QUANTUM CHAIN OF THINGS : AMALGAMATION OF BLOCKCHAIN(BC),INTERNET OF THINGS(IOT), AND QUANTUM COMPUTING(QC)- QCOT ERA

Abstract

The Internet of Things (IoT), which is building a new world where everything is interconnected and can be remotely operated, is one of the developing technologies. The epoch of machines conquering the universe is just getting warmed up. By 2025, there will be approximately 22 billion associated devices on the planet. The next technological innovation is blockchain, which uses a peer-to-peer communication link to preserve general transactional data and information (or blocks) across several repositories (orchains). The terminology "Digital Ledger" alludes to an instance of block storage.Quantum computing is the next quickly developing technology. It incorporates use of numerous quantum physics aspects, notably superposition and entanglement. Every foundational premise of the computational game is amended by quantum excellence.A new paradigm dubbed Quantum - Chain of Things (QCoT)[1], which is the most potent technology from the sub-emerging technologies, is presented when we scrutinize the collaboration of the three powerful advanced technologies (Quantum Computing, Blockchain and IOT).The BC-IOT (Blockchain coupled with IOT leveraging Arduino) and QC-IOT (Quantum computing merged with IOT using IBM Qiskit) subsystems are the cornerstones of QCoT technology [1].The prevailing breakthroughs in blockchain, quantum computing, and IOT will be addressed in this paper, then followed by an exploration of the recommended architectural model for the improved technology, designated as QCoT, and its implementations. We will employ the quantum chain of things to forecast future patterns and opportunities. It is a remedy for improving our everyday activities in a secured and beneficial way.

Keywords: Internet of things, Future Technology,Security, Quantum Technology, QCoT technology, Blockchain,Post-Quantum Cryptography

Authors

Shweta Jain
CSE(ET) Department
Panipat Institude of Engineering and Technology
Panipat, Haryana, India.
jainshweta290204@gmail.com

Anju Gandhi Bhandari
Professor
CSE(ET) Department
Panipat Institude of Engineering and Technology
Panipat, Haryana, India.
dr.anjugandhi@gmail.com

Devendra Prasad
Professor
CSE(ET) Department
Panipat Institude of Engineering and Technology
Panipat, Haryana, India.
prasad.cse@piet.co.in

Stuti Mehla
Associate Professor
CSE(ET) Department
Panipat Institude of Engineering and Technology
Panipat, Haryana, India.
stutimehla.cse@piet.co.in

I. INTRODUCTION

During the past couple of years, the online world has altered both professional and modern routines. Firstly, let's talk about the Internet of Things, which is one of the trendiest themes today as well as in present and the future world. From smart automobiles to smart wearables, smart homes to smart cities, smart education to smart farming, IOT is being implemented in every sector of the economy.[3]

The genuine technologically persuaded Network of all network systems, the Internet of things(IoT) is aorganized system of networks, not an assumption.This just happens to be the initial step of the journey. Big picture of internet of things era has just dawned. There's additionally more to explore, emerge and offer. The interconnectedness of the IoT delivers business activities an assortment of opportunities. ButIoT infrastructure must cope with a multitude of challenges as the volume of linked appliances expands. The biggest stumbling block is security, which is an utmost priority. IOT devices that are not adequately protected might act as vulnerable entry routes for cyberattacks and insecure personal information. Given the diverse characteristics of IoT and the vast volume of information yielded, specifically in this Big Data epoch, the process for sequencing, interpretation, and information management capabilities is incredibly challenging. The preponderance of systems currently leverages centralized infrastructure to parallelize information and conduct computationally demanding tasks across a worldwide cloud infrastructure. Yet, there is a perennial concern that existing cloud infrastructures won't be capable of accommodating the immense quantities of information that are processed and devoured by IoT compatible devices, in addition to support the accompanying computational load and appease scheduling expectations. To combat this problem, the large number of systems rely on presently offered technology solutions like fog computing as well as mobile cloud technologies, both of which are premised on edge transmission. IOT must be upgraded or merged with other more powerful technologies in consideration of these problems encountered with the foreseeable escalation in technological complexity, information, and consumption.

Blockchain is the next potent technology we have, and it facilitates faster, extra-productive, and smarter interactions amongst our smart gadgets. Blockchain is a decentralized record format that may be assigned throughout many operational applications and is not restricted to Bitcoin. We are embracing the blockchain agenda to support everything from non-financial applications like Ethereum and Hyperledger to financial applications like Bitcoin and Ripple[2] [40].. The accompanying summarizes a few of the significant challenges that blockchain technology brings with it: -

1. A low level of adoption
2. Augmentation to legacy infrastructure
3. Fewer employment alternatives
4. Challenges regarding confidentiality and safety
5. Increasing prevalence tied with implementing blockchain technology.
6. Attacks and criminal linkage
7. Lacking conformity.
8. Low Implementation and processing speed
9. Scalability
10. Single point failure (A server)

Quantum computing[3] [39]., which makes advantage of quantum physics, is the third game changer emerging technology.The four tenets that constitute the foundation of the quantum computing paradigm are as follows:

- A complex vector may be employed to symbolize a quantum state.
- Hermitian matrix operators are suitable to define physically demonstrable constituents of a specific quantum state.
- The phase of a quantum system crumbles into the equivalent eigenvector when we gauge it with an operator, delivering us a suitable eigen value as the output reading.
- It is conceivable to ascertain the quantum system's upcoming (or prior) state with the help of a unitary transformation matrix.

Effective applications of quantum computing can be observed in almost professions. The multiple capabilities and applications of quantum computing are illustrated in Fig.1.1, encompassing automated trading, risk assessment in the finance industry, drug and medicine prognosis in the pharmaceutical industry, and many more uses in a more efficient and optimized way[3] .

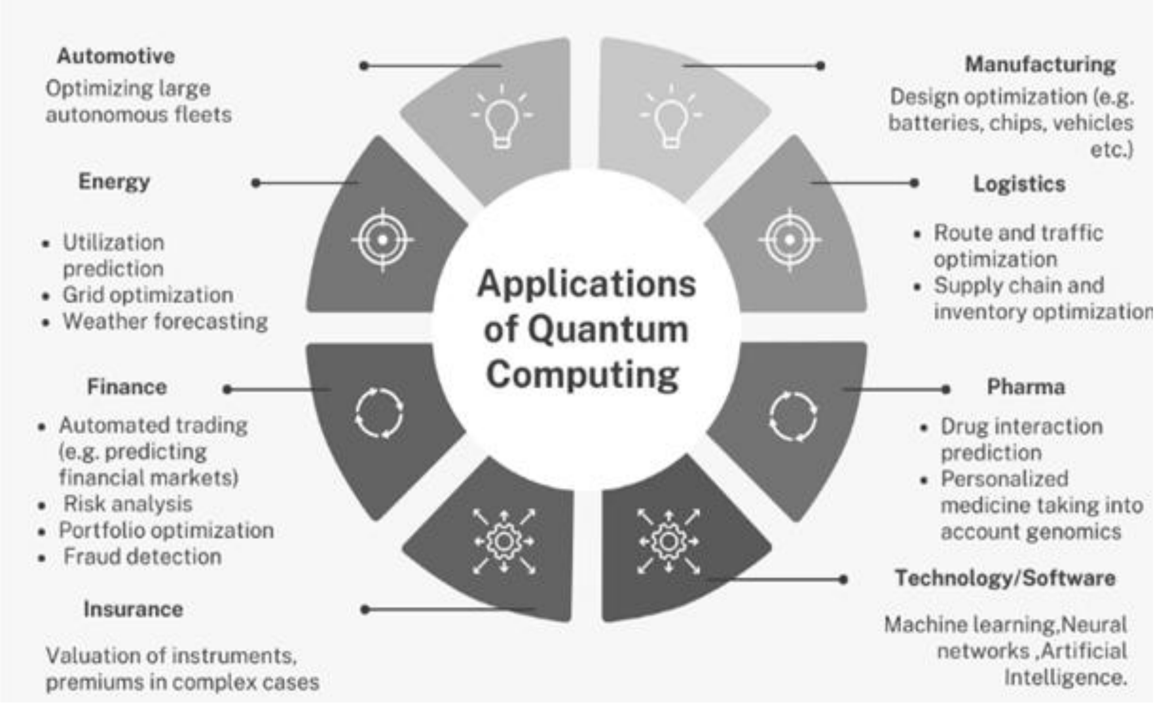

Automotive
Optimizing large autonomous fleets
Energy
• Utilization prediction
• Grid optimization
• Weather forecasting
Finance
• Automated trading (e.g. predicting financial markets)
• Risk analysis
• Portfolio optimization
• Fraud detection
Insurance
Valuation of instruments, premiums in complex cases
Applications of Quantum Computing
Manufacturing
Design optimization (e.g. batteries, chips, vehicles etc.)
Logistics
• Route and traffic optimization
• Supply chain and inventory optimizatio
Pharma
• Drug interaction prediction
• Personalized medicine taking into account genomics
Technology/Software
Machine learning,Neural networks ,Artificial Intelligence.

