[1]Dr Prasad Rayi,
2A.Venkata Raju,
3Mamatha B,
4Moilla Sai Lakshmi

Blockchain-Based Security In 5G And 6G Networks

JES Journal of Electrical Systems

Abstract*:* - An overview of Blockchain technology, as well as its applications in 5G and 6G, is provided in this research paper. The combination of four distinct technologies—blockchain, blockchain technology, 5G, and 6G—can bring forth new solutions and expansion for many businesses.

By facilitating secure identity management and creating tamper-proof communication channels, blockchain provides strong security safeguards. 5G networks may improve data privacy and reduce risks by using blockchain's decentralized design. More effective network management and enhanced performance are possible outcomes of blockchain-enabled decentralized decision-making and resource allocation.

Blockchain integration is already crucial, and it will be increasingly more so as we approach 6G. To manage the enormous connection and complicated infrastructure needs of 6G networks, blockchain offers a decentralized platform. Scalable and distributed data integrity assurance, transparent interactions between parties, and safe interoperability are all made possible by it. Improved trust, scalability, privacy, and security can be applied to both 6G and 5G networks.

Keywords: Blockchain, 5G, 6G, Bitcoin, Crypto, Ethereum, Smart Contracts, Solana, Polkadots, AI, IoT, Security

Introduction

Every single "block" that makes up a blockchain is responsible for storing some form of data, such as a record of transactions. By associating the blocks with cryptographic hashes, the data's integrity and immutability are ensured to be preserved. Once a new block is added to the chain, it becomes very difficult, if not impossible, to update or alter the data that is stored inside it.

Security, immutability, and transparency are the fundamental ideas that underpin the blockchain technology. Through its implementation, it is possible to construct a sequence of blocks, with records or transactions being listed inside each block. The transaction history is rendered unchangeable and auditable by the use of cryptographic hashes, which link these blocks.

Following the fourth generation of cellular technology, also known as LTE, comes the fifth generation, also known as 5G. Significant improvements in connection, latency, capacity, and speed are offered by its successor in comparison to its predecessor.

The next generation of wireless technology, known as 6G, is now the subject of research and development. It is believed that 6G will improve upon the innovations that were introduced by 5G and bring even more capabilities that will change the game, despite the fact that it has only just started to take form.

Literature Survey

Recent years have seen a growth in both the number of interactive devices that are connected to wireless networks and the length of time they are connected. This has resulted in the present wireless network experiencing pressure, which has therefore necessitated the implementation of innovative and creative technologies in the field of wireless communication. The traditional wireless network has a number of difficulties in terms of wireless communication. Due to the fact that the information that is sent does not achieve ideal levels of privacy in traditional wireless communication (Ling et al., 2019), network privacy is a serious problem. Additional issues include the complexity of the network, vulnerabilities, and the decentralized nature of the system. In addition to this, it is of the utmost importance to provide security and protection against the ever-increasing dangers and

[1] [1,2,3,4]International School of Technology and Sciences for Women, A.P, India.

