Journal of Intelligent Systems and Internet of Things
Vol. 18, No. 01, PP. 298-308, 2026
DOI: https://doi.org/10.54216/JISIoT.180123

# Distributed Ledger Technology-Enhanced 6G Wireless Communication: Overcoming Trust, Privacy, And Scalability Challenges

**R. Sivasankari[1,*], S. Amsavalli[2], Kamarunnisha H.[1], Vetripriya M.[1], Tamilselvi S.[3]**

[1]Dept. of Computer Science and Engg, B.S.Abdur Rahman Crescent Institute of Science and Technology, India

[2]Dept. of Computer Applications, B.S. Abdur Rahman Crescent Institute of Science and Technology, India

[3]Dept. of Networking and Communications, SRM Institute of Science and Technology, Kattankulathur, India

Emails: sivasankari.rp@crescent.education; amsavalli@crescent.education; kamarunnisha@crescent.education; vetripriya@crescent.education; stamilselvi@panimalar.ac.in

## Abstract

The transition from 5G to 6G wireless communication systems introduces new challenges, including scalability, privacy, and security. DLT (Distributed Ledger Technology) technology, with its decentralized and secure framework, offers a promising solution to address these issues in a 6G context. In a 6G environment, DLT can facilitate decentralized management, secure authentication, and trusted data exchanges. By leveraging DLT's distributed ledger system, it can support device identity verification, spectrum allocation, and secure data sharing across nodes, creating a trustworthy communication ecosystem. DLT and 6G integration enables efficient spectrum management, where smart contracts automate resource allocation, reducing bottlenecks and improving resource efficiency. Moreover, the decentralized nature of DLT enhances privacy and security by providing an authentication mechanism that works without central authority. This is crucial, as 6G will involve a vast number of connected devices. This research aims to explore the role of DLT in improving the security and scalability of 6G networks, investigate spectrum management techniques, and evaluate decentralized device authentication and trust mechanisms. Additionally, challenges such as latency, scalability, and DLT integration in 6G are examined. DLT's decentralized nature aids in network security and robustness, mitigating vulnerabilities by distributing control across nodes. It also streamlines resource allocation and device authentication, improving privacy. DLT enables users to manage access rights through decentralized mechanisms, fostering trust and compliance with privacy regulations. However, issues like latency due to transaction validation and the need for advanced techniques like sharding are challenges that must be addressed to optimize DLT for 6G applications.

**Received: March 03, 2025 Revised: June 05, 2025 Accepted: July 12, 2025**

**Keywords:** Distributed Ledger Technology (DLT); 6G Wireless Communication; Decentralized Authentication; Spectrum Management; Privacy and Scalability

## 1. Introduction

As the development of wireless communication systems moves from 5G to 6G, new paradigms and technological advancements are necessary to meet the demands of a hyper-connected society. 6G, expected to be a critical enabler for applications like smart cities, autonomous vehicles, and massive IoT networks, must overcome several challenges including scalability, privacy, and security. DLT, with its decentralized, transparent, and secure framework, presents a promising solution for these issues, providing an opportunity for a paradigm shift in wireless communications that could facilitate a robust and secure 6G ecosystem. DLT technology has emerged as a potential enabler for addressing these challenges in the 6G landscape. Known for its decentralized and immutable ledger, DLT allows for secure, transparent, and tamper-resistant record keeping without reliance on a central authority. In

a 6G environment, DLT could be leveraged to enable decentralized management, secure authentication, and trusted data exchanges. The distributed ledger system in DLT technology can provide a basis for device identity verification and management, spectrum allocation, and secure data sharing across nodes, creating a trusted environment for communication.

The synergy between DLT and 6G opens new possibilities for designing secure and scalable wireless communication networks. For instance, spectrum management—a critical issue in 6G—can benefit from DLT's automated, transparent, and dynamic resource allocation capabilities through smart contracts, potentially reducing bottlenecks and improving resource efficiency. Additionally, the decentralized nature of DLT can support authentication mechanisms, enhancing privacy and security in an environment where a massive number of devices and users interact simultaneously.

The primary objectives of this research are as follows:

1. To investigate the potential of DLT in enhancing the security and scalability of 6G wireless networks: This objective involves analysing how DLT's decentralized ledger and cryptographic properties can strengthen data integrity, prevent unauthorized access, and ensure secure communication within the 6G infrastructure.

2. To explore DLT-enabled spectrum management techniques for efficient resource allocation in 6G: As 6G networks will involve a vast number of devices requiring high-speed and reliable connections, spectrum management becomes crucial. This objective seeks to understand how DLT-based smart contracts can facilitate real-time and fair spectrum allocation to optimize network performance.

3. To evaluate DLT's role in decentralized device authentication and trust mechanisms for 6G: With device density set to grow exponentially in 6G networks, traditional centralized authentication models may not be efficient. This objective assesses the potential of DLT to provide a decentralized, tamper-resistant solution for device identity verification, enhancing network trust and reducing risks associated with a centralized approach.

4. To examine the challenges and limitations of implementing DLT within 6G networks: Although DLT offers significant potential, its integration into 6G presents technical and operational challenges, including latency, energy consumption, and compatibility with 6G's ultra-low latency requirements. This objective aims to identify and address these challenges to understand the feasibility of DLT in real-world 6G applications.

