

Review Article

Quantum-Secure IoT Networks for the 6G Era: Post-Quantum Cryptography, Blockchain Integration, and Trust Architectures - A Comprehensive ReviewKarthik Kumar Vaigandla^{1,*}¹Associate Professor, Department of Electronics and Communication Engineering, Balaji Institute of Technology and Science, Warangal, Telangana, -506331, India.Corresponding Author: Karthik Kumar Vaigandla. Email: ykvaigandla@gmail.com

Received: 11/05/2025; Revised: 18/09/2025; Accepted: 25/09/2025; Published: 30/09/2025.

DOI: <https://doi.org/10.69996/jsihs.2025014>

Abstract: The rapid convergence of sixth-generation (6G) networks and the Internet of Things (IoT) offers enormous potential for ultra-reliable, low-latency, and massive device connectivity. However, this integration also raises security and privacy concerns, particularly in light of new threats from quantum computing that could undermine traditional cryptography. The architecture of quantum-safe IoT networks that can withstand post-quantum security threats is thoroughly discussed in this review. It addresses the challenges related to how to use blockchain technology to provide decentralized trust as well as secure transactions, how to use post-quantum cryptographic algorithms to protect data confidentiality, and the best way to use a trust management architecture to improve identity verification, authorization, and authentication in the diverse IoT environment. The paper then examines scalability considerations, resource constraints, and interoperability problems that impact safe IoT deployments in the 6G era. This work serves as a roadmap for researchers and practitioners who aim to create robust and future IoT infrastructure and then maintain their security in a post-quantum world by integrating recent research patterns, solution development, and considerations related to real-world implementation.

Keywords: 6G, IoT, Quantum computing, Blockchain, security

1.Introduction

A constant push for faster data rates, reduced latency, and increased connectivity has characterized the development of wireless communication. With data rates in the terabit-per-second range, sixth-generation (6G) networks are expected to outperform 5G by providing massive machine-type communication (mMTC), enhanced mobile broadband (eMBB), and ultra-reliable low-latency communication (URLLC). Numerous uses will be made possible by these developments, ranging from immersive extended reality and precision healthcare to industrial automation and driverless vehicles. In order to enable the smooth interconnection of billions of devices, sensors, and actuators across various domains, 6G infrastructure will be deeply integrated with the Internet of Things (IoT), a crucial enabler of such applications [1].

IoT has enormous potential in the 6G era, but this integration also increases cybersecurity risks. An extensive and ever-changing attack surface is produced by the IoT nodes' extreme size, diversity, and mobility. The advent of quantum computing presents an unprecedented challenge to traditional security measures, which mainly rely on public-key cryptographic algorithms like RSA and elliptic-curve cryptography (ECC). Current key exchange, authentication, and digital signature systems could be rendered ineffective by quantum algorithms, especially Shor's



algorithm, which has the ability to crack popular asymmetric cryptosystems. Consequently, adversaries with quantum capabilities may be able to access sensitive IoT-generated data, private communications, and critical infrastructures [2].

A fundamental change toward security measures that are impervious to quantum attacks is necessary to mitigate these threats. One important remedy is post-quantum cryptography (PQC), which provides cryptographic schemes based on mathematical problems that are thought to be impervious to both classical and quantum computational attacks. Promising PQC categories include cryptosystems based on lattices, codes, hashes, multivariate polynomials, and isogeny. However, there are new difficulties in integrating them into IoT systems, such as compatibility with devices with limited resources, communication overhead, and computational complexity. The trade-offs between security, efficiency, and scalability must be carefully considered when choosing and implementing appropriate PQC algorithms in 6G-enabled IoT networks [3].

At the same time, blockchain technology has drawn interest as a way to improve integrity, transparency, and trust in decentralized IoT ecosystems. Multiple stakeholders can verify and record transactions in a way that is resistant to tampering thanks to blockchain's distributed ledger framework, which does away with the need for centralized control. Blockchain can offer two layers of protection when paired with PQC: it can protect transaction data from quantum attacks while maintaining integrity through decentralized consensus processes. Additionally, without depending on centralized authorities, blockchain-based smart contracts can automate access control, device onboarding, and security policies. Blockchain integration in large-scale IoT systems presents challenges related to latency, storage needs, energy consumption, and network throughput, despite these benefits. These issues must be resolved in light of 6G performance requirements [4].

Another essential element in protecting quantum-resistant IoT networks is trust architectures. In dynamic environments, trust management entails evaluating the dependability and behavior of devices, nodes, and communication channels. Trust in IoT networks that span several administrative domains is dynamic and changes over time in response to contextual data, observed behavior, and previous interactions. The detection of malicious or compromised devices, the prevention of false data injection, and the requirement that only verified nodes engage in network operations are all necessary for effective trust models. Strong, self-sustaining security architectures that can adjust to the changing threat landscape of 6G IoT environments can be achieved by integrating trust mechanisms with PQC and blockchain frameworks [5].

There are considerable operational and technical obstacles in the way of the shift to quantum-secure IoT networks. First and foremost, processing power limitations, energy efficiency issues, and storage constraints must all be addressed when implementing PQC algorithms in constrained IoT devices. Second, without compromising performance, blockchain systems need to be tuned to manage the high transaction rates and widespread device participation anticipated in 6G networks. Thirdly, there is still a serious problem with interoperability across various hardware platforms, communication protocols, and security frameworks. Furthermore, the implementation of quantum-secure IoT solutions will be significantly influenced by changing regulatory frameworks and standardization initiatives. PQC standardization is already being advanced by groups like the National Institute of Standards and Technology (NIST), and initiatives akin to these will be required for integrated blockchain and trust architectures [6].

Quantum-resistant security measures in IoT networks have been the subject of several recent research projects; however, there is currently no thorough synthesis that connects PQC, blockchain integration, and trust architectures in the particular context of 6G [7]. By

methodically analyzing the most recent advancements, pointing out the advantages and disadvantages of current strategies, and emphasizing important research prospects, this review aims to close that gap. It discusses design considerations for blockchain-based secure frameworks, techniques for building adaptive trust in decentralized environments, and the fundamentals of post-quantum cryptography schemes appropriate for Internet of Things devices. The interaction of these three pillars is given particular attention because their deployment together has the potential to build secure IoT infrastructures that last well into the quantum era.

This review gives to make a reference for researchers, system architects, and industry professionals who are working to secure IoT infrastructures in anticipation of quantum computing breakthroughs by combining recent developments, useful considerations, and future research directions. As 6G networks develop and quantum computing capabilities advance over the next ten years, post-quantum cryptography, blockchain integration, and adaptive trust architectures will be essential for protecting the next generation of interconnected systems. The insights offered here are meant to serve as a roadmap for creating security frameworks that can withstand the revolutionary challenges posed by quantum technologies, in addition to being resilient to present threats.

2. Introduction to IoT

Everyday physical objects, from wearable health devices to industrial machinery and home appliances, are embedded with sensors, actuators, communication modules, and processing capabilities to sense, gather, and exchange data over interconnected networks. This is known as the IoT. The Internet of Things aims to establish an intelligent environment in which gadgets can communicate with one another on their own, react to environmental changes, and work together to provide the best possible services with the least amount of human involvement. IoT has developed over the last ten years from experimental implementations to a key element of contemporary communication systems, enabling applications in industries like environmental monitoring, smart cities, manufacturing, healthcare, precision agriculture, and transportation [8-10].

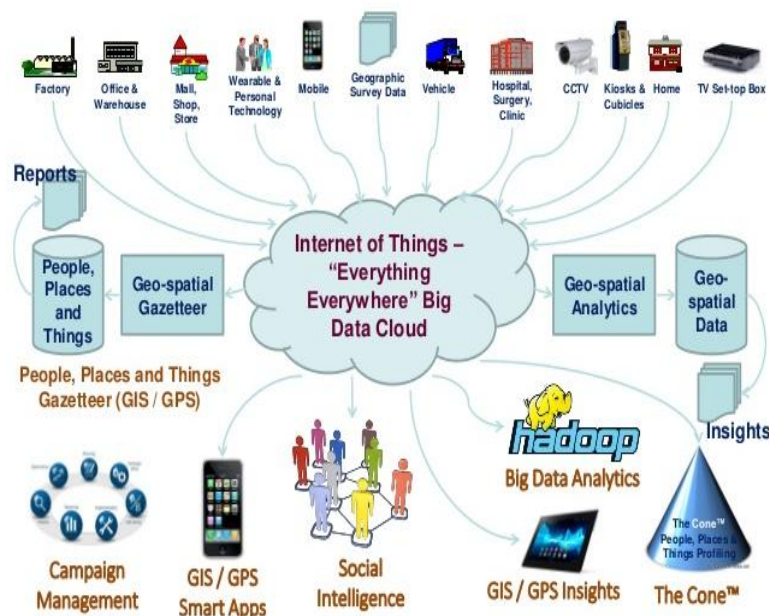


Figure 1: Internet Of Things- Connected Everything

2.1 Evolution and Fundamental Ideas

Devices in isolated, domain-specific systems connected by proprietary protocols or constrained local networks typified the first wave of IoT development [11]. Cross-domain interoperability was made possible by IoT systems' adoption of open communication standards, cloud-based platforms, and large-scale data analytics as a result of the Internet's growth and advancements in wireless technologies. IoT is fundamentally based on three principles:

- Ensuring that gadgets stay connected at all times and locations via a variety of communication channels, including Wi-Fi, cellular networks, Bluetooth, Zigbee, LoRa, and satellite links, is known as ubiquitous connectivity.
- Intelligent Processing: Using cloud-based analytics, edge computing, and embedded processors to process sensor data in real time and aid in decision-making.
- Context Awareness and Automation: Using historical patterns and real-time data to automate processes, make context-driven adjustments, and offer predictive insights.

IoT can grow from a few devices to billions of interconnected nodes thanks to these principles, which allow it to operate as a dynamic, adaptive, and service-oriented system.

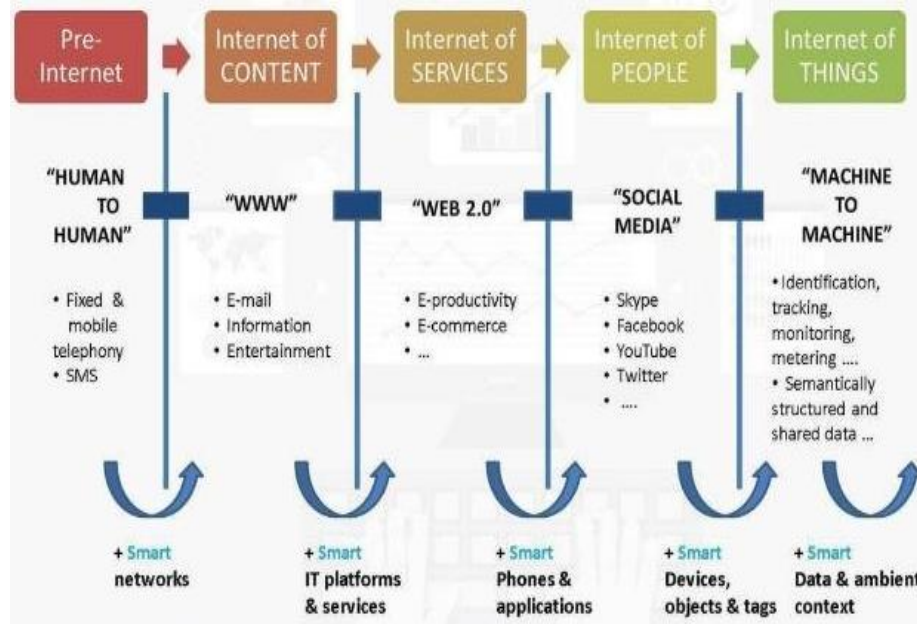


Figure 2: Evolution of IoT [12]

2.2 IoT System Architecture

Usually, there are several layers in an IoT ecosystem, each of which is in charge of a distinct set of tasks:

- Perception layer : It is made up of sensors, RFID tags, and actuators that gather environmental data, including biometric information, motion, temperature, location, and pressure.
- Network Layer: In charge of using wired and wireless technologies to transfer data between devices and processing units.
- Edge and Processing Layer: To minimize latency, computation can be done at the edge, nearer the data source, or in centralized cloud servers for more complex analysis.
- Application Layer: Providing services that are visible to users, like automated control, predictive maintenance, remote monitoring, and intelligent decision support.