Figure 1.1 : Applications of Quantum Computing

Quantum computing is used in various parts but still there are some challenges in this technology which needs to be solved. Commencing with the physical impairments, qubits, which must be maintained in a super - cooled surroundings, are an integral part of quantum computing (even for the presence for a nanoseconds)[1] [36].. Next is the fact that few companies can afford quantum technology because it is quite exorbitant. A major challenge to the ubiquitous usage of quantum computing is cosmic radiation (specially for the future usage). It can potentially outcome in inferior superconducting qubit performance. Hardware and quantum algorithms are the key concerns for quantum computing. To comprehend the hardware issues[1] [37]., we necessarily involve:

- A little bit additional qubit (64, 128, 192, 256, 512, 1024)
- Many thousands or even millions of qubits are utilized. One million qubits are encapsulated in a 1,000 by 1,000 interlayer (grid), which is still a relatively little information by today's standards.
- Vastly greater entanglement and interconnectedness with negligible constraints.
- Much reduced amount of error.
- Very high Coherence
- Very complex and deeper circuit.
- Real fault tolerance demands for error checking, which substantially redundant per qubit.
- Significantly less expensive for the entire system.
- Non -deep freezing operating levels

As we seen above,there are various good applications as well as various major challenges in the three powerful technologies (i.e.,Quantum computing, Blockchain technology, Internet of things). Now, if we blend the three most potential technologies, we can transcend a variety of important constraints (as mentioned in above paragraphs).

At the nexus of blockchain, internet of things, and quantum computing, there is a fascinating enchantment. Utilizing the positive benefits of one of the three technologies and overcoming the obstacles of another one is the core strategy of bringing together the three most effective technologies. In this paper, we will see the most potent technology (i.e., QCoT technology)[1] [38]..

II. RELATED WORK

1. **Blockchain IOT(B-IOT):** Recent works are done in Blockchain IOT(B-IOT) which are more efficient than simple IOT (Fusing Blockchain technology with Internet of things technology) which makes IOT more secure and more vulnerable. We need blockchain technology for properly securing the IOT smart devices.

The Blockchain-IOT 5 connected layers are as follows[5]-

- Network sub-layer(Severe networking services provider)
- Infrastructure sub-layer(Actual Blockchain devices)
- Consensus sub-layer(Transactions legality and protection)
- Data sub-layer(Manage the transactions)
- Service sub-layer(Interface between user and blockchain services)

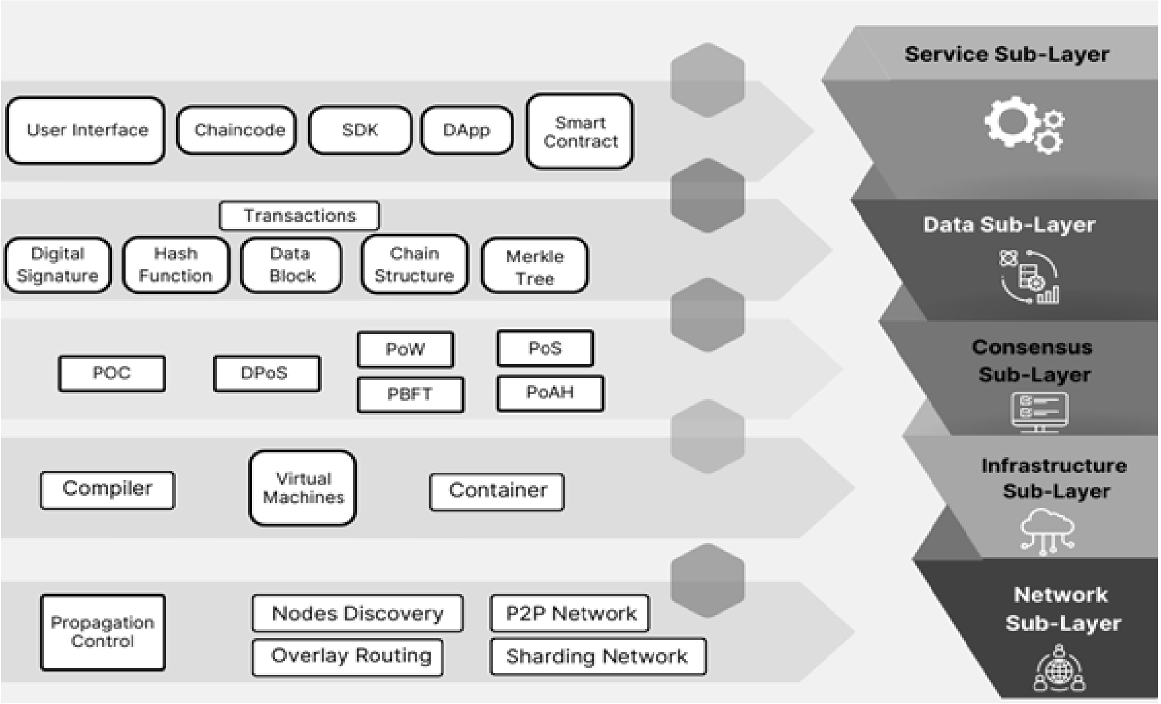


Figure 2.1: Blockchain - IOT Layers

The main objectives of adopting blockchain in IOT world are as follows[2]:

- Decentralization
- Improved Traceability
- Privacy of Data
- Super-enhanced security
- Greater transparency
- Reduction in cost

With the assistance of different frameworks like IOTA[5], Walton chain, and IOT chain, smart technologies used in the BIOT can communicate with one another straightly or indirectly via a blockchain, cloud - based solutions, or fog mainframe where every transaction's immutable documentation is preserved in a file. There are various applications of BIOT, such as in the energysector, privacypolicies, security, database and storage area, industrialized internet of things (IIOT) and many more further areas [35].

For example, in this case, any security design must take availability, confidentiality, and integrity into cognizance whenever providing protection to an IOT-based home automation which is also known as CIA security frameworks. Another two frameworks are user control and authorization. This analysis of BIOT is done in table1.

Table 2.1. Security Requirement Evaluation and Analysis for B-IOT (Blockchain -based Internet of Things)

No.	Requirements	Establishing Framework
1.	Authorization	Policy header, shared keys
2.	Availability	Limited acceptable transactions
3.	Confidentiality	Symmetric Encryption
4.	Integrity	Hashing
5.	User Control	Logging transactions into local BC

Now, after evaluating and analyzing the BIOT, there are various challenges in BIOT which need to be solved and crucial. Technologies implemented in the IOT infrastructure must cope with the challenges such as monitoring devices, RFID, and 6G/5G broadband communication. Due to the sophistication of BIOT applications, incorporating blockchain to this will create extra technological as well as operational considerations [34].

Energy management is the core concern considering blockchain adopts a great deal of energy. Since the blockchain algorithms' mining procedure needs a high amount of energy (Bitcoin). Blockchain Peer - to - peer interaction utilizes a significant amount of power. Thus, maintaining and leveraging energy is a top priority in BIOT. Scalability is an ongoing and emerging difficulty, and many researchers and practitioners are working on it as the need for excellent connectivity and productivity from devices increases constantly. The decentralization of IOT using beautifully emerging developments in technologies like big data, machine learning (ML), also various neural networks is the next move, and this is where we stumble into a massive issue: how and where to legitimize the training dataset. The privacy issue with permissionless blockchain constitutes the next issue that requires a solution. Hence, all these flaws must be remedied, and we are endeavoring to solve them in this research.[32]

2. **Post - Quantum Cryptography(PQC) and Cryptosystems:** In this below detailed segment , we will discusspost-quantum cryptography (PQC) , which acts as a state-of-the-art technologies. To try and combat attacks (like Side-channel attacks, multi-target Pre Image and many more attacks) based on quantum computing and quantum super computers, post-quantum cryptography (PQC) is being implemented. Technology for communication and information has already implemented an assortment of post-quantum cryptographic methods. The subdivisions ofpost-quantum cryptography (PQC) are categorized into 5 main parts. 82(23 signatures + 59 encryptions) methods were proposed in the initiation stage of the NIST post-quantum cryptography (NIST-PQC) Centralization at the final moment of 2017. 69 among those 82 plans were judged to be exhaustive and effective. Seven concepts were unveiled after the third stage.