## 2. Related Work

The deployment of blockchain in 6G wireless networks is being pursued to overcome limitations in centralized architectures, especially regarding security, transparency, and reliability. Xu et al. highlighted a decentralized framework to optimize device-level resource distribution, reducing latency and improving traceability [1]. Zhang et al. suggested that coupling artificial intelligence with blockchain offers a secure and self-regulating method for managing network assets in future communication systems [2]. Expanding on this, Liu et al. developed a distributed Radio Access Network (RAN) management model based on blockchain to streamline spectrum utilization [3]. These innovations contribute to forming a reliable, autonomous communication backbone. Such blockchain-based strategies are foundational for next-gen wireless trust models.

With billions of devices expected to connect via the Internet of Things (IoT) in 6G, scalability and failure resilience are crucial. Li et al. proposed a blockchain-enabled solution to handle IoT device lifecycles without relying on centralized controllers, mitigating single-point breakdowns [4]. To automate authorization, Zhao et al. incorporated smart contracts that offer self-executing access rights for connected nodes [6]. Kumar et al. also explored distributed authorization techniques using blockchain to reinforce endpoint security [10]. These models not only boost the operational range of 6G networks but also enhance their fault tolerance. Through blockchain, seamless coordination between highly heterogeneous IoT entities becomes more practical.

Ensuring confidential and verifiable data exchange across diversified networks is pivotal in 6G, and blockchain offers promising capabilities here. Liu et al. discussed blockchain-based systems that validate data lineage, ensuring reliable and authenticated information sharing [7]. Tang et al. introduced privacy-preserving blockchain structures embedded with cryptographic layers to prevent unauthorized data exposure [8]. Ortega et al. further demonstrated that decentralized identity frameworks could secure user authentication without centralized intervention [19]. These security enhancements deter impersonation and data misuse. Altogether, such systems support a trustworthy environment for global 6G communication.

Effective spectrum distribution and inter-network cooperation are central to 6G's performance. Zhao et al. proposed a blockchain-based marketplace for spectrum trading, facilitating dynamic allocation and maximizing spectral efficiency [12]. Alvarez et al. examined the use of distributed ledgers to streamline international roaming and multi-operator collaboration, minimizing service disruption [24]. Similarly, Xie et al. introduced blockchain protocols to harmonize cross-domain resource sharing and ensure interoperability [9]. These solutions not only

improve spectrum economics but also simplify compliance. Through programmable contracts, enforcement and traceability of cross-operator agreements become automatic and tamper-proof.

The shift toward edge computing and decentralized learning in 6G calls for privacy-aware frameworks. Wang et al. described a blockchain-federated learning combination that allows decentralized training while preserving user data privacy [11]. Patel et al. emphasized blockchain's role in securing computation offloading in Mobile Edge Computing (MEC) environments [16]. Ivanov et al. showcased secure edge caching using DLT to accelerate data retrieval with reduced vulnerability [28]. These techniques safeguard user information while maintaining low-latency operations. Blockchain thus provides the cryptographic and operational backbone for edge-centric intelligence in future networks.

Blockchain is also playing a key role in transport technologies supported by 6G, including unmanned aerial vehicles (UAVs) and vehicular networks. Singh et al. employed blockchain for UAV coordination, ensuring real-time trust and trajectory verification [14]. Patel et al. tackled the security of vehicle-to-everything (V2X) systems using blockchain to prevent manipulation of transmitted data [23]. These applications demand stringent time-sensitive and trust requirements, which blockchain fulfills by enabling distributed consensus. Together, they enhance the reliability of mobile infrastructures. The use of blockchain in mobility enhances safety and coordination among autonomous agents in 6G.

Power consumption is a notable concern for blockchain operations in wireless systems. Yang and Rossi assessed lightweight consensus algorithms like PoS and PBFT tailored to suit the constraints of high-speed wireless environments [5][26]. These modifications render blockchain more energy-efficient and practical for 6G scenarios. Nguyen et al. explored blockchain-driven Network Function Virtualization (NFV), enabling the decentralized hosting of network services without performance compromise [20]. These advances help manage resources efficiently while minimizing overhead. As environmental sustainability gains focus, blockchain systems must evolve to meet green networking standards in 6G.

Beyond conventional communication tasks, blockchain is expanding into immersive and high-security domains within the 6G framework. Dubois et al. introduced a trust-based blockchain mechanism for AR/VR streaming, protecting content integrity during delivery [30]. Santos et al. designed a blockchain ledger resilient to quantum computing threats, ensuring long-term security of 6G applications [21]. Russo et al. explored integration with edge-based AI for secure industrial IoT automation [22]. These pioneering applications reflect blockchain's capacity to support diverse, futuristic needs. Its adaptability and security make blockchain an indispensable pillar in the evolution of next-generation communication.

## 3. DLT-Enabled Networking

DLT-enabled networking is revolutionizing how decentralized systems manage data, resources, and communication in various sectors. The integration of DLT technology into networking creates secure, transparent, and efficient systems for resource sharing, improving both performance and trust among participants. Below are some key innovative research areas in this field.

### A. Decentralized Resource Allocation and Management

DLT can be used to decentralize resource allocation across networks, ensuring utilization that is more efficient and reducing reliance on central authorities. Smart contracts can automate resource sharing and optimize performance by dynamically adjusting to network conditions in real time. This approach has significant potential for networks such as IoT and 5G, where large numbers of devices require efficient management of computational and communication resources.