The effectiveness, dependability, and security of IoT deployments are determined by the smooth interaction between these layers [13].

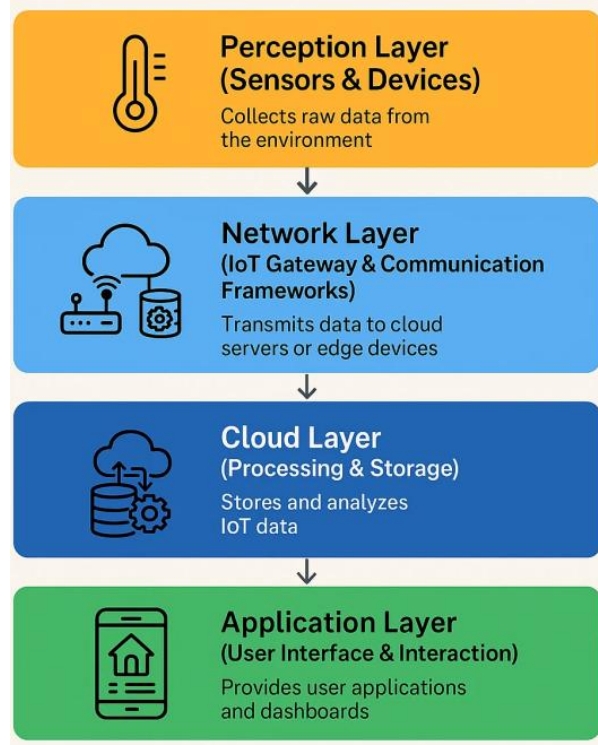


Figure 3: IoT Architecture

2.3 The IoT's Function in the 6G Era

It is anticipated that the IoT's integration with 6G networks will enable capabilities that are well beyond what is currently possible with wireless systems. 6G is expected to be the backbone of extensive IoT ecosystems, offering features like sub-millisecond latency, ultra-high reliability, terabit-per-second data rates, and ubiquitous connectivity [14]. This era's major improvements will include:

- **Massive Connectivity:** Enabling trillions of devices in both rural and urban areas without experiencing network congestion.
- **Devices can sense and transmit data simultaneously** for real-time situational awareness thanks to integrated sensing and communication.
- **Support for native artificial intelligence** enables intelligent algorithms to operate directly on network infrastructure for adaptive optimization.
- **High-Precision Positioning:** Enabling location accuracy down to the centimeter for applications like industrial robotics and driverless cars.

IoT will be able to provide more sophisticated services thanks to these capabilities, but they will also make security flaws worse, especially in environments that are latency-sensitive, distributed, and heterogeneous.

2.4 IoT Security Issues

IoT presents special security challenges because of its dispersed nature, wide range of hardware capabilities, and large attack surface, despite its revolutionary potential [15]. Typical difficulties consist of:

- **Weak Authorization and Authentication:** Because many IoT devices don't have strong identity verification systems, they are vulnerable to impersonation attacks.
- **Risks to Data Confidentiality and Integrity:** If sensitive data is not adequately protected

during transmission, it may be intercepted, changed, or fabricated.

- Resource Limitations: Computationally demanding cryptographic algorithms are frequently incompatible with low-power devices.
- Problems with scalability and interoperability: Security measures must support a variety of hardware configurations and communication protocols without compromising efficiency.



Figure 4: Security challenges in IoT [16].

These risks are greatly increased by the emergence of quantum computing, since many conventional encryption techniques might become outdated.

2.5 IoT Requires Quantum-Secure Solutions

For key exchange, authentication, and digital signatures, traditional IoT security models rely on asymmetric cryptography like RSA and ECC. However, once large-scale quantum computers are available, quantum algorithms like Shor's and Grover's may be able to crack these schemes in manageable amounts of time [17]. This increases the likelihood that encrypted Internet of Things communications could be captured and decrypted later on an attack tactic referred to as "harvest now, decrypt later." Post-Quantum Cryptography (PQC) provides mathematically sound substitutes that are impervious to quantum attacks in order to combat these dangers. PQC needs to be carefully modified for IoT systems in order to support constrained device resources while maintaining strong security.

2.6 Blockchain and Trust Frameworks for Safe IoT

Beyond encryption, IoT security necessitates transparency, trust, and resistance to data manipulation. By facilitating decentralized data storage, unchangeable transaction records, and transparent access control independent of central authorities, blockchain technology meets these demands. Blockchain and PQC together can guarantee the security of the distributed ledger and the cryptographic layer in the quantum era. By allowing devices to assess peers' dependability using behavioral metrics, previous interactions, and context-aware policies, trust architectures further improve IoT security. Adaptive trust mechanisms will be essential to preserving system integrity in 6G IoT deployments, where devices may join or exit the network on a regular basis.

This review concentrates on the joint function of post-quantum cryptography, blockchain integration, and trust architectures in protecting IoT networks, given the convergence of IoT, 6G, and quantum-resistant technologies. PQC schemes for constrained devices are introduced, followed by blockchain frameworks for the Internet of Things and adaptive trust models for large-scale decentralized environments. The interaction of these elements is specifically considered in order to achieve strong, future-proof security. IoT is essentially a foundational layer of the future digital ecosystem rather than a standalone technological trend. Comprehensive, multi-layered, and quantum-secure IoT solutions are more important than ever as 6G propels its growth and quantum computing changes its security needs.

3. Introduction to 6G

Wireless communication has developed over the course of several generations, each distinguished by important advances in technology and societal effects. First generation (1G) brought analog voice communication, followed by 2G with digital voice and basic data services, 3G with mobile internet access, 4G with broadband mobile connectivity, and 5G with improved mobile broadband, massive machine-type communication (mMTC), and ultra-reliable low-latency communication (URLLC). These capabilities are expected to be surpassed by the sixth generation (6G), which is anticipated to be commercially deployed around 2030 and offers previously unheard-of data rates, ultra-low latency, improved energy efficiency, and pervasive intelligence [18-20]. For cutting-edge applications like holographic telepresence, immersive extended reality (XR), high-precision industrial automation, and extensive Internet of Things (IoT) deployments, it is anticipated to act as a foundational infrastructure.

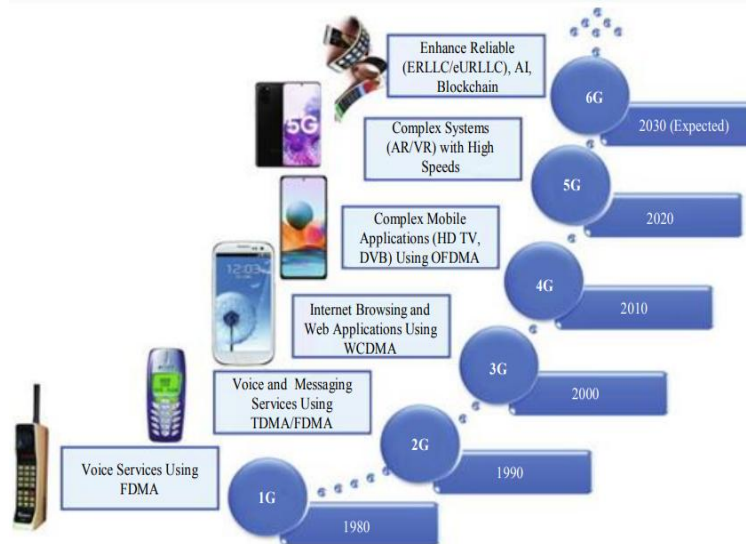


Figure 5: The evolution from 1G to 6G [21]

3.1 Features of 6G

6G is expected to push the limits of mobile network capacity by delivering peak data rates in the terabit-per-second range. It is anticipated that latency will be lowered to the order of microseconds, allowing for real-time control in vital systems like telesurgery and driverless cars. In addition, 6G seeks to attain a high connectivity density, enabling trillions of devices with reliable quality of service in remote, rural, and urban settings. In contrast to earlier iterations, intelligence will be integrated into the network fabric, allowing for native support for context-aware service delivery, self-healing, and artificial intelligence (AI)-driven optimization. The combination of communication and sensing will be another important aspect of 6G [22]. In

In addition to transmitting data, networks will be able to sense their environment, giving them high-resolution environmental awareness for uses like urban planning, precision agriculture, and environmental monitoring. It is anticipated that 6G positioning accuracy will achieve centimeter-level precision, which is crucial for location-critical services in autonomous mobility and industrial automation.



Figure 6: 6G based applications [23]

3.2 Technologies That Make Things Possible

A number of cutting-edge technologies will be necessary for 6G to become a reality:

- Communication at Terahertz (THz) : THz links, which operate in the 100 GHz to 10 THz frequency range, offer extremely high data rates and a vast amount of available bandwidth. High-throughput backhaul links and heavy traffic in urban areas will require this spectrum.
- Reconfigurable Intelligent Surfaces (RIS): Surfaces with programmable components can change electromagnetic waves in real time to increase spectral efficiency, decrease interference, and improve coverage.
- Integrated Sensing and Communication (ISAC): 6G networks will be able to transmit data and sense the environment at the same time, allowing for simultaneous communication and radar-like capabilities.
- Advanced MIMO and Beamforming: Especially in high-frequency bands, extremely large antenna arrays will allow for precise beam steering, spatial multiplexing, and energy-efficient communication [24-25].
- Native AI Support: To enable anomaly detection, predictive resource allocation, and service customization, artificial intelligence and machine learning will be incorporated into the network's control plane.

Although 6G will mostly use classical channels, integration with quantum communication protocols is being investigated for improved security in crucial situations.

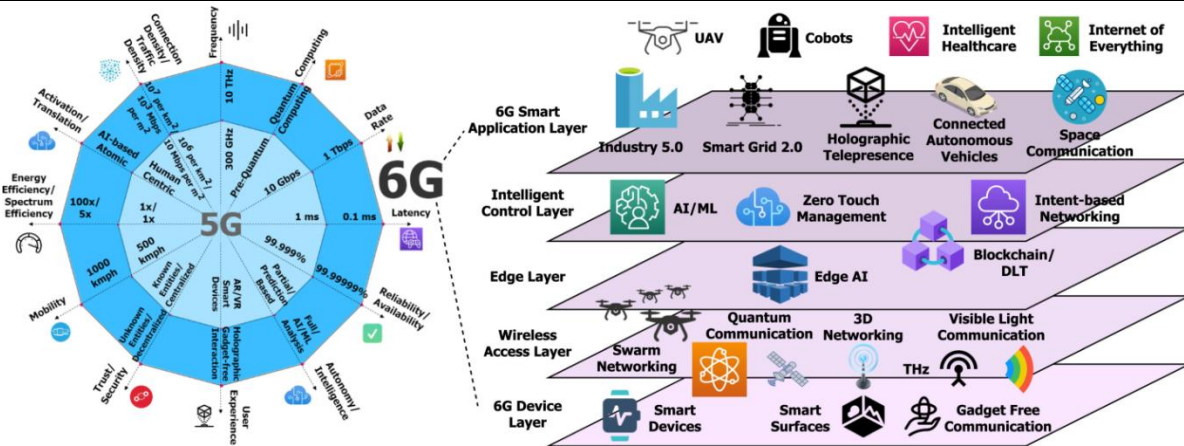


Figure 7: 6G Technologies [26]

3.3 The IoT and 6G

It is anticipated that the convergence of 6G and IoT will change how devices communicate, exchange data, and react to changing circumstances. Mission-critical healthcare applications, coordinated drone fleets, and autonomous industrial robots will all be made possible by 6G's ultra-low latency and high reliability, which will enable IoT systems to operate in real-time. Large-scale sensor deployments, spanning smart cities, agricultural fields, and environmental monitoring zones, will also be able to function without bottlenecks thanks to massive connectivity. 6G will enable time-sensitive networking (TSN) requirements for industrial IoT (IIoT), guaranteeing deterministic performance in energy grid control and factory automation. Richer user experiences and more efficient data-driven decision-making will be made possible by seamless, high-bandwidth communication in consumer IoT, wearable technology, home automation systems, and connected automobiles.