The following are the main subdivisions of PQC[5]-

- Cryptography leveraging lattice- Uses NTRU, Ring LWE, BLISS algorithms.

- Cryptography leveraging hashes (Scheme of Lamport Digital Signature, Merkle Signature)
- Cryptography leveraging isogeny.
- Multi-variable Polynomial based Cryptography (Scheme of oil and vinegar variables)-Rainbow Algorithm
- Cryptography with the help of codes-Uses McEllice and Niederreiter algorithms.

➢ **Post-Quantum Cryptosystem Types:** The entire theoretical notion was introduced by David Deutch's description of the worldwide quantum computing framework, and later on, many quantum computing researchers such as Shor and Grover started working on quantum fundamentals and built their algorithm, which we now use very efficiently. There are mainly 5 types of PQC algorithms which are as follows[6]-

- Hash-based Cryptosystems
- Code-based Cryptosystems
- Lattice-based Cryptosystems
- Multi- variate Cryptosystems
- Super-singular elliptic Curve Isogeny Cryptosystems

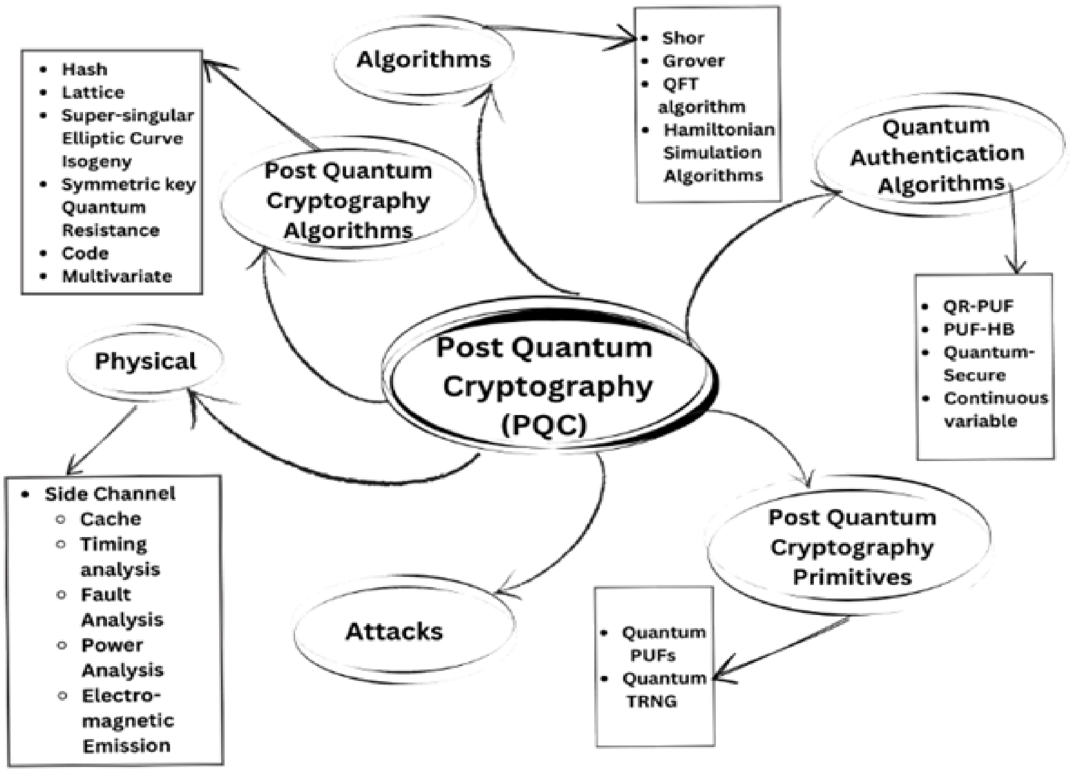

Algorithms
Shor
Grover
QFT algorithm
Hamiltonian Simulation Algorithms
Hash
Lattice
Super-singular Elliptic Curve Isogeny
Symmetric key Quantum Resistance
Code
Multivariate
Post Quantum Cryptography Algorithms
Quantum Authentication Algorithms
QR-PUF
PUF-HB
Quantum-Secure
Continuous variable
Physical
Post Quantum Cryptography (PQC)
Side Channel
Cache
Timing analysis
Fault Analysis
Power Analysis
Electro-magnetic Emission
Post Quantum Cryptography Primitives
Attacks
Quantum PUFs
Quantum TRNG

Figure 2.2: Post Quantum Cryptography with its related areas (Post Quantum cryptography primitives, PQCalgorithms, Quantum authentication algorithms, attacks)

➢ **Key Encapsulation Schemes (Key Encapsulation Schemes-KEM)[5]:** This type of methodology is an encrypted way for two different parties to acquire the exact same confidential key incorporating an asymmetrical cryptographic approach. Various approaches are used which are as following-

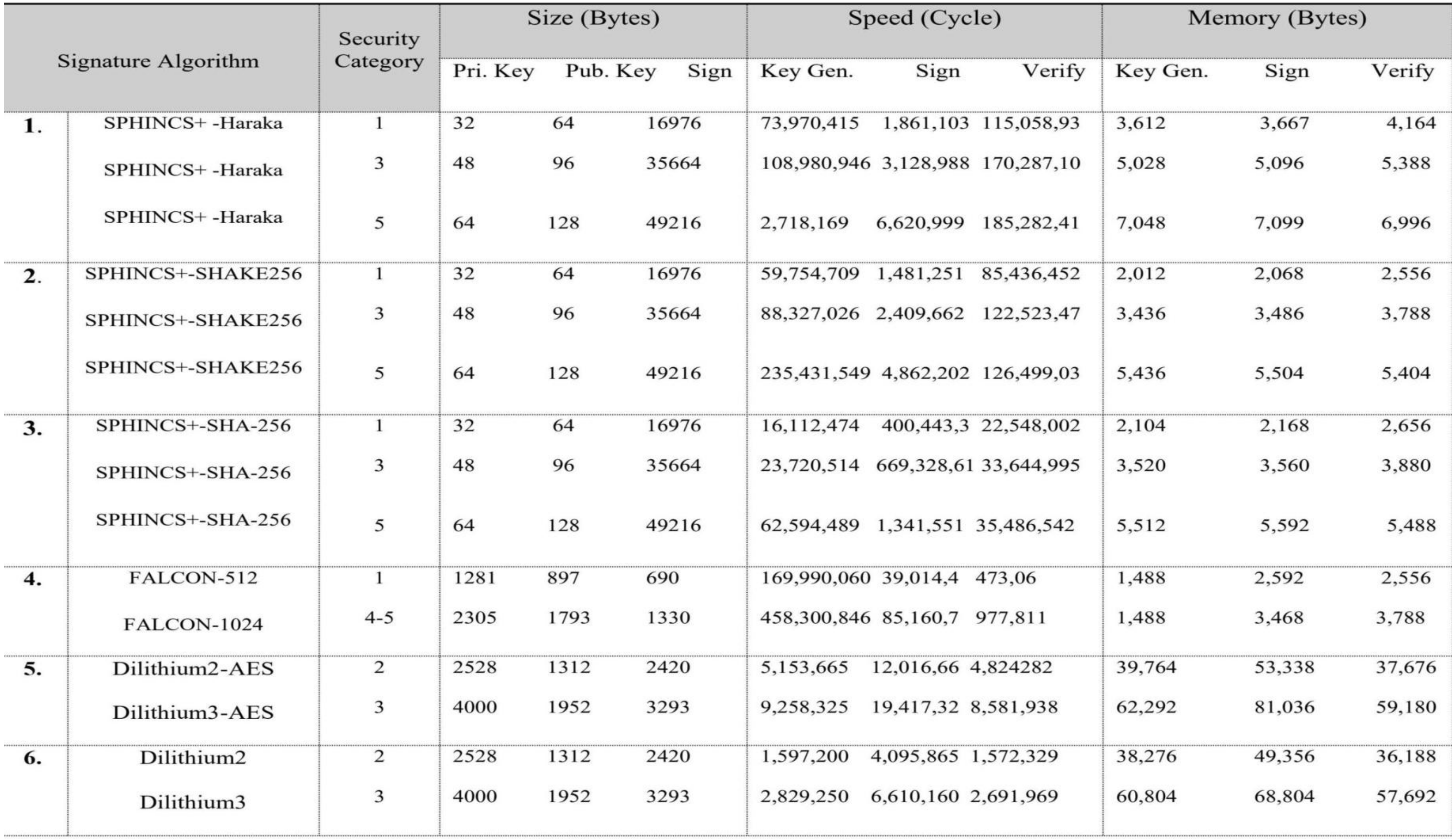
CRYSTALS: Kyber: -Kyber is a key encapsulation mechanism from the CRYSTALS initiative that has been engineered to endure crypto-analytic assaults from quantum computing systems. It is implemented to support two collaborators in communication with establishing mutual confidence and confidentiality when confronted with an Indistinguishable for non-adaptive strategies and adaptive selected Ciphertext Assault in the exchange of information. The core concepts of this asymmetric system of cryptography rely on Module-LWE problems, which are presumably an Non Polynomial time-hard(NP-hard) lattice issue.There are three various degrees of difficulty to access Kyber (Kyb), each with a unique set of individualized qualities to a particular level of security, which are as follows;