### B. Network Security and Privacy

DLT-enabled networking offers enhanced security and privacy for data exchange in distributed systems. By leveraging cryptographic techniques, DLT can provide end-to-end data integrity, preventing tampering and unauthorized access. This is particularly useful in securing sensitive data in applications such as healthcare, financial services, and supply chains, where data privacy is critical.

### C. Interoperability Between Different Networks

The ability to achieve seamless interoperability between multiple DLT networks is crucial for developing decentralized applications. Research is focused on cross-chain communication protocols and bridging technologies that allow DLT networks with different governance models and consensus mechanisms to interact and exchange data securely. This area is particularly important in the development of multi-party systems such as supply chains, energy grids, and healthcare networks.

### D. Spectrum Sharing for Wireless Networks

DLT can facilitate secure and efficient spectrum sharing in wireless communication networks, especially in 5G and 6G. Through DLT, spectrum management can be decentralized, with smart contracts governing the allocation and usage of wireless frequencies based on real-time demand. This reduces spectrum inefficiency and ensures equitable access for all stakeholders, enhancing the overall performance of wireless networks.

### E. Secure and Transparent Data Sharing in IoT

IoT devices often face challenges in ensuring secure data sharing and privacy due to their limited processing power. DLT provides a decentralized and immutable ledger for secure data exchange, allowing devices to share information without compromising security. This research area includes developing lightweight DLT protocols tailored to the constrained resources of IoT devices.

### F. Energy Resource Sharing

In decentralized energy systems, DLT can be used for peer-to-peer energy trading and resource sharing. This enables consumers to buy and sell excess energy directly with each other, facilitated by smart contracts that ensure transparent and secure transactions. DLT's role in energy sharing contributes to more sustainable energy usage, especially in smart grids and renewable energy networks.

### G. Collaborative AI and Machine Learning

DLT is being explored for its potential in facilitating collaborative machine learning (ML) and artificial intelligence (AI) by securely sharing model training data and computational resources. DLT's transparency and immutability ensure that contributions to AI model development are properly accounted for and rewarded, which is essential in federated learning environments where data privacy is a concern.

### H. Decentralized Autonomous Networks (DANs)

Decentralized Autonomous Networks (DANs) aim to replace traditional network management with autonomous, DLT-based governance models. This innovative research area focuses on creating self-organizing networks that can operate without human intervention, using smart contracts for decision-making, resource management, and security protocols. These systems have the potential to disrupt industries by enabling fully autonomous, secure, and efficient networks.

## 4. DLT-based ACCESS NETWORK for 6G

We present B-RADIO ACCESS NETWORK, an all-encompassing design for 6G wireless communications supported by DLT technology. In this paper, we take a close look at the fundamentals of the 6G B-RADIO ACCESS NETWORK paradigm, including consensus mechanisms, smart contracts, dependable access, mathematical modelling, data tracking and auditing, intelligent networking, and cross-network sharing. Along with the latest experimental results, we also provide a B-RADIO ACCESS NETWORK prototype design.

### a. Framework for Sixth Generation (6G)

In the past decade, the rapid evolution of DLT technology has catalyzed numerous studies exploring its integration into wireless networks such as 5G and IoT, as highlighted in previous sections. However, much of the existing research has focused on isolated use cases, overlooking the deeper, systemic integration of DLT within wireless communication infrastructures. For 6G networks, a more holistic approach is required to effectively integrate DLT, addressing its role not only in isolated applications but also as a foundational element of the network architecture. Trust issues in these networks cannot be resolved merely by incorporating DLT; rather, a comprehensive solution requires addressing the inherent distrust across multiple network layers to ensure a trustworthy, cohesive system.

Moreover, several critical challenges remain underexplored in DLT-based wireless networks, including security, latency, scalability, cost, and power consumption. The absence of robust mathematical models and experimental results further emphasizes the need for continued research to evaluate the performance of blockhain in wireless environments. To enable the success of 6G, it is essential to develop a unified framework that addresses these challenges while leveraging DLT's unique capabilities. The DLT-based Radio Access Network (B-RADIO ACCESS NETWORK) concept presents an innovative solution, offering a decentralized, trustworthy infrastructure for resource pooling and sharing across sectors. B-RADIO ACCESS NETWORK facilitates secure and flexible cooperation, enabling dynamic resource management through federated learning, while providing enhanced security, privacy, and data exchange capabilities critical for 6G deployment.