3.4 Security Issues in the 6G Era

Advanced performance capabilities will be offered by 6G, but it also brings with it difficult security issues. The attack surface is increased by the large number of connected devices, diverse communication protocols, and decentralized topologies. Concerns regarding data poisoning, privacy violations, and adversarial model manipulation are also raised by the incorporation of AI-driven decision-making into network operations. Most importantly, existing public-key cryptography faces an existential threat from the development of quantum computing. Algorithms like Shor's can be used by sufficiently powerful quantum computers to break many popular algorithms, including RSA, ECC, and Diffie-Hellman key exchange. For sensitive communications and long-life devices that must be kept private for decades, this vulnerability is especially worrisome. Therefore, quantum-resistant solutions must be incorporated into 6G security architectures from the beginning. One approach is post-quantum cryptography (PQC), which provides cryptographic primitives that are thought to be safe from both classical and quantum attacks. However, because 6G is distributed and heterogeneous, decentralized trust mechanisms like blockchain are necessary to guarantee data integrity, transparency, and authentication without depending on centralized control [27].

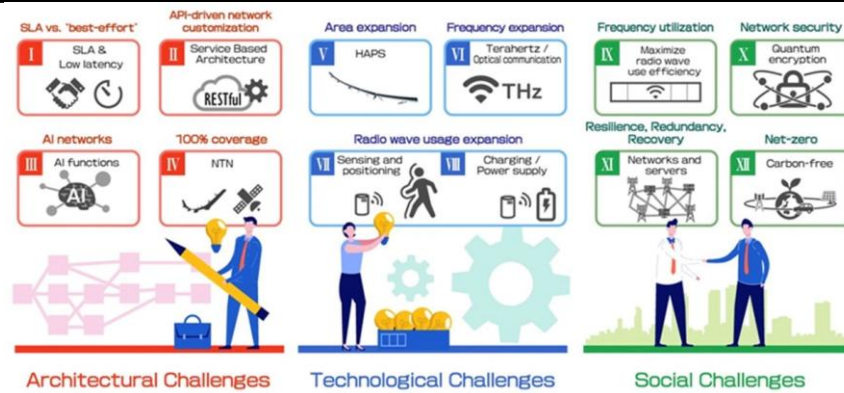


Figure 8: Challenges for 6G

3.5 Blockchain and Trust Architectures' Function in 6G

Blockchain technology, which offers transparent, decentralized, and tamper-resistant data management, can be crucial to the security of 6G-enabled IoT networks. Blockchain can protect transaction records from future quantum threats by integrating quantum-resistant cryptography. It can also facilitate safe device onboarding, access control, and automated policy enforcement through smart contracts. By facilitating the dynamic assessment of network behavior, data authenticity, and device dependability, trust architectures enhance blockchain technology. Adaptive trust management is crucial for preserving operational integrity in 6G, where devices may quickly join or exit networks and function across several domains. PQC, blockchain, and trust mechanisms work together to provide a multi-layered defense approach that is appropriate for the rigorous security standards of 6G environments.

Blockchain for 6G Networks

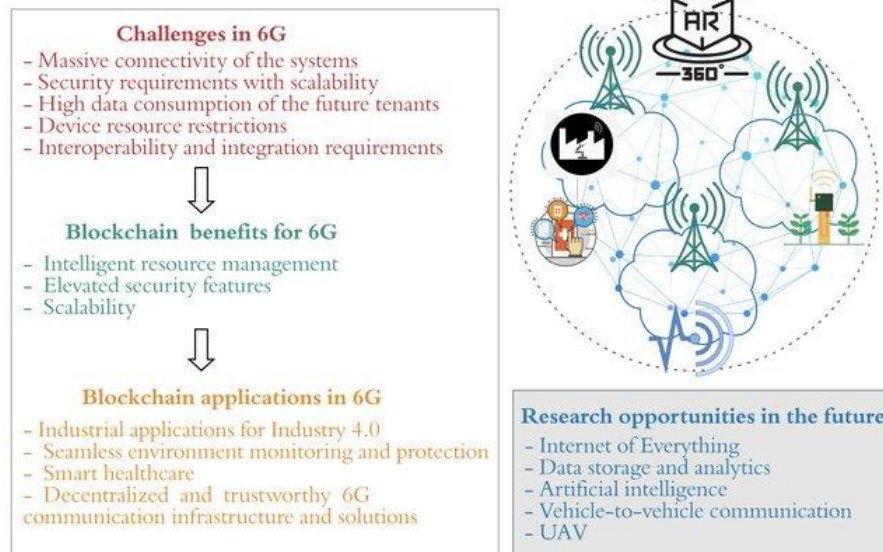


Figure 9: The role of blockchain in 6G networks [28]

3.6 Review's Place in the 6G Era

Although a lot of research has been done on the physical layer technologies and service capabilities of 6G, there are still few thorough studies that combine blockchain-based decentralization, adaptive trust architectures, and quantum-secure communication. By concentrating on how these three pillars come together in the context of IoT deployments in 6G networks, this review fills that gap. The foundations of post-quantum cryptography that can be

used with limited IoT devices, blockchain systems that are best suited for massively decentralized settings, and trust systems that can adjust to the changing and diverse 6G ecosystems. The conversation focuses on how these elements interact to create robust, future-proof IoT systems that can withstand the twin threats of adversaries with quantum capabilities and massive connectivity.

6G is a revolutionary step toward a completely intelligent, hyper-connected, and secure communication fabric rather than merely an incremental improvement over 5G. It is feasible to create strong IoT ecosystems that will prosper in the quantum era by foreseeing its potential and resolving its security issues with decentralized, trust-oriented, and quantum-resistant solutions.

4. Introduction to Blockchain Technology

A distributed network of computers can record digital transactions using blockchain technology, which is decentralized and impenetrable. Blockchain technology, which was first presented in 2008 as the underlying technology for Bitcoin, has developed significantly beyond its original use in cryptocurrencies. It is now acknowledged as a flexible platform that facilitates safe, transparent, and verifiable data exchange across a range of industries, including energy trading, healthcare, financial services, supply chain management, and, more and more, Internet of Things (IoT) ecosystems. In contrast to traditional centralized databases, which are managed and verified by a single authority, blockchain technology uses a peer-to-peer (P2P) architecture, where a shared ledger is maintained and validated by a number of nodes. By doing away with the need for middlemen, this decentralized strategy lowers the possibility of single points of failure and increases system resistance to malevolent attacks [29-31].

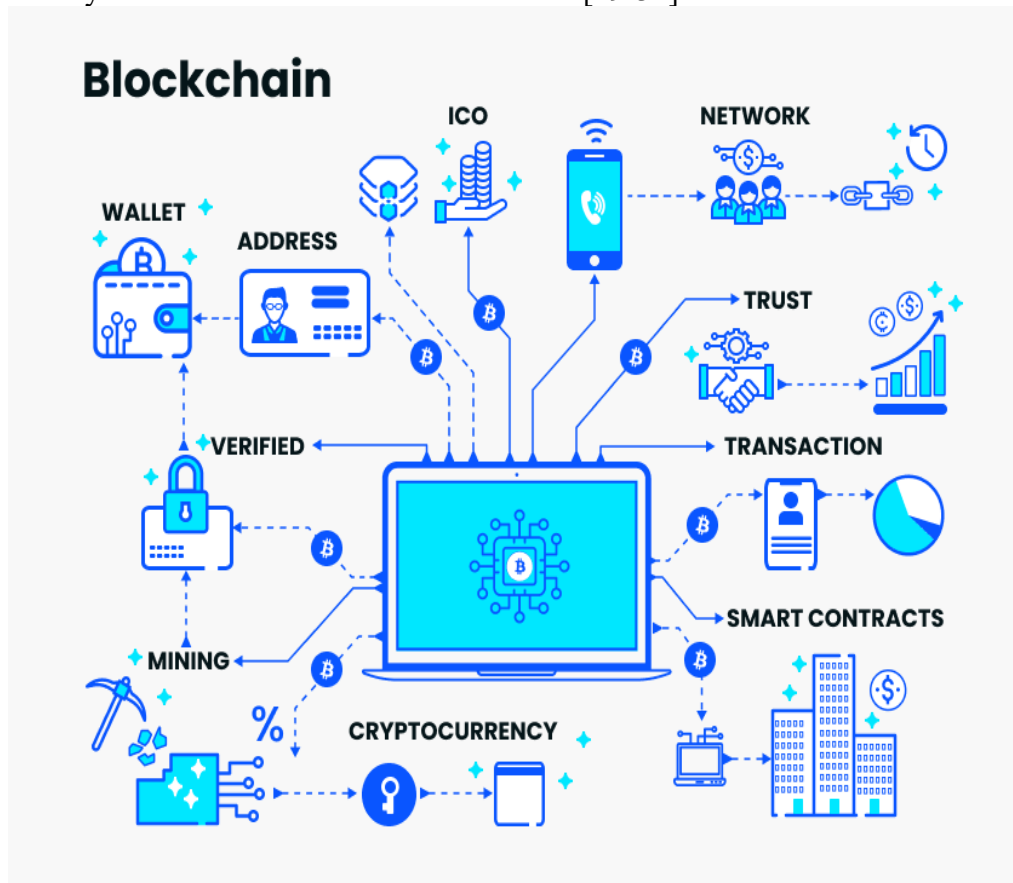


Figure 10: Blockchain

4.1 Fundamental Ideas and Framework

A blockchain is made up of a series of blocks, each of which has a list of data records or transactions. By connecting these blocks with cryptographic hashes, an immutable record is produced; once a block is added, it cannot be removed without changing all of the blocks that follow, which would require network consensus from the majority. Among the fundamental ideas of blockchain are:

- Decentralization reduces vulnerability to targeted attacks and avoids centralized control by storing data across a network of nodes [32].
- Immutability: Cryptographic hashing guarantees that historical data cannot be altered covertly.
- Consensus Mechanisms: These protocols, which ensure consensus on the ledger's current state without the need for a central authority, include Proof of Work (PoW), Proof of Stake (PoS), and more sophisticated schemes.
- Transparency and Auditability: By allowing all participants to confirm transactions in a public or permissioned ledger, trust between parties is increased.

Every block typically consists of a body with the transaction data and a header with the hash of the previous block, a timestamp, and other metadata.

4.2 Blockchain Types

Three broad categories can be used to classify blockchain networks:

Anyone can participate fully in ledger maintenance and transaction validation on a public blockchain. Ethereum and Bitcoin are two examples. Although public blockchains are very transparent, they may have issues with energy efficiency and scalability.

Only authorized participants can access and update the ledger on a private blockchain, which is managed by a single entity. Private blockchains provide greater transaction throughput and privacy despite being less decentralized.

Consortium Blockchain: Managed by a collection of companies, it strikes a balance between decentralization and requirements for governance and performance. This model works well for supply chain consortia and other industry-wide partnerships.

