Quantum Computing and Blockchain Technologies overIoT Applications: A R

Vinisha Bhagwani, Vidhi Mishra

Computer Engineering Department, K.J. Somaiya Polytechnic

KJ Somaiya Polytechnic Vidyavihar Mumbai..

Abstract— In cybersecurity, blockchain is essential for achieving privacy of IoT data as it provides the immutability feature. Blockchain is currently one of the most cutting-edge technologies, and it has received a lot of attention and research. The majority of current cryptography techniques could be broken with the efforts made to realize large-scale quantum computers. In order to create blockchain frameworks, a quantum tool must be able to execute at the level of digital computers and fend off potential attacks from both digital and quantum computers. A thorough analysis of the current literature on implementing Blockchain and Quantum Computing over IoT network will be crucial. In order to comprehend the state-of-the-art of this developing technology, this work aims to highlight unresolved issues that the IoT community will need to deal with in the upcoming years. This article also presents a comprehensive review of Quantum Computing and Blockchain Technologies deployed over IoT applications.

Keywords
Quantum Computing, Internet-of-Things (IoT), Blockchain, Cryptography, Quantum resistant Cryptosystems

I. Introduction

Quantum computing is an emerging paradigm that outperforms classical computing by taking advantage of quantum-mechanical concepts like entanglement, inference, and superposition. Numerous application areas, including medical research, data science, sustainable energy, finance, industrial chemical development, secure communications, and quantum chemistry, benefit from quantum computing's ability to handle complex and computationally intractable problems. Recent years have seen incredible advancements in both quantum hardware and software, bringing quantum computing a lot closer to becoming a reality [1].

Blockchain technology is a decentralized data exchange platform that uses cryptographic procedures to validate data. Blockchain is an immutable data record system with timestamps managed by a computer network. A blockchain database is a shared resource that is constantly balanced. This demonstrates that multiple parties can own data on a Blockchain using consensus mechanism. Each of these pieces of data is encrypted and linked together using an encryption method. Network nodes agree on how to embed data into the blockchain. Each blockchain operation must be associated with a processing cost. Far from being an ideal solution to this problem, Inter Planetary File System (IPFS), a decentralized peer-to-peer network, makes it easier to store files. For this purpose, IPFS hashes are stored as data on the blockchain. When information is distributed throughout the system, there is no central repository of information.

Data on the chain can be used by anyone on the network. So, anything created on the blockchain is very visible to the owners and stakeholders by applying appropriate consensus algorithm[2].

With the exerted efforts for realizing large-scale quantum computers, most current cryptographic mechanisms may be hacked. Accordingly, we need a quantum tool utilized for designing blockchain frameworks to have the ability to be executed at the level of digital computers and resist the probable attacks from both digital and quantum computers [3].

The fast progress of quantum computing has opened the possibility of performing attacks based on Grover’s and Shor’s algorithms in the near future. Such algorithms threaten both public-key cryptography and hash functions, forcing to redesign blockchains to make use of cryptosystems that withstand quantum attacks, thus creating what is known as post-quantum, quantum-proof, quantum-safe, or quantum-resistant cryptosystems [4].

IoT stands for “Internet of Things”. The fundamental tenet of IoT is that there are numerous things or objects all around which includes Radio-Frequency Identification

(RFID) tags, sensors, actuators, mobile phones, etc. These objects can communicate with one another and work together in a wireless network to accomplish shared objectives, thanks to special addressing schemes [5]. The term IoT refers to physical objects (or groups of such objects) equipped with sensors, computing power, software, and other technologies that communicate with one another and exchange data through the Internet or other communications networks. The term "internet of things" has been criticized because devices only need to be individually addressable and connected to a network, not the whole internet. The fusion of numerous technologies, such as ubiquitous computing, widely available sensors, sophisticated embedded systems, and machine learning, has caused this technology to advance. IoT is enabled by traditional domains such as embedded systems, wireless sensor networks, control systems, and automation both individually and collectively [5]. IoT technology is most commonly linked with consumer goods that relate to the idea of the "smart home," including gadgets and appliances that support one or more common ecosystems and may be operated by gadgets connected to that ecosystem, including smartphones and smart speakers. Systems for providing healthcare also leverage IoT [6].

