Interoperability Between Blockchain and 5G NR/6G Standardization

Leen Amro*, Bahaa Qabani*, Yara Mhameed*, Mohamad Al-Rowad*, Supervisor: Anastassia Gharib†
*Department of Computer Engineering, Princess Sumaya University for Technology, Amman, Jordan
†Department of Communications Engineering, Princess Sumaya University for Technology, Amman, Jordan
Emails: lee20210258@std.psut.edu.jo, bah20220106@std.psut.edu.jo, yar20220822@std.psut.edu.jo,
moh20200726@std.psut.edu.jo, a.gharib@psut.edu.jo

***Abstract*—The evolution of 5G New Radio (NR) and the emerging 6G vision demand secure, decentralized, and interoperable network architectures. Blockchain technology offers a trustworthy solution to ensure data integrity, trust, and automation in next-generation wireless systems. However, integrating blockchain with 5G and 6G introduces challenges related to interoperability, latency, scalability, and standard alignment. This paper reviews recent frameworks that merge blockchain with 5G and 6G infrastructures, analyzes current trends in standardization, and discusses gaps in cross-domain integration. We explore the role of blockchain in decentralized network slicing, secure message handling, identity management, and cross-domain trust in telecom environments. The paper highlights how blockchain can support secure, scalable, and interoperable network management for future wireless communication systems.**

I. Introduction

The rapid rise of connected devices and smart systems is driving wireless networks forward, pushing 5G toward the next big leap—6G. As our digital world grows to handle massive data flows, ultra-fast communication, and self-operating systems, strong and secure authentication has never been more important. Traditional security methods, built for 4G and early 5G, can't keep up with today's demands—ultra-dense networks, high-speed mobility, and the explosion of IoT devices. That's where blockchain comes in. Its decentralized, tamper-proof, and transparent nature makes it a game-changer for trust and security in next-gen networks. Recent research shows how blockchain could revolutionize authentication for 5G and 6G [1]–[3]. Models like User Equipment-Access Point Enhanced Practical Byzantine Fault Tolerance (UE-AP EpBFT) and blockchain-based digital IDs have already improved speed, cut redundancy, and strengthened access control for IoT in distributed networks [2], [4]. At the same time, industry efforts are focusing on key areas like spectrum efficiency, hybrid satellite-terrestrial networks, and secure digital identity frameworks—all crucial for future wireless systems [5]–[7]. This paper brings together the latest advances in blockchain-powered authentication, covering secure identity management, consensus methods, and real-world integration hurdles [8]. The goal? To help build authentication systems that are both tough and scalable, ready for tomorrow's networks.

A. Related Work

Several recent studies have investigated the contribution of blockchain in enhancing the management and security of next-generation wireless networks. For instance, the work in [9], [10] explores decentralized network management through smart contracts and federated learning in 6G. Efforts like [2], [4] propose blockchain-based digital identity and roaming authentication frameworks for secure access control. Other contributions address spectrum sharing [5], cross-domain trust [11], and resource allocation using DAG-based blockchains [6].

Table I summarizes notable blockchain-based proposals between 2020 and 2024, highlighting the scope, discussed challenges, and proposed solutions. These works collectively demonstrate blockchain's potential to address latency, identity, and interoperability issues, but also reveal gaps in end-to-end integration, real-time consensus adaptation, and standardization efforts.

B. Paper Contributions

This paper makes the following key contributions:

- A comprehensive review of blockchain-based authentication schemes for 5G and 6G, including digital identity models and novel consensus mechanisms such as UE-AP EpBFT.
- An analysis of the challenges that came with the integration of blockchain technology in wireless systems, focusing on latency, scalability, spectrum allocation, and cross-domain interoperability.
- A taxonomy and comparison of state-of-the-art solutions based on architectural scope, performance bottlenecks, and compliance with standardization efforts.
- A proposed reference framework for integrating blockchain-enhanced authentication in future wireless architectures, along with open research directions.

C. Paper Organization

Section II discusses the architectural integration of blockchain with 5G/6G, outlining key technologies and their benefits in terms of scalability, interoperability, and security.

Table I
EXISTING WORKS IN THE BLOCKCHAIN-ENABLED AUTHENTICATION AND NETWORK MANAGEMENT FOR 5G/6G SYSTEMS.