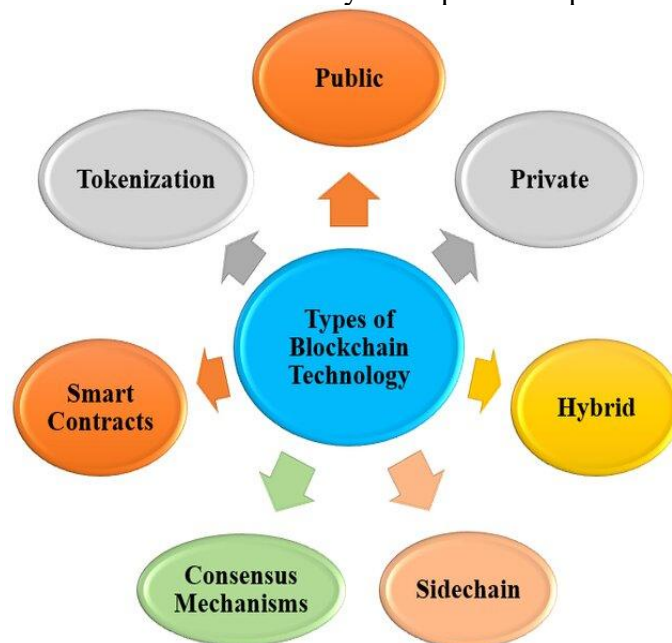


Figure 11: Example for Types of Blockchain Technology [33]

4.3 Blockchain in IoT Networks

The vast number of connected devices in IoT systems frequently function in dynamic, diverse, and widely dispersed environments. Conventional security models are susceptible to cyber attacks, performance snags, and single-point failures since they depend on centralized servers for data storage and authentication. By facilitating decentralized trust management, blockchain offers a viable substitute that allows devices to authenticate and conduct transactions independently of a centralized authority. Among the main advantages of blockchain for IoT are:

- **Decentralized Authentication:** By utilizing cryptographic credentials stored in the blockchain, devices can authenticate one another without depending on central authentication servers.
- **Tamper-Proof Data Storage:** The blockchain prevents unwanted alteration of sensor readings and operational logs.
- **Automated Control with Smart Contracts:** Smart contracts allow for the provisioning of services, access control, and automated payments without the need for human intervention by enabling predefined rules for device interactions.
- **Better Supply Chain Tracking:** Blockchain technology in industrial IoT can offer verifiable product histories, improving compliance and transparency.

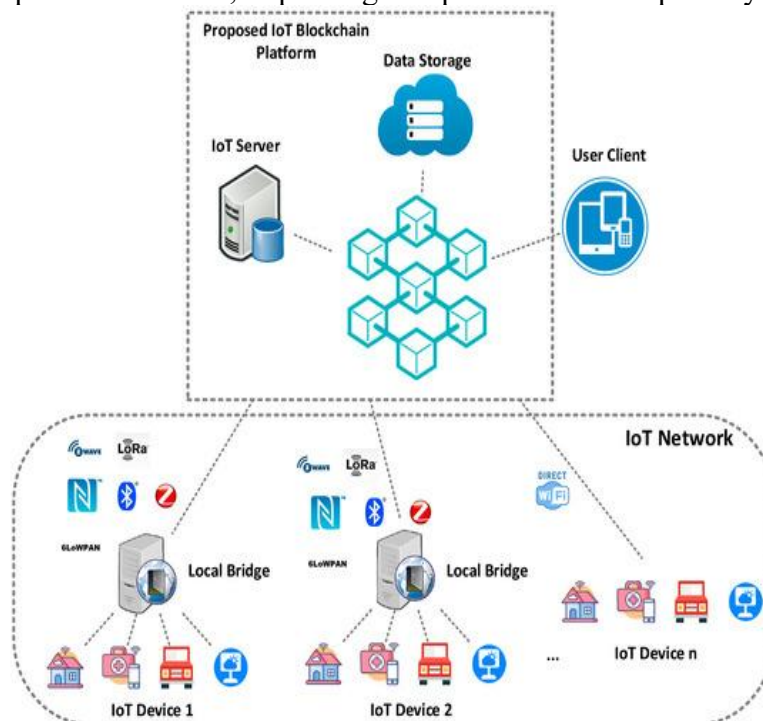


Figure 12: IoT blockchain platform [34]

4.4 Challenges in IoT Uses

Blockchain integration in IoT environments presents a number of difficulties despite its benefits:

- **Scalability:** Blockchain networks may become overloaded by the volume of IoT transactions, which could cause delays and high storage needs.
- **Energy Consumption:** Certain consensus techniques, like Proof of Work, require a lot of computation and energy, which makes them inappropriate for Internet of Things devices with constrained resources.

- Latency: Time-sensitive Internet of Things applications may require ultra-low latency, which blockchain transaction confirmation times may not be able to provide.
- Data privacy: Although openness is advantageous, keeping private information on public ledgers can cause privacy issues, which calls for off-chain storage options or encryption.

To overcome these obstacles, the type of blockchain, consensus algorithms, and data management techniques used must be carefully chosen and adapted to the unique needs of IoT deployments.

4.5 Blockchain in 6G Era

6G networks' terabit-level data rates, sub-millisecond latency, and extensive device connectivity present a chance to get around some of blockchain's present drawbacks.

- Ultra-Fast Consensus: By cutting down on the time needed for block propagation and consensus formation, high-speed 6G communication can speed up transaction finality.
- Edge Integration: By placing small blockchain nodes near data sources, edge computing in 6G can increase scalability and lower latency.
- Massive Connectivity: If consensus mechanisms are tailored for large-scale networks, blockchain-enabled IoT ecosystems can grow without sacrificing performance, as 6G supports trillions of devices [35].

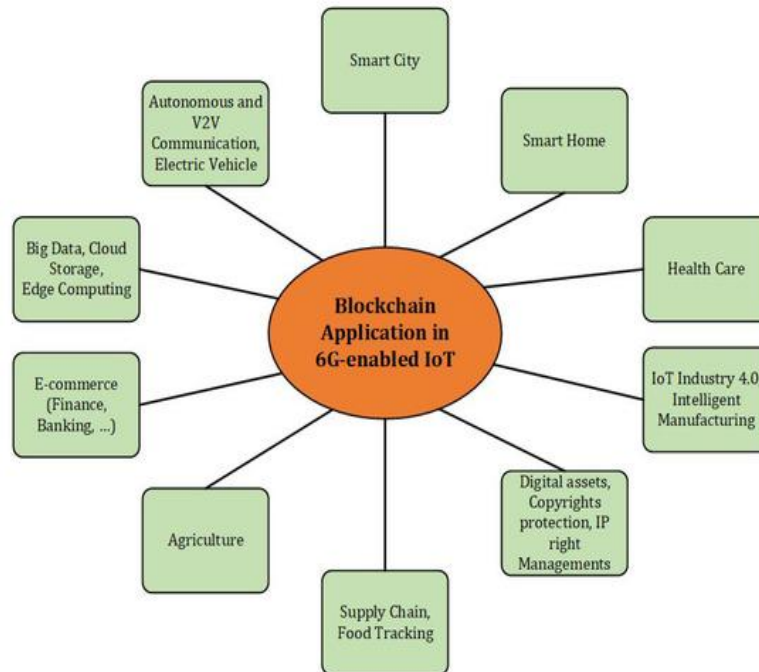


Figure 13: Blockchain applications in 6G-enabled IoT [36]

4.6 Blockchain's Quantum Threat

The cryptographic primitives used by current blockchain systems, like hash functions and elliptic curve digital signatures (ECDSA), may be susceptible to quantum attacks. For example, Shor's algorithm might jeopardize ECDSA-based authentication, giving hackers the ability to impersonate devices or forge transactions. Grover's algorithm can still give brute-force attacks a quadratic speedup, even though the hash functions used in blockchain are more resilient [37]. Blockchain systems must incorporate post-quantum cryptography (PQC) to ensure security in the quantum era. Blockchain can continue to function as a safe basis for IoT trust management in 6G networks by substituting lattice-based, hash-based, or other quantum-resistant algorithms for

weak signature schemes.

4.7 Blockchain and Trust Frameworks for Ultra-Secure IoT

Although blockchain protects data integrity after entry, it is unable to stop false data injection at the source, so it cannot by itself ensure that data sources are reliable. By continuously assessing device reliability based on behavior, context, and past interactions, trust architectures work in tandem with blockchain. Trust architectures provide a multi-layered defense against current and upcoming cyberthreats when paired with PQC's quantum resistance and blockchain's immutable ledger. In IoT ecosystems with 6G, this integration makes it possible for:

- Secure device onboarding with blockchain credentials that are resistant to quantum errors.
- Device interactions that are verifiable and transparent without centralized control.
- Real-time compromised node identification using adaptive trust scoring techniques.

Blockchain is the foundation for decentralized trust, unchangeable record-keeping, and safe automation via smart contracts in the context of quantum-secure IoT networks for the 6G era. While its integration with trust architectures offers a comprehensive security framework for large, diverse, and dynamic IoT deployments, its synergy with PQC guarantees resilience against quantum computing threats.

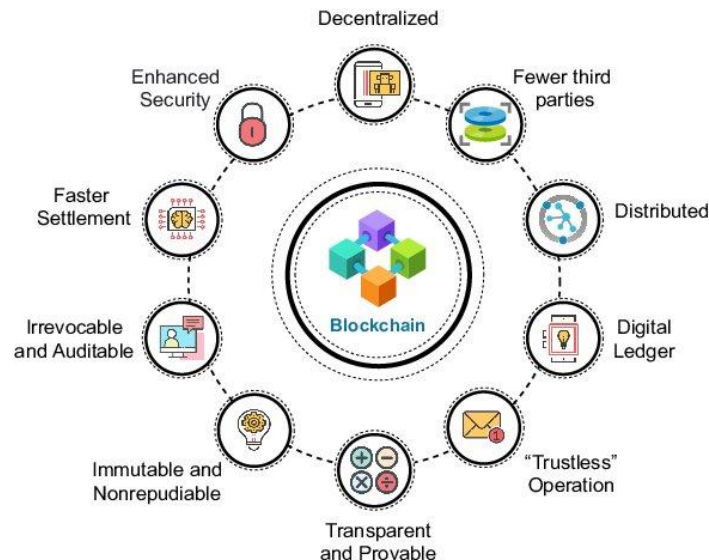


Figure 14: Key features of Blockchain technology [38]

5. Introduction to Quantum Cryptography

An emerging discipline referred to quantum cryptography uses the ideas of quantum mechanics to protect communications from attacks using both classical and quantum computing. The security of quantum cryptography is derived from the fundamental laws of physics, as opposed to conventional cryptographic techniques that depend on the computational difficulty of specific mathematical problems. In a future where large-scale quantum computers may make traditional encryption algorithms outdated, this makes it a promising method for protecting sensitive data. Quantum Key Distribution (QKD) is the most well-known and extensively researched use of quantum cryptography. With security ensured by photons' quantum characteristics, QKD allows two parties to create and exchange a secret cryptographic key. The communicating parties can discard compromised keys and continue to communicate securely because any attempt by an eavesdropper to intercept the key causes detectable disruptions [39-40].

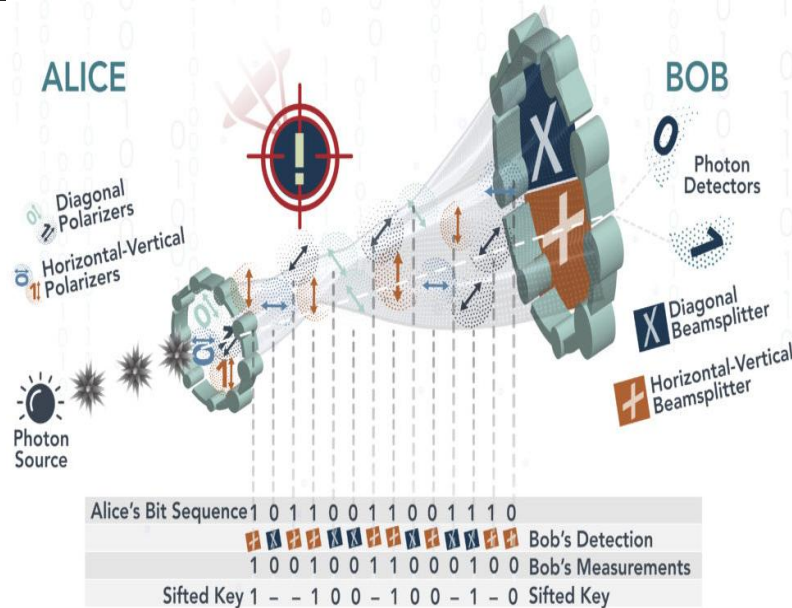


Figure 15: An example of how quantum encryption works

5.1 Quantum Cryptography Foundations

Several ideas from quantum mechanics underpin the security of quantum cryptography. Quantum Superposition is an eavesdropper cannot measure or replicate a particle's precise state without changing it because a quantum system can exist in multiple states concurrently until it is measured. Heisenberg The Uncertainty Principle states that some physical property pairs, like position and momentum or a photon's various polarization states, cannot be precisely measured at the same time [41]. This guarantees that information cannot be extracted by an eavesdropper without causing observable errors. The No-Cloning Theorem states that it is inherently impossible to replicate an unknown quantum state exactly. By doing this, the key bits are not duplicated during transmission. The detection of possible breaches is made possible by these principles, which guarantee that any unauthorized observation of a quantum communication channel will leave detectable traces.