Numerous security issues involving the network, users, hardware, and software may exist in IoT devices. Hacking techniques have greatly improved over the past few years. Attackers are using more advanced methods, which puts the security of IoT in grave jeopardy. Thanks to quantum computing, the many attack surfaces of loT can be breached in novel ways. Due to the built-in security measures, IoT devices must be resistant to hacking. Quantum encryption techniques must be developed in order to guard against breaches before quantum computers, which could be deployed commercially shortly. Big numbers can be generated instantaneously using quantum cryptography. The key could thus be kept safe, and talks could be kept private. This suggests that each gadget will have a unique, challenging-to-decipher key. The key can only be obtained by accessing the actual device's setup. It would be extremely difficult to accomplish this in tamper-resistant devices without being noticed [7]. Moreover, there could be attacks where only one IoT device out of the entire network is infected with a virus, and other devices keep exchanging data with the afflicted device until the infection is found. A significant amount of data could have been lost if the problem hadn't been identified before it was too late. It's possible that the fault won't be found until it's too late, at which point a significant amount of information could have been transmitted to any malicious entity. Industrial and corporate systems aren't typically restarted for a very long time, and some viruses may affect them in a way that makes rebooting the sole option to get rid of them [8]. As a result of the multiple unique points of vulnerability, IoT systems are especially susceptible to attacks. In this article, we look at a possible quantum cryptography strategy for IoT security.

II. Literature Survey

Haibo Yi [9] discusses the new application of IoT technology in social networks. The author proposes a privacy protection system consisting of a novel framework that contains a post quantum ring signature and a blockchain privacy system for the current Social Internet of Things (SIoTs). This proposed framework mandates all the data from SIoT be stored in blocks of the blockchain network. By integrating the proposed designs, all messages from SIoTs should be updated to the blockchain. The actions of the user look like the actions of a group. Thus, the privacy protection of blockchain is improved. The security of the blockchain is based on post quantum techniques, which are secure against both traditional computers and quantum computers.

Y. -L. Gao et. al. [10] propose a post-Quantum Blockchain-based cryptocurrency scheme. This system uses a lattice problem-based signature scheme. This scheme incorporates a first signature and last signature which collectively is called the double signature. Finally, the author proposes a Post Quantum Blockchain cryptocurrency scheme by combining the above-proposed signature scheme with the blockchain. This proposed system design does not require any third parties or users for key generation and also reduces the risk of forging a valid signature. Thus, the security of the algorithm is enhanced. The proposed system is computationally efficient by reducing the lattice short integer solution (SIS) problem, as a result, the sizes of signature and secret keys are relatively shorter than that of others. These methods make this cryptocurrency scheme more secure and efficient.

Ahmed A. Abd El-Latif et. al. [3] proposes a new authentication and encryption protocol based on quantum-inspired quantum walks (QIQW) for the secure transmission of data among IoT devices for smart water utilities. The proposed protocol makes use of Quantum Hash Function (QHF) based on QIQW for linking the blocks of the blockchain. The proposed framework helps IoT nodes to effectively share their data with other nodes and have full control of their records. This framework assumes that each user has a validated profile and his own set of key parameters for each of the nodes in the blockchain system.

Gao, YL et. al. [11] proposes a new quantum blockchain scheme based on entanglement and Delegated Proof of Stake. This scheme uses bell states to optimize blockchain security. The

technique inspired by the proposed quantum blockchain uses temporal entanglement to link these quantum blocks. Each user in the system produces verifiable quantum information via a quantum signature that is exposed on the quantum network and validated by other nodes. Other nodes then compete for new quantum blocks with fair consensus and link these quantum blocks through temporal entanglement. Finally, all nodes add this new quantum block to their own quantum blockchain via quantum channels. The authors also highlight the major security issues of blockchain and attempt to build a new quantum blockchain scheme to improve security against quantum computing attacks. It provides an open, public distributed ledger on a distributed network that can be applied to many promising applications.

Balogh S, et. al. [12] proposes that postquantum security has received a lot of attention in recent years. NIST started a standardization initiative to replace the aforementioned algorithms in 2016. For the categories—public-key encryption, key-establishment algorithms and digital signature algorithms—a new standard is necessary. The same mechanisms employed in other applications are also applied in the IoT domain. The limitations of these tiny devices, including their power processing and memory restrictions are another crucial consideration for the security of IoT devices. When selecting the appropriate postquantum mechanisms and developing postquantum protocols, these limitations should be taken into account. For instance, the difficulty of encryption/decryption or signing/verifying varies greatly among numerous ideas. Ephemeral key generation is much slower than traditional key generation, and key sizes can increase greatly. The IoT protocols used should take into account the traits of these new underlying algorithms and assign computationally more challenging tasks to the server side. The right choice of a post quantum cryptography algorithm can reduce the cost of client devices and provide IoT vendors a competitive edge.

Gill SS. [13] proposes that Blockchain technology processes data from IoT applications in a chain of blocks and is an open distributed ledger. Because data is handled in blocks, this technique is efficient at securely processing data for serverless edge computing, but it slows down calculation performance. The work required to determine the nonce values and hashes for each data-block in the entire chain is a feature of blockchain design. This operation must operate concurrently over a number of distributed architecture nodes in order to verify the Proof-of Work. Such procedures might be integrated into a Faas platform using microservices, which could then be set up on a serverless pipeline. Quantum computers can be employed to provide large-scale computation. Entanglement and superposition, two key ideas in quantum physics, are used to conduct computations in quantum computing. Today's edge computational paradigm uses the idea of "Serverless computing" to offer function as a service for load balancing and dynamic provisioning. Additionally, machine learning and AI-based approaches can be employed to enable autonomous execution, which can help quantum computers train models and accelerate processing.