- Kyb-512
- Kyb-768
- Kyb-1024

➢ **Post-Quantum Signatures Styles:** Digital signatures are used nowadays which are more efficient with Post-Quantum systems[5].Different schemes are used which are as follows;

- CRYSTALS-Dilithium (Lattice based)
- SPHINCS+ (Stateless hash -based)
- FALCON (Rapid Fourier sampling and lattice based)

Table2.2: Evaluating Various NIST Standard Post-Quantum Signatures



Signature Algorithm		Security Category	Size (Bytes)			Speed (Cycle)			Memory (Bytes)		
			Pri. Key	Pub. Key	Sign	Key Gen.	Sign	Verify	Key Gen.	Sign	Verify
1.	SPHINCS+ -Haraka	1	32	64	16976	73,970,415	1,861,103	115,058,93	3,612	3,667	4,164
	SPHINCS+ -Haraka	3	48	96	35664	108,980,946	3,128,988	170,287,10	5,028	5,096	5,388
	SPHINCS+ -Haraka	5	64	128	49216	2,718,169	6,620,999	185,282,41	7,048	7,099	6,996
2.	SPHINCS+-SHAKE256	1	32	64	16976	59,754,709	1,481,251	85,436,452	2,012	2,068	2,556
	SPHINCS+-SHAKE256	3	48	96	35664	88,327,026	2,409,662	122,523,47	3,436	3,486	3,788
	SPHINCS+-SHAKE256	5	64	128	49216	235,431,549	4,862,202	126,499,03	5,436	5,504	5,404
3.	SPHINCS+-SHA-256	1	32	64	16976	16,112,474	400,443,3	22,548,002	2,104	2,168	2,656
	SPHINCS+-SHA-256	3	48	96	35664	23,720,514	669,328,61	33,644,995	3,520	3,560	3,880
	SPHINCS+-SHA-256	5	64	128	49216	62,594,489	1,341,551	35,486,542	5,512	5,592	5,488
4.	FALCON-512	1	1281	897	690	169,990,060	39,014,4	473,06	1,488	2,592	2,556
	FALCON-1024	4-5	2305	1793	1330	458,300,846	85,160,7	977,811	1,488	3,468	3,788
5.	Dilithium2-AES	2	2528	1312	2420	5,153,665	12,016,66	4,824282	39,764	53,338	37,676
	Dilithium3-AES	3	4000	1952	3293	9,258,325	19,417,32	8,581,938	62,292	81,036	59,180
6.	Dilithium2	2	2528	1312	2420	1,597,200	4,095,865	1,572,329	38,276	49,356	36,188
	Dilithium3	3	4000	1952	3293	2,829,250	6,610,160	2,691,969	60,804	68,804	57,692

3. **Internet of Things and IOT with Quantum Technology (Q-IOT) Systems:** The genuine technologically equipped Network among all the networks, the Internet of Things, is an actual network, not an assumption. But it will be more efficacious if we consolidate it with quantum technology.

The conditions for this type of architecture are as follows-

- About Quantum states
- Random values with classical key and angles
- 2 qubits (For Q-communication)

The architecture for quantum IOT network[10] consists of four layers which is more effective and standardized; stated as follows;

- **Application Layer:** The engagement between the end user and quantum IOT networking commences at this layer. When the client wants to interface with the next layer, qubits are conveyed (instead of conventional bits).

- **Quantum Teleportation Layer:** The quantum teleportation framework makes utilization of quantum dependent repeaters to safeguard the authenticity of the quantum states (Qubit states) being transmitted to it and upwards qubits on to the subsequent hop.

- **Quantum Network Layer:** This layer mainly consists of two main parts –

- **Quantum Server:** Quantum server accommodates a quantum-based device that interprets and supervises all functions pertaining to quantum data as well as the reconfiguration of conventional bits into quantum bits and conversely.

- **Gateway:** A tunnel that facilitates the transfer of classical bits to a quantum server between the physical layer and the quantum network layer.

- **Physical Layer:** All the IOT devices, sensors and other components are put in this physical layer. It helps in the transferring of data between the layers.

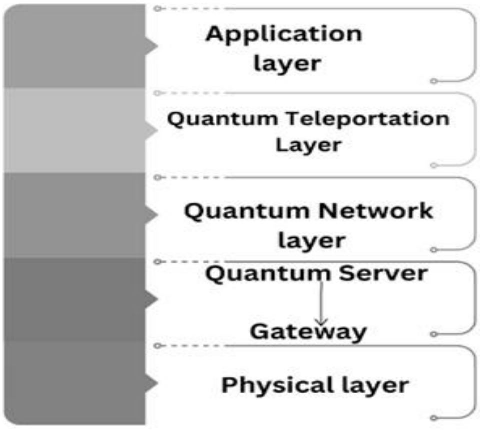


Figure 2.3: Quantum -Internet of Things Network structure

We have proposed a Quantum based IOT system model which is shown in Fig.3.2. An IoT network can have a quantum based main server, like a gateway, that performs all the quantum operational processes and propagates the conventional documentation to the IOT ecosystem, instead of designating every gadget on the network - aQuantum-controlled system. All quantum procedures will be accomplished on the server point side; a central server will oversee supervising the establishment and quantification of qubits, segregation of quantum systems, and network coverage with different external networks.

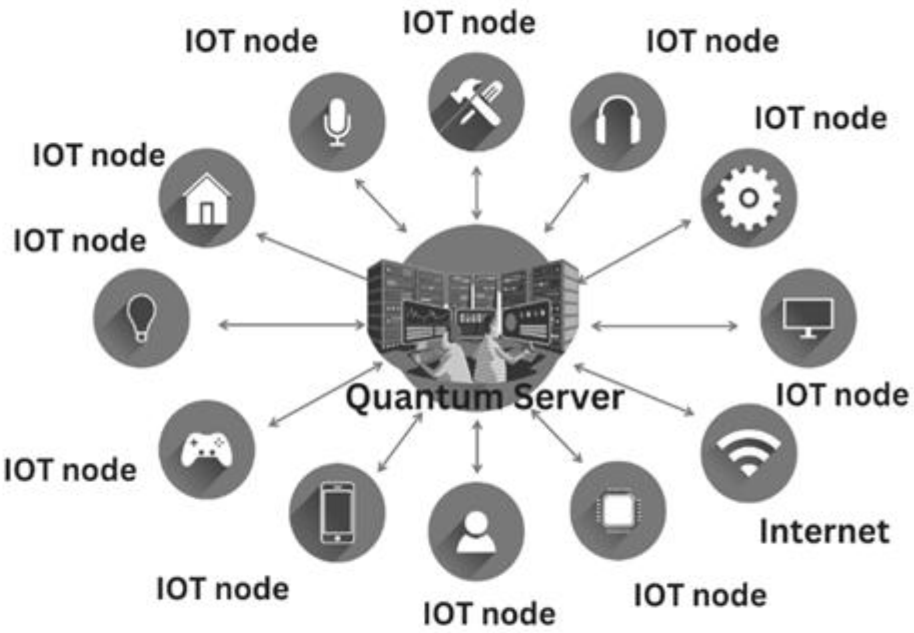


Figure 2.4: Proposed System of Quantum IOT based System

Quantum innovations and Quantum-based cryptology are enabling technologies that are blooming in every profession. They are currently still in the exploratory phase rather than being deployed in day-to-day real-world implementation applications. IoT devices with Quantum integration can generate several hurdles in this scenario that must be rectified to benefit both the present as well as the future. Since quantum computing continues to be in the exploratory and developmental stages, we must stay vigilant to how it is being formulated. The slow key generation challenge is the next stumbling block, and we need to come up with brainstorming ways to reconfigure post-quantum key generation techniques[10] for lowering power consumption.

