Wasit Journal of Engineering Sciences

Journal homepage: https://ejuow.uowasit.edu.iq

Blockchain-Enabled Secure and Decentralized Resource Management for Open Radio Access Network Cellular Networks

Dheyaa Marjan Hussein[1] and Basim K. J. Al-shammari[1]

Affiliations
[1]Department of Electrical Engineering,
University of Wasit,
Wasit, Iraq.

Correspondence
Dheyaa Marjan Hussein
dhussein@uowasit.edu.iq

Received
20-February-2024
Revised
27-February-2024
Accepted
11-July-2024

Doi:
10.31185/ejuow.Vol12.Iss3.537

Abstract

The rapid growth of Open Radio Access Networks (Open RAN) necessitates innovative resource management systems to address security and decentralization challenges. This study proposes the use of blockchain technology for enhancing the security, privacy, and decentralized decision-making in Open RAN cellular networks. The research focuses on secure communication between O-DU (Distributed Units) and O-CU (Centralized Units) using blockchain technology, along with smart contracts for O-DU to O-CU mapping, thereby ensuring data integrity and authenticity in resource management transactions. By leveraging a blockchain network and consensus methods, this study aims to validate resource management transactions securely and transparently. Smart contracts enforce resource management rules and adapt O-DU to O-CU mapping based on real-time network conditions. The experimental framework simulates an Open RAN environment with multiple O-DUs and O-CUs under dynamic network conditions and traffic demands, rigorously testing blockchain's security in O-DU to O-CU transactions. This study demonstrates that the proposed solution can improve transaction security, trust, transparency, smart contract automation, reduce resource allocation delay, and increase flexibility to dynamic network circumstances. The findings contribute to the ongoing efforts in enhancing the efficiency, security, and flexibility of 5G and beyond.

Keywords: Open RAN; resource management; blockchain technology; security; decentralization

الخلاصة: يتطلب النمو السريع لشبكات الوصول الراديوي المفتوحة (Open RAN) أنظمة مبتكرة لإدارة الموارد لمواجهة تحديات الأمن واللامركزية. تقترح هذه الدراسة استخدام تقنية blockchain لتعزيز الأمن والخصوصية واتخاذ القرار اللامركزي في الشبكات الخلوية المفتوحة RAN. يركز البحث على الاتصال الآمن بين O-DU (الوحدات الموزعة) وO-CU (الوحدات المركزية) باستخدام تقنية blockchain، إلى جانب العقود الذكية لرسم خرائط O-DU إلى O-CU، وبالتالي ضمان سلامة البيانات وصحتها في معاملات إدارة الموارد. . من خلال الاستفادة من شبكة blockchain وطرق الإجماع، تهدف هذه الدراسة إلى التحقق من صحة معاملات إدارة الموارد بشكل آمن وشفاف. تعمل العقود الذكية على فرض قواعد إدارة الموارد وتكييف خرائط O-DU مع O-CU بناءً على ظروف الشبكة في الوقت الفعلي. يحاكي الإطار التجريبي بيئة RAN مفتوحة مع وحدات O-DU وO-CU المتعددة في ظل ظروف الشبكة الديناميكية ومتطلبات حركة المرور، ويختبر بشكل صارم أمان blockchain في معاملات O-DU إلى O-CU. توضح هذه الدراسة أن الحل المقترح يمكن أن يحسن أمان المعاملات والثقة والشفافية وأتمتة العقود الذكية وتقليل تأخير تخصيص الموارد وزيادة المرونة في ظروف الشبكة الديناميكية. وتساهم النتائج في الجهود المستمرة لتعزيز كفاءة وأمان ومرونة شبكات الجيل الخامس وما بعدها.

1. INTRODUCTION

The rapid evolution of wireless communication networks, particularly Open Radio Access Networks (Open RAN), introduces new challenges in resource management. Open RAN offers an open and disaggregated approach to network deployment, allowing for increased flexibility and innovation. However, ensuring secure and decentralized resource management remains a critical challenge.[1]

Resource management in Open RAN involves allocating and optimizing resources such as bandwidth, power, and computational capacity to meet dynamic user and application demands. Traditional centralized approaches struggle with the increasing complexity and scale of Open RAN networks, leading to inefficient resource utilization, higher latency, and limited adaptability.[2]

To address these challenges, innovative solutions are needed to enhance security, privacy, and decentralized decision-making. Blockchain technology, with its inherent properties of decentralization, immutability, and transparency, offers a promising avenue for improving resource management.[3]

Blockchain secures and verifies network transactions via a distributed, tamper-resistant ledger, improving O-DU and O-CU communication security and integrity in Open RAN resource management. Furthermore, blockchain enables decentralized decision-making through smart contracts, which automate tasks like O-DU to O-CU mapping based on real-time conditions, reducing reliance on centralized entities and enabling more efficient resource allocation.[4]

This study proposes using blockchain technology to enhance Open RAN security, privacy, and decentralized decision-making. By constructing a blockchain network for O-DU to O-CU transactions and using consensus techniques, this study addresses resource management concerns securely and transparently. Smart contracts automate and enforce resource management rules, adapting O-DU to O-CU mapping to real-time network conditions.[5]

Through an experimental framework simulating an Open RAN environment with multiple O-DUs and O-CUs, this study demonstrates the benefits of the proposed blockchain-enabled solution. Expected outcomes include enhanced security against attacks and unauthorized access, improved trust and transparency in transactions, reduced latency in resource allocation, and increased adaptability to dynamic network conditions.

By contributing to the ongoing discussions on securing and decentralizing resource management in Open RAN cellular networks, our research aims to enhance the overall efficiency, security, and adaptability of Open RAN networks in the era of 5G and beyond.