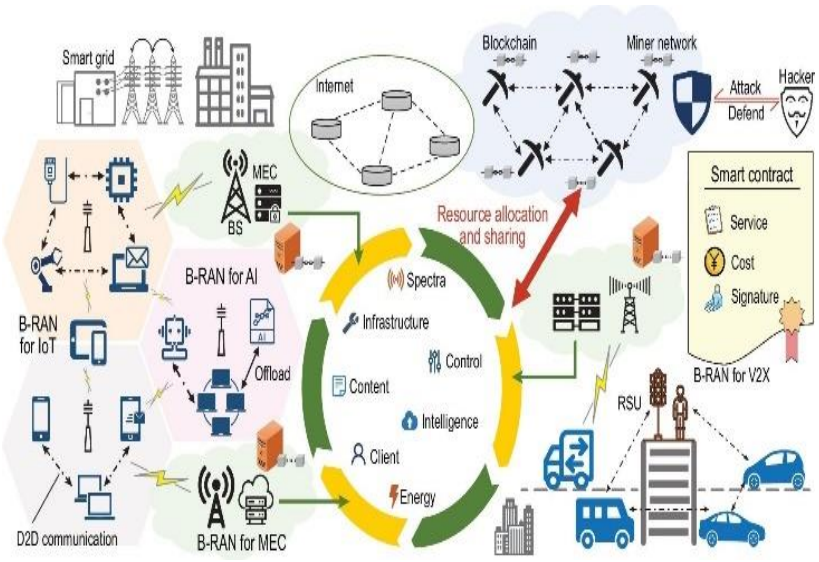


**Figure 1.** DLT Radio Access Network (B-RADIO ACCESS NETWORK): An Overview of DLT-Driven Wireless Communications

Figure 1 presents a potential design for 6G integration with DLT-based Radio Access Networks (B-RADIO ACCESS NETWORK). The Edge Super Data Centre (ESDC) consists of advanced baseband units (BBUs) and edge servers (EDGE), incorporating key technologies such as DLT, artificial intelligence (AI), and big data. The ESDC, in conjunction with remote radio units (RRUs), operates as a super base station, evolving from the eNodeB in 5G to support wireless services and local applications within the network ecosystem. DLT ensures data security through encryption, while AI and big data enhance functionalities like secure access control and mobile terminal monitoring. EDSCs, connected via high-speed optical links, rely on DLT for secure, trustworthy communication. Additionally, DLT facilitates coordination between heterogeneous terminal units, edge nodes, and core networks, regulating their interactions through on/off-chain smart contracts for efficient network orchestration.

In an IoT context, B-RADIO ACCESS NETWORK facilitates the establishment of mutual trust between IoT devices and access points (APs) in a distrustful environment through DLT technology, offering a solution for future IoT/IoE networks in a multi-operator setting. This trust framework mitigates potential selfish behavior from untrustworthy devices and encourages cooperation among individual IoT networks. By integrating multiple networks into a cohesive multi-operator system, B-RADIO ACCESS NETWORK optimizes cross-network resource utilization, including spectrum, APs, IoT devices, and user data. Consequently, IoT devices can access resources and services across networks, independent of a single service provider, through efficient incentive mechanisms.

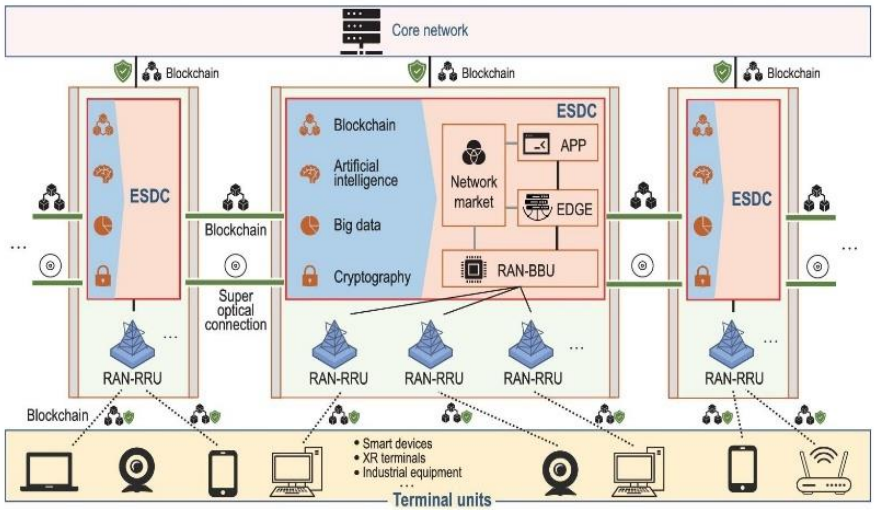


**Figure 2.** A promising architecture of 6G embedded with B-RADIO ACCESS NETWORK.

Additionally, B-RADIO ACCESS NETWORK enables DLT-powered MEC, supporting multi-party resource scheduling in an open and distributed network, while ensuring privacy and data security for users. B-RADIO ACCESS NETWORK allows direct communication between users and MEC servers from different operators without the need for intermediaries. This framework enhances the utilization of storage and computational resources within MEC, minimizing redundancy and vacancies in network management, thus achieving efficient resource sharing and scheduling.

**b. Mathematical Modelling**

Although DLT-based networking has gained prominence, research on mathematical modelling and basic analysis remains relatively scarce. A significant number of intractable problems remain unresolved. The current literature has not evaluated the effects of decentralization on RANs following the implementation of DLT, which should be analytically delineated and precisely measured. Few studies have acknowledged that service latency will provide a significant challenge for B-RADIO ACCESS NETWORK because of decentralization, the extent and manageability of which remain uncertain. Security, as another crucial element of B-RADIO ACCESS NETWORK, has not been extensively examined until now.

Consequently, an analytical model is essential to investigate the attributes of B-RADIO ACCESS NETWORK, including latency and security, and to offer valuable guidance for practical applications. In Reference [22-25], we conducted an innovative endeavor to mathematically describe B-RADIO ACCESS NETWORK and analytically delineate its features and performance metrics. We specifically modelled block generation using a Poisson process and validated it with empirical data. We subsequently developed a queueing model integrated with a continuous time-homogeneous Markov process for B-RADIO ACCESS NETWORK. Utilizing the queueing model, we introduced a comprehensive state transition graph, assessed the average service level latency, and elucidated the influence of key parameters on B-RADIO ACCESS NETWORK latency by deriving stringent upper and lower bounds. Simultaneously, we evaluated the security level of B-RADIO ACCESS NETWORK by analyzing the attacker's technique.