The most recent IOT-ICT paradigms are as follows:

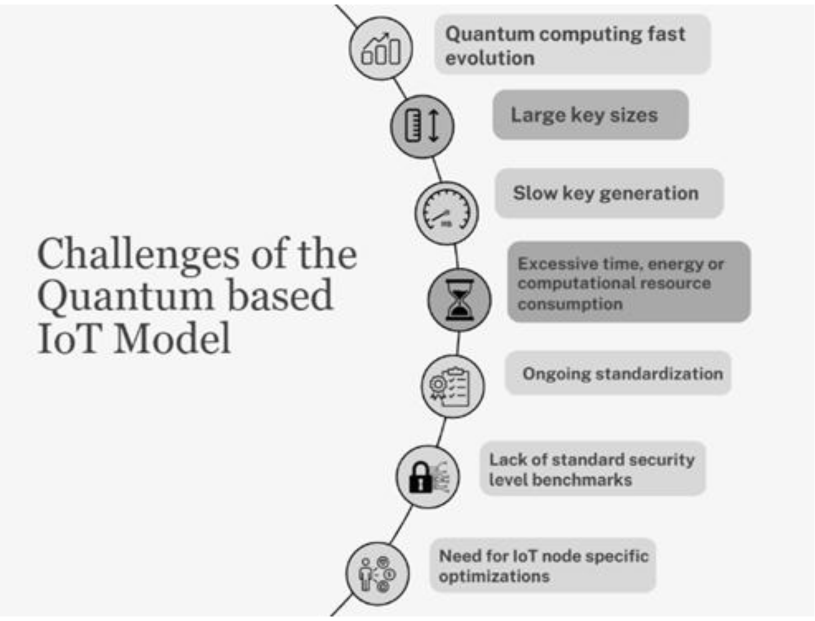
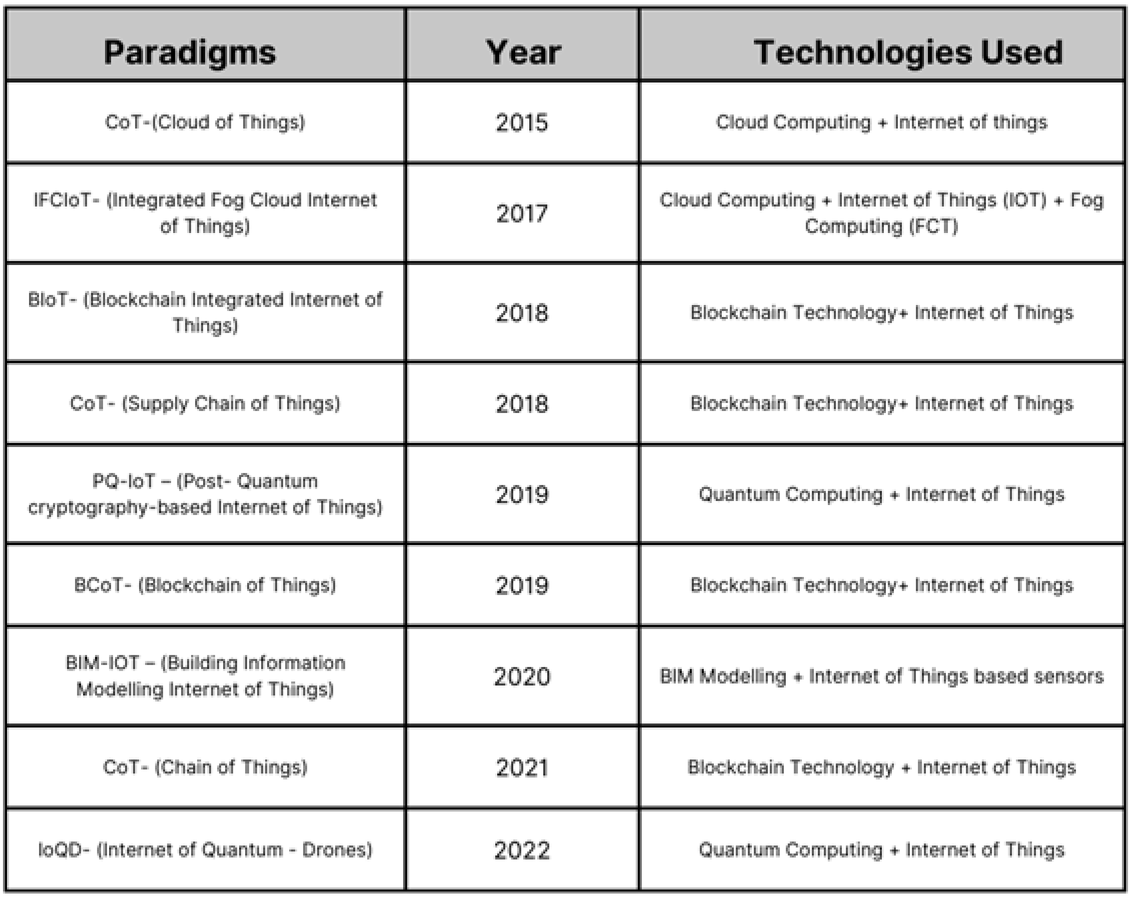

Challenges of the Quantum based IoT Model
Quantum computing fast evolution
Large key sizes
Slow key generation
Excessive time, energy or computational resource consumption
Ongoing standardization
Lack of standard security level benchmarks
Need for IoT node specific optimizations

Figure 2.5: Q-IOT Challenges in the Future World

Table 2.3. Different Versions of IOT (Integration of Information Communication Technologies with Internet of Things Paradigms



Paradigms	Year	Technologies Used
CoT-(Cloud of Things)	2015	Cloud Computing + Internet of things
IFCIoT- (Integrated Fog Cloud Internet of Things)	2017	Cloud Computing + Internet of Things (IOT) + Fog Computing (FCT)
BIoT- (Blockchain Integrated Internet of Things)	2018	Blockchain Technology+ Internet of Things
CoT- (Supply Chain of Things)	2018	Blockchain Technology+ Internet of Things
PQ-IoT – (Post- Quantum cryptography-based Internet of Things)	2019	Quantum Computing + Internet of Things
BCoT- (Blockchain of Things)	2019	Blockchain Technology+ Internet of Things
BIM-IOT – (Building Information Modelling Internet of Things)	2020	BIM Modelling + Internet of Things based sensors
CoT- (Chain of Things)	2021	Blockchain Technology + Internet of Things
IoQD- (Internet of Quantum - Drones)	2022	Quantum Computing + Internet of Things

III. THE COMBINING RESULTS OF QUANTUM COMPUTING(QC),BLOCKCHAIN TECHNOLOGY(BC), INTERNET OF THINGS(IOT) -QCOT TECHNOLOGY

The internet of things, Blockchain, and quantum innovations, obstacles, implementations, and related publications are addressed in the preceding subsection. Ergo, in this research, we have created a framework called QCOT that incorporates multiple formidable technologies: blockchain, which boosts IOT confidentiality, and quantum computing, that can offer unparalleled safety and enormous computational competence.
The most important features of this proposed model are as follows[1]

1. Proper verification of Computations.
2. Maintaining the integration of data (Before
3. storing).
4. QC and BC based IoT applications are now fully secured.
5. Decentralized way of IOT applications.
6. Quantum resistance technology is implemented instead of quantum-based computers.
7. Much Secure communication.