Wanyang Dai [14] proposes that the current Industrial 4.0 will swiftly be transiting to Industrial 6.0 with the advent of quantum computing. The Sixth Industrial Revolution (SIR) Forum predicted that the two main technologies of IR 6.0 will be blockchain and quantum computing. The future Internet of Things (IoT) is made possible by the quantum system, which will have

extraordinarily powerful processing, storage, tracing, and administration capabilities compared to the current system. The Internet of Everything can be used to describe this broader IoT. High performance network hardware and intelligent software that are well integrated are needed to achieve efficiency in order to realize the future Internet. More specifically, there is an interactive hardware and software system inside the IoT network system. Quantum blockchain, a system for storing data and managing software, must be used to connect physical Things and hardware quantum computing centers in order to actualize the interaction between the Internet of Things and the physical world. This paper views the Thing to be the future quantum MIMO wireless channel, that represents the trend of future developments on mobile cloud computing.

A. A. Abd El-Latif et. al. [15] proposes that digital and physical technologies are used in Industry 4.0 to enable responsive and connected processes. From the supply chain to the smart factory, businesses are leveraging AI, robotics, edge computing, and the cloud to make fast decisions. Real-time improvements in product quality and operating efficiency in factories are made possible by solutions created for the Industrial IoT, which leverage linked sensors and edge devices. From workshops and job sites to decision-making stations, tools and equipment are increasingly networked and connected. Machines and operators are gathering massive volumes of data through sensors, detectors, and other monitoring tools, and for businesses, managing, analyzing, and utilizing this data poses immense hurdles. The IoT offers a wealth of promise in terms of efficiency, quality, performance, and security by enabling smart manufacturing. Due to the improved failure data recording capabilities of connected sensors and detectors, this enhancement aids in the reduction of nonconformance. This makes locating the cause of nonconformance and fixing it simpler. By better directing and monitoring the various production processes, the use of IoT tools helps to increase quality. Also, the Blockchain can be used which restricts the flow of information and potential external threats by enabling objects to interact with one another directly.

A. Gupta et. al. [16] propose that a smart city is a contemporary metropolis that employs numerous technology strategies, data collecting techniques, and sensor collaborations to gather and transmit sensitive data to data centers. The metropolises strive to have connected streetlights, weather monitoring, air quality/pollution monitoring, connected public transportation, traffic monitoring and operation, water position/flood monitoring, video surveillance and analytics, connected streetlights, and smart water meters. They also monitor water quality and keep an eye on fires and banks. Sensor data is utilized to properly administer all services, and the information gathered is used to enhance the services offered to users. Without the need for a centralized director, blockchain enables network actors to exchange data with a high degree of transparency and trustability. Cities have a wide range of stakeholders, and data sharing amongst stakeholders is crucial for widely accessible civic services

Gulshan Kumar et. al.[17] proposed a new framework called Internet-of-Forensics (IoF). This architecture takes into account a blockchain-specific IoT framework for digital forensics. It offers a clear perspective of the research process from all angles, including cloud service providers and heterogeneous device manufacturers. IoT is used as the foundational technology for evidence gathering and communications in the suggested architecture for digital forensics investigation, while blockchain is used for managing digital forensic evidence. The architecture additionally makes use of a consortium blockchain to maintain a safe chain of custody across a case chain throughout the duration of the investigation. The framework is made less complicated and post-quantum resistant by combining a programmable hash function (PHF) with a lattice based sign encryption. A transparent method for all internal procedures of a digital forensic investigation is provided by the blockchain-based case chain. To prevent evidence manipulation, the IoF architecture guarantees privacy-anonymity for the forensic witnesses.

Xin Sun et. al. [18] discusses a permissioned blockchain structure of quantum security called Logicontract (LC). LC uses a digital signature scheme based on a quantum key distribution (QKD) mechanism and a voting-based consensus algorithm to achieve consensus on the blockchain. The proposed consensus protocol is a combination of an unconditional security signature scheme and YAC (Yet Another Consensus) algorithm. The authors also propose to apply the Toeplitz hash-based unconditionally secure authentication method as a basis for useful digital signatures in quantum blockchains. The logical contract of the consensus protocol scales better with the number of peers.