Ref. / Year	Scope	Challenge Discussed	Blockchain-Based Solution
[1] / 2020	Network Management for 6G	Lack of decentralized trust and resilience in network orchestration	Smart contracts and distributed ledgers enhance automation and decentralization in control functions
[3] / 2021	Roaming Authentication in 5G	Fragmented roaming agreements and latency in handovers	Smart contract-based roaming verification enables real-time decentralized authentication
[4] / 2022	Spectrum Sharing for IoT	Bandwidth competition and fairness among autonomous users	DAG-based blockchain enables efficient spectrum trading and autonomous control
[5] / 2021	Massive IoT Access in 5G	Trust gaps between SDN control and IoT devices	Blockchain integrated with SDN provides dynamic access control and verifiable trust records
[12] / 2024	Federated Learning and Network Slicing	Centralized bottlenecks in training and service-level violations	Blockchain enforces SLA terms and coordinates distributed model training across slices
[8] / 2024	Digital Identity for IoT	Risk of identity spoofing in constrained devices	Decentralized identity (DID) models offer tamper-proof identity binding through blockchain
[19] / 2022	Infrastructure-Free Wireless Access	Untrusted peer communication in ad hoc mobile networks	On-chain logging of node behavior and identity verification promotes secure cooperation
[25] / 2023	End-to-End Standardization	Interoperability gaps between telecom layers and blockchain platforms	Smart contracts and common trust anchors enable inter-domain coordination and protocol compatibility
This Paper	**Blockchain–5G/6G Integration Challenges**	**Interoperability, scalability, and secure identity management in future wireless systems**	**A unified analysis of blockchain-enhanced authentication, trust models, and deployment architecture in 5G/6G networks**

Section III presents current trends in 5G/6G standardization and highlights the gaps and interoperability issues that arise when integrating blockchain with telecom protocols.

Section IV explores blockchain-driven network management solutions, including decentralized authentication, identity management, and trust mechanisms for IoT and mobile devices.

Section V concludes the paper.

II. THE ARCHITECTURE OF 5G/6G AND BLOCKCHAIN

The architectural implementation of blockchain technology into 5G/6G networks represents a foundational step toward building decentralized, secure, and intelligent communication systems. As these next-generation networks aim to support massive device connectivity, low-latency communication, and diverse service requirements, blockchain emerges as a natural enabler of distributed trust, automation, and resilience. This section explores the specific blockchain technologies being employed and highlights the resulting advantages in security, interoperability, and scalability.

As 5G and 6G continue to grow and improve services, they also introduce new complexities. One notable challenge lies in resource allocation, latency handling, and adaptability, largely due to the continued reliance on traditional centralized architectures. To address this, modern networks have introduced the concept of *network slicing*, which divides the physical network into virtually isolated slices based on specific application and service requirements. [9], [10] Each slice functions independently, enhancing fault isolation and performance. However, as the number of slice owners increases, resource management, service-level agreements (SLAs), and trust becomes increasingly complex as shown in Fig 1.

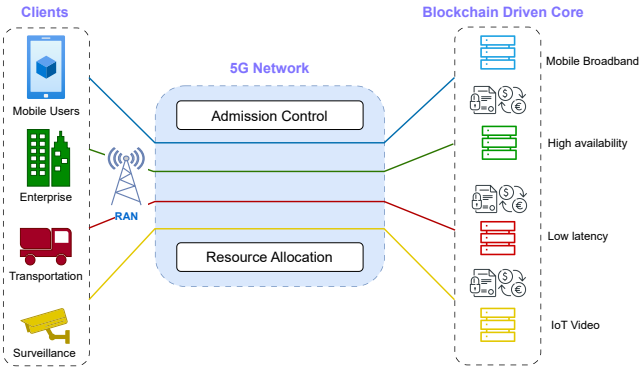

Figure 1. Blockchain Driven 5G Network Slicing.

A. Technologies of Blockchains Used for 5G/6G

The incorporation of blockchain in 5G/6G networks introduces a shift toward decentralized, secure, and programmable infrastructures. Several blockchain technologies have been explored for compatibility with the demands of next-generation

wireless systems. Permissioned blockchain platforms, such as Hyperledger Fabric and private Ethereum networks, are commonly adopted in telecom applications due to their lower latency, controlled access, and efficient consensus protocols suitable for mission-critical environments [9].