2. LITERATURE REVIEW

The literature review covers resource management, Open RAN, and blockchain technology in cellular networks. Key references highlight significant findings and contributions in this field. Xu et al. (2023) explore the integration of blockchain and Open RAN in 6G networks, addressing scalability, security, and trust issues in future networks. They discuss the benefits of blockchain for resource management and sharing in cellular networks. The following references have been relied upon to highlight key findings and contributions in this field: In this research, the authors look at 6G networks via the lens of blockchain and Open RAN integration. In order to solve problems with future cellular networks' scalability, security, and trust, it explores the advantages of using blockchain technology for managing and sharing resources [6]. Wilhelmi and Giupponi (2021) assess the performance of blockchain-enabled RAN-as-a-service in beyond 5G networks, providing insights into the practical feasibility of blockchain-based solutions. Within the framework of networks that will exist after 5G, this study assesses the efficacy of RAN-as-a-service that is enabled by blockchain. The study assesses the impact of blockchain integration on resource management efficiency, latency, and scalability, providing insights into the practical feasibility of blockchain-based solutions for RAN resource management [7]. Geoponic and Wilhelmi (2021) discuss blockchain-based network sharing in Open RAN, emphasizing improved resource utilization, enhanced trust among operators, and reduced administrative overheads. This paper focuses on network sharing in the context of Open RAN and explores the use of blockchain technology as an enabler for secure and transparent sharing of network resources and discusses the potential advantages of blockchain-based network sharing, including improved resource utilization, enhanced trust among network operators, and reduced administrative overheads [8]. Xu et al. (2021) present Blockchain-Enabled Radio Access Network (BE-RAN), a blockchain-enabled Open RAN architecture with decentralized identity management and privacy-preserving communication, enhancing trust, privacy, and security in resource management. Incorporating decentralized identity management and privacy-preserving communication, the paper presents blockchain-enabled Open RAN architecture (BE-RAN), this study takes use of blockchain technology to improve identity management and privacy in Open RAN networks, which in turn improves trust, privacy, and security in resource management [9]. Xu et al. (2020) explore blockchain for resource management and sharing in 6G communications, highlighting secure and decentralized resource allocation. This research explores the application of blockchain technology in resource management and sharing for 6G communications. It investigates how blockchain can facilitate secure and decentralized resource allocation, enabling efficient utilization of network resources, and supporting diverse use cases in future cellular networks [10]. Giupponi and Wilhelmi (2022) explore the use of blockchain technology to facilitate network sharing in Open Radio Access Networks (O-RAN) within 5G and future networks. Their study addresses key challenges such as trust, security, and decentralized decision-making. They investigate how blockchain can enable efficient sharing of network resources among multiple operators, emphasizing the potential benefits for 5G and beyond [11]. These references advance cellular network resource management, Open RAN, and blockchain technology. They emphasize the significance of security, privacy, decentralization, and efficient resource allocation in future cellular networks and discuss the pros, cons, and prospective uses of blockchain technology in Open RAN resource management.

3. METHODOLOGY

3.1 Blockchain Integration

BE-RAN incorporates modern identity management and mutual authentication to enhance the decentralized focus of traditional RAN. Figure 1 illustrates the BE-RAN architecture with network layers. What follows is a more in-depth explanation of its details. The lower layers of BE-RAN may operate autonomously from the higher-level RAN and core network (CN) components, enabling them to liberate the data held by the top-level CN and use it for the creation of functions via the down-top technique.

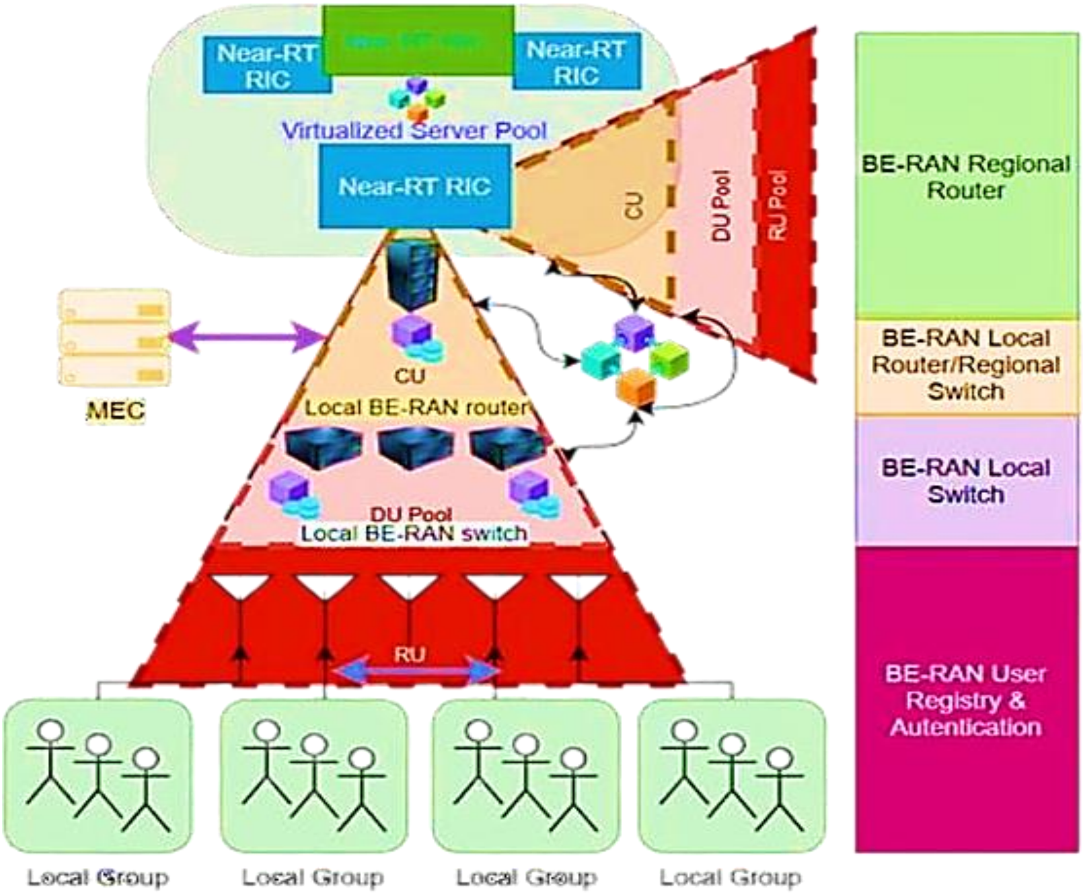


Figure 1 BE-RAN architecture with network layers [11]

