Vol.3, No.6, Page 1467- 1480, 2025 https://doi.org/10.59628/jast.v3i6.1953 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

A Conceptual Blockchain Architecture for Dynamic Spectrum Access in 6G CR-IoT Networks: An Analytical Review

NASSMAH Y. AL-MATARI * and AMMAR T. ZAHARY

Department of Information Technology, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.

*Corresponding author: nsma.almtri@su.edu.ye

Abstract

Even though 6G networks will provide not just terabit-level throughput and sub-millisecond-level latency but also connect exponentially more devices, the explosive growth of IoT applications is fueling an unprecedented demand for wireless spectrum. Traditional, static allocation schemes can't keep up with this scale and dynamism, leading to underuse and conflict. Most blockchain solutions for dynamic spectrum access lack robust security measures against emerging quantum-era threats and do not incorporate quantum-resistant cryptography, which is essential in future 6G environments. In this research article, we propose a five-layer conceptual blockchain architecture to enable DSA in 6G cognitive radio IoT networks, combining a permissioned PBFT blockchain with quantum-secure cryptography (ECC and QKD), smart contracts, edge-computing nodes, and AI-driven spectrum intelligence, the architecture integrates trust management, quantum-safe cryptography, and intelligent decision-making to ensure reliable spectrum access in future 6G environments. The system model, layered architecture, and associated security and consensus mechanisms are presented. While implementation remains future work, this conceptual design offers a strong theoretical foundation for building robust, secure, and scalable spectrum management systems in next-generation wireless networks.

Article Info

Keywords:
Blockchain, DSA, 6G, Cognitive Radio, IoT, Smart Contracts, PBFT, Quantum-Secure Cryptography.

Article History:
Received: 4-July-2025,
Revised: 11-August-2025,
Accepted: 27-August-2025,
Available online: 28 December 2025.

1. INTRODUCTION

The rapid evolution of the intelligent information age has catalyzed transformative advancements across healthcare, transportation, smart cities, and industrial automation, which demand unprecedented levels of connectivity, ultralow latency, and massive data exchange. Sixth-generation (6G) networks are poised to meet these requirements by offering terabit-per-second throughputs, submillisecond latencies, and support for millions of devices per square kilometer [1] [2]. Unlike their 5G predecessors, 6G's flexible, scalable architecture will enable ubiquitous, anywhere-anytime communication for everything [3], delivering ultra-reliable, low-latency, high-speed performance essential for applications such as autonomous systems, immersive virtual environments, and next-generation smart city services [4]. Simultaneously, the Internet of Things (IoT) has evolved into a fundamental component of modern life, emerging as a new paradigm that integrates intelligent devices, applications, and technologies to automate our environments and digitally map the physical world. This integration enables real-time data collection, monitoring, and visualization in the digital domain [5], [6]. By 2034, over 24 billion IoT devices will be connected worldwide [7], driving an enormous demand for secure, high-performance, and spectrum-efficient communication infrastructures. However, this explosive growth presents a critical challenge, namely spectrum scarcity. The increasing density of wireless terminals and data-intensive applications makes static spectrum allocation schemes impractical and inefficient, resulting in underutilization and increased interference [8] [9] [10]. To address this concern, Cognitive Radio (CR) has been proposed as the best potential creation. The CR permits secondary (unlicensed)

users to opportunistically use holes in the spectrum, thus not interfering with primary (licensed) users [11] [12], [13]. Because CR-enabled IoT (CR-IoT) devices can sense spectrum environments in real time and dynamically adjust their transmission to utilize idle frequencies, spectrum efficiency and Quality of Service (QoS) can be improved [14],[15]. Cognitive radio IoT (CR-IoT) networks are naturally susceptible owing to their dynamic and distributed nature. This creates an opportunity for adversaries to launch unauthorized access attempts, Sybil attacks, SSDFs, PUEs, and eavesdropping, all of which undermine the integrity of spectrum-allocation decisions [16]. These types of attacks undermine mutual trust and worsen reliability and performance in IoT's fragmented, decentralized landscapes that require interoperable, real-time decision-making among nodes spread across vast geographies.

To overcome such obstacles, this paper proposes a safe and extensible multilayered design that combines blockchain innovations with a cognitive radio system setup in a 6G IoT atmosphere. Blockchain technology provides decentralized and tamper-resistant infrastructure for logging spectrum-related events, enforcing policies through smart contracts, and establishing trust between distributed devices [1],[2][17]. By further adopting quantum-resilient cryptographic techniques including Elliptic Curve Cryptography (ECC) and Quantum Key Distribution (QKD), the proposed framework improves confidentiality, authentication, and robustness against impending quantum dangers. Smart decision-making enabled by AI algorithms is applied at the application layer, allowing for the identification of anomalous behavior and optimization of spectrum access strategies in real time.

The remainder of this paper is organized as follows. Section (2) summarizes the methodology used to design and test the proposed architecture. Section (3) covers the key enabling technologies for 6G, including cognitive radio networks, blockchain technology for resource management, and post-quantum security. Section (4) surveys the related work on secure dynamic spectrum access. In Section (5), we describe the system model and formulate the problem. Section (6) discusses the proposed layered architecture and its parts. Section (7) describes the consensus mechanisms and the cryptographic strategies used. Section (8) provides an overview of the main benefits and drawbacks of the framework. Section (9) presents a discussion of the conclusions and recommended areas for further research.

2. METHODOLOGY

With respect to the security, trust, and performance challenges in DSA, this study uses a conceptual design methodology to derive a layered architecture for dynamic spectrum access within 6G CR-IoT networks. The process starts with an analytical evaluation of the performance goals of 6G, for example, ultralow latency, ultrahigh reliability, and massive device connectivity, and the effect of these goals on spectrum management in a cognitive environment. Following these requirements, the architecture is organized into five interoperable functional layers: Physical, Network, Blockchain, Cryptographic and Application. Every layer is precisely articulated with clear roles, technologies, and interdependencies, including advanced mechanisms like spectrum sensing, decentralized consensus (PBFT), postquantum cryptography (ECC + QKD), and AI-driven threat detection. Logical interactions and data flows between the layers are modeled to represent end-to-end spectrum access processes from robust real-time spectrum sensing to secure distributed decision-making. Furthermore, we introduce a theoretical evaluation framework that can be used to conceptually assess important system properties, such as latency, throughput, scalability, and resistance to adversarial threats, providing a comparative perspective to existing centralized and auction-based spectrum access models.

3. BACKGROUND

This section lays the groundwork by establishing key technological trends and challenges that ground our proposed architecture, from next-generation wireless systems to the security architectures required for resilient 6G CR-IoT deployments.

3.1. Sixth Generation (6G) Networks

Wireless technology today is a far cry from 1G's voice-only service to today's 5G multi-gigabit speeds, ultra-reliable low-latency communication (URLLC), massive MIMO, millimeter-wave bands, and support for applications including VR, UAVs, IoT, and V2X [18],[19],[20]. Deployed worldwide by 2020, 5G subscriptions skyrocketed to nearly 2.1 billion by the end of 2024, almost double that of 2023, and are projected to reach 5.5 billion by 2029 [21],[22]. Riding the decade-long generational cycle, 6G will come in with the next decade, roughly around 2030, [23] aiming for terabit-per-second throughputs, submillisecond latencies, and device densities over 10 devices/km^2 [24],[25]. To cope with the increasing IoE requirements from autonomous vehicles to remote health monitoring, 6G will unify terrestrial and non-terrestrial links, leverage terahertz and visible-light communications, and complex access-backhaul topologies, ensuring massive QoS improvement, security, and AI-based optimization over 5G [20][26]. As shown in Table(1), the performance enhancement of 6G is substantial in comparison to 5G [3],[26],[27],[28]. According to previous studies [22],[29], the rapid exponential growth of IoT is the high-density deployment of 6G, which creates digital twins of physical worlds and enhances cognitive ma-

chines through super intelligence. To ensure increasingly faster data rates, every wireless generation has opened larger bands, from 3 to 6 GHz and 24–50 GHz in 5G to terahertz (0.3–10 THz) and even optical spectra in 6G, providing up to 1,000× more throughput. To ease congestion below 6 GHz, regulators open centimeter-wave (3–30 GHz) and even higher mmWave bands (30–300 GHz). The intervening 275–300 GHz band connects mmWave to the far-infrared using sub-millimeter wavelengths to support ultra-high-capacity free-space links [30],[31].

Table[1]: Comparison of 5G and 6G performance indicators.