5.2 Distribution of Quantum Keys (QKD)

The most developed type of quantum cryptography is QKD protocols. A typical QKD setup involves the transmission of quantum states, which are typically encoded in photons, via free-space links or optical fibers. Bennett and Brassard introduced the most well-known protocol, BB84, in 1984. Bits are encoded using randomly selected polarization states, which are changed by any eavesdropping attempt, raising the key's error rate. The E91 Protocol uses correlated particles to create a shared key and is based on quantum entanglement [42]. Rather than using discrete photon polarization states, Continuous Variable QKD (CV-QKD) makes use of continuous properties like the amplitude and phase of light waves. The purpose of Measurement-Device-Independent QKD (MDI-QKD) is to eliminate the vulnerabilities brought on by subpar detectors. The communicating parties carry out a traditional post-processing step that includes error correction and privacy amplification to obtain a final secret key after the quantum transmission phase is finished.

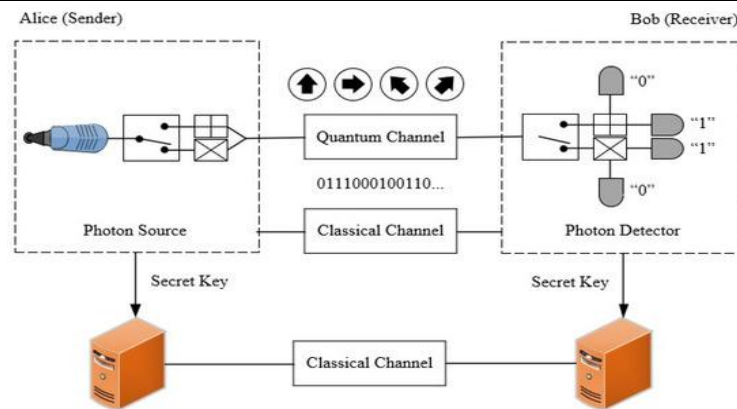


Figure 16: QKD Mechanism [43]

5.3 Beyond QKD, Quantum Cryptography

Quantum cryptography has several uses, even though QKD is the most well-known. Using quantum states, quantum digital signatures (QDS) offer message authentication and non-repudiation. Messages can be sent directly over a quantum channel using quantum secure direct communication (QSDC), which eliminates the need to generate a key beforehand. Secure cryptographic keys require quantum random number generation (QRNG), which generates genuinely unpredictable random numbers. These methods broaden the application of quantum cryptography to more secure communication services.

5.4 Benefits of Quantum Cryptography for 6G and IoT

Quantum cryptography has various benefits over traditional security techniques in the context of IoT and 6G networks.

- Future-Proof Security: Able to withstand attacks from quantum computers and other computational advances.
- Eavesdropping Detection: Proactive security measures are made possible by the instantaneous detection of any interception attempt.
- Unconditional Security: Security is founded on the laws of physics rather than on unproven mathematical presumptions.

Establishing secure communication channels that are impervious to present and potential threats is crucial as 6G networks link billions of diverse IoT devices.

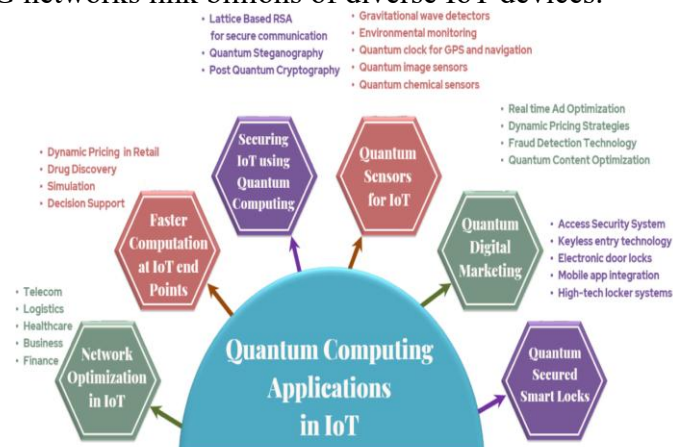


Figure 17: Quantum computing applications in IoT [44]

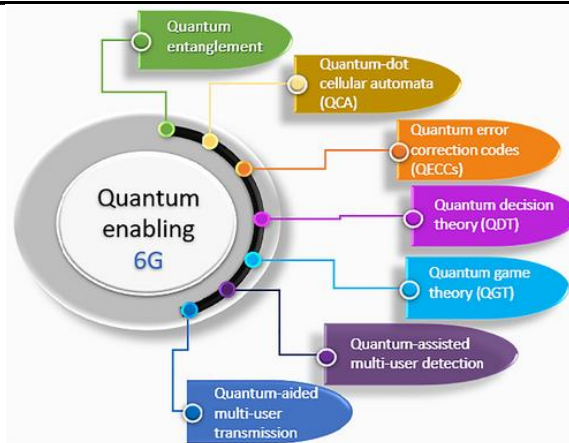


Figure 18: Enabling quantum technologies in 6G [45]

5.5 Difficulties in Applying Quantum Cryptography to the IoT

Despite its potential, there are a number of obstacles preventing quantum cryptography from being widely used, particularly in IoT environments:

- **Infrastructure Requirements:** Not all IoT devices may be able to support QKD because it usually requires specialized hardware, such as photon sources, detectors, and low-loss optical fibers.
- **Distance Restrictions:** Without reliable repeaters or quantum satellites, the range of QKD is limited by photon loss in optical fibers.
- **Integration with Classical Networks:** Since IoT systems primarily employ classical communication protocols, hybrid architectures are needed to integrate quantum channels.
- **Cost and Energy Restrictions:** Limited Resources The hardware and computational requirements of quantum cryptography might be beyond the capabilities of IoT devices.

Innovations in hybrid quantum-classical architectures, lightweight quantum cryptography protocols, and affordable hardware solutions will be needed to meet these challenges.



Figure 19: Challenges of Quantum Computing

5.6 Quantum Cryptography in the Security Environment of 6G

Security needs in the 6G era will go beyond safeguarding individual communication links to include safeguarding large, dynamic networks with a variety of service needs. Creating quantum-secure connections between base stations and essential network components is known as secure backhaul links. Protecting control systems in autonomous vehicles, smart grids, and healthcare networks is known as critical infrastructure protection. Satellite-Based Global QKD using low-Earth orbit satellites, this technology provides quantum-secure keys to IoT devices in

remote or mobile environments [46]. Quantum cryptographic systems can provide hybrid security when combined with post-quantum cryptography; PQC algorithms are used for data encryption and authentication, while QKD is used for key distribution. Both the flexibility of software-based cryptography schemes and the physical-layer security of quantum methods are offered by this hybrid approach.

5.7 Connection to Trust Architectures and Blockchain

By protecting the key exchange procedure in blockchain-based Internet of Things systems, quantum cryptography enhances blockchain technology. To ensure that ledger updates and consensus procedures are safe even from adversaries with quantum capabilities, QKD can be used, for example, to create quantum-secure session keys for blockchain node communication.

By securing the transmission of trust-related metrics and guaranteeing that trust scores are not manipulated during transmission, quantum cryptography can also help trust architectures, which assess the dependability of network participants. Quantum cryptography is a supplementary technology to PQC and blockchain in the context of Quantum-Secure IoT Networks for the 6G Era, as well as a defense against quantum-enabled threats. Blockchain decentralizes trust and PQC fortifies software-level algorithms, but quantum cryptography adds a physics-based layer of security that guarantees safe key distribution and eavesdropping detection. Quantum cryptography is regarded in this review as a crucial component of the multi-layered security architecture needed for upcoming IoT deployments. In order to create scalable, robust, and quantum-resistant IoT infrastructures in 6G networks, it looks at the most recent developments in QKD, lightweight quantum protocols for devices with limitations, and integration techniques with classical and post-quantum security measures.

6. Post-Quantum Cryptography for IoT Security

Existing cryptographic systems face a serious threat as well as an opportunity due to the quick development of quantum computing. The security underpinnings of popular cryptographic algorithms like RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange are threatened by quantum technology, despite its promise of previously unheard-of computational power. These algorithms rely on the computational difficulty of discrete logarithms and integer factorization, which quantum algorithms like Shor's and Grover's can solve exponentially more quickly than traditional techniques. The IoT extensive network of resource-constrained devices is becoming more and more susceptible to quantum-enabled attacks as it integrates smart cities, autonomous systems, industrial automation, and healthcare, making it a crucial component of the 6G ecosystem. PQC becomes an important field of study and application to tackle this impending problem.

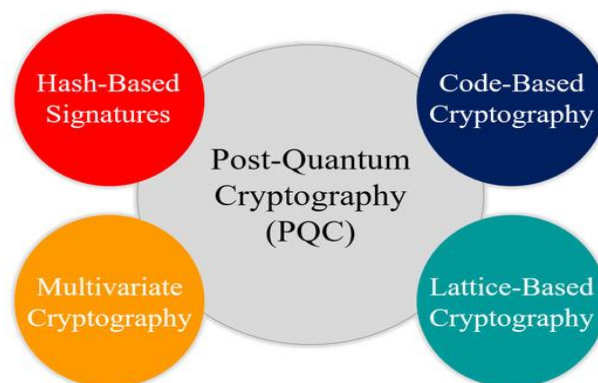


Figure 20: Basic types of Post-Quantum Cryptography [47]

6.1 Post-Quantum Cryptography's Need in the Internet of Things

IoT devices frequently function in settings where authentication, confidentiality, and integrity are crucial. When large-scale quantum computers become a reality, traditional cryptographic schemes might no longer be secure. Adversaries can store encrypted IoT communications today and decrypt them later when quantum capabilities advance thanks to the so-called "harvest-now, decrypt-later" attack model. Systems that need long-term confidentiality, like government surveillance feeds, industrial control logs, or medical data archives, are especially at risk from this. Therefore, switching to PQC is a practical requirement for future-proof IoT security, not just a theoretical one.

6.2 Features of Algorithms for Post-Quantum Cryptography

PQC functions within the classical computing paradigm and is made to withstand quantum attacks, in contrast to QKD, which is based on the physical concepts of quantum mechanics. The mathematical problems that post-quantum algorithms are usually based on are thought to be impervious to both classical and quantum attacks. Lattice-based cryptography is depends on how challenging problems like the Shortest Vector Problem (SVP) and Learning with Errors (LWE) are. CRYSTALS-Dilithium (digital signatures) and CRYSTALS-Kyber (key encapsulation) are two examples. Error-correcting codes serve as the foundation for encryption in code-based cryptography, such as the McEliece cryptosystem. Rainbow signatures and other systems of multivariate quadratic equations are used in multivariate polynomial cryptography. XMSS and SPHINCS+ are two examples of hash-based signatures that take advantage of the security of cryptographic hash functions. The mathematical structure of supersingular elliptic curve isogenies, like SIKE, is used in isogeny-based cryptography. To ensure widespread adoption across industries, including IoT, the National Institute of Standards and Technology (NIST) is actively evaluating these approaches for standardization [48].

6.3 Difficulties with Integration in IoT Settings

Although PQC provides a safe base, there are significant obstacles to its IoT adoption:

- **Computational Overhead:** Compared to modern lightweight cryptography schemes, many PQC algorithms demand more processing power. Real-time encryption and decryption may be difficult for IoT devices with constrained CPU power.
- **Memory Footprint:** Large public key sizes are a feature of some algorithms, especially code-based cryptography, which makes them inappropriate for limited IoT devices with little storage.
- **Communication Overhead:** IoT networks with limited bandwidth may experience strain from larger key sizes and longer ciphertexts.
- **Energy Consumption:** If cryptographic calculations are too taxing, the lifespan of battery-operated Internet of Things sensors may be shortened.

