Securing 5G Networks with Blockchain: On Authentication Strategies and Challenges

[1]*Jaskiranjit* Kaur, [2]*Parvesh* Kumar
[1]Panjab University, India
[2]Parvesh Kumar, Chandigarh University, India

Abstract—Fifth generation (5G) cellular network has an incredible feature to connect massive devices and gives promising services to various applications. EAP-AKA and 5G-AKA protocols are used in 5G for authentication. These existing authentication mechanisms is not well effective and challenged by vulnerabilities. This is posing serious threats to both privacy and network security. Blockchain is one of method to secure 5G authentication parameters. So, This paper is based on an analysis of blockchain-enabled authentication methods for 5G networks. It reviews multiple frameworks and provides a comparative analysis of their advantages, drawbacks, and opportunities for future research. we examine literature from three databases (Scopus, WoS, and MDPI) from 2019 to 2025. Inclusion and exclusion criteria are selected for extract quality of papers for analysis. only those papers are considered which have clear methodology, architectures, frameworks, or protocols relevant to the study. Finally, it gives future research directions by discussing challenges of existing frameworks.

Keywords— 5G, Blockchain, Authentication, Security, Privacy

1 Introduction

With its ultra-fast speed, low latency, and massive connectivity features, 5G introduces significant improvement in businesses[1], industries[2]-[4], and consumer experiences. As a result of this, the number of devices and applications connected in 5G environments grows exponentially[5]. This rapid growth of connected networks unlocks various opportunities while simultaneously introducing significant challenges[6][7], such as managing a high density of connection demands, a robust and secure system. For that, the authentication process plays a vital role in building trust between user equipment (UE) and the network. Standard approaches such as EAP-AKA[8], EAP-TLS[9], and 5G-AKA offer improvements over previous generations, but these still face many vulnerabilities[10][11]. In response to these challenges, the integration of 5G with blockchain technology has emerged as a potential game-changer. Blockchain has an immutable, transparent, cryptographic-based decentralized system[12]. Based on these features, researchers proposed frameworks to improve the authentication process for 5G networks. The aim of this study is to analyze how blockchain helps to improve existing authentication methods and what challenges these new frameworks face. The implication of this study for both

1 Corresponding author: er.jaskiran@gmail.com

academia and industry, including researchers, security analysts, and policymakers and guides the design of future-ready network architectures.

For this study we extract and examine 60 recent literates from January 2019 to May 2025 related to the fusion of blockchain with 5G. For the selection of these papers, we selected 3 well-reputed databases (Scopus, WoS, and MDPI Journals). Only those papers are extracted that give clear methodology, architectures, frameworks, or protocols relevant to the study. The screening criteria is shown in figure 1.The target keywords "Blockchain-based authentication," "Blockchain-enabled 5G authentication," "Decentralized authentication in 5G," "Decentralized AKA in 5G," and "Smart contract-based 5G authentication" are used to search papers. After that, research questions are formulated to make a systematic understanding. These research questions give summarized findings of proposed frameworks alongside challenges related to proposed work.

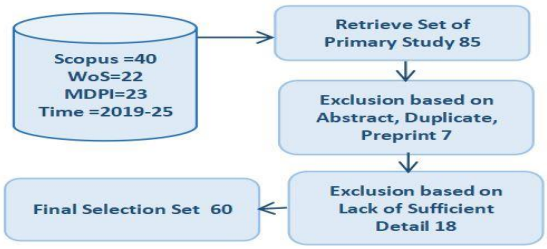

Fig 1 : Flow diagram of systematic selection of literature

2 Research Outcomes and Insights

This section gives a detailed look at existing research on blockchain based authentication i n 5G Systems. To answer the first research question (RQ1), we will examine how blockchain can help deal with security risks and make the overall securit y of 5G networks stronger. For research question (RQ2), we will look at the problems and difficulties of using blockchain for authentication in 5G networks. These research questions are formulated in table 1.

Table 1: Key contributions of this work

Research Question	Considerations
RQ1: How does Blockchain technology support and strengthen authentication parameter in 5G networks?	To investigate the specific ways in which Blockchain can address security vulnerabilities and improve the overall security framework of 5G systems.
RQ2: What are the issues and challenges in Blockchain-based authentication solutions for 5G networks?	To explore the factors that hinder the effectiveness of these solutions.

The integration of blockchain technology into 5G networks has seen a lot of research in recent years, especially regarding authentication in 5G network. Blockchain's decentralized structure, along with its strong cryptographic methods, presents a promising way to handle the growing security challenges as 5G networks become more complex and widespread. This section reviews existing studies, organized into different classes, and highlights the main findings, issues and area that still need more research.