KPIs	5G	6G
Peak data rate	10–20 Gbps	1 Tbps
Latency	1 ms	0.1 ms
Reliability	99.99%	$>$ 99.99999%
Device density	1 million/km^2	10 million/km
Spectral efficiency	30 bps/Hz	100 bps/Hz
Mobility	500 km/h	1000 km/h
Frequency range	600 MHz to 100 GHz	95 GHz to 3 THz
Max. frequency	100 GHz	10 THz
Max. bandwidth	1 GHz	100 GHz
AI	Partial	Fully
Security	Medium	Further strengthened

3.2. Internet of Things and Spectrum Demands

As mentioned in the previous section, 6G mobile networks are heralded to achieve unprecedented levels of speed, connectivity, reliability, and energy efficiency while reducing latency. Among the challenges ahead of 6G networks is a crucial challenge of spectrum scarcity, caused by the growing connected devices and data requirements:[32] when massive IoT terminals bring spectrum access of mobile communications to billions of devices connecting, the available spectrum resources are scarce and affect the communication requirement for each terminal [9],[10]. As IoT applications become ubiquitous, new challenges arise. CRNs, a relatively new yet widely adopted alternative approach, have proven to be effective in creating intelligent next-generation networks. They improved the spectrum allocation and utilization of IoT devices[12].

3.3. Cognitive Radio and Dynamic Spectrum Access

Although dynamic spectrum access (DSA) techniques are lauded as a solution, spectrum scarcity has been exacerbated by the swift growth of wireless IoT rollouts [33]. CR technology, which was first created to solve this problem, provides a potential game-changing solution by allowing IoT devices to dynamically tap into an underutilized licensed spectrum [34]. This integration, termed Cognitive Radio IoT (CR-IoT), enables devices to constantly sense the wireless environment, identify the currently available spectrum bands (called "spectrum holes"), and opportunistically use these unoccupied channels without negatively affecting primary users (PUs)[35],[36],[37]. In the example shown in figure(1), CR networks dynamically change transmission settings and promiscuously assign a spectrum to secondary users (SUs), thus increasing spectrum use and network efficiency through interweave (transmit when idle), underlay (power-limited coexistence), and overlay (orthogonal signaling) models. CR can enable billions of IoT devices, extending the spectrum burden from 76 GHz under fixed assignments to as low as 19 GHz using DSA. Moreover, with the help of spectrum holes and real-time spectrum resource management, DSA further increases spectrum utilization, improves efficiency, and supports opportunistic access without requiring extra bandwidth acquisition [35],[38],[39],[40].

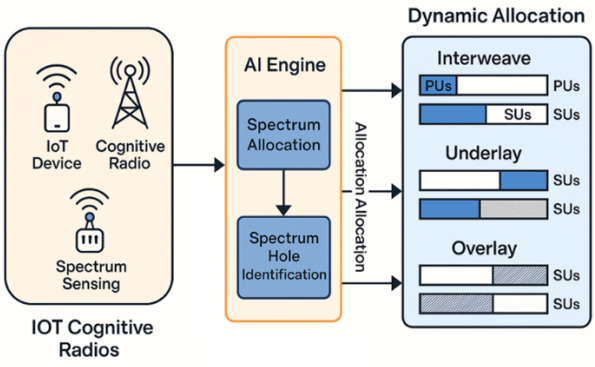

Figure 1. DSA Mechanism in Cognitive Radio for IoT.

3.4. Security in CR-IoT

CR-IoT networks face several security and privacy issues related to their dynamic spectrum access and distributed infrastructure. In addition to the wide flexibility of attack vectors, these systems are susceptible to attacks, such as Spectrum Sensing Data Falsification (SSDF), Primary User Emulation (PUE), Sybil attacks, eavesdropping, and denial-of-service (DoS) attacks [16],[41],[42],[43]. Without the ability to guarantee the integrity of spectrum sensing, access decisions can be corrupted, and

the integrity of communication among rapidly expanding, ever-more interconnected devices may be lost. Moreover, physical-layer vulnerabilities such as jamming and tampering threaten system reliability and data confidentiality. Identity spoofing and unauthorized spectrum monitoring lead to privacy concerns, especially in large and heterogeneous IoT deployments [43],[44],[45]. Given the decentralized, opportunistic nature of CR-IoT, it requires a departure from traditional centralized security models, highlighting the need for adaptive and context-aware threat mitigation strategies [41].

3.5. Blockchain and Decentralization

The stable development of blockchain technology is attributed to its decentralized architecture, cryptographic integrity, and capability to develop network environments with security and trust elimination, which has led to its rapid embrace by both academia and industry [46]. First presented by Nakamoto in 2009 as the underlying technology for Bitcoin [47], blockchain has since been transformed into a revolutionary, foundational technology that is sweeping across multiple industries, ranging from telecommunications and finance to industrial IoT. Blockchain with IoT guarantees data integrity, facilitates security, and enables decentralized decision making across heterogeneous and large-scale environments [48]. Blockchain is a distributed digital ledger technology that allows different nodes in a decentralized peer-to-peer (P2P) network to collectively record, verify, and update a continuous ledger of transactions without the need for a central authority [49][50]. This decentralization removes any single point of failure, promotes greater transparency, and creates trust among previously untrusted parties through guaranteed data immutability and verifiability [1][51][46]. Within the milieu of 6G CR-IoT networks, blockchain offers a groundbreaking solution for decentralized spectrum access management, replacing centralized authorities prone to inefficiency and scalability issues. Its distributed architecture records all spectrum activities in an immutable cryptographically linked ledger, making tampering impossible [52],[53][54]. The blockchain's immutable ledger and decentralized consensus mechanisms enable a tamper-resistant environment that strengthens trust and mitigates common attacks in distributed systems [55]. Using permissioned blockchains, only authorized nodes, such as base stations, fusion centers, or trusted IoT devices, can participate in the consensus process, achieving a balance between scalability and control [54],[56]. Smart contracts built directly into the blockchain allow for more automatic enforcement of policies and rules of spectrum use, ensuring that the spectrum can be shared fairly and securely in real time [53],[57],[58]. As we detail in [59], blockchain reinforces cooperative spectrum sensing by removing centralized fusion centers, providing transparency, enabling distributed decision-making, and mitigating risks such as SSDF attacks via a public, auditable, tamper-resistant ledger. Consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) can provide consensus across the entire network on sensing data and access logs, allowing quick and secure coordination across decentralized CR-IoT infrastructures [60],[61]. Figure(2) shows the general architecture and flow of data of a blockchain-enabled decentralized spectrum management system in 6G CR-IoT networks, depicting major elements such as permissioned ledgers, smart contracts, consensus processes, and authorized nodes working in a distributed structure.

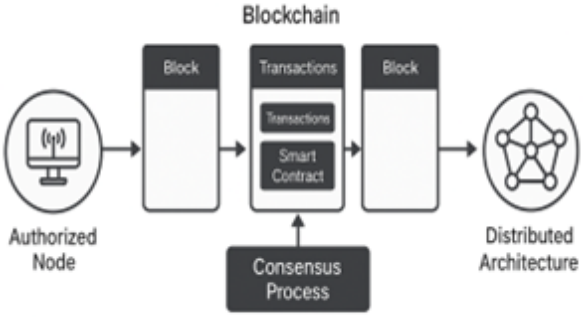

Figure 2. Blockchain-enabled decentralized spectrum management system.

Ultimately, the intrinsic properties of the blockchain provide scalable, resilient, and secure spectrum management, allowing 6G CR-IoT systems to flourish in a rich ecosystem of diverse wireless communication. Figure(3) shows a radar chart that contrasts the major characteristics of different network types. Public permissionless blockchains deliver high decentralization and security guarantees, although usually at the expense of scalability and privacy. Permissioned blockchains offer a middle ground, with security and scalability, as well as a consensus-driven governance model, which makes them ideal for more specialized applications such as 6G CR-IoT. Centralized systems value efficiency, control, and privacy over decentralization but are prone to single points of failure [56],[62].