Chaoyang Li et. al. [19] discusses methods to eliminate the quantum vulnerability of existing blockchain-based systems and applications. The authors propose an efficient blind signature method based on an anti-quantum grid. The bimodal Gaussian distribution is used to hide the original message, thus protecting the user's sensitive information. The proposed blind signature scheme ensures data security and hides confidential user information. It also provides anti quantum security as a lattice assumption for blockchain-enabled systems. On the other hand, signatures provide a strong guarantee that users cannot reject transactions with their signatures. The lattice assumption makes the proposed technique more secure from quantum attacks, and the blind property ensures the security of confidential information of system users. The security of the proposed method can be reduced to the SIS problem, and can greatly improve user privacy and system data security in blockchain-enabled systems and applications.

Wusheng Wang et. al. [20] offers a blockchain technology based on a stake vote consensus process and asymmetric quantum encryption. This approach combines a consensus process based on the fully flipped permutation (QSCDff) problem, node behavior, and delegated proof of stake (DPoSB) with quantum digital signature technology based on quantum state computational distinguishability. While the quantum signature employs quantum one-way functions to ensure the security of transactions, DPoSB is utilized to produce blocks through voting. The fairness, effectiveness, and security of the blockchain system can be increased by the stake vote, punishing the bad actions of DPoSB, and also by employing asymmetric quantum encryption.

S. Banupriya et. al. [21] proposes a novel effective, privacy-preserving, and quantum-resistant key generation technique, called lattice-based hierarchical deterministic key generation (LB HDKG), to protect user privacy in public blockchains. To conceal the connections between the transactions of the same user, the LB-HDKG scheme creates several cryptographic keys from a single seed in the form of a tree-like structure. The end user side is where the hierarchical key derivation process is applied; other network users do not need to be modified. Key generation techniques are implemented using the lattice-based NTRU (Nth degree truncated polynomial ring) scheme and are quicker than those based on RSA and ECC. The process reduces the possibility of key leaking, does away with the hassle of storing and maintaining several key pairs, and creates a fresh public key for every transaction.

E. M. Abou-Nassar et. al. [22] offers a New Decentralized Interoperable Trust model (DIT) Blockchain framework for IoT (IoHT) systems in the healthcare industry. It is intended to provide dependable mutual information integration between its members and dependable cooperative IoT eco-systems (zones). In order to achieve reliable communication, the proposed DIT IoHT uses a private Blockchain ripple chain to validate nodes based on their interoperable structure. The proposed DIT Blockchain IoHT system has a four-layer overall architecture. Sensors and actuators that are used exclusively for gathering and processing information make up the first layer. The network pathways and gateways needed to transfer IoT data are included in the second layer. Between the technology and application levels are interposed sub-layers that make up the framework's third layer, often known as middleware. The application layer is the last.

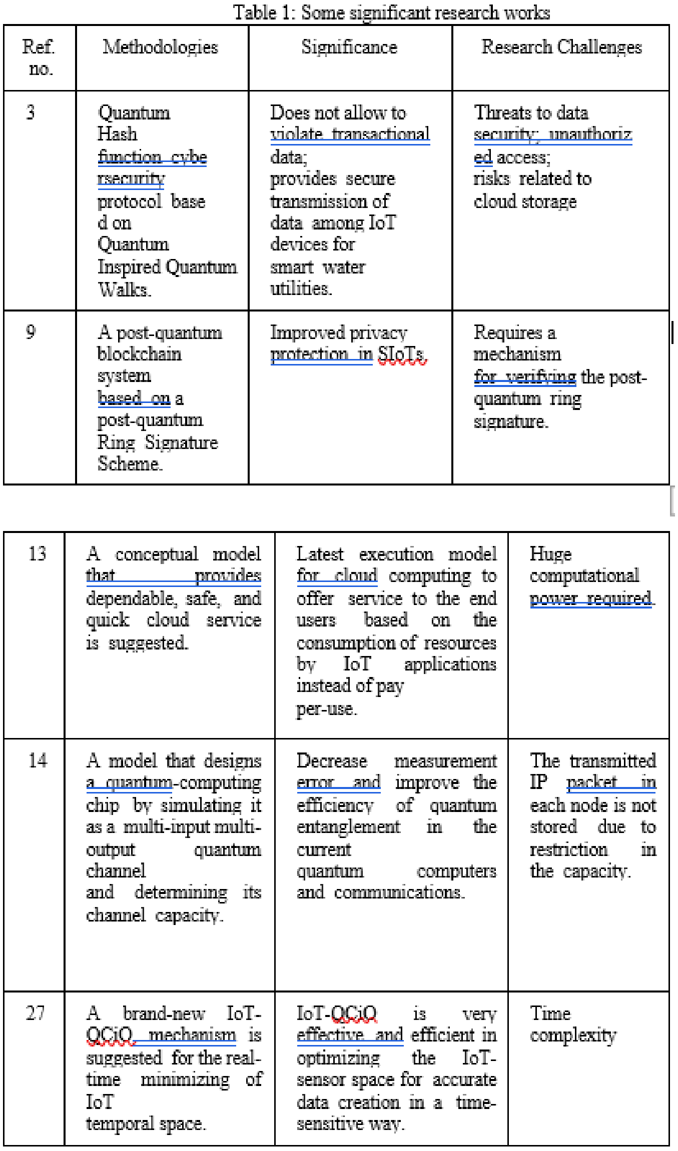
Alessio Faccia et. al. [23] has conducted an analysis to emphasize not only the susceptibility of the financial industry to the technologies (FinTech) that are fueling its exponential growth, as well as the conclusions with various scientific disciplines, including fractal geometry, quantum physics, and database systems (blockchain distributed ledger). The probable repercussions of each scientific development on Fintech are then evaluated using a SWOT analysis to formally and consistently prove those presumptions. The authors in this article aim to highlight the effects that paradigm shifts in three interrelated sciences are having on the Fintech industry, including geometry (from normal to fractal distribution), physics (from classical bit to quantum bit), and database systems (from centralized to the distributed ledger—blockchain). This is because new Open Innovation business models are required. It was possible to show that the majority of the upcoming Fintech applications are based on and attributable to at least one of them or to a combination of them (i.e., forecasting algorithms to be run on a cloud quantum environment) after briefly and thoroughly analyzing the shifts in those paradigms. The inability to anticipate which of these technologies will have the biggest impact on the Fintech industry is the primary drawback of this research, although it does have the advantage of shedding light on the Fintech industry. The systematic survey enables readers (scholars, regulators, entrepreneurs, and Fintech stakeholders in general) to comprehend and anticipate the majority of future technology trends through a classification that can be traced back to major paradigms.