In the context of 6G, Directed Acyclic Graph (DAG)-based blockchain architectures have been proposed to overcome the scalability and speed limitations of traditional blockchains [5], [6]. These DAG frameworks enable faster transaction validation and reduce computational overhead, making them ideal for spectrum sharing and decentralized decision-making in 6G-enabled IoT ecosystems.

Emerging solutions also incorporate blockchain-SDN (Software Defined Networking) architectures, where the blockchain manages trust, access control, and transaction records, while SDN provides dynamic control of network flows [12]. Additionally, federated learning frameworks empowered by blockchain enable distributed AI training across network slices, ensuring both privacy and data integrity [10].

Moreover, blockchain is being embedded at the edge of networks to support edge computing scenarios, where latency sensitivity and mobility require localized trust management and data processing [7]. These architectures allow blockchain nodes to operate on lightweight devices while maintaining synchronization with central infrastructure nodes, offering both scalability and responsiveness.

B. Advantages of Security, Interoperability, and Scalability

Blockchain enhances the security posture of 5G and 6G networks by introducing immutability, decentralized authentication, and encrypted consensus mechanisms [3], [5]. The immutable nature of blockchain records ensures tamper-proof logging of transactions and network events, which is crucial for detecting and auditing malicious behavior. Furthermore, blockchain-based Decentralized Identity (DID) systems eliminate reliance on centralized authorities, enabling secure and self-sovereign authentication for IoT and mobile devices [2], [4].

From an interoperability standpoint, blockchain enables seamless collaboration between diverse stakeholders in telecom ecosystems. Smart contracts can automate trust between different network operators, service providers, and vendors [4]. For example, cross-domain authentication protocols facilitate roaming and service provisioning across multiple administrative boundaries without requiring centralized clearinghouses. This capability is particularly valuable for 6G, where decentralized service orchestration is a core requirement.

Scalability challenges in dense 5G/6G environments are addressed through blockchain design optimizations. Mechanisms such as sharding, lightweight consensus protocols (e.g., Proof of Authority, Byzantine Fault Tolerance), and edge-supported blockchain nodes allow the system to scale with growing numbers of devices and data transactions [6], [9]. These enhancements ensure that blockchain remains efficient and responsive even under ultra-dense and high-mobility conditions.

From our perspective, integrating blockchain into 5G and 6G architectures presents a timely and strategic solution to the growing complexity of next-generation networks. We believe that blockchain's ability to decentralize control, automate trust relationships, and enhance scalability is well-aligned with the dynamic and service-oriented nature of modern telecom infrastructures. As the demand for secure and adaptive communication grows, embracing blockchain technologies such as DAG frameworks, federated learning, and edge-compatible chains becomes not just advantageous, but essential.

Ultimately, we view blockchain as a cornerstone technology for enabling secure, interoperable, and highly scalable mobile ecosystems in the 5G/6G era.

III. Trends and Standardizations in 5G/6G

As 5G deployment expands and 6G development accelerates, the intersection of blockchain and mobile networks has drawn increasing attention from standardization bodies. However, integration remains hindered by fragmented standards, protocol mismatches, and regulatory uncertainty. Despite blockchain's promise to decentralize trust and automate network operations, its deployment in telecom infrastructure is constrained by the absence of harmonized standards and interfaces tailored for mobile networks.

A. Relevant IEEE and International Standardization Efforts

Several IEEE working groups and international organizations have initiated efforts to bridge the gap between blockchain and telecom networks:

- **IEEE P2418.1** – Provides a standard framework for blockchain in Internet of Things (IoT) applications, relevant to edge-device interoperability in 5G/6G environments [**?**].
- **IEEE P2140 Series** – Aims to define architecture standards for edge and mobile computing, which are critical for decentralized blockchain services [**?**].
- **IEEE P1912** – Specifies privacy and security architecture for next-generation networks, including support for decentralized identity and blockchain-based authentication [**?**].
- **ETSI ISG PDL (Permissioned Distributed Ledger)** – Focuses on integrating distributed ledger technologies into NFV and MEC-based infrastructures [**?**].
- **ITU-T FG DLT** – Offers guidance on distributed ledger architecture and interoperability, though not yet aligned with mainstream telecom deployments [**?**].
- **3GPP SA6 and SA3** – While not blockchain-specific, these groups are involved in developing standards for service layer architecture and security mechanisms that intersect with blockchain-based approaches [**?**], [**?**].