At its heart, BE-RAN is an identity management system that uses mutual authentication, User equipment UE feasibility, and attach-request to enhance locality and latency during random RAN access. If the target users are in range of groups that are serviced by the same DU, as shown in Fig. 1 for the Local Group, and have access to reduced latency and privacy-enhanced networks, BE-RAN may enable UE-to- UE mutual authentication via ad hoc network switching after the UE registration is finished. By exchanging conventional RAN element Identifiers (IDs) and Public Key Infrastructure (PKI)-based credentials, advanced operation RAN elements can fight the Certificate Authority CA and other PKI resource threats. They can also associate with each other simultaneously utilizing Blockchain Addressing (BC ADD). When Layer 2 DUs lack valid interfaces to upper CU or other DUs in the same server pool, BE-RAN promotes communication via specific packet headers and settings. BE-RAN and CU-level routing services collaborate to secure UE and RAN components through firewalls and traffic restrictions. Multi-access Edge Computing (MEC), part of BE-RAN at the network layer, communicates with user devices and RAN components via MEC BC ADD bounded traffic filtering. BE-RAN and routing services at the CU level may work together to protect UE and RAN components by constructing firewalls and other traffic restrictions. According to the right-hand side of Figure 1, MEC is also a part of the BE-RAN at the network layer and communicates with all user devices and RAN components via MEC BC ADD bounded traffic filtering. Under BE-RAN, the RAN transforms into an Edge Network devoid of CN if it handles the majority of the traffic. Under BE-RAN, the RAN transforms into an Edge Network, handling most traffic without CN. The RAN intelligent controller (RIC) identifies BE-RAN features, enabling better service and policies like zero-rated QoS and QoE.

3.2 Experimental Framework

Figure 1 shows BE-RAN using the same RU, DU pool, and CU for local user groups per the 3GPP-specified RAN functional split option. Figure 2 provides a case study of the stacked RU, DU, and CU. Blockchain technology is used by all BE-RAN components except RU due to the lack of encoded information at the PHY interface. Figure 3 assesses the BE-RAN User/UE registry with Be Mutual protocols driving local and regional switching and routing.

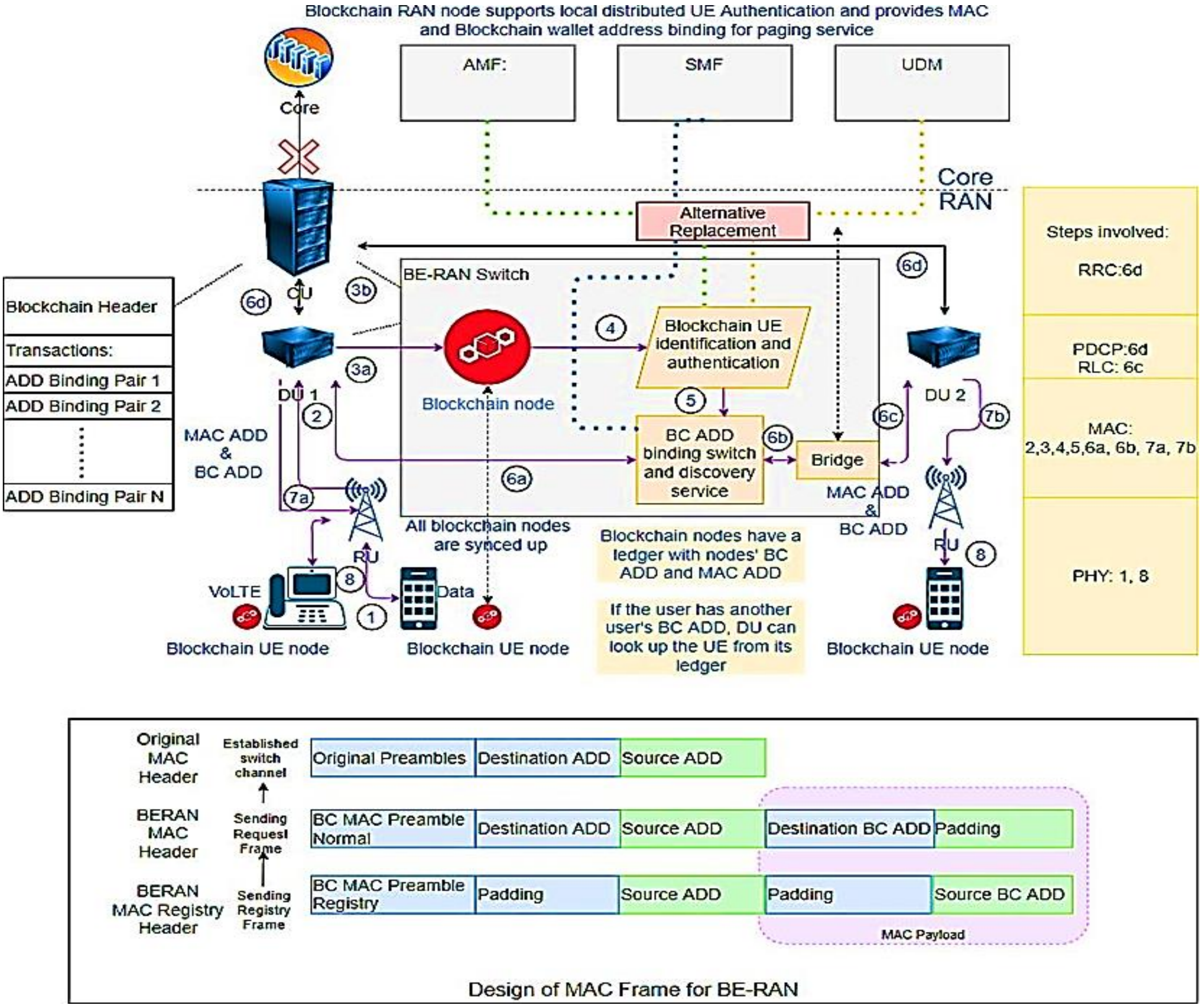


Figure 2 Framework and Frame structure of BE-RAN at Layer 2/MAC layer [11]

For BE-RAN's distributed architecture to function, all RAN logical units share the blockchain node, benefiting from virtualized hosting. Policing and QoS enhancements are achievable by influencing RIC and control panel interface administration. Communication between UEs, UEs and RAN elements, RAN elements and RAN elements, etc., is possible provided that the interfaces feature BC-ADDs. Although this study addresses RAN to the best of its abilities, its methodology does not restrict network topology or user responsibilities.