Aman Kaushik et. al. [24] highlight the advantages of combining both fields to the current IoT network design. The authors list the limitations and hurdles in integrating IoT and quantum computing and propose a solution for overcoming the same. The solution states that an IoT network can have a main server (quantum), similar to a gateway, that does all the quantum operations and transmits the classical information to the IoT network, rather than making every device in the network a quantum operated device. All quantum operations will be performed on the server side; a core server will be in charge of managing the creation and measurement of qubits, isolation of quantum systems, and connectivity with external networks.

M. S. Rahman et. al. [26] formulated a hybrid IoT network infrastructure called the "Quantum Security layer" which is one of the layers in the proposed system which supports the overall administration of quantum communication route that enables and drives the quantum cryptography. Only the security key is protected by this channel. Using the same protocol, the other levels communicate with one another. Prior to this, the layer introduced the traditional avenue of communicating the information that will be delivered in the form of a bundle with a serialized encoding of traditional bits. The adaptive features use quantum physics laws and hybrid nature of the system. For private industries like banking, quantum cryptography is becoming increasingly successful. However, with the IoT putting billions of people's personal data and device data at risk, it is now more important than ever to implement quantum cryptography algorithms in this field. The system presented in this paper by the authors is one that is hypothetical. Greater insights and opportunities, as well as new difficulties, may be revealed by additional research and experience with this idea.

M. Bhatia et. al. [27] suggested that IoT technology uses a huge number of devices that are focused on achieving a particular goal for a certain application. In this research, the authors proposed to deploy a novel IoT-QCiO mechanism for the real-time minimizing of IoT-temporal space. Further the authors also discuss about formalization based on quantum computing for IoT devices in terms of sensor-specific properties. Based on two factors of System Information Viewer (SIV) and Operation Support System (OSS), a unique IoT-QCiO has been proposed by decreasing IoT-sensor space for data collecting in real-time. The three key performance indicators are data communication, data assimilation and data terminal equipment which are used to examine the suggested IoT-QCiO methodologies. Utilizing a variety of heterogeneous WiSense Nodes, Raspberry Pis, and the quantum simulator toolkit in a real-world scenario of vehicle data collecting serves, the system validates the offered approach. The suggested model in this paper can be expanded for future research to include distributed network latency enhancement for overall adoption. Additionally, a crucial area for scientific inquiry is security and authenticity on the quantum platform.

Table 1: Some significant research works



Ref. no.	Methodologies	Significance	Research Challenges
3	Quantum Hash function cybe rsecurity protocol base d on Quantum Inspired Quantum Walks.	Does not allow to violate transactional data; provides secure transmission of data among IoT devices for smart water utilities.	Threats to data security; unauthoriz ed access; risks related to cloud storage
9	A post-quantum blockchain system based on a post-quantum Ring Signature Scheme.	Improved privacy protection in SIoTs.	Requires a mechanism for verifying the post-quantum ring signature.
13	A conceptual model that provides dependable, safe, and quick cloud service is suggested.	Latest execution model for cloud computing to offer service to the end users based on the consumption of resources by IoT applications instead of pay per-use.	Huge computational power required.
14	A model that designs a quantum-computing chip by simulating it as a multi-input multi-output quantum channel and determining its channel capacity.	Decrease measurement error and improve the efficiency of quantum entanglement in the current quantum computers and communications.	The transmitted IP packet in each node is not stored due to restriction in the capacity.
27	A brand-new IoT-QCiQ mechanism is suggested for the real-time minimizing of IoT temporal space.	IoT-QCiQ is very effective and efficient in optimizing the IoT-sensor space for accurate data creation in a time-sensitive way.	Time complexity