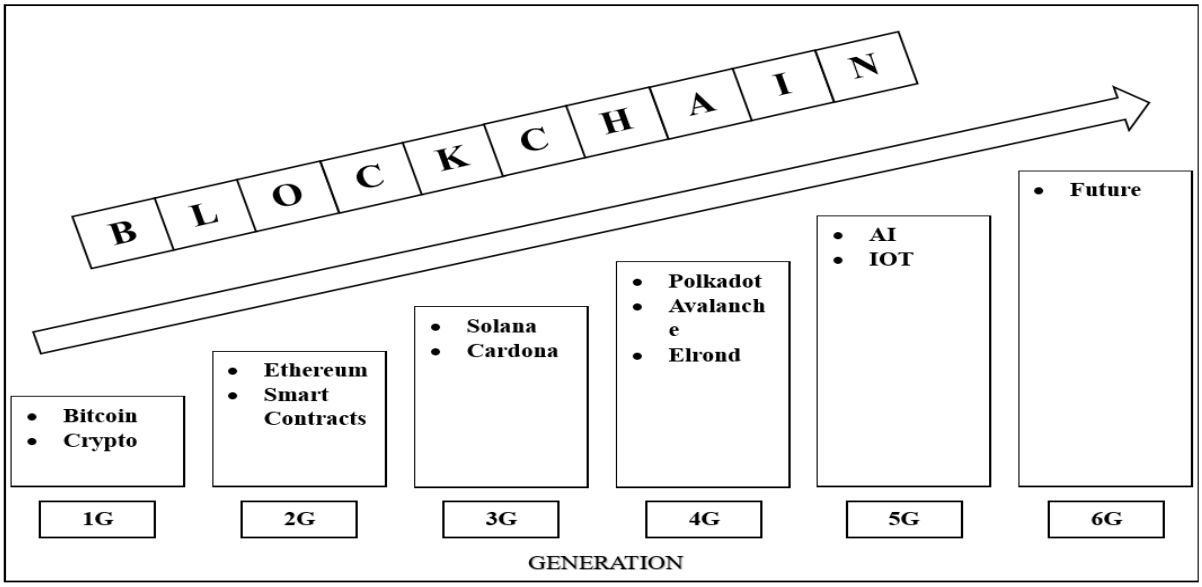
attack vulnerabilities. The use of wireless communication technologies has become more widespread in several aspects of our everyday life. In a variety of public settings, including hospitals, colleges, and airports, amongst others, they have the potential to be used to improve information management, wireless communication, and computing. The advent of wireless communication has made it possible for mobile devices, such as smartphones, to get access to the internet, calendars, emails, and contacts with an unparalleled level of ease. According to Wang et al. (2021), the Internet of Things (IoT) has seen a fast growth, which has led to an increase in the number of IoT devices that are networked among themselves via the use of wireless networks.

There is the potential for blockchain technology to be used in wireless communication in order to improve network security in confidential transactions. Because of the potential benefits that blockchain technology might provide to a variety of industries and businesses, it has recently been a major topic of research because of its potential. The technology known as blockchain offers a number of benefits, including enhanced security, better transparency, faster transaction speed, and higher efficiency. Every single block that is added to the blockchain is directly dependent on the information that is contained in the blocks that come after it. Significant data is produced as a result of the combining of the blocks, 3 In light of this, it becomes difficult to make changes to the information that is stored in blockchain. According to Ling et al. (2019), blockchain technology improves the safety of financial transactions by making it easier to facilitate the flow of information in a way that is both more secure and safeguarded.

The protection of information that is broadcast on social networking platforms, banking networks, and other networks is necessary in order to guarantee the confidentiality, integrity, and security of the data they contain. The conventional method of wireless communication, on the other hand, is not capable of delivering the satisfactory level of safety in the modern day. Because of the nature and range of modern threats, the defensive capabilities of traditional wireless networks are no longer enough to deal with current threats. Wireless communication that is enabled by blockchain technology may be able to alleviate some of the difficulties and challenges that are associated with traditional wireless communication.