RQ1: How does Blockchain technology support and strengthen authentication parameter in 5G networks?

In [13], the authors proposed a framework which is blockchain based authentication handover in 5G network and address low delay among heterogeneous cells by reducing authentication overhead which is less then 1 ms.It used Encryption and consensus mechanism for applied to protect privacy and security by transmitting the key in handover process. A user equipment (UE) registered on Blockchain Center (BC) and assigns public and private keys to the UE for secure communication and authentication.The UE's authentication request validates through the UE's public key with the SDN controller which communicate with BC while UE moves new cells without re-authentication, as the BC has already shared the necessary information with the SDN controllers of adjacent cells.The BC also manages dynamic key attributes for the UE, optimizing the key transfer process during handovers to minimize key transfer time and ensure efficient key management.On detection of malicious UE , the SDN controller notifies the BC and other SDN controllers and updates the ledger to prevent further attacks.The SDN controllers participate in the upgraded Delegated Proof of Stake (DPOS) consensus mechanism to validate transactions and add new blocks to the blockchain.The upgraded DPOS algorithm reduces the number of nodes involved in consensus, making it scalable and energy-efficient for 5G networks.

The authors in [14] fortified the 5G-AKA protocol through the integration of blockchain technology and one-time secret hashes as device secrets, causing an increase in both security and efficiency in the operation of the developed system. The system not only guarantees mutual authentication and confidentiality of the data but also does not incur high computation and energy usage costs.This approach involve decentralized authentication whicch make system less vulnerable. In this authentication checks through a secret hash record stored on blockchain. These records are immutable.Elliptic Curve Diffie-Hellman (ECDH) method is used when generated session key. Scyther and BAN logic are formal verification tools applied to ascertain the correctness and safety of the operation.This ensures that the system remains secured and operates energy-efficiently with all its features.

The 5G networks faced new problems in the area of authentication in connection with the growth of IoT devices. In a wide-ranging review of the pertinent existing literature, the author in [15] pointed out the intricate nature of the trust issues between many functional components (like AUSF/UDM, AMFs, SEAFs, etc.) concerning security. To counter these issues, the author has presented an integration of a framework with blockchain technology for authentication with low communication latency. The framework is such that it stores the security credentials of IoT devices on decentralized ledgers to preserve confidentiality. The scheme was evaluated and found safe and secure, as per informal and formal security analysis, carried out using the Scyther tool.

Mutual consensus in communication can be achieved by installing a multisignature smart contract on the consortium blockchain [16]. This approach based on consortium Blockchain

maintains a ledger currency to coordinate and manage inter-domain operations using private ledgers. The CAIoV scheme uses IPFS storage together with blockchain ledgers to achieve reactive efficiency coupled with data integrity. HMAC-SHA256 and nonce mechanisms make attack resistance system.This framework reduce authentication latency by 20% and maintain less than 0.5% error rates in cross-domain handshakes.It also strengthens the systems against 51% attacks through domain-specific consensus rules which ensures secure operation in the dynamic IoT environment.This proposed system work on cross-domain verification in 5G-enabled drones.This cross-domain verification address challenges which are related to storage space and authentication latency [17].

In this framework [18] author works on Network function (NFs) sharing during various network slicing. It introduces a multi-party, fully distributed Public Key Infrastructure (PKI).The blockchain based framework generates the certificates that NFs authenticate.The other component Network Repository Function (NRF) verifies certificates from the ledger to ensure valid node. In order to access shared resources, the NRF subsequently generates a JSON Web Token (JWT) that contains the slice ID, the NF's ID, and other pertinent information. The JWT and the shared NF are displayed when an NF requests access to a shared resource. The JWT is presented by the NF when it requests access to a shared resource, and the shared NF confirms the token with the NRF before allowing access. This method proves that only authorized NFs access specific slices and preventing unauthorized access which protect against data leakage.The security of the model is verified using both informal and formal security verification mechanisms, RealOr-Random (ROR) logic and the Scyther validation tool.

In [19], the author introduces a approach that provides a secure and efficient method for authentication on supply chain system by segregation RFID (Radio Frequency Identification) technology with blockchain.. This system is based on initialization and authentication key agreement using bitwise exclusive-or (XOR) and one-way cryptographic hash functions. A private blockchain with the Raft consensus mechanism is used which prevents adversaries from injecting false data.Additionally,Blockchain ensures that supply chain transactions using cartographic hashed XOR, hash functions (e.g., SHA-1/SHA-256), and bitwise rotation instead of resource-heavy operations like elliptic curve cryptography (ECC), making it suitable for IoT devices in 5G MEC environments and prevents tampering and guarantees authenticity. This proposed framework addresses and eliminates the security and privacy vulnerabilities present in previous protocols[20-25] and offering a more robust.light weighted framework for modern supply chain management.