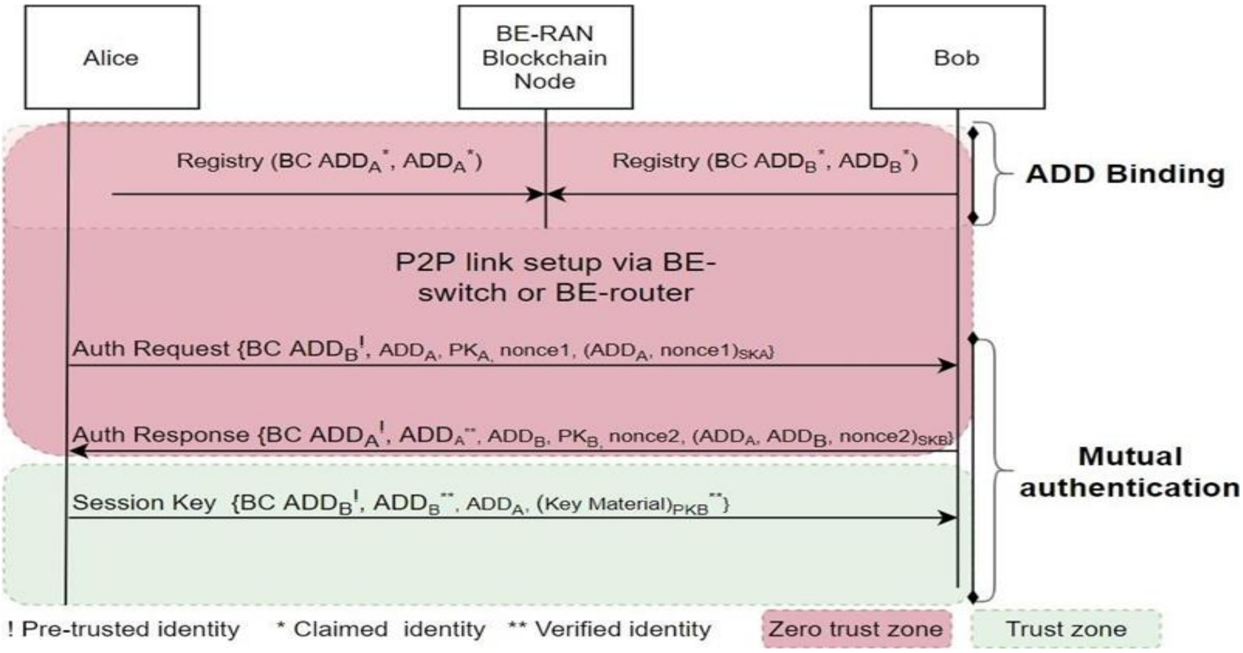

Alice
BE-RAN Blockchain Node
Bob
Registry (BC ADDA*, ADDA*)
Registry (BC ADDB*, ADDB*)
ADD Binding
P2P link setup via BE-switch or BE-router
Auth Request {BC ADDB!, ADDA, PKA, nonce1, (ADDA, nonce1)SKA}
Auth Response {BC ADDA!, ADDA**, ADDB, PKB, nonce2, (ADDA, ADDB, nonce2)SKB}
Session Key {BC ADDB!, ADDB**, ADDA, (Key Material)PKB**}
Mutual authentication
! Pre-trusted identity
* Claimed identity
** Verified identity
Zero trust zone
Trust zone

Figure 3 Mutual authentication of BE-RAN [12]

3.3 the procedure of privacy and security preserving in the BE-RAN communication.

Privacy and security measures to maintain blockchain-enabled RAN communications include many measures, including:

1- Data encryption: Used an advanced encryption techniques to protect data sent and received over the network. Ensure data is encrypted during transmission and storage to prevent unauthorized access.

2- Identity verification: Implemented identity verification protocols to ensure that entities participating in the network are trusted parties. Use digital certificates and electronic signatures to verify the authenticity of devices and users.

3- Key management: Use strong and secure key management to ensure that the keys used for encryption remain protected and Provide mechanisms to rotate and update keys regularly to enhance security.

4- Recording of operations: Use a blockchain ledger to record all transactions permanently and immutably and provide an accurate chronological record of all activities to ensure transparency and traceability.

5- Multiple agreement protocols: Implement multiple consensus protocols to ensure that all parties involved in the network agree and validate operations and Use consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) to ensure the security of operations.

6- Security policies: Develop and implement comprehensive security policies covering all aspects of blockchain-enabled RAN operation and maintenance. Conduct regular security audits and penetration tests to discover and address security vulnerabilities.

7- Access control: Implement access control mechanisms to ensure that access to the network and data is limited to authorized persons only. Use techniques such as Role-Based Access Control (RBAC) to determine user permissions.

By following these measures, a high level of privacy and security can be guaranteed for blockchain-enabled radio access network communications.