3.6. Quantum-Safe Crypto

As 6G CR-IoT networks become more complex and larger in scale, their dependence on real-time spectrum sharing, decentralized decision-making, and massive device connectivity creates significant and unique security risks, particularly with the rise of quantum computing. Classic cryptography, such as RSA and standard ECC, has known vulnerabilities against quantum attacks [63], thus creating strong demands for quantum-safe crypto-

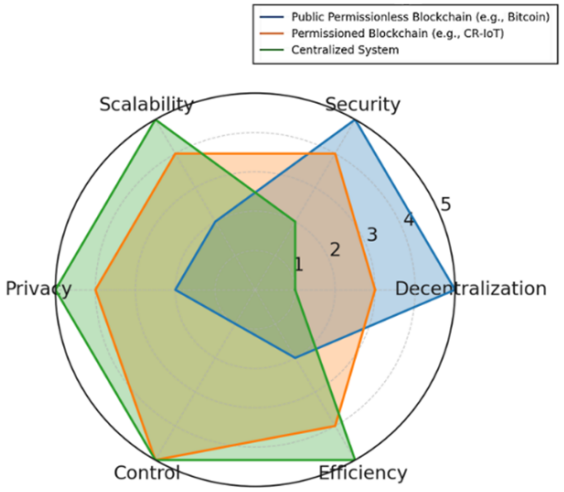

Figure 3. Comparative Radar Chart of Blockchain architectures.

graphic solutions. As analyzed in [43], combining ECC with Quantum Key Distribution (QKD) increases the confidentiality and integrity of spectrum access communications, while offering resistance against quantum-enabled attacks. [64] presented a two-layer security paradigm that combines QKD with Public Key Infrastructure (PKI) and smart contracts, enabling secure identity authentication, anti-tampering spectrum logs, and decentralized access management. Furthermore, [65] it highlights the benefits of integrating lightweight cryptographic primitives with AI-based spectrum management to reduce authentication latency, limit duplicate communication, and enhance spectrum sensing accuracy. Together, these strategies highlight the wealth of need for post-quantum cryptographic paradigms tailored to meet the dynamic, distributed, and latency-sensitive nature of 6G CR-IoT networks.

4. RELATED WORKS

Therefore, the secure and efficient management of DSA in CR-IoT systems is discussed with increasing interest in 6G networks. Our researchers have tested many different solutions, such as blockchain, artificial intelligence, and cryptographic mechanisms, to alleviate spectrum scarcity and security challenges. However, combining these technologies within a unified architecture that meets 6G performance expectations remains a challenge yet to be explored.

A number of these studies have investigated how blockchain technology can promote trust and decentralization and reduce the burden of central authorities in CR-IoT systems. For instance, Pajooh et al.[1] and Xu et al. [61] highlighted the security advantages of blockchain when paired with the 6G-enabled IoT. Jahid et al. [2] and Zainuddin et al. [66] examines how blockchain technology can help decentralize the control of data and provide auditability and privacy to massive IoT deployments. Most of these studies do not suggest any layered architecture or evaluate spectrum access in CR-specific settings. Other studies such as those by Wang et al.[54] and Reypnazarov et al.[13] examined the use of blockchain in spectrum governance. The Blockchain Radio Access Network (B-RAN) proposed by Wang et al. is an example of a secure and efficient model that can be tailored for future wireless systems. Reypnazarov's work explores smart contracts for dynamic spectrum allocation, but lacks post-quantum security considerations and realistic CR attack models. In the cognitive radio domain, studies by Al-Dulaimi et al.[67], Awin et al.[68], and Manco et al. [69] discussed spectrum sensing and management, and did not incorporate a new layer of security through the incorporation of blockchain or cryptographic resilience. Khaf et al.[70] proposed machine-learning-based sensing algorithms, such as PCMARL, to improve resilience; however, these lack a full-stack security framework.

Several recent studies have advanced the individual aspects of 6G CR-IoT security and resource management. Saraswathi and Dayana proposed a blockchain-based severity-aware attack mitigation system for CRNs using quantum cryptography and fuzzy logic, achieving strong detection accuracy, but focusing only on spectrum sensing without addressing scalable 6G spectrum governance [71]. Aljaedi et al. developed a lightweight quantum-chaotic encryption scheme for constrained IoT devices that offers post-quantum resilience, although it remains isolated from dynamic spectrum access frameworks [72].

Yaraziz and Hill reviewed resource allocation strategies for 6G-enabled IoT, highlighting AI-driven and distributed approaches; however, their work did not consider CR-specific spectrum scarcity or integrated security layers, such as blockchain or QKD [73]. Table (2) summarizes and contrasts the methodologies, focus areas, and limitations. In contrast, the architecture proposed in this study offers a comprehensive layered framework for secure, dynamic spectrum access. By combining blockchain (PBFT), ECC-QKD-based cryptography, and AI-enhanced spectrum governance, it fills not only the prior loopholes, but also the tighter requirements of the 6G CR-IoT system.

5. SYSTEM MODEL AND PROBLEM FORMULATION

This section introduces a systematic system model to realize secure and efficient spectrum sharing in decentralized 6G CR-IoT networks and formulates the fundamental DSA problem. The model addresses practical issues such as latency, interference, trust, and post-quantum security through a layered blockchain and cognitive radio integration.

Table[2]: Summary of Related Works and Contribution Gap.

Ref	Year	Objective	Domain (6G/CR/IoT/BCT)	Methodology	Main Contribution	Key Limitation
[68]	2019	Spectrum sensing taxonomy in CR-IoT	CR, IoT	Survey	Categorized sensing strategies	No integrated security
[39]	2020	Blockchain -based spectrum sharing in edge IoT	CR, IoT, BCT	Semi-distributed blockchain + edge computing	Virtual token (Xcoin), decentralized spectrum negotiation	No integration of cryptographic or quantum methods
[54]	2021	B-RAN for decentralized trust in 6G	6G, BCT	Blockchain Radio Access Network	Enhances trust in wireless systems	No AI or quantum security
[74]	2021	Cooperative DSA using blockchain with sensing-mining policies	CR, BCT	Token-based incentives + heuristic optimization	Improves sensing efficiency and miner fairness	Does not address full-stack security or AI integration
[1]	2022	Blockchain for secure 6G-IoT	6G, IoT, BCT	Conceptual architecture	Trust enhancement for 6G-IoT	No CR/DSA support
[70]	2022	SDF-resilient CR spectrum sensing	CR, IoT	PCMARL algorithm	ML-based sensing with coalition voting	No blockchain or 6G readiness
[13]	2023	Smart contract-based spectrum trading	CR, BCT	Blockchain + smart contracts	Transparent spectrum allocation	No cryptographic or AI integration
[75]	2024	Cooperative DSA using blockchain with sensing-mining policies	CR, BCT	Token-based incentives + heuristic optimization	Improves sensing efficiency and miner fairness	Does not address full-stack security or AI integration
[72]	2025	Lightweight post-quantum encryption for IoT	IoT, BCT	Quantum-chaotic + DWT + metaheuristics	Post-quantum IoT encryption	Not integrated into DSA {A lightweight encryption algorithm}
[73]	2025	Resource allocation in 6G IoT networks	6G, IoT	Game-theoretic + AI offloading	Distributed task scheduling and allocation	No CR or blockchain layer-Review of Resource Allocation
[71]	2025	Severity-aware attack mitigation in CRNs	CR, BCT	Blockchain + LRQF + GFHQDC	98.42% accurate mitigation of high-severity threats	No DSA scalability or 6G latency optimization
This Work	2025	Secure layered architecture for 6G CR-IoT spectrum access	6G, CR, IoT, BCT	Blockchain (PBFT), ECC-QKD, AI	Full-stack secure DSA with post-quantum resilience	Conceptual stage; future prototype needed

5.1. System Model

The proposed system models heterogeneous 6G-enabled CR-IoT environments, including Primary Users (PUs), Secondary Users (SUs), Base Stations (BSs), Edge Nodes, and a blockchain layer managed by a Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. The radio spectrum is licensed to Primary Users (PUs) but can be used opportunistically by Secondary Users (SUs) when the PUs are idle, facilitated by Dynamic Spectrum Access (DSA) methods. Each SU is endowed with cognitive radio functionalities for intelligent and dynamic spectrum sensing in real time, and each SU is in charge of reporting the spectrum status to the FC. Thus, the system considers the presence of adversarial SUs—nodes that can perform attacks such as PUE, SSDF, or Sybil attacks, seeking to distort the spectrum sensing results or command bandwidth. To counter these risks, both sensing data and access decisions are published in a permissioned blockchain, where edge devices and authorized nodes serve as validators. Smart contracts automatically enforce access policies, validate the trustworthiness of data [58], and provide a way to make all decision-making processes tamper-proof and fully auditable [46]. The cryptographic layer, underpinned by size-efficient ECC and Quantum Key Distribution (QKD), safeguards data transfers and confirms identities, thereby guaranteeing immunity against quantum-capable foes [43].