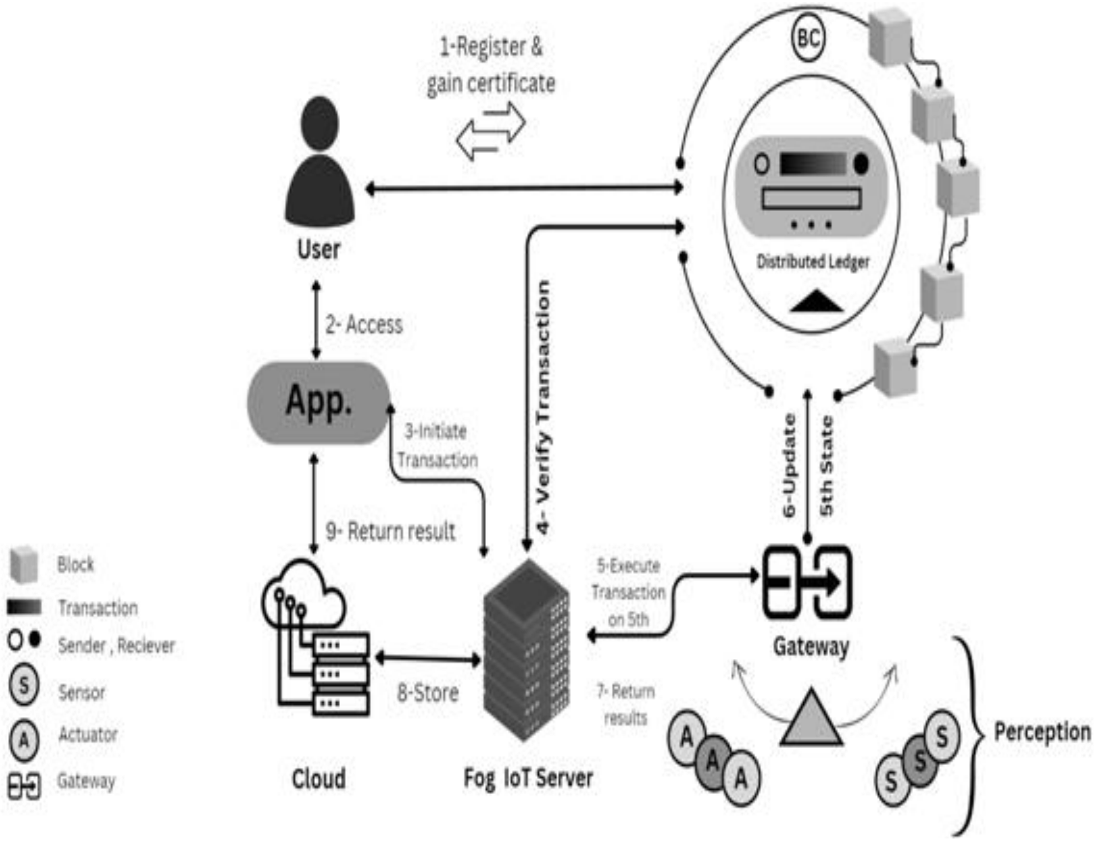


Figure 3.1: Proposed Architectural Model of QCoT Technology (Quantum Chain of Things)

Table3.1: Various IOT Systems based on Post Quantum Blockchain

No.	**Application**	**Structure**	**Blockchain Type**	**Consensus Mechanism**	**Cryptosystem Type**	**Cryptosystem Sub-type**	**Contribution**	**Missing Aspect**
1.	Smart City	Blockchain	Public	PoW(Proof Of Work)	Multi-variate	Identity-based	Presenting a shorter block interval generation (compared with Bitcoin) and more lightweight	Need of scalability and there is high computational cost with implementation as well as for evaluation.
2.	Smart Home	Blockchain	Consortium	PoW(Proof Of Work)	Lattice	SVP	Considering cloud server with a subunit of consortium blockchain (Helps in controlling the amount of data)	Dependent on a cloud server, high computational cost, low transaction speed, semi-centralized
3.	Smart Farming	DAG	Private	PoW(Proof Of Work)	Hash	W-OTS(Winternitz One time signature)	Used for medium-large sized farms	Peer and coordinator nodes dependent and less decentralized

4.	Internet of vehicles(IoV)	Blockchain	Consortium	BFT	Lattice	ISIS	Gives good communication and computation performance in systems	Not scalable at a higher level and also risky
5.	Social IOT(SIoT)	Blockchain	No mention	No mention	Multi-variate	Ring signature	Privacy and confidentiality extended in the systems	Not used in real time
6.	Internet of vehicles (IoV)	DAG	Private	PoW(Proof of work)	Lattice	Ring-LWE Dilithium	For implementing IOV systems, Dilithium signatures are used very efficiently.	Not for limited resource devices
7.	General IoT	Blockchain	No mention	No mention	Lattice	NTRU	For shorter transaction size ,we presented a best scalable structure used in the system.	Not experimentally evaluated
8.	General IoT	Data Ledger	No mention	No mention	Hash	OTS(One Time signature)	Reduces key and signature sizes	Not experimentally evaluated and not for limited resources

The table 3.1. shows the comparison between the different post quantum blockchain based IOT Styles which differentiates the styles based on application, DL structure, post-quantum signatures types as well as subtypes [5] [41].

QKD (Quantum key distributions) algorithms are incorporated into the proposed model of QCOT technology to mitigate espionage(eavesdropping) at the physical layer (in the IOT subsystem of the approach). In the client-server configuration (communicating parties), bits and data are interchanged on a quantum core principle[1] [44].. One-way hashing strategies (hash key) are deployed by the receiving antenna (or server) for relatively secure transmission and connection. The QCoT initiative resulted in meagre public and private key ratios, size minimization of hash length, and fulfilling the CIA's performance standards (Confidentiality, Integrity, and Authorization) which are the major challenges in the historical works. Quantum teleportation, which unfolds between the layer upon layer and facilitates highly secure data transmission, is another strategy executed in the framework [45]. A QISKIT-based quantum simulator that is compatible with quantum circuit design and has a plethora of simulation features and configuration-modifying functions accomplishes this technique.[1]

IV. RESEARCH CHALLENGES AND OPPORTUNITIES DIRECTIONS

There are various challenges and opportunities that arises from the amazing convergence of quantum Technology, internet of things and blockchain(BC) [5] [46]. The opportunities are the various domains which are as follows;

1. Large key as well as signature size
2. Post Quantum Blockchain (PQBs)
3. Energy and computational Cost
4. Shared security and security threats (Threshold Signatures)
5. Scalability (Aggregate signature and public key recovery)
6. Data Management
7. Privacy with respect to Transparency

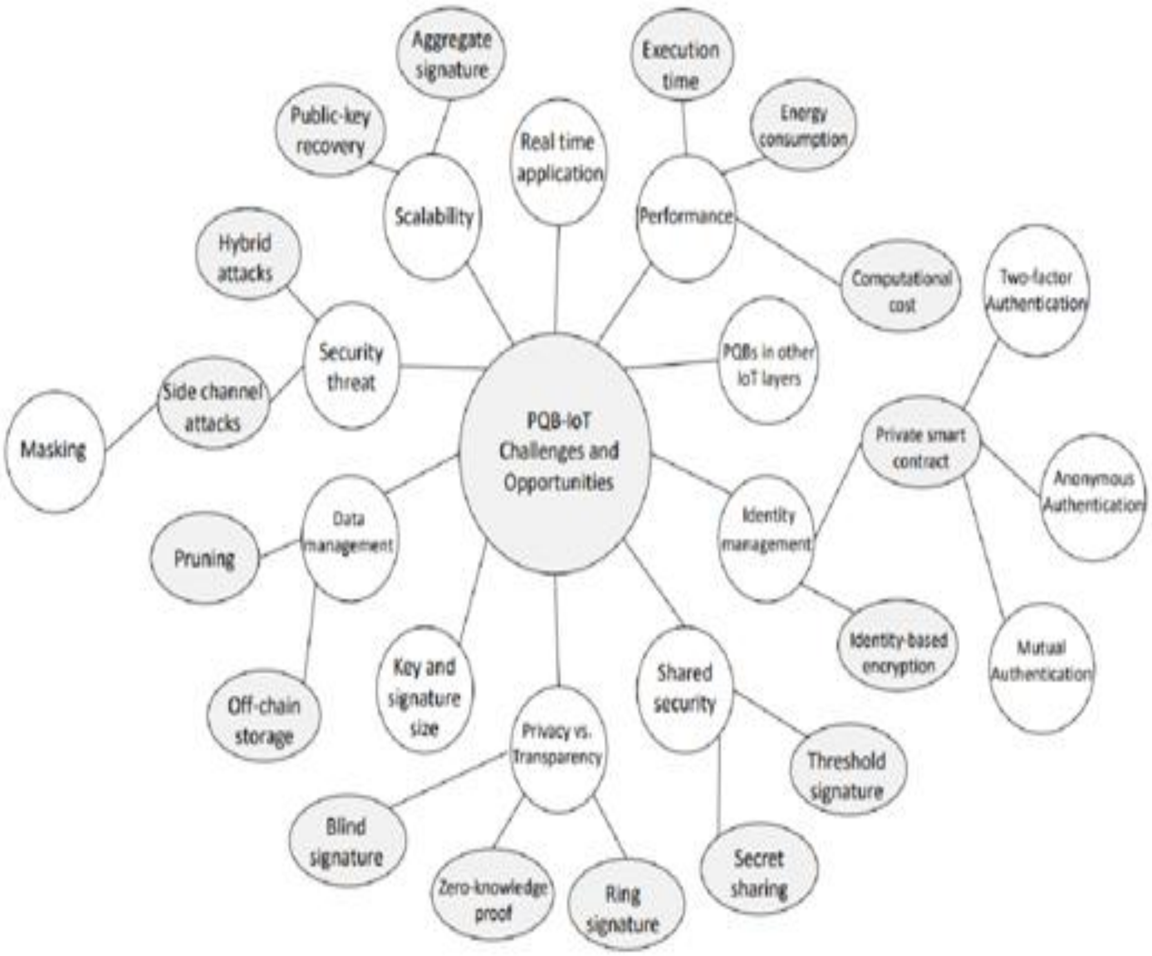


Figure 4.1: Various Challenges and Research Opportunities for QCOT Systems (Quantum Chain Of Things)