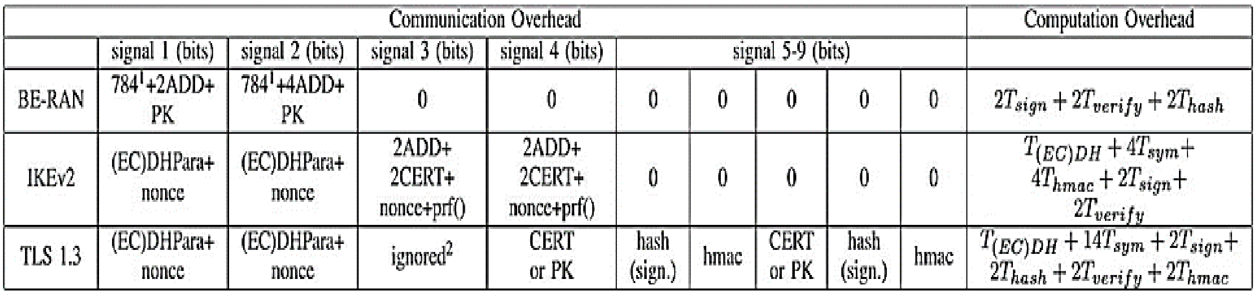
4. RESULT

BE-RAN has two fundamental function groups: mutual authentication performance is assessed through communication and computation metrics. Figures 4 and 5 present benchmarking results comparing BE-RAN, Internet Key Exchange version 2 (IKEv2), and transport layer security (TLS) with Rivest-Shamir-Adleman algorithm/Elliptic Curve Digital Signature Algorithm (RSA/ECDSA).

4.1 Studying the efficacy of protocols for reciprocal authentication: (communication, computation, and signalling)

Public-key authentication techniques, suited for mutual authentication, are used to compare the protocol stacks are commonly found in Transportation Layer or Network Layer. An evaluation of the potential of Be Mutual's signalling, communication, and computing capabilities using certificate-based IKEv2 and either certificate-based or public-key TLS 1.3 was carried out. Optional setup parameters like algorithm configurations, IKE header, etc. are disregarded to facilitate comparison. Table I excludes optional payloads like CERT REQ for IKEv2, trust anchors, and integrity checks from comparisons. Fairness of size and computing need is compared using just the essential parameters and simplest authentications. Both the Initial Exchange (IKE − IN IT) and the Authentication Exchange (IKE − AU T H) are components of IKEv2, a mutual authentication protocol that relies on certificates. These phases are responsible for authentication and security association, respectively. To calculate KEY SEED, a handshake secret of IKEv2, two signal messages are sent in IKE − IN IT together with the nonce and Elliptic Curve Diffie-Hellman (EC)DH Parameter. In IKE−AU T H, the secrecy and integrity of signal messages are protected by creating multiple keys from a key seed. Authentication signature values, including the sender's ID and certificate, are included in the IKE − AU T H signal messages. To get the AU T H value, we add the nonce and the result of the PRF function to the message.

Table 1 COMPARISON TABLE OF SELECTED COMMON MUTUAL AUTHENTICATION PROTOCOLS



Communication Overhead										Computation Overhead
	signal 1 (bits)	signal 2 (bits)	signal 3 (bits)	signal 4 (bits)	signal 5-9 (bits)					
BE-RAN	784^1+2ADD+ PK	784^1+4ADD+ PK	0	0	0	0	0	0	0	$2T_{sign} + 2T_{verify} + 2T_{hash}$
IKEv2	(EC)DHPara+ nonce	(EC)DHPara+ nonce	2ADD+ 2CERT+ nonce+prf()	2ADD+ 2CERT+ nonce+prf()	0	0	0	0	0	$T_{(EC)DH} + 4T_{sym} + 4T_{hmac} + 2T_{sign} + 2T_{verify}$
TLS 1.3	(EC)DHPara+ nonce	(EC)DHPara+ nonce	ignored^2	CERT or PK	hash (sign.)	hmac	CERT or PK	hash (sign.)	hmac	$T_{(EC)DH} + 14T_{sym} + 2T_{sign} + 2T_{hash} + 2T_{verify} + 2T_{hmac}$

On the Internet, TLS based on public keys and certificates is extensively used. Here are the stages of a typical TLS version 1.3 handshake: The following steps must be completed before the server can be started: server greeting, encrypted extensions, server certificate request, server certificate receipt, server certificate certification, server certificate completion, client certificate certification, and client certificate completion. For the sake of uniformity, we will not be comparing signal packets like Encrypted Extensions or setup parameters like algorithm, version, etc. The procedure for authenticating with TLS 1.3: You may use nonce and Elliptic Curve Diffie-Hellman Ephemeral (EC)DHE with Client Hello and Server Hello. A handshake secret is generated by (EC)DHE after the Client Hello and Server Hello. Encryption keys for subsequent signal messages will originate from this handshake secret. The context strings are part of the Certificate Request message. The raw public key or certificate is included in the message certificate. The handshake is signed using Transcript Hash by Certificate Verify. completes the handshake and sets the MAC value for the whole system.

4.2 Communication Overhead Comparisons

By adding the length of authentication signal messages as communication overhead, a group of the most commonly used authentication protocols and public key options, namely, IKEv2 with RSA and ECDSA, and TLS 1.3 with RSA and ECDSA, are selected as the baseline for the proposed Be Mutual protocols in the following comparison. As indicated by Fig. 4 (note that the unit has been converted to bytes for shortening numbers), BE-RAN yields better performance with Finite Field-based algorithms, such as RSA, in the test, and has similar performance (355 bytes vs. 319 bytes by TLS) to TLS in terms of the Elliptic Curve Cryptography ECC-based algorithms. The communication overhead results suggest that BE-RAN has good potential for use in high-performance and low-latency authentication. Note that, as discussed in external overhead, the cost of running blockchain infrastructure and other external environments is not considered for BE-RAN, nor for IKEv2 and TLS 1.3.