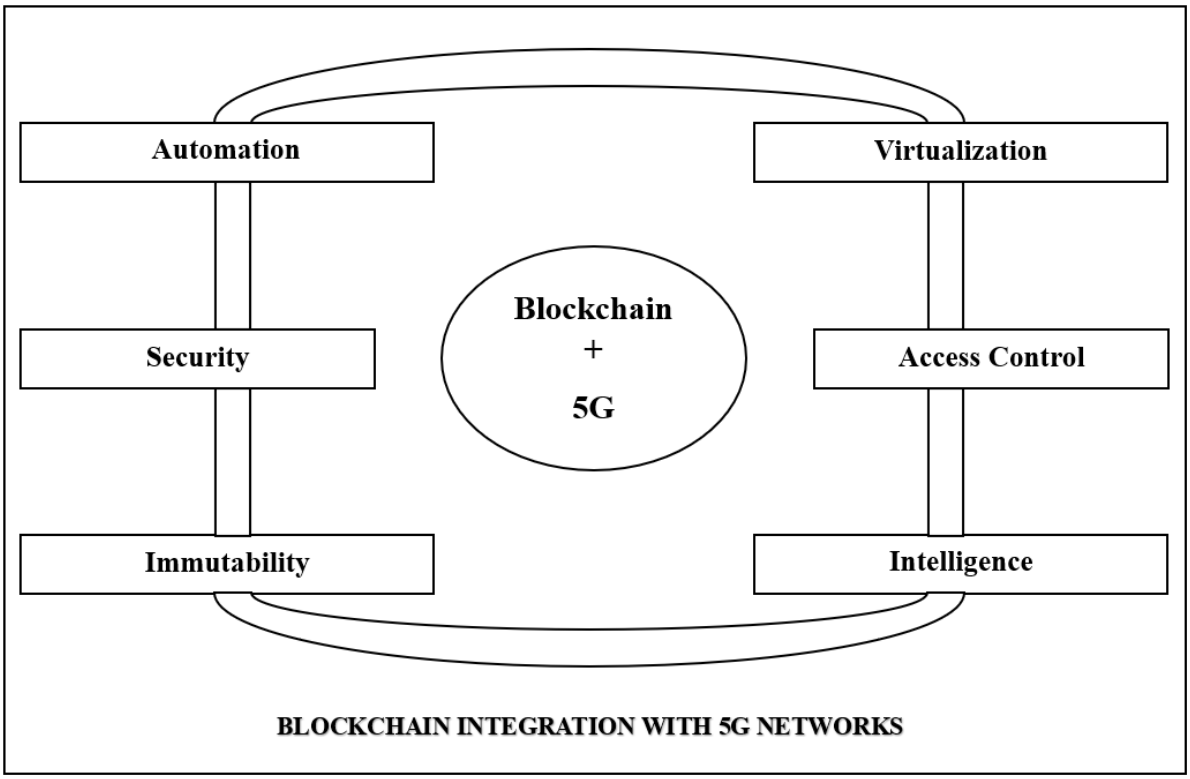
Decentralization is the fundamental advantage that distributed ledger technology (blockchain) brings to wireless communication. It makes it possible to conduct operations that are both secure and robust over the defined network that is involved in wireless communication. Blockchain technology is becoming more attractive as a potential solution for wireless networks and communication in the future. This is due to the many benefits that blockchain technology provides to wireless communication. Increasing the level of network security is the primary benefit that blockchain technology will provide to wireless communication. This is the first and most basic advantage. According to Chithaluru et al. (2021), this will guarantee that the information that is sent over the wireless network is uncompromised and protected from unauthorized access and alterations.

The increase of resource utilization and the potential for effective network monitoring are two additional advantages that may be gained from wireless communication that is enabled by blockchain technology. The combination of blockchain technology with cognitive wireless communication allows for the most efficient use of the wireless communication network architecture that is already into existence. Having this understanding of four. The breakthroughs in blockchain technology were accomplished by the substantial research that was conducted in the subject. The identification of possible dangers in wireless communication may be accomplished by the monitoring of the efficiency of wireless communication networks using this method. According to Ling et al.'s 2019 research, the study places an emphasis on the historical elements of blockchain technology and its use in wireless communication. In addition, both the advancements made and the limitations of blockchain-enabled wireless communication communication are discussed.



Blockchain Technology for 5G

There is a significant impact that 5G networks will have on all digital technologies, including Blockchain, Bitcoin, and decentralized finance (DeFi), since they will make it possible for devices to interact with one another. These growing markets have an equal impact on the characteristics of future networks since they shape the requirements of the market and the expectations of consumers. 5G has the potential to revolutionize business and communication by providing an unparalleled increase in the speed and power of internet connections. As a result, the junction of 5G technology with Blockchain provides a transformational breakthrough for the whole world. The wireless connection was improved, which made it possible to transmit considerable amounts of data with low latency via a variety of cloud-native apps, updated hardware, Internet of Things devices, and mission-critical equipment.



BLOCKCHAIN INTEGRATION WITH 5G NETWORKS

6G in Blockchain Technology:

The sixth generation of wireless technology is now in the early stages of development and has the potential to dramatically improve Blockchain technology. This technology is currently in its developing phase. The limits of 5G technology will be addressed by the 6G network, which will result in an improvement in the latency difficulties that were present in the 5G system. This article provides an overview of the potential ways in which 6G might potentially impact Blockchain technology:

In comparison to the three generations that came before it, it is projected that the sixth generation would provide higher data transfer speeds and increased network capacity. It is possible that this will make it possible for Blockchain networks to handle a much larger quantity of transactions and data, which would ultimately improve the scalability and performance of decentralized applications (dApps) that are created on cryptocurrency platforms.