The preceding analysis of latency and security revealed an intrinsic relationship between the two, illustrated by the latency-security trade-off curve depicted in Fig. 7. The request latency of B-RADIO ACCESS NETWORK is approximately linear to the block generation time, increasing with the number of confirmations required for verification or the duration of block generation. Conversely, further confirmations are necessary to diminish the likelihood of a successful attack. The confirmation number is crucial for balancing service latency and system security in B-RADIO ACCESS NETWORK and must be meticulously chosen. This trade-off thoroughly characterizes the achievable performance of B-RADIO ACCESS NETWORK. The analytical model in Ref. [26-29] offers valuable insights for the design of DLT-based wireless networks that ensure sufficient security against rogue miners while maintaining reasonable access latency.

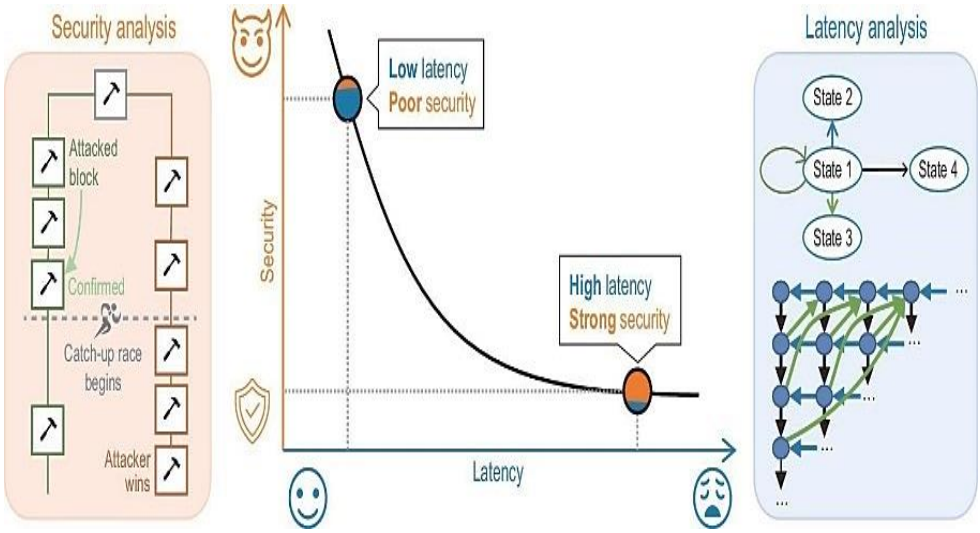


**Figure 3.** Mathematical model of B-RADIO ACCESS NETWORK and the latency-security trade-off

### c. Data Monitoring and Verification

The exponential growth of data in the big data era has introduced significant challenges for enterprises, societies, and governments, particularly with the rising frequency of data breaches that pose serious security threats [30]. Wireless networks, due to their inherent openness and mobility, are especially vulnerable to data leakage and malicious intrusions. As demands for data security and user privacy continue to escalate, effective data tracking and auditing mechanisms are essential for detecting breaches and preventing unauthorized access to sensitive information. In response, various nations and organizations have implemented regulations aimed at mitigating data leakage and ensuring robust data tracking and auditing. For instance, the European Union introduced the General Data Protection Regulation (GDPR) in 2018, and the United States enacted the National Security and Personal Data Protection Act (NSPDPA) in 2019.

In the B-RADIO ACCESS NETWORK (B-RAN), data is transmitted through multiple relay paths involving various devices and infrastructures. DLT, with its decentralized structure and transparency, is well suited for recording and auditing these routing paths securely. By integrating data marking techniques, a comprehensive data tracking and auditing framework for B-RAN is proposed, as illustrated in Fig. 4. This system enables routing nodes, potentially operated by different manufacturers and service providers, to report their routing data to the DLT via smart contracts. To authenticate the data and verify its origin, the source device generates an immutable digital label using a Trusted Platform Module (TPM). This label and the corresponding source information are then recorded in the smart contract. Each relay node also appends its digital signature and updates the contract on the DLT, ensuring that the routing path is tamper-proof, auditable, and transparent. This collaborative approach to data routing enhances trust in the network, allowing regulatory bodies to conduct audits and monitor potential violations effectively.