5.2. Problem Formulation

The goal of this work was to optimize DSA in a decentralized 6G CR-IoT environment. The objective is to ensure secure, fair, and efficient utilization of the underutilized licensed spectrum by authenticated, trustworthy Secondary Users while protecting Primary Users and maintaining ultra-low latency. To achieve this, the system incorporates blockchain consensus, quantum-safe cryptographic authentication, and AI-powered trust management.

Let:

- $S=\{s_1, s_2, ..., s_m\}$: Set of Secondary Users
- $C=\{c_1, c_2, ..., c_n\}$: Set of available spectrum channels
- $x_{ij} \in \{0,1\}$: Binary variable, where x_{ij}=1 if SU_{si} is granted access to channel c_j and x_{ij}=0 otherwise

The Objective Function is:

$$\max \sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} \quad (1)$$

That is Subject to the following constraints:

a. PU Protection Constraint:

$$x_{ij} = 0 \;\; if \; PU_j = active \quad (2)$$

Access is denied if the primary user occupies the channel, preserves PU priority, and avoids inter-ference [76].

b. Authentication Constraint (Quantum-Safe)

$$x_{ij} = 1 \;\; only \; if \; s_i \in V_{verified\ ECC+QKD} \quad (3)$$

SUs must be authenticated using quantum-resistant cryptography such as ECC-QKD be-fore being granted access [43].

c. Blockchain Validation Constraint

$$x_{ij} = 1 \; only \; if \; approved \; by \; Smart \; Contract_{\;PBFT} \quad (4)$$

Spectrum access requests must be validated through the PBFT consensus on blockchain us-ing smart contracts [77][60].

d. Latency Constraint (6G Compliance)

$$T_{access} \leq 1 \; ms \quad (5)$$

Access decisions must be completed within the sub-millisecond latency bounds required by 6G systems [78].

e. Trustworthiness Constraint (Adversary Resilience)

$$E\left[x_{ij}\right] \propto Trust\left(s_i\right), Trust \; updated \; by \; ML \quad (6)$$

The probability of providing access to the spectrum to each SU is proportional to a trust score that is updated in real-time using AI-based anomaly detection. This makes access decisions adaptive to behavioral trustworthiness and resistant to adversarial attacks [45].

This mathematical formulation guarantees that only authenticated, behaviorally trustworthy, and consensus-approved devices are granted access to the spectrum, while maintaining responsiveness to the environment and PUs. It augments resilience towards adversarial SSDF, PUE, and Sybil attacks, while ensuring cryptographic security and decentralized decision-making adapted for 6G CR-IoT ecosystems.

6. PROPOSED LAYERED ARCHITECTURE

This section introduces a five-layer conceptual architecture to facilitate secure and efficient dynamic spectrum access (DSA) in 6G Cognitive Radio Internet of Things

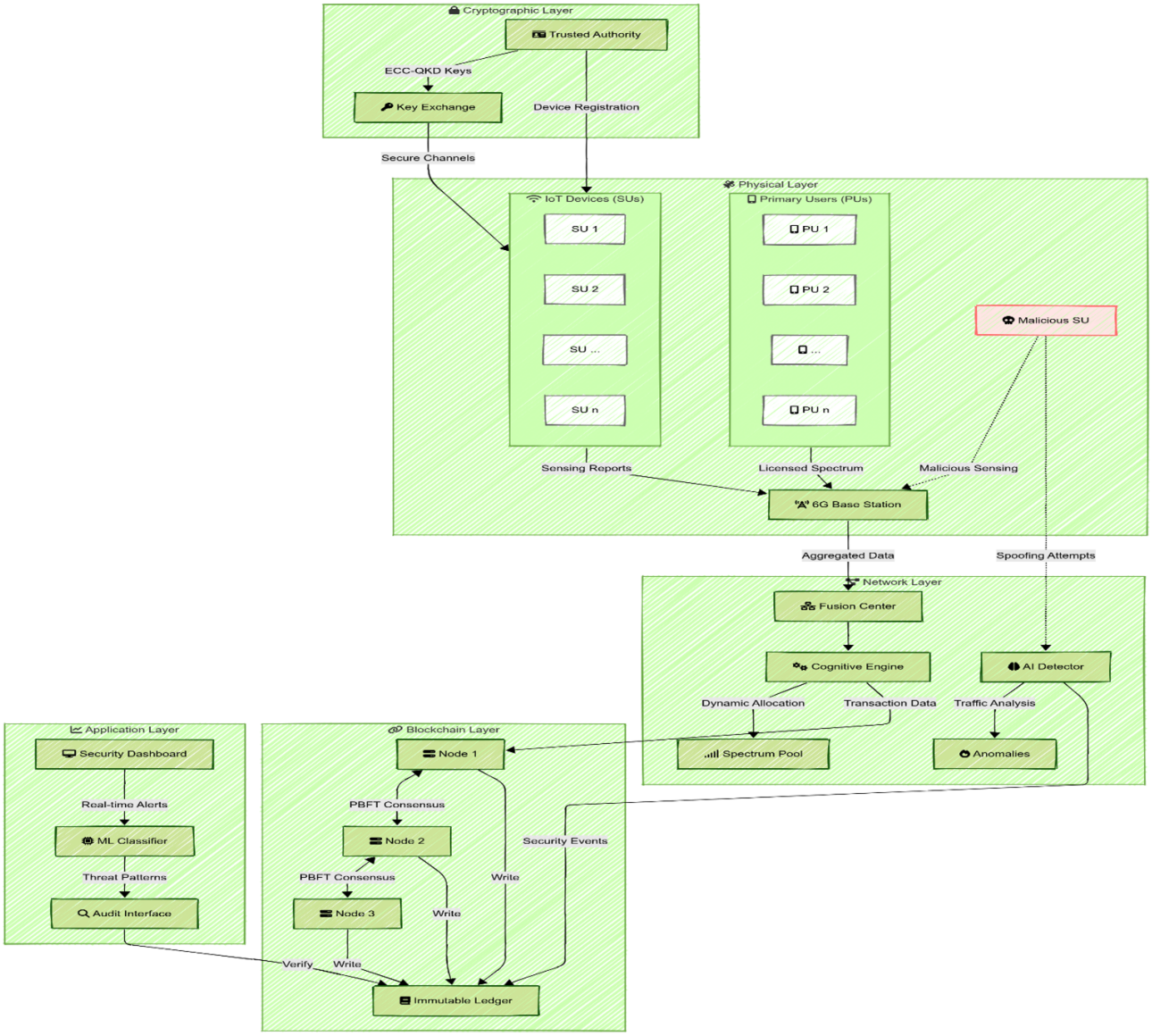

Figure 4. Multi-layered Architecture for Securing Dynamic Spectrum Access in 6G CR-IoT Networks.

(CR-IoT) networks. Every layer holds separate but overlapping responsibilities, from spectrum sensing in the physical layer to smart threat intelligence and blockchain-enabled spectrum governance. As shown in Figure(4), the architecture that supports the environment combines quantum-safe cryptography, permissioned blockchain, smart contracts, and machine learning to develop scalable, resilient, and decentralized spectrum sharing.

6.1. Physical Layer

The physical layer includes core wireless communication entities operating in a spectrum environment. Primary Users (PUs) are licensed users with guaranteed spectrum rights, and their transmissions take precedence. Secondary Users (SUs) are IoT devices equipped with cognitive radio capabilities that actively sense the spectrum to identify idle channels and opportunistically access them without interfering with the PUs [9][11][13]. Some devices may behave maliciously, called malicious SUs, by attempting to spoof primary user activity or submit falsified sensing reports. A 6G base station acts as a high-capacity access point, collecting sensing reports and supporting high-speed, ultra-reliable communication across a network [8]. This layer forms a sensing foundation upon which the higher-layer decisions are based.

6.2. Cryptographic Layer

The cryptographic layer secures the identity and authenticity of IoT devices before any interactions occur across the network layers [43], [72]. In the proposed architecture, each Secondary User (SU) must first be registered with a Trusted Authority (TA) to obtain cryptographic credentials. Once authenticated, the device generates an Elliptic Curve Cryptography (ECC) key pair and securely transmits its public key to the network. ECC was selected because of its strong security guarantees and

reduced computational load, making it ideal for resource-constrained IoT environments [79],[80]. To strengthen post-quantum resilience, A Quantum Key Distribution (QKD) session was attempted [81], [82]. If it is successful, the QKD-generated session key becomes the master key for data signing. Otherwise, the system reverts to the ECC-derived key. This dual-key strategy ensures both availability and security against emerging quantum attacks. After the key establishment, the SU signs its spectrum sensing reports using its ECC private key. These signed reports are forwarded to the validators who verify the signature and associated session key. Only reports from cryptographically valid devices were accepted for further processing. Invalid signatures or key mismatches result in data rejection and alert logged for potential malicious activity. Figure(5) Conceptual workflow outlining the step-by-step cryptographic workflow used at the SU level. This process consists of TA validation, key generation, QKD fallback logic, ECC signature application, and verification before data are passed to the network layer.