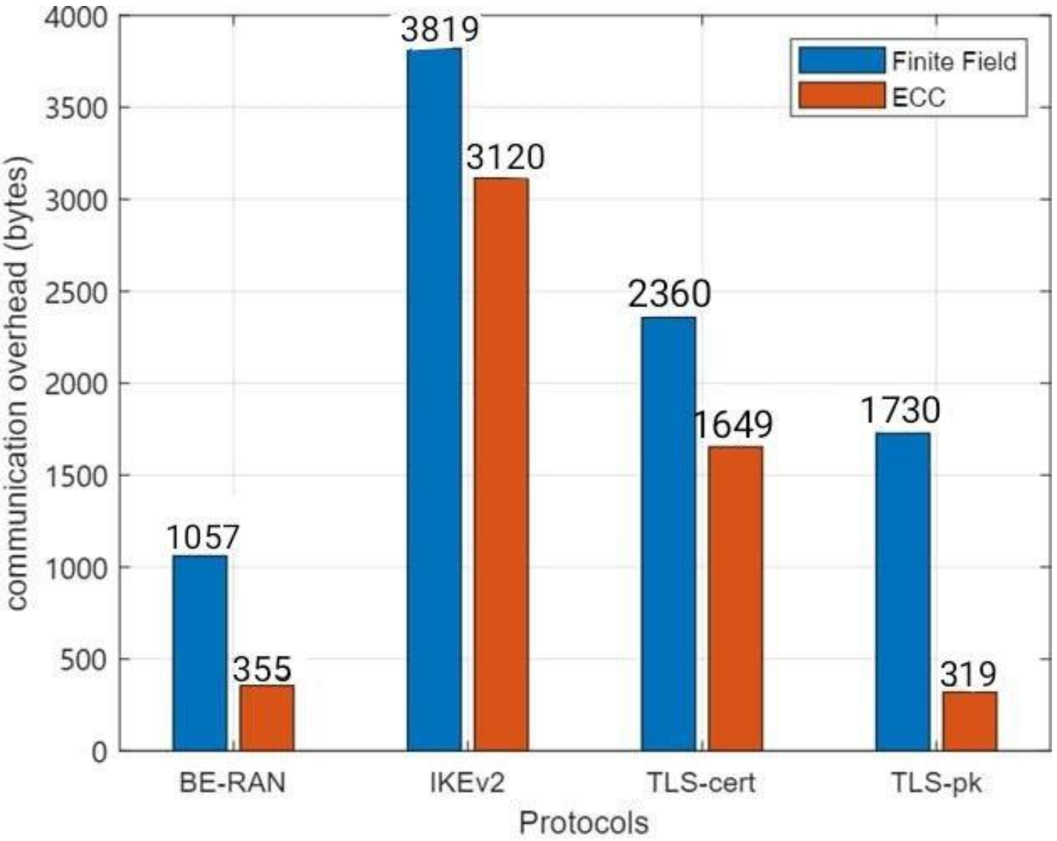
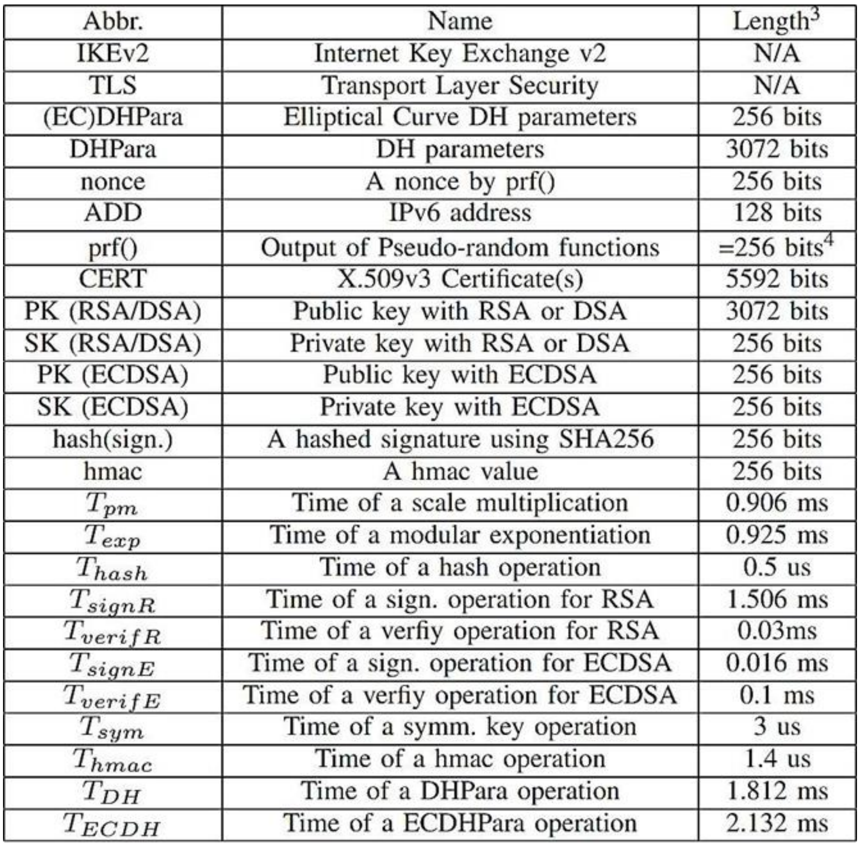


Figure 4 Communication overheads for Finite field and ECC crypto protocols

4.3 Computational Overhead Benchmark

The computational cost is assessed by protocol execution time on Ubuntu 20.04.1 4GB RAM, 4 Cores at 4.2 GHz virtualized on Windows 10 PC. Table 2 shows how computational overhead is measured in the same physical context by comparing platform execution time. Select authentication mechanisms include IKEv2, TLS 1.3, and BE-RAN with RSA/ECDSA.

Table 2 TABLE OF PARAMETERS



Abbr.	Name	Length[3]
IKEv2	Internet Key Exchange v2	N/A
TLS	Transport Layer Security	N/A
(EC)DHPara	Elliptical Curve DH parameters	256 bits
DHPara	DH parameters	3072 bits
nonce	A nonce by prf()	256 bits
ADD	IPv6 address	128 bits
prf()	Output of Pseudo-random functions	=256 bits[4]
CERT	X.509v3 Certificate(s)	5592 bits
PK (RSA/DSA)	Public key with RSA or DSA	3072 bits
SK (RSA/DSA)	Private key with RSA or DSA	256 bits
PK (ECDSA)	Public key with ECDSA	256 bits
SK (ECDSA)	Private key with ECDSA	256 bits
hash(sign.)	A hashed signature using SHA256	256 bits
hmac	A hmac value	256 bits
T_{pm}	Time of a scale multiplication	0.906 ms
T_{exp}	Time of a modular exponentiation	0.925 ms
T_{hash}	Time of a hash operation	0.5 us
T_{signR}	Time of a sign. operation for RSA	1.506 ms
T_{verifR}	Time of a verfiy operation for RSA	0.03ms
T_{signE}	Time of a sign. operation for ECDSA	0.016 ms
T_{verifE}	Time of a verfiy operation for ECDSA	0.1 ms
T_{sym}	Time of a symm. key operation	3 us
T_{hmac}	Time of a hmac operation	1.4 us
T_{DH}	Time of a DHPara operation	1.812 ms
T_{ECDH}	Time of a ECDHPara operation	2.132 ms