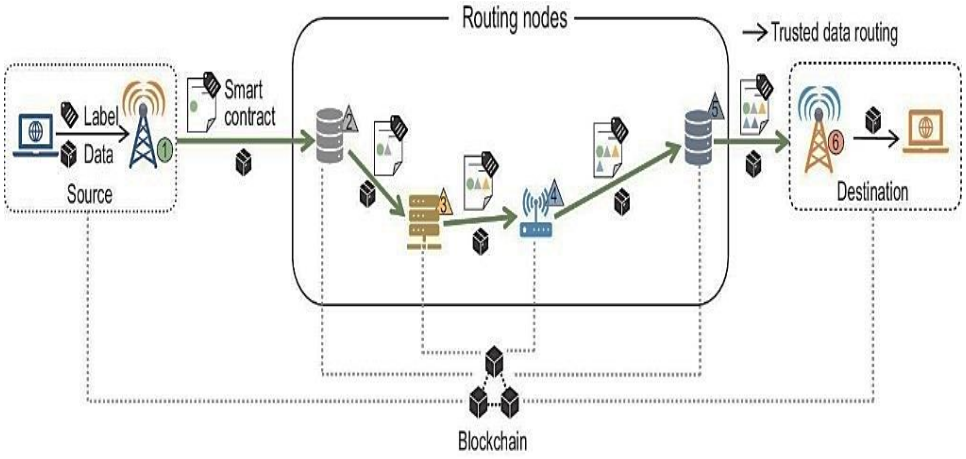


**Figure 4.** Data monitoring and verification in B-RADIO ACCESS NETWORK.

### d. Prototype Development

To implement the proposed design and assess its performance, we evaluate the basic capability requirements of B-RADIO ACCESS NETWORK and develop a corresponding prototype. These requirements span six aspects: physical storage, secure links, network, DLT consensus, resource and asset trading, and user applications. Based on these needs, we design an architecture comprising the access control, tunnel, consensus, and trading layers, along with traditional network layers (storage, structure, network, and application). Additionally, mechanisms such as FSCD, HTLC, and Hash Access are integrated to enhance the prototype's performance, as detailed in Fig.5.

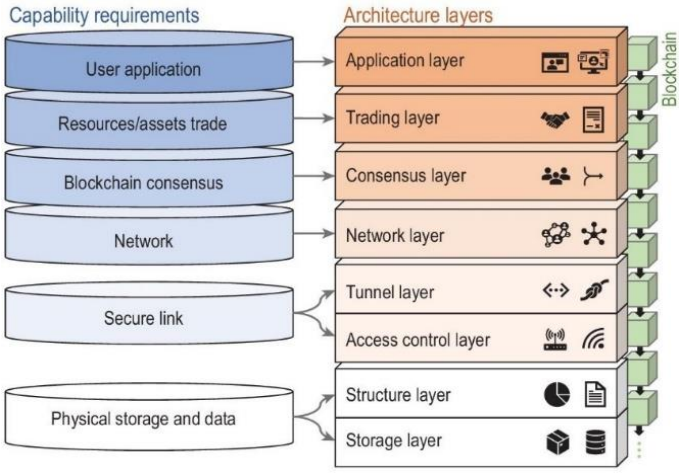


**Figure 5.** Functionality requirements and architectural layer design of B-RADIO ACCESS NETWORK

In B-RADIO ACCESS NETWORK, DLT data such as transactions and cryptographic keys are stored in the structure layer by servers or active devices. Some mobile devices store partial DLT information as lightweight nodes. Secure links are established using HTLC principles, ensuring trust-free payment channels, with reliability ensured by flow control and error detection. Subnetworks form the network, responsible for node discovery and synchronization. Consensus mechanisms validate blocks, and smart contracts govern resource and asset trading, ensuring fairness. User applications interact with the DLT via APIs, enabling additional functionalities beyond basic services.

## 5. Experimental Results

This section presents several experiments to evaluate the performance of B-RADIO ACCESS NETWORK under varying conditions. The prototype is implemented using Python and tested on a cluster of single-board computers connected within the same local area network. Data collection is automated through a pre-designed script. To assess the performance of B-RADIO ACCESS NETWORK, we compare it with traditional RANs and PoW-based DLTs, such as Bitcoin and Ethereum, as benchmarks. The experiments focus on service latency, resource utilization, and request processing.

Figure 11 illustrates a comparison of service latency between the PoW-based B-RADIO ACCESS NETWORK prototype and other PoW-based DLTs. In the experiment, the block time is set to 10 seconds, requiring two blocks for DLT confirmations. As shown, B-RADIO ACCESS NETWORK demonstrates significantly lower service latency than typical PoW-based DLTs, where service latency often lasts several minutes. By incorporating the FSCD mechanism, B-RADIO ACCESS NETWORK reduces the required service period, bringing service latency down to seconds. This reduction positively affects user satisfaction and enhances system security, as discussed in the section on cross-network sharing.

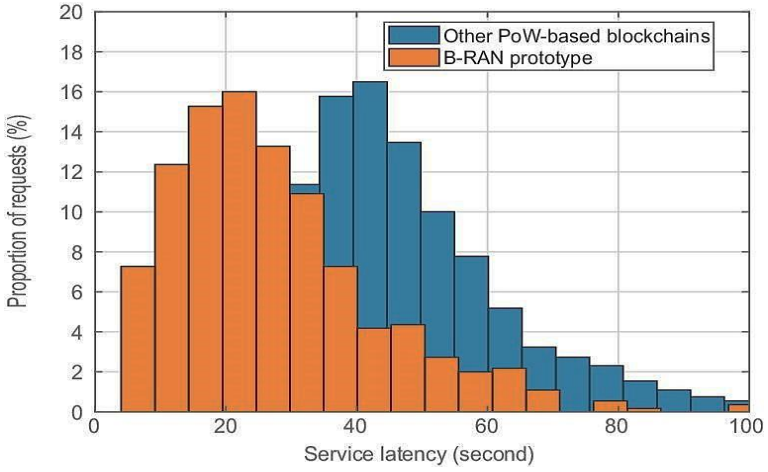


**Figure 6.** We compare the B-RADIO ACCESS NETWORK prototype's service latency distribution to that of other PoW-based DLTs.