6.3. Network Layer

The network layer acts as the intermediate intelligence layer responsible for aggregating, validating, and analyzing the spectrum-sensing data. The Fusion Center collects reports from all SUs and conducts preliminary validation to eliminate flawed or inconsistent submissions [11], [14]. A Cognitive Engine processes validated reports to determine the spectrum availability using cooperative sensing logic. The engine also detects unusual traffic behavior and flagging anomalies such as sensing conflicts or suspicious access attempts [12], [70]. Once verified, the engine interacts with the Spectrum Pool Manager, which allocates the available channels to eligible SUs. Thus, the network layer filters malicious input, manages access contention, and prepares trustworthy access requests for blockchain validation.

6.4. Application Layer

The application layer delivers system-wide intelligence, high-level threat analytics, and decision automation by leveraging machine learning (ML) for both attack classification and trust estimation. This layer continuously monitors each Secondary User's (SU) behavior—specifically, their sensing consistency, report integrity, and access patterns—to identify abnormal or malicious activity. ML classifiers are trained to detect well-known attack vectors, including PUE, SSDF, Sybil, and Jamming attacks, where behavioral patterns deviate from statistical norms [38], [45], where behavioral patterns deviate from statistical norms. In cases of compromised or tampered reports (e.g., falsified channel occupancy claims), the system uses ECC to verify the legitimacy of the data. Valid signatures ensure that only trustworthy and untampered

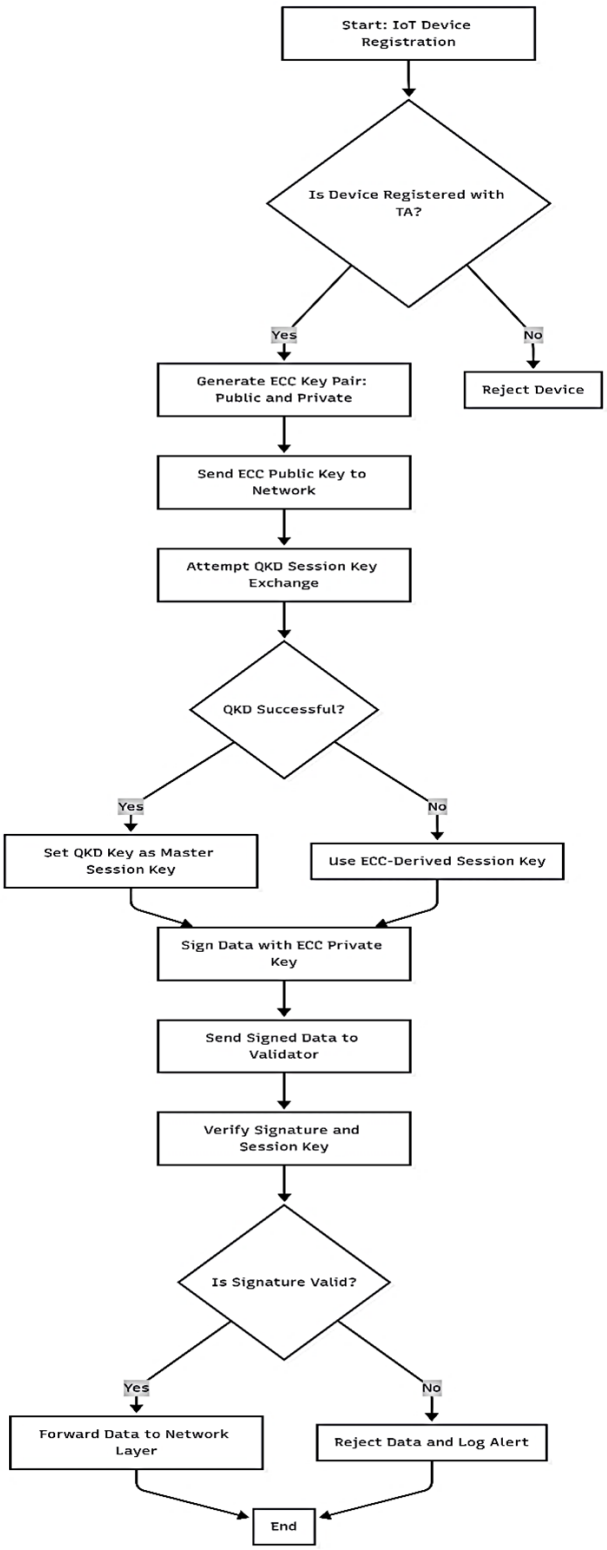

Figure 5. Cryptographic Workflow for 6G CR-IoT Devices.

sensing values are processed, thereby enhancing the reliability even under adversarial conditions. Additionally, ML-based trust metrics were computed for each SU by evaluating historical behavior, report accuracy, and communication integrity. These dynamic trust scores directly influence the weighting of sensing inputs during cooperative decision making and channel assignments,

reducing the influence of potentially malicious users. To ensure transparency and operator oversight, the application layer also incorporates a security dashboard and audit interface. The dashboard visualizes ongoing threats, flagged device identities, and trust scores in real time, whereas the audit interface allows system administrators and investigators to trace all actions through immutable blockchain records [83]. This synergistic integration of machine intelligence, cryptographic verification, and blockchain-based accountability enhanced both the responsiveness and resilience of the overall architecture.

6.5. Blockchain Layer

At the core of decentralized governance, the blockchain layer ensures that all spectrum-access decisions are transparent, verifiable, and tamper-proof. Permissioned validator nodes collaboratively execute a PBFT consensus protocol to approve or reject spectrum access requests, maintaining a low latency suitable for 6G IoT environments [74], [84]. Smart contracts deployed in this layer encode system-wide policies, including interference thresholds, trustworthiness constraints, behavioral audit history, and authorized access conditions, and automatically evaluate whether a device should be granted spectrum access [75]. These smart contracts interact closely with the network layer, which first aggregates and validates sensing data. Only finalized and filtered decisionsaugmented with trust metrics from the application layerare submitted to the blockchain. When an access request reaches the blockchain layer:

1- Smart contracts verify whether the request complies with policy rules.

2- Trust scores (computed via ML classifiers in the application layer) are checked against predefined thresholds.

3- The device's signature, verified earlier via ECC in the cryptographic layer, ensures identity legitimacy.

4- If access is approved, the spectrum allocation decision and its metadata (e.g., timestamp, SU ID, trust score, assigned channel) are recorded immutably on the distributed ledger.

The blockchain layer enables traceable and auditable spectrum access by recording the validated decisions on an immutable ledger. This ensures accountability, deters tampering, and supports decentralized trust among diverse IoT nodes. By bridging sensing validation, trust assessment, and access control, secure and scalable spectrum sharing in 6G CR-IoT networks is reinforced. This approach not only decentralizes trust but also creates an auditable trail of all sensing and access activities, strengthening accountability and eliminating single points of failure.

7. CONSENSUS AND SECURITY FEATURES

Our architecture lays the foundation for secure, transparent, and auditable dynamic spectrum access through the layered synthesis of consensus protocols and cryptographic primitives. Beyond engineering rigor, specifically at the blockchain layer, the architecture leverages the widely documented PBFT consensus algorithm, which is known for its high-throughput and fault tolerance in permissioned networks [60][77]. By enabling rapid consensus and coordination among distributed nodes such as base stations and edge servers, PBFT can help power the ultralow-latency-demanding environments of 6G. Ultimately, spectrum access requests that enter and exit the system would need to be validated through a decentralized consensus-based process, similar to what would have a supermajority of validator nodes approve each transaction. Systems of care are designed to improve health outcomes, provide satisfying patient experience, and control per capita costs [85]. This infrastructure design would greatly reduce the chance of unpermitted spectrum use, reduce double-reporting or false-reporting of sensing data, and increase the robustness in competitive or adversarial environments. To enhance the attack resilience against hardware, the architecture introduces a minimal cryptographic layer with ECC for low-power identity authentication and QKD for post-quantum secure key exchange. This dual-faceted strategy aims not only to boost performance but also to be future-proof, especially with regard to the growing threats posed by quantum dangers [86]. Devices would still need to sign sensing reports using ECC, but using ECC-based key exchange through QKD would bring unconditional secrecy to communication between trusted nodes. Moreover, the adoption of smart contracts — which allow access policies to be automatically enforced — embedded in the blockchain layer provides a robust new vehicle to do this. These smart contracts must be used to verify trust scores, verify digital signatures, and enforce restrictions, such as protection against unauthorized access [87][88]. While this architecture has not been implemented or empirically validated, it is designed in theory to address several other common vulnerabilities in CR-IoT, such as SSDF, PUE, Sybil attacks, identity impersonation, and unauthenticated or replay access requests. By integrating the PBFT consensus, quantum-safe cryptography, and trust-aware smart contracts, it offers a robust and scalable foundation for decentralized spectrum sharing within 6G CR-IoT networks. Future real-world implementation and simulation studies will be needed to validate its performance and security assertions in achieving these goals under real-world conditions.