Table 2 shows benchmarked results for all computational components, and Fig. 5 compares chosen methods. The computational comparison reveals BE-RAN outperforms Finite-Field-based algorithms like RSA and DSA and other protocols using the elliptical curve technique. Due to the lower authentication cost, ECC- based results support BE-RAN for IoT and other thin-clients.

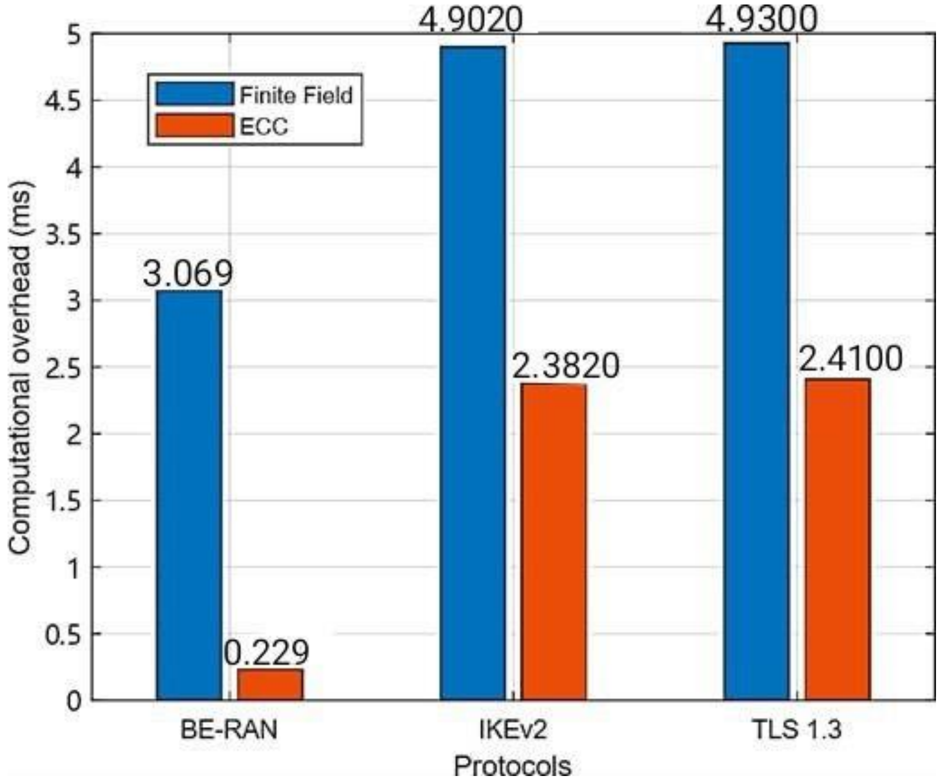


Figure 5 Computational overhead for Finite field and ECC crypto protocols

5. CONCLUSIONS

Blockchain and smart contracts improve resource management in Open RAN networks by enhancing efficiency, security, and flexibility. The proposed blockchain-enabled solution demonstrates secure, transparent validation of O-DU to O-CU transactions, improving resource management. Smart contracts enable decentralized decision-making, reducing latency and optimizing resource use based on real-time conditions. Through the use of MATLAB and conducting simulations, the effectiveness of this technology was verified in managing open RAN resources, improving network resource consumption, enhancing performance, and supporting various applications.

6. FUTURE RECOMMENDATIONS

The results and consequences of this study suggest various areas for additional inquiry and improvement:

Future research should address blockchain integration challenges in Open RAN networks, focusing on performance and scalability optimization through sharing, off-chain transactions, and layer two solutions. Enhancing privacy and confidentiality in blockchain-enabled resource management is crucial, employing zero-knowledge proofs, homomorphic encryption, and secure multi-party computing. Standardizing protocols and interfaces for blockchain-enabled resource management in Open RAN networks requires research and industry collaboration. Energy-efficient blockchain technology measures should be implemented, focusing on energy-saving methods like proof of stake algorithms. Real-world deployment and field experiments will validate the blockchain-enabled solution's performance and scalability in realistic Open RAN networks.

7. CONTRIBUTIONS

The contribution of this research is the proposal of a blockchain-enabled secure and decentralized resource management system for Open Radio Access Networks (Open RAN) in cellular networks. This research aims to address the challenges of security, privacy, and decentralized decision-making in these networks by leveraging blockchain technology and smart contracts. The specific contributions are:

1. **Enhanced Security and Privacy**: By using blockchain technology, the research enhances secure communication between Distributed Units (O-DU) and Centralized Units (O-CU), ensuring data integrity and authenticity in resource management transactions.
2. **Decentralized Decision-Making**: The use of smart contracts allows for decentralized decision-making, automating resource management rules, and adapting O-DU to O-CU mapping based on real-time network conditions.
3. **Improved Transaction Security and Transparency**: The blockchain network and consensus methods validate resource management transactions securely and transparently, improving trust and reducing the delay in resource allocation.
4. **Increased Flexibility**: The proposed solution enhances the flexibility of the network in dynamic conditions, contributing to the ongoing efforts to improve the efficiency, security, and adaptability of 5G networks and beyond.