Figure 6 a illustrates the impact of average request interarrival time on the resource utilization of the B-RADIO ACCESS NETWORK (B-RAN). Resource utilization is defined as the ratio of link busy time to available time, which reflects the efficiency of link usage relative to availability. As the average request interarrival time decreases, resource utilization increases significantly, independent of service time. Additionally, comparison across three different service time configurations shows that longer average service times or increasing service time trends are associated with higher request intensity (i.e., more active users), leading to a more pronounced increase in resource utilization compared to shorter service times. Thus, enhanced resource utilization is closely tied to both network expansion and increased user engagement in the B-RAN.

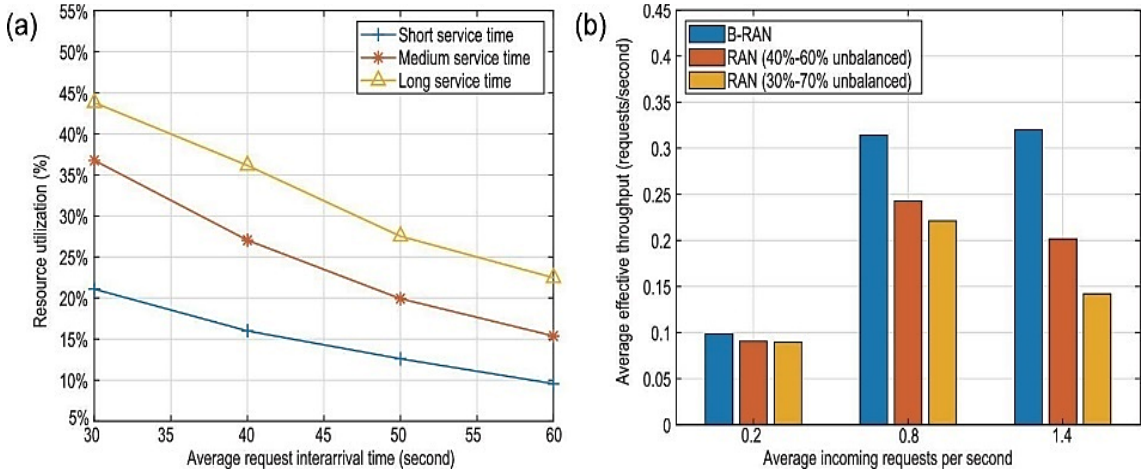


**Figure 7.** The B-RADIO ACCESS NETWORK prototype evaluates resource use and throughput: (a) Average request interarrival time influences resource utilization across service (b) B-RADIO ACCESS NETWORK throughput vs. imbalanced RANs at varying traffic intensities.

Figure 7 presents a comparison of the average effective throughput per subnetwork for the B-RADIO ACCESS NETWORK (B-RAN) and two unbalanced Radio Access Networks (RANs) under varying incoming request frequencies. In the experiment, both the B-RAN and RANs are configured with two subnetworks, but the RANs exhibit unequal traffic distribution, with load ratios of 40%/60% and 30%/70%, respectively. The results demonstrate that the B-RAN consistently achieves the highest average effective throughput, particularly at higher incoming request rates. This superior performance is attributed to B-RAN's ability to integrate subnetworks effectively and balance traffic loads across them. The simulation results underscore B-RAN's advantages in minimizing service latency, optimizing resource utilization, and ensuring efficient load balancing. Furthermore, the FSCD (Fast Smart Contract Deployment) mechanism significantly reduces contract deployment delays, thereby improving both resource usage and throughput performance.

## 6. Conclusion

In this paper, we address the critical trust-related challenges that hinder the evolution from existing 5G networks to the more secure, efficient, and robust 6G systems. After introducing the principles of Distributed Ledger Technology (DLT), we conducted an in-depth analysis of recent research focused on the application of DLT in wireless network environments. Our review covers several essential areas that directly influence the effectiveness of next-generation networks, including resource sharing, trusted data exchanges, secure access control mechanisms, privacy protection, data traceability, network certification, and overall network supervision. These aspects are becoming increasingly important as wireless networks face growing demands for transparency, accountability, and security. Building on these findings, we propose the B-RADIO ACCESS NETWORK (B-RAN) framework as a comprehensive, secure, and scalable solution for 6G network architectures. This framework leverages DLT to enhance the efficiency, security, and trustworthiness of wireless communications. We offer a detailed examination of key B-RAN components; including consensus protocols, smart contracts, trustworthy access models, and mathematical models for network interactions. Additionally, we explore the integration of cross-network resource sharing, data tracking, auditing mechanisms, and intelligent network management to facilitate seamless operation across heterogeneous network entities.

Furthermore, we present the design of a prototype B-RAN system, along with recent experimental results that demonstrate its feasibility and performance. These results underscore the potential of DLT to address longstanding trust issues in next-generation networks. By ensuring secure, transparent, and reliable communication between network entities, the proposed B-RAN framework provides a promising foundation for the evolution of 6G networks. It offers a scalable, decentralized model that can meet the increasing complexity and security requirements of future wireless communication systems.