Table[3]: Theoretical Advantages and Implementation Challenges of the Proposed Architecture [13],[19],[20],[23],[34],[66],[89] .

Feature / Component	Anticipated Advantages	Implementation Challenges
PBFT Consensus Protocol	Fast agreement among authorized nodes with fault tolerance; low energy use compared to PoW	Scalability to large validator networks; communication complexity in high-density deployments
Permissioned Blockchain	Decentralized yet controlled environment; tamper-proof spectrum access logs	Overhead in consensus delay; managing identity and role revocation
Smart Contracts for Access Control	Automated policy enforcement; trust-based spectrum decisions	Complexity of contract logic; security of smart contract code
ECC-based Authentication	Lightweight cryptographic signatures ideal for constrained IoT devices	Vulnerable to quantum attacks if QKD is unavailable; key management overhead
Quantum Key Distribution (QKD)	Quantum-resilient encryption; unbreakable key exchange for trusted node pairs	High infrastructure cost; feasibility limited to specific topologies
AI-based Trust Evaluation	Adaptive to new attack patterns; improves resilience against SSDF and Sybil attacks	Requires training datasets; risk of bias or false positives
Auditable Ledger for Spectrum Decisions	Enhanced accountability and transparency in spectrum allocation	Data privacy and storage cost of detailed sensing/access logs
Layered Modular Design	Supports separation of concerns and scalability across heterogeneous IoT nodes	Coordination between layers may introduce latency or integration complexity
6G Compatibility (Latency, Mobility, Density)	Designed to align with URLLC and mMTC goals of 6G	Real-time constraints under high load remain to be evaluated

8. ADVANTAGES AND CHALLENGES

The proposed conceptual architecture has several theoretical benefits designed to remedy the inequities associated with today's spectrum access designs in decentralized 6G CR-IoT networks. By combining the permissioned blockchain technology, quantum-safe cryptography, and AI-based trust evaluation, this architecture can offer increased scalability, transparency, and security for spectrum management. Second, as the architecture is yet to be deployed outside controlled settings, there are many challenges and open questions that persist, especially related to implementation viability, latency overheads, and trust modeling accuracy. These challenges extend to the feasibility of deploying QKD in large-scale networks, communication overhead of PBFT in dense environments, potential latency and security vulnerabilities in smart contract execution, and coordination complexity across all five architectural layers, which are detailed in Table(3).

9. CONCLUSION AND FUTURE DIRECTIONS

This paper introduced a conceptual layered architecture to cater to the security, trust, and efficiency challenges related to DSA in 6G CR-IoT networks. By combining advanced cognitive radio functionality to enhance blockchain-enabled decentralized governance mechanisms with quantum-safe cryptographic algorithms and AI-based trust networks, the resulting framework is intended to provide resilient, scalable, and auditable dynamic spectrum sharing. Each architectural layer—physical, network, cryptographic, application, and blockchain— is purposefully crafted to serve a distinct function, working in tandem to enable secure, decentralized access decisions. Although this model promises benefits such as tamper-proof auditability, adaptive threat mitigation, and compliance with 6G latency and throughput requirements, it remains at the conceptual stage. This design is theoretical and has not yet been validated under real-world or simulated conditions. Therefore, future work should be directed toward creating simulation prototypes with platforms such as OMNeT++, NS-3, or MATLAB to further test the performance under more realistic traffic and attack scenarios. Advancing lightweight post-quantum cryptographic protocols and scalable consensus mechanisms are pivotal for practical deployment. AI approaches for real-time trust management, governance, regulatory compliance on heterogeneous 6G infrastructures (e.g., UAVs, satellites, and edge nodes), and privacy-preserving blockchain technologies, including zero-knowledge proofs, are important research AI application foundations. In addition, future work will involve formal threat modeling, cryptographic strength proofs, and performance benchmarking under realistic attack scenarios to complement the conceptual design described herein. In short, this study is a key starting blueprint for constructing robust, secure, and intelligent spectrum access frameworks for dynamic next-generation wireless networks.

REFERENCES

[1] H. H. Pajooh, S. Demidenko, S. Aslam, and M. Harris, "Blockchain and 6g-enabled iot," *Inventions*, vol. 7, no. 4, p. 109, 2022. DOI: 10.3390/inventions7040109.

[2] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, iot and 6g: Potential, opportunities, challenges and research roadmap," *J. Netw. Comput. Appl.*, vol. 217, p. 103 677, 2023. DOI: 10.1016/j.jnca.2023.103677.

[3] R. Chataut, M. Nankya, and R. Akl, "6g networks and the ai revolution—exploring technologies, applications, and emerging challenges," *Sensors*, vol. 24, no. 6, p. 1888, 2024. DOI: 10.3390/s24061888.

[4] S. P. Tera, R. Chinthaginjala, G. Pau, and T. H. Kim, "Towards 6g: An overview of the next generation of intelligent network connectivity," *IEEE Access*, vol. 12, 2024. DOI: 10.1109/ACCESS.2024.3523327.

[5] A. Choudhary, "Internet of things: A comprehensive overview, architectures, applications, simulation tools, challenges and future directions," *Discov. Internet Things*, 2024. DOI: 10.1007/s43926-024-00084-3.

[6] X. Liu, M. F. Antwi-Afari, J. Li, Y. Zhang, and P. Manu, "Bim, iot, and gis integration in construction resource monitoring," *Autom. Constr.*, 2025. DOI: 10.1016/j.autcon.2025.106149.

[7] *Number of iot connected devices worldwide from 2019 to 2034*, Online, Statista, 2025.

[8] X. Liu, H. Ding, and S. Hu, "Uplink resource allocation for noma-based hybrid spectrum access in 6g-enabled cognitive internet of things," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15 049–15 058, 2021. DOI: 10.1109/JIOT.2020.3007017.

[9] A. U. Khan, G. Abbas, Z. H. Abbas, M. Bilal, S. C. Shah, and H. Song, "Reliability analysis of cognitive radio networks with reserved spectrum for 6g-iot," *IEEE Trans. on Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2726–2737, 2022. DOI: 10.1109/TNSM.2022.3168669.

[10] 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*, 2023. DOI: 10.1016/j.icte.2022.06.006.

[11] D. Pari and J. Natarajan, "Secure spectrum access, routing, and hybrid beamforming in an edge-enabled mmwave massive mimo crn-based internet of connected vehicle environments," *Sensors*, vol. 22, no. 15, 2022. DOI: 10.3390/s22155647.

[12] T. S. Malik et al., "Rl-iot: Reinforcement learning-based routing approach for cognitive radio-enabled iot communications," *IEEE Internet Things J.*, vol. 10, no. 2, pp. 1836–1847, 2023. DOI: 10.1109/JIOT.2022.3210703.

[13] E. Reypnazarov, H. Khujamatov, D. Das, D. Khasanov, E. Nurullaev, and T. Babazhanova, "Research of the application of blockchain and smart contract technologies in spectrum management and trading in cognitive radio networks," in *E3S Web of Conferences*, EDP Sciences, 2023. DOI: 10.1051/e3sconf/202345203005.

[14] M. Liu, H. Zhang, Z. Liu, and N. Zhao, "Attacking spectrum sensing with adversarial deep learning in cognitive radio-enabled internet of things," *IEEE Trans. on Reliab.*, vol. 72, no. 2, pp. 431–444, 2023. DOI: 10.1109/TR.2022.3179491.