III. Case Studies on Blockchain and quantum computing deployment in IoT applications

a. **Healthcare systems:** Healthcare systems are desperately needed, yet it takes a lot of time and effort to transfer Electronic Health Records (EHR) from one institution to another [25]. Furthermore, there isn't a tried-and-true approach to solving this problem. Healthcare practitioners might have direct access to a blockchain. A distinct patient ID that may be used for all blockchain transactions [28] involving all the diagnostic data related to that patient. Data can be sent to the blockchain network using a variety of APIs. Smart contracts can be used to control incoming transactions. All patient-related transactions will be conducted using the patient's public ID, which is completely anonymous. Finally, the patient can provide the healthcare service provider their private key if they want to share their data with them. Factorization is a known issue for ordinary encryption; therefore, data is kept secret until the private key is utilized. The blockchain, in contrast, can offer a decentralized network to manage the issue, which also addresses security in the healthcare system because data kept on the blockchain cannot be modified. We suggest the healthcare industry put a secure blockchain-based solution in place. In order to defend the system from quantum attacks, we can also link the theoretical features of quantum technology with blockchain.

b. **Post-Quantum Blockchain for a Scalable Smart City**: The data gathered from a huge number of sensors used in a Smart City application helps to create precise corporate decisions. However, a Smart City's connection between its various apps and components urges security precautions because it frequently suffers from integrity problems and serious security attacks. Researchers have employed Blockchain to protect Smart Cities and boost their decision-making precision in order to treat this conundrum. However, with the advent of quantum computing, quantum-based algorithms are undoubtedly posing a threat to both the security of traditional encryption and the blockchain itself. The insurance of Blockchain-based systems, particularly crucial applications like Smart Cities, is at risk as a result. The use of post-quantum blockchain technology [29] can solve these problems. Post-quantum blockchain technology, a distributed peer-to-peer secure ledger, will enable smart cities to securely manage and coordinate data communication between various components without jeopardizing the privacy and security of that data.

c. **A blockchain-based digital forensics framework for IoT applications**: Due to its variability and lack of transparency in the processing of evidence, digital forensics in the IoT paradigm is crucial. Furthermore, cross-border legalization hinders this procedure with regard to cloud forensic difficulties. This calls for the development of an IoT forensic framework that enables distributed computing, decentralization, and transparency of forensic analysis of digital evidence from a global perspective. In order to achieve this, the author offers a framework for IoT forensics that takes care of the aforementioned problems. The Internet-of-Forensics (IoF) solution [17] takes into account a blockchain-tailored IoT infrastructure for digital forensics. It offers a clear perspective of the research process from all angles, including cloud service providers and heterogeneous device manufacturers. To handle the chain of custody and evidence chain involved in an investigation, a blockchain-based case chain is used. To address the issues with cross-border legalization, consortiums use consensus mechanisms. Additionally, this makes forensic references transparent and simple. Lattice-based cryptographic primitives that can be programmed result in less complexity. It adds to the uniqueness of the suggested approach and demonstrates advantages for power-conscious gadgets. Because IoF is broad, it can be used by independent security operation centers, cyber-forensic investigators, and manually initiated evidence in a chain of custody for crimes committed by humans.

IV. **Applications of post-Quantum Cryptography along with blockchain** a. **Power Industry**: The power industry has seen tremendous transformation in recent years as utilities have adopted cutting-edge technology and methods of energy production. The proliferation of smart and IoT-enabled devices (such as electric vehicles, smart meters, and smartphones) with variable power requirements is making managing the power grids more and more challenging. Blockchain technology has the potential to speed up this global energy transition by lowering transaction costs and improving grid operation. By permitting smart contracts between the various smart grid devices and components, they make it possible for the grid to operate efficiently. Additionally, blockchain enables users to become prosumers (those who both consume and generate) by enabling them to monetize their plentiful power [30] through the use of smart contracts created on systems like Ethereum.

b. **E-Commerce and Retail Industry**: Soon advancements in blockchain technology may also assist e-commerce and retail businesses. Researchers have started looking into this area to see if blockchain technology may be used in it. The IoT-based e-commerce model is a novel one that has strict requirements for transactions, including security, autonomy, and lightness. A lightweight blockchain platform[30] for managing transactions in e-commerce is proposed by the authors in using the Practical Byzantine Fault Tolerance consensus mechanism (PBFT). This three-layered blockchain network has been demonstrated to be very efficient, scalable, and safe against cyberattacks. Instead, than using a common blockchain framework like Ethereum, they construct this blockchain using C++ for improved performance in terms of decreased overhead. Blockchain technology provides transparency and traceability, which may help to remove challenges experienced in the retail industry and give customers a sense of confidence, value, and incentive. With blockchain, it is possible to track a retail goods all the way back to its point of origin. Researchers suggest a consumer feedback privacy-preserving reputation system for retail businesses. They created this system utilizing the PoS consensus mechanism and the Ethereum platform.