General Challenges In 6G

Behnaam et al. elucidate some noticeable obstacles in 6G in [1]. Furthermore, Biral et al. [16] elucidate the obstacles associated with M2M communications.

A. Extensive interconnectedness in forthcoming systems

1) Scalability: Proponents of industrial IoT anticipate that billions of devices will be interconnected and function within future industrial ecosystems, facilitated by the advent of ideas like massive Machine Type Communication (mMTC). Consequently, it would be difficult to customize the architecture of 6G networks to accommodate such extraordinary traffic needs.

2) Real-time communication with low latency is an essential prerequisite for future computer ecosystems. Device-to-device and machine-to-machine communication need strong precision with minimal latency for accurate functioning. Use cases such as autonomous driving and augmented reality-assisted healthcare systems may need a consistently low latency in communication capabilities amid increased transaction volume.

3) Enhanced throughput: Mission-critical systems that use future 5G and subsequent communication ecosystems need simultaneous connection for billions of devices. The network infrastructure, including base stations, must manage the substantial amount of transactions in real-time.

4) Synchronization: Synchronization is a crucial need in time-sensitive industrial applications. Power generating and distribution systems, as well as vehicle networks, need security against errors in communication and synchronization.

B. Security prerequisites in forthcoming computing ecosystems

1) Confidentiality: Future computer infrastructures, such as the Internet of Things, present significant vulnerabilities due to wireless communication. Encryption methods, such as symmetric key algorithms, must be lightweight for low-power IoT devices. The lightweight encryption methods provide privacy threats to data owing to computational limitations.

2) Integrity: The substantial quantity of data generated by future systems necessitates that authorized users access and modify the data while it is in transit. The interception and alteration of data during transmission will disrupt the system's functioning from its anticipated performance.

3) Availability: Service availability is a fundamental necessity in future ecosystems. The complexity of 5G ecosystems, characterized by a substantial number of networked devices, increases the danger of DDoS assaults. The present network security tools' specialization cannot be directly used to identify attacks and attempts in 5G and beyond networks.

4) Authentication and access regulation: The data produced by communicating nodes and data in transit necessitates the implementation of access control systems to delineate the scope of data access for different users. The authentication systems that use a centralized base station generate a bottleneck in the extensive nodes within the ecosystem. The intricacy of network service use imposes considerable expense on the establishment of various access control systems for the tenants of the 5G network.

5) Audit: An audit is necessary to assess the adherence of tenants' conduct inside the network ecosystem. To meet heightened security requirements, a deep packet-level audit may be necessary to detect and report the behaviors of tenants inside the 5G ecosystem. The audit of a substantial number of renters will provide a considerable difficulty in terms of ensuring security.

C. Increased data usage in advanced solutions

The elevated data rate is a vital expectation inside the 5G network ecosystems. Applications such as augmented reality (AR), virtual reality (VR), high definition (HD), and hyper 3D video need elevated data rates and increased data usage.

D. Limitations on device resources

Future computer ecosystems are expected to have computational and storage limitations. The limits constrain the functionalities of cryptographic algorithms and ultimately diverge from the conventional procedures. The conventional implementation of security is more challenging due to the limitations of device resources.

The Contributions Of Blockchain To 6G

Blockchain is a leading technology poised to realize the promise of 6G systems. This section outlines the potential and strengths of blockchain-based smart contracts in addressing the previously listed difficulties.