REFERENCES

1. Liyanage, M., Braeken, A., Shahabuddin, S., & Ranaweera, P. (2023). Open RAN security: Challenges and opportunities. Journal of Network and Computer Applications, 214, 103621.
2. Moussaoui, M., Aryal, N., Bertin, E., & Crespi, N. (2022, September). Distributed Ledger Technologies for Cellular Networks and Beyond 5G: a survey. In 2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 37-44). IEEE.
3. Kaur, U., & Shalu. (2021). Blockchain-and deep learning-empowered resource optimization in future cellular networks, edge computing, and IoT: Open challenges and current solutions. Blockchain for 5G-Enabled IoT: The new wave for Industrial Automation, 441-474.

4. Okon, A. A., Elgendi, I., Sholiyi, O. S., Elmirghani, J. M., Jamalipour, A., & Munasinghe, K. (2020). Blockchain and SDN architecture for spectrum management in cellular networks. Ieee Access, 8, 94415-94428.
5. Tahir, M., Habaebi, M. H., Dabbagh, M., Mughees, A., Ahad, A., & Ahmed, K. I. (2020). A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. IEEE Access, 8, 115876-115904.
6. Xu, H., Klaine, P. V., Onireti, O., & I, C. L. (2023). 6 G Resource Management and Sharing: Blockchain and O-RAN. Blockchains: Empowering Technologies and Industrial Applications, 253-285.
7. Wilhelmi, F., & Giupponi, L. (2021, December). On the performance of blockchain-enabled RAN-as-a-service in beyond 5G networks. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 01-06).IEEE.
8. Giupponi, L., & Wilhelmi, F. (2021). Blockchain-enabled network sharing for o-ran. arXiv preprint arXiv:2107.02005.
9. Xu, H., Zhang, L., & Sun, Y. (2021). BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication. arXiv preprint arXiv:2101.10856.
10. Xu, H., Klaine, P. V., Onireti, O., Cao, B., Imran, M., & Zhang, L. (2020). Blockchain-enabled resource management and sharing for 6G communications. Digital Communications and Networks, 6(3), 261-269.
11. H. Xu, L. Zhang, Y. Sun, and C.-L. I, "BE-RAN: Blockchain-enabled Open RAN with Decentralized Identity Management and Privacy-Preserving Communication," no. May, 2021, [Online]. Available: http://arxiv.org/abs/2101.10856
12. H. Xu, Z. Li, Z. Li, X. Zhang, Y. Sun, and L. Zhang, "Metaverse Native Communication: A Blockchain and Spectrum Prospective," 2022 IEEE Int. Conf. Commun. Work. ICC Work. 2022, no. March, pp. 7–12, 2022, doi: 10.1109/ICCWorkshops53468.2022.9814538.
13. Giupponi, L., & Wilhelmi, F. (2022). Blockchain-enabled network sharing for O-RAN in 5G and beyond. IEEE Network, 36(4), 218-225.
14. Wang, C., & Feng, J. (2010, October). A study of mutual authentication for P2P trust management. In 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 474-477). IEEE.
15. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.
16. Bittorrent Foundation, "BitTorrent (BTT) White Paper," pp. 1–21, 2019. [Online]. Available: https://www.bittorrent.com/btt/btt-docs/
17. Era of TLS 1.3: Measuring Deployment and Use with Active and Passive Methods," jul 2019. [Online]. Available: http://arxiv.org/abs/1907.12762
18. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," jul 2014. [Online]. Available: http://arxiv.org/abs/1407.3561
19. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf
20. S. Troia, L. M. M. Zorello, A. J. Maralit, and G. Maier, "Sd-wan: An open-source implementation for enterprise networking services," in 2020 22nd International Conference on Transparent Optical Networks (ICTON), 2020, pp. 1–4.
21. W. Tong, X. Dong, Y. Shen, and J. Zheng, "BC-RAN: Cloud radio access network enabled by blockchain for 5G," Computer Communications, vol. 162, pp. 179–186, 2020.
22. O-RAN Alliance, "O-RAN-WG1.OAM-Architecture-v02.00," Tech. Rep., 2020. [Online]. Available: https://www.o-ran.org/specifications/O-RAN Architecture Description 2.0
23. P. networks, "What is SASE?" 2020. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-sase
24. D. Yu, W. Li, H. Xu, and L. Zhang, "Low Reliable and Low Latency Communications for Mission Critical Distributed Industrial Internet of Things," IEEE Communications Letters, vol. 25, no. 1, pp. 313–317, jan 2021.
25. R. Zheng and W. Yang, "H-mpls: A lightweight nfv-based mpls solution in access network," in 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014, pp. 887–892.
26. ETSI, "TS 123 501 - V15.9.0 - 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.9.0 Release 15)," Tech. Rep., 2020.
27. O-RAN Alliance, "The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components," 2020. [Online]. Available: https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles- security-challenges-on-all-o-ran-interfaces-and-components
28. E. Westerberg, "4G/5G RAN architecture: How a split can make the difference," Ericsson Review (English Edition), vol. 93, no. 2, pp. 52– 65, 2016.

29. L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, “How Much Communication Resource is Needed to Run a Wireless Blockchain Network?” jan 2021. [Online]. Available: http://arxiv.org/abs/ http://arxiv.org/abs/2101.10852
30. S. Van Rossem, W. Tavernier, B. Sonkoly, D. Colle, J. Czentye,
31. M. Pickavet, and P. Demeester, “Deploying elastic routing capability in an SDN/NFV-enabled environment,” in 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN). IEEE, nov 2015, pp. 22–24. [Online]. Available: http://ieeexplore.ieee.org/document/7387398/
32. W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, “A Scalable Multi-Layer PBFT Consensus for Blockchain,” IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 5, pp. 1146–1160, may 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9279277/
33. D. Ongaro and J. Ousterhout, “In Search of an Understandable Consen- sus Algorithm,” in Proceedings of the 2014 USENIX Annual Technical Conference, USENIX ATC 2014, vol. 22, no. 2, 2014, pp. 305–320.
34. 3GPP, “NG-RAN; Architecture description (Release 15),” Tech. Rep., 2018. [Online]. Available: https://www.3gpp.org/DynaReport/38401.htm
35. X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, “Blockchain Radio Access Network Beyond 5G,” IEEE Wireless Communications, vol. 27, no. 6, pp. 160–168, 2020.