c. **Drone Industry**: The newest industry where blockchain technology is being tested is the drone industry. Drones, also known as Unmanned Aerial Vehicles (UAVs), are increasingly commonly utilized for civilian purposes, in contrast to their previous use in military applications. Security of UAV nets (UAV networks) is a prominent research area with a wealth of publications. According to research, UAV net and blockchain technology might be combined [30], with each UAV acting as a node for the blockchain. This tactic aims to protect the network against hacking efforts in which the attacker tries to eavesdrop on control and communication commands to take control of the network's individual nodes. Another study recommends using an asymmetric key encryption technique to recognize compromised UAVs when they are being used for spying. Using the ABS-Security UAV simulator [32], they show the efficacy of their approach by demonstrating that 90% of the UAVs were able to obtain the necessary consensus and identify the hacked UAV. A compromised UAV giving fake information (in the form of false alarms of detecting an intruder) will not be able to add data blocks to this blockchain because the other UAVs in the network also take part in the consensus process.

d. **Educational Industry**: The necessity for an impartial and open method of certifying students' academic records and transcripts grows along with the effectiveness of web based distance learning. A blockchain-based network [30] might act as a notary for academic documents, giving educational institutions and companies' access to safe transcripts and records. Additionally, it might make it possible for universities and other academic institutions to work together. As career pathways diverge across fields and companies, the increasingly dynamic nature of employment suggests that more qualifications are needed. Qualifications are frequently required even to apply for a position, and as demand rises, academic dishonesty is also rising. Blockchain, on the other hand, can support educational evidence and provide employers with the information they need to assess the validity of a candidate's resume. MIT is utilizing blockchain technology already in the US. They created an app called Blockcerts Wallet [31] that allows graduates to safely exchange a tamper-proof and verifiable digital copy of their diplomas with potential employers. It is easy to use and comprehend: credentials may be uploaded to the app and are represented by a digital token, which gives users a digital degree and quick authenticity verification. The gateway searches the digital ledger for the transaction ID, verifies the keys, and checks to see whether anything has changed since the record was added. It avoids tampering or fraud because each certificate is recorded as a transaction on the blockchain network.

V. Conclusion and Future Work

In this article, we review the current state of quantum blockchain research. The architecture and design of the quantum blockchain along with its usage were disscussed. Decentralization and distributed were two features that the quantum blockchain has in common with the regular blockchain. Two of the essential characteristics of quantum blockchain are security and efficiency. The security of the quantum blockchain must be ensured. Quantum secure direct communication (QSDC) and quantum key distribution are two methods that can ensure the security of communication between nodes (QKD). As a result, quantum physics ensures network authentication. Using the digital signature, a typical blockchain can be used to confirm that the bitcoin belongs to its rightful owner. The quantum blockchain thus has quantum security properties. Attacks from quantum computers might not even have an effect on the quantum blockchain. Additionally, transactions on IoT networks can be processed quickly thanks to blockchain-based quantum technology. This endeavor will be very helpful in reviewing the current state of the art in post-quantum cryptography. Overall, the effectiveness and security of the quantum blockchain beat those of the conventional blockchain. Last but not least, quantum blockchain will have a variety of applications in the future especially in internet of everything deployment as well as distinct research focuses due to its advantages of faster processing and safer transactions based on quantum physics.

References

1. Ayoade, O.; Rivas, P.; Orduz, J. Artificial Intelligence Computing at the Quantum Level. *Data* **2022**, *7*, 28. https://doi.org/10.3390/data7030028

2. Manoj, M. K., & Krishnan, S. S. R. (2020). Decentralizing privacy using blockchain to protect private data and challanges with ipfs. In Transforming Businesses With Bitcoin Mining and Blockchain Applications (pp. 207-220). IGI Global.

3. Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, Irfan Mehmood, Khan Muhammad, Salvador E. Venegas-Andraca, Jialiang Peng, "Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities", Information Processing & Management, Volume 58, Issue 4, 2021,

4. T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in *IEEE Access*, vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

5. Roberto Minerva, Abyi Biru, Domenico Rotondi, "IEEE IoT Towards Definition Internet of Things Revision1" 27 May 2015.

6. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

7. https://www.iotforall.com/securing-iot-with-quantum-cryptography

8. Bhatt, A. P., &amp; Sharma, A. (2019, December 11). security.https://www.sciencedirect.com/science/article/pii/S1674862X19300345

9. H. Yi, "Secure Social Internet of Things Based on Post-Quantum Blockchain," in *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp.