B. Standard Gaps and Interoperability Challenges

Current 5G/6G systems lack formal definitions for integrating blockchain components—such as smart contracts, distributed ledgers, or consensus protocols—into telecom architectures. Key missing elements include:

- Standardized APIs for integrating blockchain with 5G core functions and orchestration layers.
- Performance benchmarks to meet ultra-low-latency and high-reliability demands, such as those for URLLC.
- Governance and trust frameworks to support multi-operator, inter-chain blockchain deployments.

Although initiatives such as those from ITU-T and ETSI are promising, fragmentation persists due to inconsistent protocol definitions, identity schemes, and consensus approaches across the ecosystem.

C. Toward Harmonization and Practical Adoption

For blockchain to achieve scalable adoption within 5G/6G networks, future standardization must address:

- Unified telecom-grade smart contract standards.
- Lightweight, latency-aware consensus algorithms suitable for real-time applications.
- Cross-layer security and governance models that enable trusted interoperation across networks and jurisdictions.

A coordinated approach involving IEEE, ETSI, ITU-T, 3GPP, and industry stakeholders is essential to enable secure, interoperable, and scalable blockchain deployments in next-generation networks.

IV. Blockchain-Driven Network Management in 5G/6G

With the evolution of 5G/6G networks it introduced challenges in scalability, security, and service differentiation. Blockchain technology has been implemented into this architecture to enable decentralized, secure, and interoperable network management, the focus of this section will include an explanation of how blockchain was implemented in many applications.

A. Decentralized Network Control and Slicing

Blockchain plays a critical role in addressing these challenges by enabling decentralized control through smart contracts and token-based transactions as shown in figure 1 [4], [9], [12]. These mechanisms allow mobile network operators (MNOs) to securely and dynamically share spectrum and infrastructure [5], [9]. Blockchain also provides trustless coordination between tenants, eliminating the need for intermediaries, and ensures transparency in resource allocation, improving auditability. Furthermore, slices can trade bandwidth, storage, and other unused resources with each other dynamically on demand [10]. These features improve data integrity, access control, and security across slices in the network slicing architecture.

B. Collaborative Learning and Resource Trading

The efficient allocation of resources in 5G/6G networks is essential to accommodate fluctuating network conditions and diverse user demands. Traditional centralized resource management approaches are increasingly insufficient due to scalability and privacy limitations. Blockchain-based solutions, especially when integrated with federated learning, offer a promising alternative [10]. Blockchain supports trustless coordination through smart contracts, while federated learning protects user privacy by enabling machine learning models to be trained on dispersed data.

Collaborative learning further enhances this system by emphasizing intelligence and security at the network edge [13]. Nodes periodically contribute to shared federated models, helping to preserve privacy, reduce redundancy, and promote trustworthy cooperation across networks [10]. This decentralized architecture effectively replaces traditional centralized managers while improving scalability, privacy, and responsiveness [9], [10].

C. Blockchain for Message and Data Handling

Secure and reliable message and data handling is critical in 5G/6G networks, especially with the proliferation of IoT devices transmitting sensitive information. Poor message control can lead to data loss or breaches. Blockchain ensures consistent policy enforcement across communication flows, including spam filters and transmission logs [14], [15].

Authentication and authorization are key concerns in secure data handling. Improper handling of these can result in unauthorized access or data tampering. Blockchain-based Public Key Infrastructure (PKI) provides a solution by offering decentralized and tamper-proof certificate distribution [16]. In infrastructure-less environments such as Mobile Ad Hoc Networks (MANETs), blockchain enhances robustness and trust propagation by recording routing history, trust scores, and packet integrity [17]. Nodes validate each message and log actions on-chain, with malicious behavior reducing the node's trust score.

These capabilities demonstrate blockchain's value as a unifying security layer for message integrity and decentralized data management. Hybrid models combining smart contracts and decentralized trust verification have become essential for next-generation communication.

D. Cross-Domain and Infrastructure-Free Security

Device mobility across different network domains creates challenges in maintaining consistent security policies and trust relationships. Traditional roaming mechanisms become inefficient due to complex agreements and manual configurations. Blockchain enables streamlined cross-domain authentication and authorization by maintaining shared ledgers and trusted identities across networks [11].