This anonymity protects user privacy and provides secure access to data. The paper[26] designed Blockchain-based trusted authentication for cloud-based radio access networks (C-RAN) which allow users to authenticate without revealing their identities. This anonymity protects user privacy at same time as ensuring secure access to network resources.This framework also address improving network operation, connection cost and resource optimization.

Blockchain also plays a significant role in preventing the system from attacks. In [27] author not only address impersonation attack and MitM attacks which exist in [28][29]but also work on key secrecy to improve the security level of authentication by replacing all the signaling messages in 5G-AKA.The time overhead also improved which reflects the less complexity of the authentication protocol.This proposed model replace the core network with distributed CN nodes using Ethereum and ECC-Secp256k1 methods.

Blockchain used to management and the automatic data synchronization in network. Moreover, communication between core nodes also done by function calling chain method. Security is enhanced by replacing symmetric keys with asymmetric keys, with the public keys of the UE and CN node stored on the blockchain. A smart contract manages data access permissions, while the authentication process uses public/private key pairs to generate the authentication key. Table 2 describes the brief summary of existing literature.

Table 2: Summary of existing literature

Paper	Findings	Challenges	Used techniques
[13]	Minimizing Authentication Handover Delays, Eliminating Redundant Re- authentication,Enh ancing Network Efficiency, Mitigating Performance Degradation	Not lightweight blockchain,sc alability, optimized energy consumption.	OMNeT ++, DPOS algorithm
[14]	Decentralize subscription repository ,Strengt hened Security,Mitigatio n of DDoS and DoS Attack Mitigation,Formal Verification,Mini mized Computational Overhead	Slightly added overhead in computationa l overhead, Communicati on overhead, More energy consumption	Burrows– Abadi– Needham (BAN) logic and the Scyther tool used to formal verification.
[15]	No Additional Computation for IoT Devices,Forward and Backward Secrecy, Formal and Informal Security Analysis	Slightly additional computational complexity	Scyther tool
[16]	Cross-Domain Authentication,Ad aptive Identity Management, Privacy Safeguarding, Tamper-Proof Security, Digital Identity for External Authentication	Blockchain Latency,High transaction failure rate	Raft algorithm,H yperledger Fabric
[18]	Mitigate the single point of failure, Distribution of CA Functionality for Enhanced Trust,Optimized Lightweight Certificates, Rapid and Automated Certificate Revocation,Secure Communication,Pr evention of Unauthorized Service Access, Elimination of Denial of Service (DoS) Attacks, Protection Against Data Leakage Between Slice	Requires slightly more time to issue certificates which increase latency,Issue related to Optimized storage mechanism	Hyperledger Fabric,Proof of Concept (PoC), RealOr- Random (ROR) logic and Scyther Validation tool
[19]	Optimized for both communication and computational efficiency,Lightwe ight blockchain- powered RFID	Not discuss scalability and Resource optimization	Formal security verification using the broadly-accepted

	authentication,Rep lay Attack Prevention, Protection Against Ephemeral Secret Leakage (ESL) Attacks, Defense Against Man-in-the-Middle Attacks		Automated Validation of Internet Security Protocols.
[26]	Maintains the key secrecy, Resistance from impersonation attack, Resistance from MitM attack, Overcome single point of failure, Deployment complexity.Reduc e the network overhead and service latency effectively	Not discuss scalability and Resource optimizatio n,Time overhead indicates the complexity involved in the authenticati on protocol .	Ethereum and ECC-Secp256k1
[27]	IoT Device to Device authentication,Red uce computation cost,IoTD anonymity,Endure a variety of attacks	Congestion and energy related issues	Proverif tool, Random Oracle Model (RoM),Inform al security analysis.
[28]	Secure AKA handover scheme,Prevent from Denial of service (DoS) attacks, Lower the communication and computation overhead.	Constraints in ensuring users' location privacy	Kovan Blockchain,Po S algorithm,SHA -256 hash function
[29]	Design lightweight and compliant 5G- HandoverAKA protocol, Anonymity,Desyn chronization, Eavesdropping, Backward Secrecy, Forward Secrecy, Denial-of-Service (DoS), Replay attack, Man-in-the- Middle (MitM), Impersonation, Pre-shared key leakage, Plaintext attack	Scalability Challenges ,Processing overhead	BAN logic, Scyther tool
[30]	Communication and Computation overhead, MitM, Impersonating attacks, IMSI catching, Location privacy attacks	No discuss about scalibility, Congestion parameters	Etherum,Solidity

RQ2: What are the issues and challenges in Blockchain- based authentication solutions for 5G networks?