Algorithmic optimization, hardware acceleration, and hybrid strategies that combine PQC with already-existing lightweight protocols are necessary to address these problems.

6.4 Strategies for Hybrid Cryptography

Using hybrid cryptographic protocols, which blend classical algorithms with their post-quantum counterparts, is a promising short-term solution. This method introduces quantum resistance while guaranteeing backward compatibility with current systems. Elliptic Curve Diffie–Hellman (ECDH) and a lattice-based key encapsulation mechanism, for instance, could be combined in a hybrid key exchange to ensure that security is maintained even in the event that one scheme is compromised. IoT ecosystems can adopt PQC without interfering with ongoing operations thanks to this strategy's ability to facilitate gradual migration.

6.5 Secure 6G-Enabled IoT and PQC

Ultra-low-latency and high-reliability communication will be crucial to IoT networks in the 6G era, allowing for applications like industrial robotics, telesurgery, and driverless cars. The foundation for defending these services against upcoming quantum threats will be PQC. Lattice-based encryption can safeguard communications between vehicles and infrastructure in autonomous transportation. Post-quantum signatures can authenticate firmware updates in industrial IoT (IIoT) and stop malicious code injection. PQC can secure wearable medical devices that send private patient data to remote monitoring systems in the context of healthcare IoT. PQC's incorporation into IoT gateways and edge computing nodes will also assist in transferring demanding computations from limited devices, improving deployment viability.

6.6 International Initiatives and Standardization

To guarantee interoperability and broad adoption, groups like NIST, ETSI, and ISO are actively working on PQC standardization. Algorithms like CRYSTALS-Kyber and Dilithium have already been chosen for standardization as a result of NIST's PQC competition, and other algorithms are being considered for specific use cases. Respecting these new standards will be essential for IoT in order to facilitate safe, international, and multi-vendor communications.

In order to protect IoT networks from the new threats posed by quantum computing, post-quantum cryptography is a crucial change. It is imperative to move away from weak cryptographic systems, even though there are still obstacles to overcome, particularly for low-power, limited devices. IoT networks in the 6G era can guarantee data security and privacy even in the face of future quantum threats by implementing PQC in conjunction with complementary technologies like blockchain and trust architectures.

Table 1: Post-Quantum Cryptography (PQC) Algorithm Families

Family	Example Algorithms	Security Basis	Suitability for IoT
Lattice-based	CRYSTALS-Kyber, NTRU	Shortest Vector Problem (SVP)	Efficient key sizes, moderate computation
Code-based	Classic McEliece	Error-correcting codes	Large keys, long-term security
Multivariate-based	Rainbow, GeMSS	Multivariate quadratic equations	Small signatures, fast verification
Hash-based	XMSS, SPHINCS+	Hash functions	Stateless options available
Isogeny-based	SIKE (deprecated post-attack)	Elliptic curve isogenies	Compact keys, now less trusted

7. Blockchain Integration for Decentralized IoT Security

The IoT explosive growth across a wide range of industries, from healthcare to industrial automation, has made it extremely difficult to maintain reliable, scalable, and secure communication networks. Large-scale IoT deployments present inherent challenges for traditional centralized security models because of the potential for vulnerabilities caused by single points of failure, data validation bottlenecks, and trust dependencies on centralized authorities. As IoT ecosystems link billions of disparate devices in the 6G era, the security model needs to be robust, dispersed, and responsive to threats in real time. By providing a decentralized, transparent, and immutable framework for managing trust relationships and safeguarding IoT data transactions without the need for centralized middlemen, blockchain technology emerges as a crucial enabler for tackling these issues [49].

7.1 Blockchain Foundations for IoT Security

Blockchain is basically a distributed ledger system in which cryptographic hashes are used to link blocks of data together. A set of verified transactions is included in each block, and once the data is added to the chain, it cannot be changed without network participants' consent. Blockchain ensures integrity and traceability in the context of the Internet of Things by enabling a secure record of device interactions, data transmissions, and system updates. The system lowers the attack surface for malevolent actors and mitigates the risks associated with centralized data storage by distributing the ledger among several nodes. A key component of blockchain security is the consensus process. Power limitations, network latency, and scalability requirements can be used to customize mechanisms like Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) for Internet of Things environments. Lightweight consensus protocols are especially important in Internet of Things scenarios to reduce computational overhead on devices with limited resources.

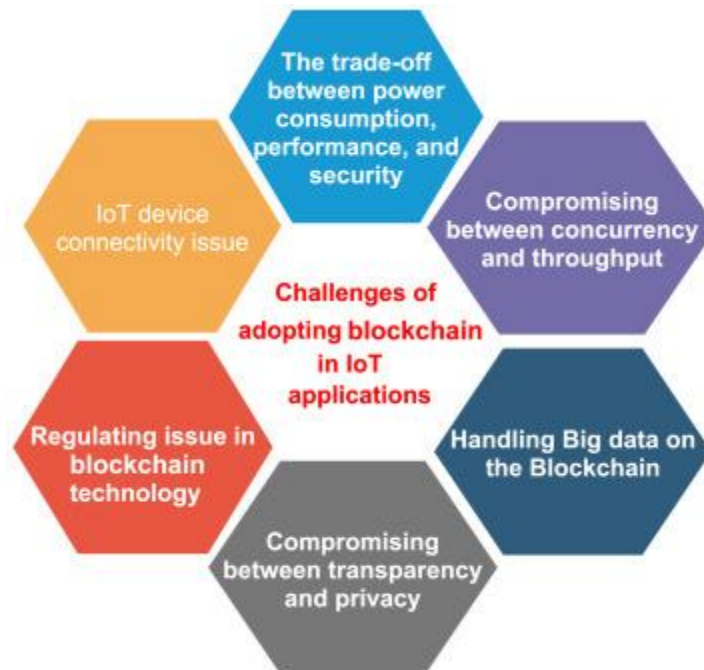


Figure 21: The challenges of adopting blockchain in IoT [50]

7.2 Management of Decentralized Trust

Decentralized trust management is one of blockchain's most significant contributions to IoT security. Blockchain enables trust to be built through cryptographically signed transactions and verifiable device identities stored on the ledger, as opposed to depending on a central authority for device authentication and authorization. By preventing single-point compromise and supporting dynamic trust models, this method allows device roles and permissions to be changed or revoked without interfering with network operations as a whole. Automated trust enforcement is made possible by smart contracts, which are self-executing scripts integrated into blockchain technology. Smart contracts in the Internet of Things can be configured to validate device credentials, grant access to resources, or sound an alarm in the event that unusual activity is noticed. Because these contracts don't require human intervention, they ensure consistent policy enforcement and speed up response times to security events.

7.3 Improving Confidentiality and Data Integrity

Applications such as industrial control systems, autonomous vehicles, and healthcare

monitoring depend on data integrity in IoT networks. By guaranteeing that every transaction entered into the ledger is verifiable and unchangeable, blockchain protects data. The distributed consensus model makes it nearly impossible to change historical data without being discovered, even in the event that a device is compromised. Blockchain technology can be used in conjunction with encryption techniques to maintain confidentiality by safeguarding private information prior to its inclusion in the ledger. Off-chain storage solutions can be employed in more complex implementations, where the real data is kept in secure repositories and only cryptographic hashes of the data are kept on-chain. This hybrid strategy strikes a balance between the immutability of blockchain records and the requirement for privacy.

7.4 Scalability Issues with IoT Integration

Blockchain has strong security advantages, but there are scalability issues when applying it directly to the Internet of Things. Public blockchains are not appropriate for extensive IoT deployments because they frequently have low transaction throughput and energy-intensive consensus techniques like PoW. To increase performance, new approaches like sharding, sidechains, and ledgers based on Directed Acyclic Graphs (DAG) are being investigated. Permissioned blockchains, in which transactions can only be validated by authorized participants, are becoming more popular in IoT-specific contexts. These blockchains are more useful for connected healthcare systems, smart grids, and industrial IoT because they speed up transactions and simplify consensus.

7.5 Quantum-Resistant Security and Blockchain

RSA and ECC, two traditional cryptographic algorithms used in blockchain systems, are in danger due to the emergence of quantum computing. Long-term security for IoT networks is ensured by combining blockchain technology with post-quantum cryptographic primitives. In order to avoid future vulnerabilities while preserving the fundamental characteristics of blockchain, quantum-resistant consensus and signature schemes are being developed. Blockchain systems created with quantum security in mind will be crucial for long-term IoT protection in the 6G era, when quantum threats are more likely to materialize.

7.6 Decentralized IoT Security Use Cases

Several IoT security scenarios have seen the successful application of blockchain, including:

Authenticity and traceability of products from manufacturing to delivery are guaranteed by supply chain management.

Securely managing dispersed energy resources without centralized control is possible with smart energy grids.

Healthcare IoT is enabling safe communication between medical devices and healthcare providers while safeguarding patient data.

Autonomous Vehicle Networks are using tamper-proof transaction logs to coordinate communication between vehicles.

7.7 Challenges and Potential Opportunities

Blockchain integration in IoT is not without difficulties, despite its potential. It is necessary to address problems like storage overhead, network latency, and interoperability amongst various blockchain platforms. Furthermore, more research is still needed in the areas of regulatory compliance with data protection laws and permissioned blockchain governance models. Future studies should concentrate on hybrid architectures that integrate blockchain with other distributed security measures, lightweight blockchain frameworks tailored for the Internet of Things, and integration with edge computing for quicker consensus. Blockchain-based IoT

security solutions will need to change to provide seamless, scalable, and quantum-resistant protection as 6G networks introduce ultra-low latency and high device density. By facilitating automated policy enforcement, guaranteeing data integrity, and decentralizing trust, blockchain provides a revolutionary method of IoT security in the 6G era. Blockchain can serve as the cornerstone of an IoT security framework that is robust and future-proof, able to withstand both present and emerging threats, when paired with post-quantum cryptography and trust architectures.

8. Trust Architectures for Quantum-Secure IoT

Establishing and preserving trust among interconnected entities has become more difficult due to the quick spread of IoT devices in a variety of industries, including manufacturing, transportation, healthcare, and critical infrastructure. Strong trust architectures are crucial as the ecosystem moves toward 6G-enabled environments, which are distinguished by ultra-low latency, high bandwidth, and dense device deployments. Trust mechanisms in a quantum-secure Internet of Things setting need to be resilient against the computational might of quantum adversaries in addition to addressing more conventional security issues like integrity, authorization, and authentication.

8.1 Foundations of IoT Trust

In IoT networks, trust is the confidence that participating devices, users, and services will act in a predictable and safe way. When devices perform vital tasks or exchange sensitive data, this assurance is crucial. IoT trust models usually depend on factors like policy enforcement, cryptographic validation, behavioral history, and device identity verification. Public key infrastructures (PKI) and digital certificates serve as the foundation of trust in traditional systems, but they are susceptible to attacks from quantum computers that can decipher popular algorithms like RSA and ECC. Trust architectures need to be redesigned to incorporate secure key management systems, dynamic trust evaluation frameworks that adjust to shifting network conditions, and quantum-resistant cryptographic techniques in order to meet future challenges. This entails taking into account the distributed nature of IoT deployments, resource constraints, and device heterogeneity.

8.2 Quantum-Safe Mechanisms' Function in Building Trust

Establishing trust in the post-quantum era is largely dependent on cryptographic schemes that are impervious to quantum attacks. Vulnerable classical techniques are being replaced by post-quantum cryptography algorithms, such as hash-, code-, and lattice-based schemes. Identity verification, data exchange, and transaction validation are all protected when these algorithms are incorporated into trust architectures. Furthermore, a layered security approach is provided by the combination of post-quantum algorithms and quantum key distribution (QKD). While post-quantum algorithms safeguard other protocol layers, QKD can offer unconditional key security. Energy-efficient cryptographic primitives and lightweight quantum-safe algorithms can be combined in hybrid approaches to preserve security and operational efficiency in the Internet of Things, where processing efficiency is crucial.