Smart contracts can dynamically enforce access policies, ensuring real-time access control while reducing administrative overhead and the risk of human error [4]. Furthermore, in infrastructure-free scenarios, blockchain facilitates decentralized trust establishment. Devices can authenticate one another and establish secure communication using blockchain-verified credentials, promoting a secure and scalable architecture without relying on a central authority.

E. Authentication and Identity Management

As 5G and 6G networks expand to support massive IoT ecosystems, scalable and secure authentication becomes critical. Blockchain-based authentication models have been proposed using Markov Decision Models (MDM) to dynamically authenticate users based on context. Additionally, DAG-based blockchains within network slices offer seamless and secure handovers between access points, ensuring low latency and high throughput [3], [6].

The DIA-BC framework introduces a blockchain-based identity mechanism that integrates PKI with smart contracts for decentralized access control [2]. These methods enable tamper-proof authentication and identity management. Combined, they form a strong foundation for scalable, efficient, and interoperable identity systems in next-generation networks.

F. Trust for IoT and Consumer Devices

The incoporation of IoT devices into 5G/6G networks introduces major security challenges, particularly related to attacks known as distributed denial of service (DDOS) and unauthorized access [1], [3]. Establishing trust among heterogeneous and often resource-constrained devices is essential [18].

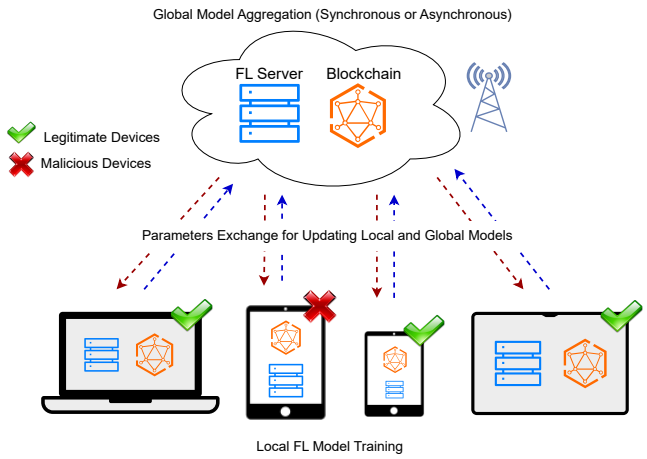

Figure 2. Identifying Malicious Nodes.

Blockchain provides a foundational layer of trust for IoT ecosystems. Devices can register their identities on-chain and log interactions immutably, determining malicious behavior and enabling the identification and isolation of compromised nodes as shown in Figure 2.

In DDoS mitigation, devices can share threat intelligence—such as suspicious IP addresses—with the network, allowing smart contracts to enforce blacklist policies [1].

Moreover, blockchain integrated with Software-Defined Networking (SDN) enhances security by enabling fine-grained policy enforcement [12]. SDN controllers can utilize blockchain data to make informed routing and access decisions, improving flexibility and resilience in network security.

We suggest that implementing Blockchain technology within the 5G/6G network could significantly impact both the network and the architecture. The integration of having isolated networks with a trading mechanism and malicious node detection offers an approach to the needs of next-generation networks.

V. Conclusion

As 5G New Radio (NR) networks evolve and the groundwork for 6G begins to take shape, the demand for secure, scalable, and interoperable communication frameworks has never been greater. This paper examined the intersection of blockchain technology with the standardization efforts of 5G NR and emerging 6G architectures, particularly in the context of secure authentication, identity management, and spectrum efficiency. Blockchain, with its decentralized trust model, immutability, and auditability, presents a compelling solution to many of the security and interoperability challenges currently facing ultra-dense, high-speed wireless environments [9], [18]. Through a comparative analysis of blockchain-based approaches—including optimized consensus algorithms like UE-AP EpBFT and digital identity frameworks such as DIA-BC—this study highlighted how blockchain can reduce redundant authentications, increase authentication rates, and support secure IoT access within next-generation networks. Moreover, the integration of blockchain with standardization initiatives reinforces the need for unified frameworks that support trusted interactions between heterogeneous devices, access points, and network functions [8], [19]. Ultimately, achieving interoperability between blockchain systems and 5G NR/6G standards will require coordinated efforts from industry, academia, and standardization bodies. The findings from recent literature and implementations demonstrate that blockchain is not just an add-on but a foundational component in building resilient, transparent, and future-proof communication infrastructures.