By virtue of its decentralized nature, strong security best practices, and disintermediation features, blockchain technology is getting prominent attention as a mechanism for refining authentication in 5G networks. Nevertheless, despite its promise, the integration of blockchain into 5G authentication sets in some challenges that ought to be addressed for smooth deployment. Some of these pertinent challenges are discussed hereafter along with some references from the available literature..

***a)* Scalability and Network Congestion**

5G networks are designed to handle an enormous number of connected devices, including IoT sensors, autonomous vehicles, and industrial systems. However, blockchain-based authentication often lacks the scalability required to process high transaction volumes efficiently [13], [14], [16]. In blockchain, the consensus mechanism will take more

processing and computation time if we scale more networks. As a result, authentication verification becomes slow, which affects overall network performance[16][18]. But this delay is not acceptable in the case of smart transportation and remote healthcare.
To a large extent, blockchain can address scalability challenges by adopting Layer-2 solutions, such as sidechains, rollups, and state channels. These approaches reduce network congestion and enhance overall system performance. Another effective technique is sharding, which distributes authentication processes across multiple network nodes. This method helps prevent bottlenecks and improves efficiency in large-scale networks. AI-powered authentication management can used accelerate verification tasks and reduce computational load on other blockchain-based processes.

b) **Energy Consumption and Resource Utilization**
Literature [28], [29], and [15] proposed frameworks applicable to real-world mobile and edge computing scenarios but also face the problem of high energy consumption. Blockchain authentication mechanisms are based on cryptographic computations that require inordinate computational resources. This is a critical challenge for battery-powered devices such as IoT sensors, mobile phones, and drones operating in 5G environments.
To address energy consumption and resource utilization challenges, blockchain systems should adopt optimized consensus algorithms that minimize computational overhead. consensus algorithm such as Proof of Authority (PoA), Federated Byzantine Agreement (FBA), and Lightweight Delegated Proof of Stake (L-DPoS)can help reduce unnecessary energy consumption to some extent. We can integrated system with Some lightweight cryptographic methods to optimize authentication processes.These approaches collectively contribute to enhancing energy efficiency in blockchain-based authentication systems.

c) Data Storage and Blockchain Ledger Growth
Some authentication schemes store security credentials directly on the blockchain, increasing storage costs and slowing down transaction verification. If not managed properly, storage overhead can become unsustainable, particularly for resource-limited devices.
There are applications of off-chain storage solutions that could help to reduce the size of the data stored on the blockchain, such as IPFS(InterPlanetary File System) and cloud-based log authentication. Suitable techniques in blockchain for removing old authentication records without jeopardizing any security. The tree structure in the Merkle approach can also add to the efficiency of storing such authentication data and saving memory.

c) **Lack of Interoperability**
A new challenge linking with blockchain-based authentication is providing seamless authentication among various 5G network operators and service providers across dissimilar regions. For the most part, current solutions based on blockchain tend to be building specific limits to their cross-network applicability [16][18].
Among the more feasible solutions are the development of cross-chain communication protocols, such as those used by Polkadot, Cosmos, and Atomic Swaps; these enable authentication data to be securely transferred across different blockchain systems. Standardization of authentication frameworks that could be adopted by various network providers would facilitate cross-domain authentication. The establishment of federated identity management will permit a user to authenticate once in order to securely access multiple services provided by different network providers.

3 Conclusion

Blockchain technology has the potential to improve authentication in 5G networks by addressing security vulnerabilities and eliminating centralized authentication methods. This survey identify key contribution, research trends and gaps in blockchain-enabled 5G authentication systems. Second part discuss major challenges that must be addressed for enable large-scale deployment of blockchain-based authentication in 5G networks.Overcoming these challenges will enable blockchain to play a pivotal role in securing next-generation 5G networks, ensuring seamless and trustworthy authentication mechanisms.