[15] M. Khasawneh, A. Azab, S. Alrabaee, H. Sakkal, and H. H. Bakhit, "Convergence of iot and cognitive radio networks: A survey of applications, techniques, and challenges," *IEEE Access*, vol. 11, pp. 71 097–71 112, 2023. DOI: 10.1109/ACCESS.2023.3294091.

[16] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6g security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021. DOI: 10.1109/OJCOMS.2021.3078081.

[17] *2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland: IEEE, 2020.

[18] A. Mathew, "Artificial intelligence and cognitive computing for 6g communications & networks," *Int. J. Comput. Sci. Mob. Comput.*, vol. 10, no. 3, pp. 26–31, 2021. DOI: 10.47760/ijcsmc.2021.v10i03.003.

[19] K. M. Bin Hasan, M. Sajid, M. A. Lapina, M. Shahid, and K. Kotecha, "Blockchain technology meets 6g wireless networks: A systematic survey," *Alex. Eng. J.*, 2024. DOI: 10.1016/j.aej.2024.02.031.

[20] Y. Li, J. Huang, Q. Sun, T. Sun, and S. Wang, "Cognitive service architecture for 6g core network," *IEEE Trans. on Ind. Informatics*, vol. 17, no. 10, pp. 7193–7203, 2021. DOI: 10.1109/TII.2021.3063697.

[21] P. Taylor, *Forecast number of mobile 5g subscriptions worldwide from 2019 to 2028*, Statista, Accessed: Jun. 03, 2024, 2024.

[22] M. Gupta, R. K. Jha, and S. Jain, "Tactile based intelligence touch technology in iot configured wcn in b5g/6g-a survey," *IEEE Access*, vol. 11, pp. 30 639–30 689, 2023. DOI: 10.1109/ACCESS.2022.3148473.

[23] L. P. Rachakonda, M. Siddula, and V. Sathya, "A comprehensive study on iot privacy and security challenges with focus on spectrum sharing in next-generation networks (5g/6g/beyond)," *High-Confidence Comput.*, 2024. DOI: 10.1016/j.hcc.2024.100220.

[24] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Ai and 6g security: Opportunities and challenges," in *2021 Joint European Conference on Networks and Communications and 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 616–621. DOI: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[25] S. P. V, A. J. Albert, K. N. K. Thapa, and R. Krishnaprasanna, "A novel enhanced security architecture for sixth generation (6g) cellular networks using authentication and acknowledgement (aa) approach," *Results Eng.*, vol. 21, 2024. DOI: 10.1016/j.rineng.2023.101669.

[26] M. M. Aslam, L. Du, X. Zhang, Y. Chen, Z. Ahmed, and B. Qureshi, "Sixth generation (6g) cognitive radio network (crn): Application, requirements, security issues, and key challenges," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021. DOI: 10.1155/2021/1331428.

[27] M. Banafaa et al., "6g mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities," *Alex. Eng. J.*, 2023. DOI: 10.1016/j.aej.2022.08.017.

[28] W. M. Othman et al., "Key enabling technologies for 6g: The role of uavs, terahertz communication, and intelligent reconfigurable surfaces in shaping the future of wireless networks," *J. Sens. Actuator Networks*, 2025. DOI: 10.3390/jsan14020030.

[29] Y. Hao, Y. Miao, M. Chen, H. Gharavi, and V. C. M. Leung, "6g cognitive information theory: A mailbox perspective," *Big Data Cogn. Comput.*, vol. 5, no. 4, 2021. DOI: 10.3390/bdcc5040056.

[30] W. K. Alsaedi, H. Ahmadi, Z. Khan, and D. Grace, "Spectrum options and allocations for 6g: A regulatory and standardization review," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1787–1812, 2023. DOI: 10.1109/OJCOMS.2023.3301630.

[31] H. Viswanathan and P. E. Mogensen, "Communications in the 6g era," *IEEE Access*, vol. 8, pp. 57 063–57 074, 2020. DOI: 10.1109/ACCESS.2020.2981745.

[32] Y. Dursun, S. Al Basit, and Z. Ding, "Wireless powered noma-based cognitive radio for 6g networks," *Comput. Networks*, vol. 248, 2024. DOI: 10.1016/j.comnet.2024.110497.

[33] G. Narayan and A. Singh, "Future spectrum allocation for mobile broadband and internet of things," *Int. J. Sci. Res. Arch.*, vol. 14, no. 1, pp. 1848–1851, 2025. DOI: 10.30574/ijsra.2025.14.1.0308.

[34] C. S. Gowda, *Cognitive radio in iot and network security*, International Journal of Recent Research in Physics and Applied Sciences, Available online, 2022.

[35] M. Y. I. Idris, I. Ahmedy, T. K. Soon, M. Yahuza, A. B. Tambuwal, and U. Ali, "Cognitive radio and machine learning modalities for enhancing the smart transportation system: A systematic literature review," *ICT Express*, 2024. DOI: 10.1016/j.icte.2024.05.001.

[36] H. Al-Sudani, A. A. Thabit, and Y. Dalveren, "Cognitive radio and its applications in the new trend of communication system: A review," in *5th International Conference on Engineering Technology and its Applications (IICETA)*, IEEE, 2022, pp. 419–423. DOI: 10.1109/IICETA54559.2022.9888674.

[37] K. Lahrouni, H. Semlali, G. Andrieux, J.-F. Diouris, and A. Ghammaz, "A systematic literature review on spectrum detection for cognitive radio–internet of things networks," *Ad Hoc Networks*, p. 103 857, 2025.

[38] S. T. Muntaha, P. I. Lazaridis, M. Hafeez, Q. Z. Ahmed, F. A. Khan, and Z. D. Zaharis, "Blockchain for dynamic spectrum access and network slicing: A review," *IEEE Access*, vol. 11, pp. 17 922–17 944, 2023. DOI: 10.1109/ACCESS.2023.3243985.

[39] X. Fan and Y. Huo, "Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems," *IEEE Access*, vol. 8, pp. 64 486–64 498, 2020. DOI: 10.1109/ACCESS.2020.2985580.

[40] F. Li, K. Y. Lam, L. Meng, H. Luo, and L. Wang, "Trading-based dynamic spectrum access and allocation in cognitive internet of things," *IEEE Access*, vol. 7, pp. 125 952–125 959, 2019. DOI: 10.1109/ACCESS.2019.2937582.

[41] W. Khalid, M. A. U. Rehman, T. Van Chien, Z. Kaleem, H. Lee, and H. Yu, "Reconfigurable intelligent surface for physical layer security in 6g-iot: Designs, issues, and advances," *IEEE Internet Things J.*, 2023. DOI: 10.1109/JIOT.2023.3297241.

[42] P. Deepanramkumar and N. Jaisankar, "Blockcrn-iocv: Secure spectrum access and beamforming for defense against attacks in mmwave massive mimo crn in 6g internet of connected vehicles," *IEEE Access*, vol. 10, pp. 74 220–74 243, 2022. DOI: 10.1109/ACCESS.2022.3187745.

[43] N. Y. Al-Matari, A. T. Zahary, and A. A. Al-Shargabi, "A survey on advancements in blockchain-enabled spectrum access security for 6g cognitive radio iot networks," *Sci. Reports*, vol. 14, no. 1, 2024. DOI: 10.1038/s41598-024-82126-y.

[44] E. M. Ghourab, L. Bariah, S. Muhaidat, P. C. Sofotasios, M. Al-Qutayri, and E. Damiani, "Reputation-aware relay selection with opportunistic spectrum access: A blockchain approach," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 389–403, 2023. DOI: 10.1109/OJVT.2023.3263804.

[45] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly detection in 6g networks using machine learning methods," *Electronics*, vol. 12, no. 15, 2023. DOI: 10.3390/electronics12153300.

[46] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustain. Energy Technol. Assessments*, vol. 52, p. 102 039, 2022. DOI: 10.1016/j.seta.2022.102039.

[47] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, Online, Available at: https://www.bitcoin.org, 2008.

[48] A. T. Zahary and W. A. N. A. Alnbhany, "Blockchain-iot healthcare applications and trends: Review," *J. Sana'a Univ. for Appl. Sci. Technol.*, vol. 3, no. 1, pp. 577–586, 2025. DOI: 10.59628/jast.v3i1.1297.

[49] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Inf. Manag. Data Insights*, 2021. DOI: 10.1016/j.ijin.2021.09.005.

[50] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, "Accounting and auditing with blockchain technology and artificial intelligence: A literature review," *Int. J. Account. Inf. Syst.*, vol. 48, 2023. DOI: 10.1016/j.accinf.2022.100598.