8.3 Quantum-Secure IoT Trust Management Models

The concepts, procedures, and algorithms used to evaluate and uphold trust in a distributed system are defined by trust management models. Three general trust models are especially pertinent to quantum-secure IoT networks:

- **Centralized Trust Models:** Credentials for trust are assessed and issued by a central authority. This method has single-point-of-failure and scalability issues, despite being easier to administer. Post-quantum PKI infrastructures and quantum-resistant certificate authorities would be necessary for quantum-secure centralized systems.

- **Distributed Trust Models:** In this method, several parties work together to assess trust, and trust records are safely stored using distributed ledger technology or blockchain. Tamper-resistant trust propagation is made possible by the immutability of blockchain technology in conjunction with quantum-safe consensus techniques.
- **Hybrid Trust Models:** These maximize resilience, scalability, and dependability by combining distributed and centralized features. Blockchain-based frameworks for continuous trust assessment and audit, and central authorities for initial onboarding, are examples of hybrid systems.

8.4 Trust Measures and Assessment in a Post-Quantum Environment

In IoT networks, trust is frequently assessed using a variety of metrics, including availability, data integrity, dependability, energy usage trends, and security protocol compliance. Quantum resilience parameters, such as algorithm robustness against Shor's or Grover's algorithms, quantum-safe certificate validity, and secure key exchange latency, must be added to these metrics in a post-quantum setting. These new metrics can be added to machine-driven trust evaluation techniques, enabling real-time device trust scoring. These ratings may have an impact on network resource allocation, data sharing authorization, and routing choices. For instance, until its security posture is strengthened, a device with a low quantum-resilience score might only be allowed to handle non-essential data flows.

8.5 Trust Architectures Powered by Blockchain

Decentralized trust in quantum-secure IoT systems can be based on blockchain technology. Blockchain removes the need for a fully centralized trust authority by storing transactions, trust ratings, and security credentials on a tamper-resistant ledger. Blockchain-enabled trust architectures can guarantee that recorded data is still verifiable even against quantum adversaries when combined with post-quantum cryptographic signatures. In order to resist quantum attacks, consensus algorithms must also adapt. For instance, quantum-resistant consensus mechanisms can be used to strengthen or replace traditional proof-of-work or proof-of-stake schemes, lowering the possibility of ledger manipulation.

8.6 Difficulties in Putting Trust Architectures into Practice for Quantum-Secure IoT

Although the idea of quantum-secure trust architectures seems promising, there are still a number of obstacles to overcome:

- **Computational Overhead:** Post-quantum cryptography algorithms frequently require more resources than their classical counterparts, which presents challenges for IoT devices with limited resources.
- **Interoperability:** Standardization efforts are necessary to guarantee compatibility between devices that use various quantum-safe schemes.
- **Scalability:** It's not easy to maintain secure communications and trust assessments across billions of IoT nodes.
- **Dynamic Threat Landscape:** Trust infrastructures must be flexible and upgradeable due to the ongoing development of quantum algorithms.
- **Integration with Legacy Systems:** Phased transition strategies are necessary because many IoT deployments involve legacy devices that lack quantum-safe capabilities.

A convergence of technologies is probably in store for the future of trust architectures in quantum-secure IoT. Adaptive and scalable solutions can be obtained by combining blockchain-based decentralized trust models with AI-assisted trust evaluation and lightweight post-quantum cryptography algorithms. Protection will be further improved by research into hardware-assisted trust anchors, such as quantum-safe secure elements. Determining universally applicable

interoperability standards and trust frameworks will require international cooperation. Prior to widespread deployment, testbeds and pilot deployments will assist in confirming performance, locating bottlenecks, and improving trust mechanisms.

In order to survive quantum threats in the 6G era, trust architectures the foundation of secure IoT communications must adapt. Building IoT networks that maintain integrity, confidentiality, and dependability even in the face of sophisticated quantum adversaries is feasible by combining post-quantum cryptography, blockchain frameworks, and adaptive trust evaluation models. In the upcoming decades, these kinds of architectures will play a key role in enabling safe, extensive, and robust IoT deployments for vital applications.

9. Open Research Challenges

A revolutionary route to safe, high-performing digital ecosystems is provided by the convergence of the Internet of Things (IoT) with 6G networks, post-quantum cryptography, blockchain technology, and trust management frameworks. However, before quantum-secure IoT networks can be widely deployed, a number of unresolved technical, operational, and policy-related issues need to be addressed. These issues include interoperability, network scalability, energy optimization, standardization, governance, and cryptographic efficiency. In order to guarantee that the anticipated advantages of quantum-resilient architectures are actually achieved, it is imperative that these issues be resolved.

9.1 Post-Quantum Cryptography's Scalability in Internet of Things Devices

Compared to traditional algorithms like RSA or ECC, post-quantum cryptography algorithms like lattice-based, code-based, and multivariate schemes frequently call for larger key sizes and more processing power. IoT devices, which normally have limited processing power, memory, and battery life, are severely constrained by this rise in computational demand. Although lightweight post-quantum algorithms and hardware acceleration are being researched, it is still difficult to integrate them on a large scale. To create small, energy-efficient implementations that maintain security strength and are still feasible for embedded systems, more research is needed.

9.2 Energy Efficiency and Blockchain Throughput

Although blockchain's consensus mechanisms, like Proof of Work (PoW) or Proof of Stake (PoS), may require a lot of resources, they can provide decentralized trust for Internet of Things systems. Scalability issues may lead to higher transaction costs, more energy consumption, and network delays in high-density IoT networks intended for 6G. Although sharding, Layer-2 scaling, and new lightweight consensus protocols are being investigated, many of these strategies need to be tested in actual Internet of Things scenarios. In blockchain-integrated IoT networks, striking a balance between high throughput, low latency, and strong security is still a major challenge.

9.3 Managing Trust in Diverse Settings

A diverse range of devices, communication protocols, and application domains are commonly found in IoT deployments. It is difficult to create a single trust management framework that can handle different operational contexts, data sensitivity levels, and device capabilities. The static trust parameters or centralized authorities that are frequently used in existing trust models might not be well suited to the dynamic 6G IoT environments. An ongoing research priority is creating adaptive trust models that can integrate context awareness, real-time behavioral analysis, and historical reputation data without incurring undue computational overhead.

9.4 Standardization and Interoperability

Standardized protocols that guarantee smooth interoperability between devices, networks,

and security frameworks are critical to the success of quantum-secure Internet of Things systems. As of right now, there is no widely recognized standard for incorporating blockchain-based trust layers into heterogeneous networks or for post-quantum cryptography protocols in the Internet of Things. Cross-vendor compatibility is hampered by this lack of standardization, which may also delay worldwide adoption. To speed up the creation of common frameworks, industry-academic cooperation and active involvement from international standardization organizations are required.

9.5 Key Management with Quantum Safety

To stay safe from quantum adversaries, key generation, distribution, storage, and revocation processes need to be redesigned. Because they rely on algorithms that are susceptible to quantum attacks, traditional Public Key Infrastructures (PKIs) might not be directly compatible with post-quantum schemes. A transition path is provided by research into hybrid key exchange mechanisms, which combine classical and post-quantum algorithms. However, these solutions need to be thoroughly tested for performance and reliability. A critical issue is also the secure key lifecycle management for billions of IoT devices, many of which may be left unattended for years.

9.6 Real-time constraints and network latency

Ultra-low latency communication is necessary for many Internet of Things applications in the fields of healthcare, autonomous driving, and industrial automation. Due to computation and verification delays, integrating blockchain and post-quantum cryptography into the communication stack may result in higher latency. Achieving real-time responsiveness in resource-constrained environments is still challenging, even though 6G's high data rates and edge computing capabilities may help to mitigate some of these problems. To optimize consensus procedures and cryptographic operations for time-sensitive use cases, more study is required.

9.7 Data Sovereignty and Privacy Protection

IoT systems must protect privacy in accordance with laws like the GDPR and new data sovereignty regulations, in addition to protecting communications from quantum attacks. Although blockchain's transparency fosters trust, it may clash with privacy regulations, particularly when it comes to the storage of sensitive IoT data. Although they show promise, privacy-preserving strategies like off-chain storage with verifiable proofs, homomorphic encryption, and zero-knowledge proofs need to be further modified for low-power Internet of Things devices.

9.8 Quantum-secure Protocols with Limited Resources

One major challenge is to design quantum-resistant lightweight protocols that work well with low-power IoT devices. Due to their high bandwidth or memory requirements, many post-quantum algorithms can overwhelm devices with limited resources. Algorithmic optimizations, hardware-assisted security modules, and adaptive security mechanisms that can modify their cryptographic strength according to threat levels and device capabilities require further study.

9.9 Legal and Governance Structures

Without strong governance structures, technological advancements alone are insufficient. In cross-border IoT environments, the implementation of blockchain-based trust frameworks presents concerns regarding jurisdiction, liability, and accountability. In a similar vein, coordination between technology providers, standards organizations, and regulatory bodies is necessary for the deployment of post-quantum cryptography. Policy frameworks that can support innovation while addressing ethical issues, compliance, and dispute resolution are required.

9.10 Shift from Conventional to Quantum-Secure Systems

There will be a gradual shift from classical security protocols to quantum-secure

architectures, necessitating hybrid systems that can support both post-quantum and legacy algorithms. Security assurance, backward compatibility, and protocol design become more complicated during this coexistence phase. Furthermore, unless clear migration strategies are developed, adoption may be hampered by the significant costs and operational disruptions associated with large-scale infrastructure upgrades.

A wide range of technical and non-technical issues must be resolved in order to develop quantum-secure IoT networks for the 6G era. These consist of regulatory alignment, latency optimization, scalability, interoperability, algorithmic efficiency, and privacy protection. It will take cooperation from the fields of cryptography, blockchain engineering, network architecture, hardware design, and policy development to overcome these challenges. The goal of creating a secure, robust, and future-ready IoT ecosystem that is impervious to quantum threats can be accomplished by addressing these open research challenges.

10. Future Directions

The advent of 6G-enabled IoT systems and the impending effects of quantum computing call for a fundamental change in the way security, privacy, and trust are conceived and applied. Future developments in quantum-secure IoT networks will necessitate multi-layer technological innovations that combine decentralized control mechanisms, intelligent trust management, and cryptographic breakthroughs. The effective implementation of post-quantum cryptography (PQC) in resource-constrained Internet of Things devices is one important avenue. Despite the fact that many PQC algorithms have been proposed or standardized, their energy consumption, memory needs, and computational overhead continue to be a barrier to their integration in wearable technology, low-power sensors, and autonomous Internet of Things nodes. Future research should concentrate on hardware acceleration methods, lightweight PQC schemes, and network-condition-based adaptive cryptographic selection. Distributed ledger technologies (DLTs) and blockchain will also develop to satisfy the unique requirements of IoT ecosystems that are quantum resilient. Creating scalable consensus systems that can manage billions of linked devices without sacrificing security or throughput is part of this. Decentralized authentication, safe firmware updates, and reliable data sharing will probably be made possible by quantum-resistant blockchain protocols that use PQC-based signatures. Additionally, hybrid blockchain architectures that combine consortium, private, and public models might be best suited for Internet of Things settings where efficiency and latency are crucial. The next generation of IoT security frameworks will depend more and more on dynamic, context-aware trust evaluation models in the field of trust architectures. These models will use real-time threat intelligence, privacy-preserving analytics, and artificial intelligence to make decisions about trust on their own. Integrating zero-trust network principles into Internet of Things systems, where each device and transaction is constantly checked regardless of where it is located within the network perimeter, is one possible approach. The creation of IoT systems enabled by QKD is another important area of research. Developments in satellite-based quantum communication and integrated photonics may enable quantum-secure key exchange in larger IoT deployments, despite QKD's present limitations in terms of cost, range, and infrastructure needs. Hybrid models that combine PQC and QKD may provide increased resistance to both classical and quantum threats. In order to process PQC and blockchain workloads closer to IoT devices, minimize latency, and conserve bandwidth, edge and fog computing integration will be essential. Quantum-secure edge gateways that can carry out local authentication, encryption, and trust verification without totally depending on cloud infrastructure should be investigated in future architectures. The adoption of quantum-secure IoT will be shaped by standardization and regulatory alignment. Establishing interoperability standards, compliance frameworks, and

certification procedures for PQC, blockchain, and trust-based IoT systems will require concerted international efforts from academic institutions, business organizations, and governmental entities. The convergence of decentralized architectures, intelligent trust frameworks, and cryptographic innovation will define the future of quantum-secure IoT networks in the 6G era. Achieving genuinely resilient, long-term security in a world that is becoming more interconnected will require addressing computational efficiency, scalability, and interoperability.