V. APPLICATIONS OF THE RECOMMENDED LAYOUT–QCOT SYSTEM

This model has the highest applications including the applications of three powerful technologies (internet of Things, blockchain(BC) World, and quantum computing(QC) (post-quantum Technology)). The following are the wonderful applications of QCoT world with real-world[1]: -

1. **In the Health Care World :** Everyone knows that the public healthcare system and services are extremely pertinent and vulnerable, and they pressingly need to be energized and productive. It is simple to make improvements to the hospitals and healthcare framework's confidentiality (safeguarding against different real-time assaults and eavesdropping) by incorporating quantum computing in health care [7] [42].

   Blockchain and quantum technology solutions make it simple to succeed in creating patient-based systems that are exceedingly advantageous to patients. But the major challenges which we are facing with blockchain-quantum based are effectively solvable with the help of QCoT technology like;

- Using quantum computing on a massive scale would not be favorable for the healthcare industry (not environmentally effective). So, we must incorporate it with other efficacious technologies.

- Only the integrated version (i.e., QCoT) can stabilize the potentiality in actual world to assemble the QC infrastructure and resources, specifically for the leading developed countries.

- With the intervention of QCoT technology, the challenge with the exchanging of electronic health records (EHR) between the organizations is accomplished [47].

2. **In Digital(Smart Cities):** The main challenges occurred with establishment and management of digitaltowns and cities with respect to CIAs are as follows;

- **Confidentiality:** Disclose of sensitive data and information by an illegal party or user.

- **Integrity:** Integrity problem is Manipulationand modifications in data by an unauthorized person.

- **Authorization:** Reluctance on behalf of the associated entity to pass along or receive an informational message [4] [48].

Security assaults have tremendously increased as the proliferation of smart connected cities and the records they accumulate (using many sensors) has been extended (through various apps and devices). Many blockchain concepts are used, yet they aren't very advantageous, specifically for the foreseeable. We need an optimized methodology, which QCoT Technology brings (Most secure version in technology). This technology can manage all the items extremely in an efficient manner and can safeguard everything.

3. **In Drone Industry:** The latest innovative industry, which is continuously expanding, is the drone industry. UAVs are implemented in every business; yet again, security showcases the biggest challenge. A remedy for this is proffered by QCoT, which incorporates use of very cutting-edge technologies including quantum blockchain (Quantum Block), Quantum based AI(Artificial Intelligence), Quantum-inspired interactions, and Digital Twin (Quantum based) [18] [43].

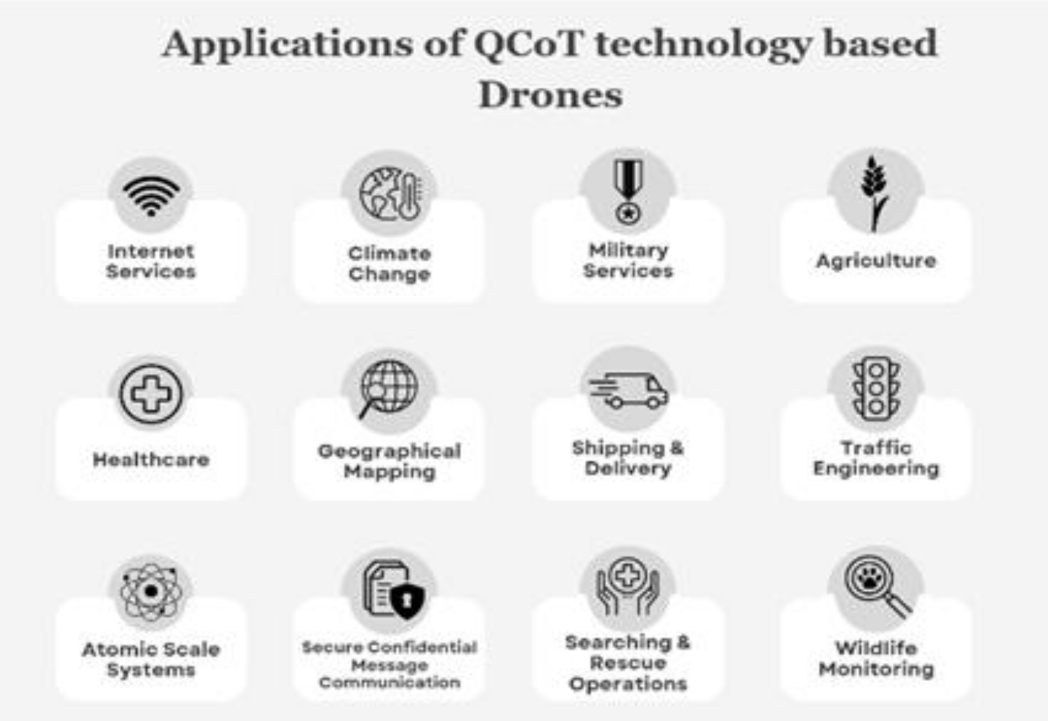


Figure 5.1: Applications of the QCoT Technology-Based Drones in Various Industries

VI. CONCLUSION

The present status of technical research, approaches adopt quantum blockchain architectures, blockchain-based IOT Smart devices, and different issues with this strategy are all covered in this research. Quantum Chain of Things (QCoT) technology, which provides an approach to all the vulnerabilities concerning the safety of the CIA and many more, is the integrated model that is being recommended. If we employ the evolving technologies individually, this is less effective, and we must overcome the difficulties brought on by that. A model that incorporates all three technologies results in fewer issues and new, improved applications for every industry (like in health care, educational sector, drone industry, retail, and ecommerce industry and many more). The suggested system is currently simply an architectural model that is still being explored and put into practice. Regrettably, it will result in improved achievements in terms of privacy, computing efficiency, networking, and storage capacity.

REFERENCES

[1] Younan, Mina, Mohamed Elhoseny, Abdelmgeid A. Ali, and Essam H. Houssein. "Quantum Chain of Things (QCoT): A New Paradigm for Integrating Quantum Computing, Blockchain, and Internet of Things." In 2021 17th International Computer Engineering Conference (ICENCO), pp. 101-106. IEEE, 2021.

[2] Habib, Gousia, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Shaima Qureshi, and Malik Ishfaq. 2022. "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing" Future Internet 14, no. 11: 341. https://doi.org/10.3390/fi14110341

[3] Bova, F., Goldfarb, A. &Melko, R.G. Commercial applications of quantum computing. EPJ Quantum Technol. 8, 2 (2021). https://doi.org/10.1140/epjqt/s40507-021-00091-1

[4] Gill, Sukhpal Singh, Shreshth Tuli, Minxian Xu, Inderpreet Singh, Karan Vijay Singh, Dominic Lindsay, Shikhar Tuli et al. "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges." Internet of Things 8 (2019): 100118.

[5] Gharavi, Hadi (2023): Post Quantum Blockchain Security for the Internet of Things Survey and Research Directions. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.22821692.v1

[6] Ebrahimi, Shahriar, Siavash Bayat-Sarmadi, and HatamehMosanaei-Boorani. "Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT." IEEE Internet of Things Journal 6, no. 3 (2019): 5500-5507.

[7] Qadri, Yazdan Ahmad, Ali Nauman, Yousaf Bin Zikria, Athanasios V. Vasilakos, and Sung Won Kim. "The future of healthcare internet of things: a survey of emerging technologies." IEEE Communications Surveys & Tutorials 22, no. 2 (2020): 1121-1167.