[51] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-twin-enabled 6g: Vision, architectural trends, and future directions," *IEEE Commun. Mag.*, vol. 60, no. 1, pp. 74–80, 2022.

[52] Institute of Electrical and Electronics Engineers, *Dynamic spectrum access via smart contracts on blockchain*, IEEE, 2019.

[53] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, 2019. DOI: 10.1109/TCCN.2019.2914052.

[54] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: A new paradigm towards 6g," *National Sci. Rev.*, 2021. DOI: 10.1093/nsr/nwab069.

[55] F. AlHrazi, M. Algabri, and A. A. Al-Khulaidi, "Hierarchical blockchain as line defense of attacks to messages propagation in vanet," *J. Sana'a Univ. for Appl. Sci. Technol.*, vol. 1, no. 3, 2023. DOI: 10.59628/jast.v1i3.370.

[56] K. K. Vaigandla, M. Siluveru, M. Kesoju, and R. Karne, "Review on blockchain technology: Architecture, characteristics, benefits, algorithms, challenges and applications," *Mesopotamian J. Comput. Sci.*, 2023. DOI: 10.58496/MJCS/2023/012.

[57] A. Kalla, C. de Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6g: Technical aspects, use cases, challenges and research directions," *Internet Things*, 2022. DOI: 10.1016/j.jii.2022.100404.

[58] Q. Wu, W. Wang, Z. Li, B. Zhou, Y. Huang, and X. Wang, "Spectrumchain: A disruptive dynamic spectrum-sharing framework for 6g," *Sci. China Inf. Sci.*, Mar. 2023. DOI: 10.1007/s11432-022-3692-5.

[59] D. Balakumar and S. Nandakumar, "Blockchain-enabled cooperative spectrum sensing in 5g and b5g cognitive radio via massive mimo-noma," *Results Eng.*, vol. 24, 2024. DOI: 10.1016/j.rineng.2024.102840.

[60] Z. Zeng et al., "Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application," *Energies*, 2020. DOI: 10.3390/en13040881.

[61] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6g communications," *Digit. Commun. Networks*, vol. 6, no. 3, pp. 261–269, 2020. DOI: 10.1016/j.dcan.2020.06.002.

[62] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Networks*, vol. 7, no. 3, pp. 295–307, 2021. DOI: 10.1016/j.dcan.2020.05.008.

[63] K. K. Singamaneni, A. K. Budati, S. Islam, R. A. L. Kolandaisamy, and G. Muhammad, "A novel hybrid quantum-crypto standard to enhance security and resilience in 6g enabled iot networks," *IEEE J. Sel. Top. Appl. Earth Obs. Remote. Sens.*, 2025. DOI: 10.1109/JSTARS.2025.3540905.

[64] P. Deepanramkumar and A. Helensharmila, "Ai-enhanced quantum-secured iot communication framework for 6g cognitive radio networks," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3471711.

[65] M. N. Khan, S. Lee, and M. Shah, "Adaptive scheduling in cognitive iot sensors for optimizing network performance using reinforcement learning," *Appl. Sci.*, vol. 15, no. 10, 2025. DOI: 10.3390/app15105573.

[66] A. A. Zainuddin, N. F. Omar, N. N. Zakaria, and N. A. M. Camara, "Privacy-preserving techniques for iot data in 6g networks with blockchain integration: A review," *Int. J. on Perceptive Cogn. Comput.*, vol. 9, no. 2, pp. 80–92, 2023. DOI: 10.31436/ijpcc.v9i2.405.

[67] O. Al-Dulaimi, M. Al-Dulaimi, A. Al-Dulaimi, and M. O. Alexandra, "Cognitive radio network technology for iot-enabled devices," *Eng. Proc.*, vol. 41, no. 1, 2023. DOI: 10.3390/engproc2023041007.

[68] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical issues on cognitive radio-based internet of things systems: A survey," *IEEE Access*, vol. 7, pp. 97 887–97 908, 2019. DOI: 10.1109/ACCESS.2019.2929915.

[69] J. Manco, I. Dayoub, A. Nafkha, M. Alibakhshikenari, and H. Ben Thameur, "Spectrum sensing using software defined radio for cognitive radio networks: A survey," *IEEE Access*, vol. 10, pp. 131 887–131 908, 2022. DOI: 10.1109/ACCESS.2022.3229739.

[70] S. Khaf, M. T. Alkhodary, and G. Kaddoum, "Partially cooperative scalable spectrum sensing in cognitive radio networks under sdf attacks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8901–8912, 2022. DOI: 10.1109/JIOT.2021.3116928.

[71] S. Vedachalam and D. Raj, "Development of a severity-based attack mitigation system in cognitive radio networks using blockchain and gfhqdc," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3553628.

[72] A. Aljaedi, A. R. Alharbi, A. Aljuhni, M. K. Alghuson, S. Alassmi, and A. Shafique, "A lightweight encryption algorithm for resource-constrained iot devices using quantum and chaotic techniques with metaheuristic optimization," *Sci Rep*, vol. 15, no. 1, Dec. 2025. DOI: 10.1038/s41598-025-97822-6.

[73] M. S. Yaraziz and R. Hill, "A review of resource allocation for maximizing performance of iot systems," 2025. DOI: 10.1109/ACCESS.2025.3576716.

[74] S. Hu, Y. Pei, and Y. C. Liang, "Sensing-mining-access trade-off in blockchain-enabled dynamic spectrum access," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 4, pp. 820–824, Apr. 2021. DOI: 10.1109/LWC.2020.3045776.

[75] D. Cuellar, M. Sallal, and C. Williams, "Bsm-6g: Blockchain-based dynamic spectrum management for 6g networks: Addressing interoperability and scalability," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3393288.

[76] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, 2011. DOI: https://doi.org/10.1016/j.phycom.2010.12.003.

[77] K. Venkatesan and S. B. Rahayu, "Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques," *Sci Rep*, vol. 14, no. 1, Dec. 2024. DOI: 10.1038/s41598-024-51578-7.

[78] A. Salh and et al., "A survey on deep learning for ultra-reliable and low-latency communications challenges on 6g wireless systems," Institute of Electrical and Electronics Engineers Inc., 2021. DOI: 10.1109/ACCESS.2021.3069707.

[79] T. Sudhakar, R. Praveen, and V. Natarajan, "An efficient ecc and fuzzy verifier based user authentication protocol for iot enabled wsns," *Sci Rep*, vol. 15, no. 1, Dec. 2025. DOI: 10.1038/s41598-025-94550-9.

[80] N. Alzahrani, "Security importance of edge-iot ecosystem: An ecc-based authentication scheme," *PLoS One*, vol. 20, no. 6 June, Jun. 2025. DOI: 10.1371/journal.pone.0322131.

[81] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing iot devices: A novel approach using blockchain and quantum cryptography," *Internet Things (Netherlands)*, vol. 25, Apr. 2024. DOI: 10.1016/j.iot.2023.101019.

[82] Y. Yang, Y. Lin, J. Xiao, and Z. Zhong, "Feasibility discussion of quantum cryptography for internet of things security: A literature review," *Opt Quantum Electron*, vol. 57, no. 5, p. 264, Apr. 2025. DOI: 10.1007/s11082-025-08168-2.

[83] M. Shahjalal and et al., "Enabling technologies for ai empowered 6g massive radio access networks," Jun. 2023. DOI: 10.1016/j.icte.2022.07.002.

[84] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet Things J*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019. DOI: 10.1109/JIOT.2019.2920987.

[85] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, DOI: 10.1109/MVT.2017.2740458.

[86] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6g era," *IEEE Access*, vol. 9, pp. 142 314–142 327, 2021. DOI: 10.1109/ACCESS.2021.3120143.

[87] R. Akhras, W. El-Hajj, M. Majdalani, H. Hajj, R. Jabr, and K. Shaban, "Securing smart grid communication using ethereum smart contracts," IEEE, 2020.

[88] F. Patel, P. Bhattacharya, S. Tanwar, R. Gupta, N. Kumar, and M. Guizani, "Block6tel: Blockchain-based spectrum allocation scheme in 6g-envisioned communications," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, 2021, pp. 1823–1828.

[89] P. Deepanramkumar and N. Jaisankar, "Blockcrn-iocv: Secure spectrum access and beamforming for defense against attacks in mmwave massive mimo crn in 6g internet of connected vehicles," *IEEE Access*, vol. 10, pp. 74 220–74 243, 2022. DOI: 10.1109/ACCESS.2022.3187745.