11. Conclusion

As IoT networks advance into the 6G era, they present previously unheard-of possibilities for automation, intelligent connectivity, and real-time decision-making. However, traditional cryptographic techniques alone are unable to handle the disruptive security challenge brought about by the development of quantum computing. This review has examined how strong trust architectures, blockchain-based decentralization, and post-quantum cryptography can all work together to create quantum-secure Internet of Things networks. Adaptive trust models allow for continuous verification in dynamic and heterogeneous environments, blockchain offers transparent and tamper-resistant data management, and post-quantum algorithms provide resilience against future quantum attacks. Scalability, computational efficiency, and interoperability across various IoT ecosystems must all be carefully considered when integrating these technologies. Coordinated research, standardization initiatives, and workable deployment plans that take into account both technological and legal limitations will be necessary to realize this vision. Advanced communication architectures, distributed trust, and cryptographic innovation will be crucial in protecting IoT infrastructures in the quantum era as the shift to quantum-resilient security frameworks quickens.

Acknowledgment: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study

References

- [1] I. F. Akyildiz, A. Kak and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE access*, vol.8, pp.133995-134030, 2024.
- [2] W. Ahmad, A. Rasool, A.R. Javed, T. Baker and Z. Jalil, "Cyber security in iot-based cloud computing: A comprehensive survey," *Electronics*, vol.11, no.1, pp.16, 2021.
- [3] G.S. Mamatha, N. Dimri and R. Sinha, "Post-quantum cryptography: Securing digital communication in the quantum era," arXiv preprint arXiv:2403.11741, 2024.
- [4] A.M.S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and Applications*, vol.5, no.3, pp.100193, 2024.
- [5] K.H.Wang, C.M. Chen, W. Fang and T.Y. Wu, "A secure authentication scheme for internet of things," *Pervasive and Mobile Computing*, vol.42, pp.15-26, 2017.
- [6] S.J. Chen and Y.H. Tsai, "Quantum-safe networks for 6G an integrated survey on PQC, QKD, and satellite QKD with future perspectives," *Computing and AI Connect*, vol.2, no.1, pp.1-10, 2025.
- [7] E. Zeydan, C. De Alwis, R. Khan, Y. Turk, A. Aydeger, T.R. Gadekallu and M. Liyanage, "Quantum Technologies for Beyond 5G and 6G Networks: Applications, Opportunities, and Challenges," arXiv preprint arXiv:2504.17133, 2025.
- [8] K.K.Vaigandla, R. Karne, M.K. Vanteru, M. Devsingh, D. Prasad, R.K. Siddoju and N. Dharavath, "Artificial Intelligence in Industrial IoT: Trends, Challenges, and Future Directions," *Journal of Computer Allied Intelligence*, vol.3, no.2, pp.37-55, 2025.

-
- [9] K.K. Vaigandla, "An Extensive Examination on IOT and Industrial IOT Attacks, Security, Detection Methods, Blockchain Solutions and Challenges," *Babylonian Journal of Internet of Things*, vol.2025, PP.89-100, 2025.
 - [10] K.K.Vaigandla, "Role of IoT and ML in Healthcare," *Babylonian Journal of Artificial Intelligence*, vol.2025, pp.23-36, 2025.
 - [11] J.Wang, M.K. Lim, C. Wang and M.L.Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Computers and Industrial Engineering*, vol.155, pp.107174, 2021.
 - [12] A. Dash, S. Pal and C. Hegde, "Ransomware auto-detection in IoT devices using machine learning," no. December, pp.1-10, 2018.
 - [13] T. Domínguez-Bolaño, O. Campos, V. Barral, C.J. Escudero and J. García-Naya, "An overview of IoT architectures, technologies, and existing open-source projects," *Internet of Things*, vol.20, pp.100626, 2022.
 - [14] V. Mandawaria, C. Majumdar, S. Park, N. Sharma, A. Nigam and J. Jung, "Grant-free massive access for LEO-satellite based 6G IoT networks," *In 2022 IEEE Globecom Workshops (GC Wkshps)*, pp. 862-867, 2022.
 - [15] A. C. Naik, M. K. Vanteru, B. Sanjeev, S. K. V, and K. K. Vaigandla, "A comprehensive survey on applications, security concerns, attack mitigation and secure routing in IoT," *Int. Res. J. Multidiscip. Scope*, vol. 5, no. 3, pp. 894–906, 2024
 - [16] U. Khadam, M.M. Iqbal, M. Alruily, M.A. Al Ghamdi, M. Ramzan and S.H. Almotiri, "Text data security and privacy in the internet of things: threats, challenges, and future directions," *Wireless Communications and Mobile Computing*, vol.2020, no.1, pp.7105625, 2020.
 - [17] N. Sharma and R. Ketti Ramachandran, "The emerging trends of quantum computing towards data security and key management," *Archives of Computational Methods in Engineering*, vol.28, no.7, pp.5021-5034, 2021.
 - [18] K.K.Vaigandla, N. Azmi, R. Podila and R.K.Karne, "A survey on wireless communications: 6g and 7g," *International Journal Of Science, Technology and Management*, vol.2, no.6, pp.2018-2025, 2021.
 - [19] K.K.Vaigandla, "Communication technologies and challenges on 6G networks for the Internet: Internet of Things (IoT) based analysis," *In 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, vol. 2, pp. 27-31, 2022.
 - [20] Q. Cui, X. You, N. Wei, G. Nan, X. Zhang, J. Zhang et al., "Overview of AI and communication for 6G network: fundamentals, challenges, and future research opportunities," *Science China Information Sciences*, vol.68, no.7, pp.171301, 2025.
 - [21] N. Sivapriya, M.K. Vanteru, K. K., Vaigandla and G. Balakrishna, "Evaluation of PAPR, PSD, Spectral Efficiency, BER and SNR Performance of Multi-Carrier Modulation Schemes for 5G and Beyond," *SSRG International Journal of Electrical and Electronics Engineering*, vol.10, no.11, pp.100-114, 2023.
 - [22] M.H. Alsharif, A. H. Kelechi, M.A. Albreem, S. A. Chaudhry, M.S. Zia and S. Kim, "Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions," *Symmetry*, vol.12, no.4, pp.676, 2020.
 - [23] Z. Qadir, K.N. Le, N. Saeed and H.S.Munawar, "Towards 6G Internet of Things: Recent advances, use cases, and open challenges," *ICT express*, vol.9, no.3, pp.296-312, 2023.
 - [24] K.K. Vaigandla and D.N.Venu, "A survey on future generation wireless communications-5G: multiple access techniques, physical layer security, beamforming approach," *Journal of Information and Computational Science*, vol.11, no.9, pp.449-474, 2021.
 - [25] K.K. Vaigandla and D.N. Venu, "Survey on massive MIMO: Technology, challenges, opportunities and benefits," 2021
-

- [26] C. De Alwis, P. Kumar, Q.V. Pham, K. Dev, A. Kalla, M. Liyanage and W.J. Hwang, "Towards 6G: Key technological directions," *ICT Express*, vol.9, no.4, pp.525-533, 2023.
- [27] A. G.Tripi, L. Iacobelli Rinieri and M. Prandini, "Security and trust in the 6g era: Risks and mitigations," *Electronics*, vol.13, no.11, 2162, 2024.
- [28] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp.1-5, 2020.
- [29] K.K. Vaigandla, M. K., Vanteru and M. Siluveru, "An extensive examination of the IoT and blockchain technologies in relation to their applications in the healthcare industry," *Mesopotamian Journal of Computer Science*, vol.2024, pp.1-14, 2024.
- [30] R. Yadav, K.K. Vaigandla, G.P. Ghantasala, R. Singh and D. Gangodkar, "The block chain technology to protect data access using intelligent contracts mechanism security framework for 5G networks," *In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 108-112, 2022.
- [31] K.K.Vaigandla, R. Karne, M. Siluveru and M. Kesoju, "Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications," *Mesopotamian journal of Cybersecurity*, vol.2023, pp.73-84, 2023.
- [32] B. Shrimali and H.B. Patel, "Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities," *Journal of King Saud University-Computer and Information Sciences*, vol.34, no.9, pp.6793-6807, 2022.
- [33] H. Hikal, M. Altarawneh, A.H. Ahmad, Z. Jaradat and A. Elfedawy, "Blockchain technology and virtual asset accounting in the metaverse," *In Technological Innovations for Business, Education and Sustainability*, pp. 71-78, 2024.
- [34] L.Hang and D.H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *sensors*, vol.19, no.10, pp.2228, 2019.
- [35] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp.1-5, 2020.
- [36] H.H.Pajoo, S. Demidenko, S. Aslam and M. Harris, "Blockchain and 6G-enabled IoT," *Inventions*, vol.7, no.4, pp.109, 2022.
- [37] W.Z. Khan, M. Raza and M. Imran, "Quantum cryptography a real threat to classical blockchain: Requirements and challenges," *Authorea Preprints*, 2022.
- [38] A. Alkhayyat and M. Adhikari, "Blockchain-aided Integrated Edge Framework of Cybersecurity for Internet of Things," 2022
- [39] T. Vidick and S. Wehner, "Introduction to quantum cryptography," *Cambridge University Press*, 2023.
- [40] S.Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar et al., "Advances in quantum cryptography," *Advances in optics and photonics*, vol.12, no.4, pp.1012-1236, 2020.
- [41] G. Brassard and C.A. Fuchs, "Quantum foundations in the light of quantum cryptography," 2005.
- [42] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati et al., "Using quantum key distribution for cryptographic purposes: A survey," *Theoretical Computer Science*, vol.560, pp.62-81, 2014.
- [43] M.H. Adnan, Z. Ahmad Zukarnain and N.Z. Harun, "Quantum key distribution for 5g networks: A review, state of art and future directions," *Future Internet*, vol.14, no.3, pp.73, 2022.
- [44] M.S. Peelam, A.A. Rout and V. Chamola, "Quantum computing applications for Internet of

-
- Things,” *IET Quantum Communication*, vol.5, no.2, pp.103-112, 2024.
- [45] M.Z. Ali, A. Abohmra, M. Usman, A. Zahid, H. Heidari, M.A. Imran and Q.H. Abbasi, “Quantum for 6G communication: A perspective,” *IET Quantum Communication*, vol.4, no.3, pp.112-124, 2023.
- [46] R. Saini, A. Bera, B.K. Behera, E.A. Ahmed, M. Jamjoom and A. Farouk, “Designing quantum blockchain system integrated with 6G network,” *Journal of King Saud University-Computer and Information Sciences*, vol.35, no.10, pp.101847, 2023.
- [47] R. Asif, “Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms,” *IoT*, vol.2, no.1, pp.71-91, 2021.
- [48] E. Lella and G. Schmid, “On the security of quantum key distribution networks,” *Cryptography*, vol.7, no.4, pp.53, 2023.
- [49] M.A.Obaidat, M. Rawashdeh, M. Alja’afreh, M. Abouali, K. Thakur and A. Karime, “Exploring IoT and blockchain: a comprehensive survey on security, integration strategies, applications and future research directions,” *Big Data and Cognitive Computing*, vol.8. no.12, pp.174, 2024.
- [50] M.A. Uddin, A. Stranieri, I. Gondal and V. Balasubramanian, “A survey on the adoption of blockchain in iot: Challenges and solutions,” *Blockchain: Research and Applications*, vol.2, no.2, pp.100006, 2021.