[8] Fraga-Lamas, Paula, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo, and Miguel González-López. "A review on internet of things for defense and public safety." Sensors 16, no. 10 (2016): 1644.

[9] Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." In 2016 2nd international conference on contemporary computing and informatics (IC3I), pp. 463-467. IEEE, 2016.

[10] 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), Dhaka, Bangladesh, 2019, pp. 269-272, doi: 10.1109/ICREST.2019.8644342.

[11] Suhail, Sabah, Rasheed Hussain, Abid Khan, and Choong Seon Hong. "On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions." IEEE Internet of Things Journal 8, no. 1 (2020): 1-17.

[12] Hassija, Vikas, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and BiplabSikdar. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

[13] Dahmen, Erik, KatsuyukiOkeya, Tsuyoshi Takagi, and Camille Vuillaume. "Digital signatures out of second-preimage resistant hash functions." In Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 Proceedings 2, pp. 109-123. Springer Berlin Heidelberg, 2008.

[14] McEliece, Robert J. "A public-key cryptosystem based on algebraic." Coding Thv 4244 (1978): 114-116.

[15] Humble, Travis. "Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications." IEEE Consumer Electronics Magazine 7, no. 6 (2018): 8-14.

[16] Alagic, Gorjan, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu et al. "Status report on the second round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST 2 (2020).

[17] Dang, Viet B., FarnoudFarahmand, Michal Andrzejczak, Kamyar Mohajerani, Duc T. Nguyen, and Kris Gaj. "Implementation and benchmarking of round 2 candidates in the NIST post-quantum cryptography standardization process using hardware and software/hardware co-design approaches." Cryptology ePrint Archive: Report 2020/795 (2020)..

[18] A. Kumar et al., "Survey of Promising Technologies for Quantum Drones and Networks," in IEEE Access, vol. 9, pp. 125868-125911, 2021, doi: 10.1109/ACCESS.2021.3109816.

[19] Bogomolec, Xenia, John Gregory Underhill, and StiepanAurélien Kovac. "Towards post-quantum secure symmetric cryptography: A mathematical perspective." Cryptology ePrint Archive (2019).

[20] Passian, Ali, Gilles Buchs, Christopher M. Seck, Alberto M. Marino, and Nicholas A. Peters. "The Concept of a Quantum Edge Simulator: Edge Computing and Sensing in the Quantum Era." Sensors 23, no. 1 (2023): 115.

[21] Hülsing, Andreas, Joost Rijneveld, and Fang Song. "Mitigating multi-target attacks in hash-based signatures." In Public-Key Cryptography–PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I, pp. 387-416. Springer Berlin Heidelberg, 2016.

[22] Bavdekar, Ritik, Eashan Jayant Chopde, Ashutosh Bhatia, Kamlesh Tiwari, and Sandeep Joshua Daniel. "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research." arXiv preprint arXiv:2202.02826 (2022).

[23] Pulipeti, Srikanth, and Adarsh Kumar. "Secure quantum computing for healthcare sector: A short analysis." Security and Privacy: e293.

[24] Ayoade, Olawale, Pablo Rivas, and Javier Orduz. "Artificial Intelligence Computing at the Quantum Level." Data 7, no. 3 (2022): 28.

[25] Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks." IEEE access 8 (2020): 21091-21116.

[26] Gao, Yu-Long, Xiu-Bo Chen, Yu-Ling Chen, Ying Sun, Xin-Xin Niu, and Yi-Xian Yang. "A secure cryptocurrency scheme based on post-quantum blockchain." Ieee Access 6 (2018): 27205-27213..

[27] Sun, Xin, Mirek Sopek, Quanlong Wang, and Piotr Kulicki. "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic." Entropy 21, no. 9 (2019): 887.

[28] Bhatia, Munish, and Sandeep K. Sood. "Quantum computing-inspired network optimization for IoT applications." IEEE Internet of Things Journal 7, no. 6 (2020): 5590-5598.

[29] Alagic, Gorjan, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu et al. "Status report on the first round of the NIST post-quantum cryptography standardization process." (2019).

[30] Li, Shancang, Li Da Xu, and Shanshan Zhao. "The internet of things: a survey." Information systems frontiers 17 (2015): 243-259.

[31] B. Farahani, F. Firouzi, and M. Luecking, “The convergence of iot and distributed ledger technologies (dlt): Opportunities, challenges, and solutions,” Journal of Network and Computer Applications, vol. 177, p. 102936, 2021.

[32] S. Singh, A. S. Hosen, and B. Yoon, “Blockchain security attacks, challenges, and solutions for the future distributed iot network,” IEEE Access, vol. 9, pp. 13 938–13 959, 2021.

[33] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, “A secure cryptocurrency scheme based on post-quantum blockchain,” IEEE Access, vol. 6, pp. 27 205–27 213, 2018.

[34] Kumar, R., Khanna, R., & Kumar, S. (2022). Technological Transformation of Middleware and Heuristic Approaches for Intelligent Transport System. Autonomous Vehicles Volume 1: Using Machine Intelligence, 61-82.

[35] Kumar, R., Soni, P., Aggarwal, A., Kumar, M., & Mishra, N. (2022). An Analytical Approach for Sustainable Development in Smart Society 5.0 Using Swasthya Sahayak Application. In Decision Analytics for Sustainable Development in Smart Society 5.0: Issues, Challenges and Opportunities (pp. 131-152). Singapore: Springer Nature Singapore.

[36] Keshav Garg, R. K., Gupta, A., & Nirwal, A. (2022). What and why you need to know about Non-Fungible Tokens (NFTs). International Journal of Scientific Research in Engineering and Management, 6(6), 1-4. Retrieved from https://ijsrem.com/download/what-and-why-you-need-to-know-about-non-fungible-tokens-nfts/

[37] Chatha, D., Aggarwal, A., & Kumar, R. (2022). Comparative Analysis of Proposed Artificial Neural Network (ANN) Algorithm With Other Techniques. In Research Anthology on Artificial Neural Network Applications (pp. 1218-1223). IGI Global.

[38] Kumar, R., Khanna, R., & Kumar, S. (2021). Vehicular middleware and heuristic approaches for intelligent transportation system of smart cities. In Cognitive Computing for Human-Robot Interaction (pp. 163-175). Academic Press.

[39] Kumar, R., Khanna, R., & Kumar, S. (2018). Deep learning Integrated approach for collision avoidance in Internet of Things based smart vehicular networks. Journal of Advanced Research in Dynamical and Control Systems, 10(14), 1508-1512.

[40] Kumar, R., Khanna, R., & Kumar, S. (2018). An effective framework for security and performance in Intelligent Vehicular ad-hoc network. Journal of Advanced Research in Dynamical and Control System, 10(14), 1504-1507.

[41] Kumar, R., & Kumar, R. (2016). A Comparative Analysis of Performance Metrics of Different Cloud Scheduling Techniques. International Journal of Innovations in Engineering & Technology, 7(2), 222-226. ISSN: 2319-1058.

[42] Sardana, S., & Kumar, R. (2016). Energy Efficient Target Tracking in Wireless Sensor Networks. International Journal of Innovations in Engineering & Technology, 7(2), 271-275. ISSN: 2319-1058.

[43] Gupta, G., & Kumar, R. (2016). Acoustic Channel Modeling and Simulation for Underwater Acoustic Wireless Sensing Networks. International Journal of Computer Applications, 975, 8887.

[44] Kumar, R., Khanna, R., & Verma, P. K. (2014). Middleware Architecture of VASNET and Its Review for Urban Monitoring & Vehicle Tracking. International Journal of Emerging Research in Management & Technology, 3(1), 41-45.

[45] Garg, T., Kumar, R., & Singh, J. (2013). A way to cloud computing basic to multitenant environment. International Journal of Advanced Research in Computer and Communication Engineering, 2(6), 2394-2399.

[46] Kumar, R., Khanna, R., & Kumar, S. (2013). A Proposed work on Node Clustering & Object Tracking Processes of BFOA in WSN. International Journal of Computer Science & Communication, 4(2), 207-212.

[47] Kumar, R., Verma, P. K., & Verma, P. K. (2012). Role of Information Communication Technology and its Impact on Health Sector. ijarcs, 1(2), 122-125.

[48] Kumar, R., & Batra, A. (2011). Employing Grid Comparative Strategies in Cloud Computing. IJCSIT-ISSN 0**975-9646, 2(5), 2246-2253.**