References

1. Ionescu, Constantin Aurelian, et al. "The new era of business digitization through the implementation of 5G technology in Romania." *Sustainability* 13.23 (2021): 13401.
2. Peraković, Dragan, et al. "Development and implementation possibilities of 5G in Industry 4.0." *Design, Simulation, Manufacturing: The Innovation Exchange*. Cham: Springer International Publishing, 2020. 166-175.
3. Attaran, Mohsen. "The impact of 5G on the evolution of intelligent automation and industry digitization." *Journal of ambient intelligence and humanized computing* 14.5 (2023): 5977-5993.
4. Rao, Sriganesh K., and Ramjee Prasad. "Impact of 5G technologies on industry 4.0." *Wireless personal communications* 100.1 (2018): 145-159.
5. https://sqmagazine.co.uk/5g-statistics.
6. Shafi, Mansoor, et al. "5G: A tutorial overview of standards, trials, challenges, deployment, and practice." *IEEE journal on selected areas in communications* 35.6 (2017): 1201-1221.
7. Salahdine, Fatima, Tao Han, and Ning Zhang. "Security in 5G and beyond recent advances and future challenges." *Security and Privacy* 6.1 (2023): e271.
8. Edris, Ed Kamya Kiyemba, Mahdi Aiash, and Jonathan Loo. "Formalization and evaluation of EAP-AKA'protocol for 5G network access security." *Array* 16 (2022): 100254.
9. Shi, Min, et al. "A Formal Analysis of 5G EAP-TLS Protocol." *IEEE Transactions on Networking* (2025).
10. You, Ilsun, et al. "5G-AKA-FS: A 5G authentication and key agreement protocol for forward secrecy." *Sensors* 24.1 (2023): 159.
11. Cheng, Ya-Chu, and Chung-An Shen. "A new tracking-attack scenario based on the vulnerability and privacy violation of 5G AKA protocol." *IEEE Access* 10 (2022): 77679-77687.
12. Yue, Kaifeng, et al. "A survey of decentralizing applications via blockchain: The 5G and beyond perspective." *IEEE Communications Surveys & Tutorials* 23.4 (2021): 2191-2217.
13. Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Choo, K. K. R. (2019). Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. IEEE Transactions on Network Science and Engineering, 8(2), 1120-1132.
14. Haddad, Z. (2023). Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks. Journal of King Saud University-Computer and Information Sciences, 35(6), 101458.
15. Goswami, B., & Choudhury, H. (2022). A blockchain-based authentication scheme for 5g-enabled iot. Journal of Network and Systems management, 30(4), 61.

16. Feng, C., Liu, B., Guo, Z., Yu, K., Qin, Z., & Choo, K. K. R. (2021). Blockchain-based cross-domain authentication for intelligent 5G- enabled internet of drones. IEEE Internet of Things Journal, 9(8), 6224-6238.
17. Ali, G., Ahmad, N., Cao, Y., Khan, S., Cruickshank, H., Qazi, E. A., & Ali, A. (2020). xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE access, 8, 58800-58816.
18. Wijethilaka, S., Yadav, A. K., Braeken, A., & Liyanage, M. (2024). Blockchain-based secure authentication and authorization framework for robust 5g network slicing. IEEE Transactions on Network and Service Management.
19. Jangirala, S., Das, A. K., & Vasilakos, A. V. (2019). Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. IEEE Transactions on Industrial Informatics, 16(11), 7081-7093.
20. He, D., Kumar, N., Chilamkurti, N., & Lee, J. H. (2014). Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. Journal of medical systems, 38, 1-6
21. Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad hoc networks, 18, 133-146.
22. He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal, 2(1), 72-83.
23. Fan, K., Gong, Y., Liang, C., Li, H., & Yang, Y. (2016). Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G.Security and Communication Networks, 9(16), 3095-3104.
24. Safkhani, M., & Shariat, M. (2018). Implementation of secret disclosure attack against two IoT lightweight authentication protocols. The Journal of Supercomputing, 74(11), 6220-6235.
25. Sidorov, M., Ong, M. T., Sridharan, R. V., Nakamura, J., Ohmura, R., & Khor, J. H. (2019). Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access, 7, 7273-7285.
26. Gao, Z., Zhang, D., Zhang, J., Liu, Z., Liu, H., & Zhao, M. (2022). Bc-aka: Blockchain based asymmetric authentication and key agreement protocol for distributed 5g core network. China Communications, 19(6), 66-76.
27. Vivekanandan, M., VN, S., & U, S. R. (2021). BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology. Peer-to-Peer networking and applications, 14(1), 403- 419.
28. Haddad, Z., Baza, M., Mahmoud, M. M., Alasmary, W., & Alsolami, F. (2021). Secure and efficient AKA scheme and uniform handover protocol for 5G network using blockchain. IEEE Open Journal of the Communications Society, 2, 2616-2627
29. Goswami, B., & Choudhury, H. (2024). A Secure and Fast Handover Authentication Scheme for 5G-Enabled IoT Using Blockchain Technology. Wireless Personal Communications, 138(4), 2155-2181.
30. Haddad, Z. (2023). Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks. Journal of King Saud University-Computer and Information Sciences, 35(6), 101458.