References

[1] R. Bala and R. Manoharan, "Blockchain based secure and effective authentication mechanism for 5g networks," in *2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Sep. 2022, pp. 1–6.

[2] V. Aanandaram and P. Deepalakshmi, "Blockchain-based digital identity for secure authentication of iot devices in 5g networks," in *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Mar. 2024, pp. 1–6.

[3] L. M. Alkwai and K. Yadav, "Blockchain-based secure 5g/6g communication for internet of things devices in consumer electronic systems," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 6327–6338, Sep. 2024.

[4] B. Mafakheri, A. Heider-Aviet, R. Riggio, and L. Goratti, "Smart contracts in the 5g roaming architecture: The fusion of blockchain with 5g networks," *IEEE Communications Magazine*, vol. 59, no. 3, pp. 77–83, Mar. 2021.

[5] H. Zhang, S. Leng, F. Wu, and H. Chai, "A dag blockchain-enhanced user-autonomy spectrum sharing framework for 6g-enabled iot," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8012–8023, Mar. 2022.

[6] J. Xie, K. Zhang, Y. Lu, and Y. Zhang, "Resource-efficient dag blockchain with sharding for 6g networks," *IEEE Network*, vol. 36, no. 1, pp. 189–196, Nov. 2022.

[7] F. Miatton, "Blockchain at the edge: The nexus of capturing new value in 5g," in *2020 International Conference on Technology and Entrepreneurship - Virtual (ICTE-V)*, Apr. 2020, pp. 1–6.

[8] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5g and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115 876–115 904, Jun. 2020.

[9] T. Maksymyuk, J. Gazda, M. Volosin, G. Bugar, D. Horvath, M. Klymash, and M. Dohler, "Blockchain-empowered framework for decentralized network management in 6g," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, Sep. 2020.

[10] D. Ayepah-Mensah, G. Sun, G. O. Boateng, S. Anokye, and G. Liu, "Blockchain-enabled federated learning-based resource allocation and trading for network slicing in 5g," *IEEE/ACM Transactions on Networking*, vol. 32, no. 1, pp. 654–669, Aug. 2024.

[11] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, Sep. 2022.

[12] A. Hakiri and B. Dezfouli, "Towards a blockchain-sdn architecture for secure and trustworthy 5g massive iot networks," in *Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security*, ser. SDN-NFV Sec'21. New York, NY, USA: Association for Computing Machinery, Apr. 2021, p. 11–18. [Online]. Available: https://doi-org.psut.idm.oclc.org/10.1145/3445968.3452090

[13] A. Zhivtsova, V. Beschastnyi, Y. Koucheryavy, and K. Samouylov, "A survey of delay-oriented dynamic link scheduling policies for 5g/6g integrated access and backhaul systems," *IEEE Access*, vol. 12, pp. 118 565–118 586, Aug. 2024.

[14] P. William, A. K. Rai, P. Madan, C. P. Kumar, A. Shrivastava, and A. Rana, "Analysis of blockchain technology to protect data access using intelligent contract mechanism for 5g networks," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 6, Sep. 2023, pp. 1651–1657.

[15] W. Ke, H. Yaling, and H. Yuhuang, "Research on blockchain usage for 5g message service," in *2022 International Conference on Networking and Network Applications (NaNA)*, Dec. 2022, pp. 501–505.

[16] F. A. Shewajo, A. Boualouache, S. M. Senouci, I. El-Korbi, B. Brik, and K. Anlay Fante, "Integrating blockchain technology with pki for secure and interoperable communication in 5g and beyond vehicular networks," in *2024 IEEE 21st Consumer Communications Networking Conference (CCNC)*, Jan. 2024, pp. 998–1001.

[17] M. Baumgartner and J. Papaj, "Robust data transmission in 5g networks without infrastructure based on blockchain technology," in *2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)*, Apr, 2022, pp. 01–04.

[18] G. Bindu, I. T. J. S, V. R. Kanakala, G. L. K. Niharika, and B. E. Raj, "Impact of blockchain technology in 6g network: A comprehensive survey," in *2022 International Conference on Inventive Computation Technologies (ICICT)*, Jul. 2022, pp. 328–334.

[19] Nidhi, B. Khan, A. Mihovska, R. Prasad, and F. J. Velez, "Trends in standardization towards 6g," *Journal of ICT Standardization*, vol. 9, no. 3, pp. 327–348, 2021.