950-957, 1 May-June 2022, doi: 10.1109/TNSE.2021.3095192.

10. 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," in *IEEE Access*, vol. 6, pp. 27205-27213, 2018, doi: 10.1109/ACCESS.2018.2827203.

11. Gao, YL., Chen, XB., Xu, G. *et al.* A novel quantum blockchain scheme base on quantum entanglement and DPoS. *Quantum Inf Process* **19,** 420 (2020). https://doi.org/10.1007/s11128-020- 02915-y

12. Balogh S, Gallo O, Ploszek R, Špaček P, Zajac P. IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques. Electronics. 2021; 10(21):2647. https://doi.org/10.3390/electronics10212647

13. Gill SS. Quantum and blockchain based Serverless edge computing: A vision, model, new trends and future directions. Internet Technology Letters. 2021 Feb:e275. https://doi.org/10.1002/itl2.275

14. Wanyang Dai (2019) Quantum-computing with AI & blockchain: modelling, fault tolerance and capacity scheduling, Mathematical and Computer Modelling of Dynamical Systems, 25:6, 523-559, DOI: 10.1080/13873954.2019.1677725.

15. A. A. Abd El-Latif, Y. Maleh, M. Petrocchi and V. Casola, "Guest Editorial: Advanced Computing and Blockchain Applications for Critical Industrial IoT," in IEEE Transactions on Industrial Informatics, 2022, doi: 10.1109/TII.2022.3183443.

16. A. Gupta, A. Pachauri, P. Pachauri, S. V. Singh, P. Chaturvedi and S. Sharma, "A review on conglomeration of Technologies for Smart Cities," 2021 International Conference on Technological Advancements and Innovations (ICTAI), 2021, pp. 526-530, doi: 10.1109/ICTAI53825.2021.9673458.

17. Kumar, Gulshan & Saha, Rahul & Lal, Chhagan & Conti, Mauro. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Generation Computer Systems. 120. 10.1016/j.future.2021.02.016.

18. Sun, Xin, Mirek Sopek, Quanlong Wang, and Piotr Kulicki. 2019. "Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic" *Entropy* 21, no. 9: 887. https://doi.org/10.3390/e21090887

19. Li, C., Tian, Y., Chen, X., & Li, J. (2020,August 15) An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems.
21. Wang, W., Yu, Y. & Du, L. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. *Sci Rep* **12,** 8606 (2022). https://doi.org/10.1038/s41598-022-12412-0

21. Banupriya, S., Kottursamy, K. & Bashir, A.K. Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain. *Peer-to-Peer Netw. Appl.* **14,** 2813–2825 (2021). https://doi.org/10.1007/s12083-021-01117-2

22. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. -Y. Song, A. K. Bashir and A. A. A. El Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, vol. 8, pp. 111223-111238, 2020, doi: 10.1109/ACCESS.2020.2999468.

23. Mosteanu, N.R.; Faccia, A. Fintech Frontiers in Quantum Computing, Fractals, and Blockchain Distributed Ledger: Paradigm Shifts and Open Innovation. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 19. https://doi.org/10.3390/joitmc7010019

24. Integration of Quantum compiting with Iot. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

25. Amrit Mukherjee (2022). Quantum inspired next generation ICT for smart healthcare, IEEE.

26. M. S. Rahman and M. Hossam-E-Haider, "Quantum IoT: A Quantum Approach in IoT Security Maintenance," 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), 2019, pp. 269-272, doi: 10.1109/ICREST.2019.8644342.

27. M. Bhatia and S. K. Sood, "Quantum Computing-Inspired Network Optimization for IoT Applications," in *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5590-5598, June 2020, doi: 10.1109/JIOT.2020.2979887.

28. Makwana Bhavin, Sudeep Tanwar , Navneet Sharma , Sudhanshu Tyagi , Neeraj Kumar, “Blockchain and Quantum Blind Signature-Based Hybrid Scheme for Healthcare 5.0 Applications - ScienceDirect.” *Blockchain and Quantum Blind Signature-Based Hybrid Scheme for Healthcare 5.0 Applications - ScienceDirect*, 29 Dec. 2020,

29. Abir EL Azzaoui, Jong Hyuk Park, "Post-Quantum Blockchain for a Scalable Smart City," *Journal of Internet Technology*, vol. 21, no. 4 , pp. 1171-1178, Jul. 2020.

30. T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, “Blockchain Applications for Industry 4.0 and Industrial

IoT: A Review," IEEE Access, vol. 7, pp.176935–176951, 10.1109/ACCESS.2019.2956748.

31. https://www.blockcerts.org/

32. García-Magariño, I., Lacuesta, R., Rajarajan, M., & Lloret, J. (2019). Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Networks, 86, 72-82.