Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access*, 7, 85727–85745, 2019.

9. Grover, L.K., A fast quantum mechanical algorithm for database search, in: *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp. 212–219, 1996.
10. Bennett, C.H. and Brassard, G., Quantum cryptography: Publickey distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE, New York, pp. 175–179, 1984.
11. Bennett, C.H., Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68, 21, 3121–3124, 1992.
12. Bruß, D., Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81, 14, 3018–3021, 1998.
13. Bennett, C.H., Brassard, G., Mermin, N.D., Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68, 5, 557–559, 1992.
14. Ekert, A.K., Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67, 6, 661–663, 1991.
15. Inoue, K., Waks, E., Yamamoto, Y., Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89, 3, Article ID 037902, 3 pages, 2002.
16. Stucki, D., Brunner, N., Gisin, N. *et al.*, Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.*, 87, 19, Article ID 194108, 3 pages, 2005.
17. Bostrom, K. and Felbinger, T., Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.*, 89, 18, Article ID 187902, 4 pages, 2002.
18. Lucamarini, M. and Mancini, S., Secure deterministic communication without entanglement. *Phys. Rev. Lett.*, 94, 14, Article ID 140501, 4 pages, 2005.
19. Cerf, N.J., Levy, M., Assche, G.V., Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63, 5, Article ID 052311, 5 pages, 2001.
20. Grosshans, F. and Grangier, P., Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88, 5, Article ID 057902, 4 pages, 2002.
21. Weedbrook, C., Lance, A.M., Bowen, W.P. *et al.*, Quantum cryptography without switching. *Phys. Rev. Lett.*, 93, 17, Article ID 170504, 4 pages, 2004.
22. Jouguet, P., Kunz-Jacques, S., Leverrier, A. *et al.*, Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics*, 7, 5, 378–381, 2013.
23. Acın, A., Massar, S., Pironio, S., Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.*, 8, 8, Article ID 126, 11 pages, 2006.
24. Branciard, C., Cavalcanti, E.G., Walborn, S.P. *et al.*, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85, 1, Article ID 010301, 5 pages, 2012.
25. Pawlowski, M. and Brunner, N., Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A*, 84, 1, Article ID 010302, 4 pages, 2011.
26. Liu, Y., Chen, T.Y., Wang, L.J. *et al.*, Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 111, 13, Article ID 130502, 5 pages, 2013.

27. Yang, G. and Li, C., A design of blockchain-based architecture for the security of electronic health record (EHR) systems. *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 261–5, 2018.
28. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W., Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.*, 40, 10, 218, 2016.
29. Zhang, J., Xue, N., Huang, X., A secure system for pervasive social network-based healthcare. *IEEE Access*, 4, 9239–50, 2016.
30. Xia, Q., Sifah, E., Smahi, A., Amofa, S., Zhang, X., Bbds: blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8, 2, 44, 2017, https://doi.org/10.3390/info8020044.
31. Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D., Integrating blockchain for data sharing and collaboration in mobile healthcare applications. *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on*, IEEE, pp. 1–5, 2017.
32. Lin, L. and Guo, Y., Constructions of quantum blind signature based on two-particle-entangled system. *2009 Second International Symposium on Information Science and Engineering*, pp. 355–8, 2009.
33. Khodambashi, S. and Zakerolhosseini, A., A quantum blind signature scheme for electronic payments. *2014 22nd Iranian Conference on Electrical Engineering (ICEE)*, pp. 879–84, 2014.
34. Lin, T., Chen, Y., Chang, T., Lu, C., Kuo, S., Quantum blind signature based on quantum circuit. *14th IEEE International Conference on Nanotechnology*, pp. 868–72, 2014.
35. Minghui-Zhang, Huifang-Li, Yun-Zhou, Xiaoyi-Feng, Zhengwen-Cao, Jinye-Peng, A weak blind quantum signature protocol based on four-particle cluster state. *2017 International Conference on the Frontiers and Advances in Data Science (FADS)*, pp. 125–9, 2017.
36. Cai, Z., Qu, J., Liu, P., Yu, J., A blockchain smart contract based on light-weighted quantum blind signature. *IEEE Access*, 7, 138657–138668, 2019.
37. Sharma, G. and Kalra, S., Identity based secure authentication scheme based on quantum key distribution for cloud computing. *Peer Peer Netw. Appl.*, 11, 2, 220–234, 2018.
38. Kanamori, Y., Yoo, S.M., Gregory, D.A., Sheldon, F.T., On quantum authentication protocols, GLOBECOM '05. *IEEE Global Telecommunications Conference*, pp. 1650–1654, 2005.
39. Dong, Y., Xiao, S., Ma, H., Chen, L., Research on quantum authentication methods for the secure access control among three elements of cloud computing. *Int. J. Theor. Phys.*, 55, 12, 5106–5117, 2016.
40. Murali, G. and Prasad, R.S., Secured cloud authentication using quantum cryptography. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, pp. 3753–3756, 2017.

41. Ankur, L. and Karambir, Using quantum key distribution and ecc for secure inter-device authentication and communication in IoT infrastructure, (April 20, 2018). *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, http://dx.doi.org/10.2139/ssrn.3166511.
42. Chen, Z., Zhou, K., Liao, Q., Quantum identity authentication scheme of vehicular ad-hoc networks. *Int. J. Theor. Phys.*, 58, 40–57, 2019.
43. Chang, Y., Xu, C., Zhang, S., Yan, L., Controlled quantum securedirect communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *Chin. Sci. Bull.*, 59, 21, 2541–2546, 2014.
44. Mehic, M., Maurhart, O., Rass, S., Implementation of quantum key distribution network simulation module in the network simulator NS-3. *Quantum Inf. Process.*, 16, 253, 2017.
45. Scarani, V. and Renner, R., Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100, 20, 200501, 2008.
46. Cai, Z., Qu, J., Liu, P., Yu, J., A blockchain smart contract based on light-weighted quantum blind signature. *IEEE Access*, 7, 138657–138668, 2019.