**Conflicts of Interest:** The authors assert that there are no conflicts of interest.

**Authors' Contributions:** All writers made substantial contributions to the finalization of this publication.

**References**


[1] M. Xu *et al*., "Blockchain-Enabled Resource Sharing for 6G: Challenges, Solutions, and Future Directions," *IEEE Network*, vol. 35, no. 5, pp. 122–129, Sep.–Oct. 2021.

[2] Z. Zhang *et al*., "AI and Blockchain for 6G: Enabling Secure and Intelligent Resource Management," *IEEE Wireless Communications*, vol. 30, no. 1, pp. 80–87, Feb. 2023.

[3] X. Liu *et al*., "Blockchain-Based Radio Access Network for 6G: A Decentralized Resource Management Architecture," *IEEE Transactions on Communications*, vol. 70, no. 3, pp. 1892–1904, Mar. 2022.

[4] F. Li *et al*., "Decentralized IoT Device Management in 6G Using Blockchain," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 18–24, Sep. 2021.

[5] X. Yang *et al*., "Consensus Mechanisms for 6G: Requirements and Performance," *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5780–5793, Sep. 2021.

[6] S. Zhao *et al*., "Smart Contract-Based Access Management in 6G Networks," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14721–14730, Oct. 2021.

[7] C. Liu *et al*., "Data Trust in 6G: Blockchain-Enabled Secure Information Sharing," *IEEE Communications Letters*, vol. 26, no. 2, pp. 420–423, Feb. 2022.

[8] W. Tang *et al*., "Privacy Preservation in 6G with Blockchain-Based Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1923–1936, May 2022.

[9] L. Xie *et al*., "Blockchain for Cross-Network Collaboration in 6G," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6055–6066, Oct. 2020.

[10] R. Kumar *et al*., "Smart Contracts for 6G Access Control," *IEEE Wireless Communications*, vol. 30, no. 3, pp. 72–79, Jun. 2023.

[11] H. Wang *et al*., "Federated Learning and Blockchain for 6G Edge Intelligence," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 1, pp. 150–162, Jan. 2022.

[12] Y. Zhao *et al*., "DLT-Based Spectrum Trading and Management in 6G Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 4, pp. 819–830, Dec. 2023.

[13] J. Chen *et al*., "Secure Device-to-Device Communication in 6G via Blockchain," *IEEE Transactions on Mobile Computing*, vol. 21, no. 5, pp. 2102–2114, May 2022.

[14] P. Singh *et al*., "Blockchain-Enabled UAV Management for 6G," *IEEE Communications Magazine*, vol. 60, no. 7, pp. 104–110, Jul. 2022.

[15] A. Kumar *et al*., "DLT-Assisted Network Slicing in 6G," *IEEE Network*, vol. 36, no. 4, pp. 56–64, Aug. 2022.

[16] N. Patel *et al*., "Blockchain for Secure MEC in 6G," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 344–356, Mar. 2023.

[17] R. Chen *et al*., "DLT-Enhanced RAN Orchestration in 6G Systems," *IEEE Access*, vol. 11, pp. 11200–11213, 2023.

[18] S. Lee *et al*., "Blockchain-Aided Privacy in 6G: Edge Data Protection," *IEEE Communications Letters*, vol. 27, no. 9, pp. 2067–2070, Sep. 2023.

[19] M. Ortega *et al*., “DLT-Based Identity Management for 6G Networks,” *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 4001–4012, May 2024.

[20] T. Nguyen *et al*., “Decentralized Network Function Virtualization with Blockchain in 6G,” *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 278–290, Apr. 2024.

[21] E. Santos *et al*., “Quantum-Secure Blockchain for 6G: Post Quantum Ledger Design,” *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 3, pp. 890–903, Mar. 2024.

[22] G. Russo *et al*., “Blockchain and Edge AI for Secure 6G IoT Applications,” *IEEE Transactions on Industrial Informatics*, vol. 20, no. 6, pp. 5567–5578, Jun. 2024.

[23] H. Patel *et al*., “Securing 6G V2X Communications via Distributed Ledgers,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 4, pp. 2038–2049, Apr. 2024.

[24] J. Alvarez *et al*., “DLT Based Roaming and Inter Operator Coordination in 6G,” *IEEE Communications Magazine*, vol. 62, no. 2, pp. 58–66, Feb. 2024.

[25] K. Müller *et al*., “Blockchain-Integrated Network Monitoring in 6G,” *IEEE Sensors Journal*, vol. 24, no. 8, pp. 12655–12663, Apr. 2024.

[26] L. Rossi *et al*., “Energy Efficient Consensus Protocols for 6G DLT Systems,” *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 2, pp. 317–330, Jun. 2024.

[27] M. Yamamoto *et al*., “Privacy Preserving Data Marketplaces in 6G Using Blockchain,” *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 5680–5692, Jul. 2024.

[28] N. Ivanov *et al*., “DLT Based Secure Edge Caching for 6G,” *IEEE Transactions on Mobile Computing*, vol. 23, no. 2, pp. 789–801, Feb. 2024.

[29] O. Ahmed *et al*., “Distributed Ledger for 6G Smart Grid Connectivity,” *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 345–357, Jan. 2024.

[30] P. Dubois *et al*., “Blockchain Enabled AR/VR Streaming over 6G: A Trustworthy Framework,” *IEEE Transactions on Multimedia*, vol. 27, no. 5, pp. 1204–1216, May 2025.