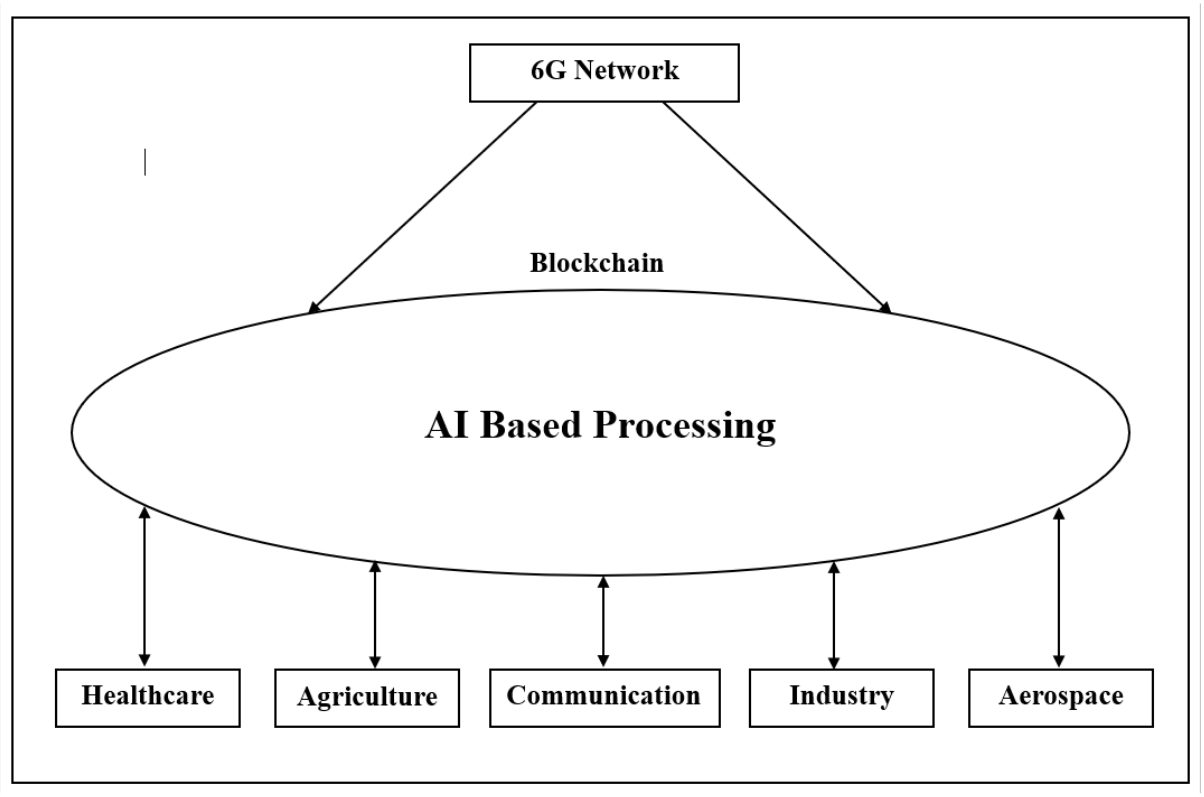
A. Strategic resource management

Network resource management and sharing is crucial in 6G. Particularly, because to the exponential growth of tenant futures, resource management activities such as spectrum sharing, orchestration, and decentralized computing must be compatible with substantial infrastructure volumes.

Zhang et al. [17] introduced a framework for edge intelligence and Industrial Internet of Things (IIoT) that features safe and adaptable service management in the context of beyond 5G technology. Maksymyuk et al. [18] presented an intelligent network design that use blockchain technology to manage the connection between operators and users via the use of smart contracts. The authors devised an unlicensed spectrum sharing method using game theory. Dai et al. [19] demonstrated the use of blockchain and deep reinforcement learning for the effective administration of resources, including spectrum sharing and energy management.

Mafakheri1 et al. [20] used blockchain for resource sharing to leverage smart contracts for self-organizing network capabilities.

Application And Service Prospects Through Blockchains In 6G Systems



Section I delineates that the 6G vision encompasses several applications that may be facilitated or enhanced via the use of blockchains. The foundation of blockchains for enhancing applications in 6G arises from the capabilities outlined in Section III, which are facilitated by its fundamental characteristics: decentralization, transparency, immutability, availability, and security.

A. Industrial Applications for Post-Industry 4.0

In 6G, industrial applications will be significant catalysts for using the anticipated 6G capabilities. The principal characteristics of blockchains and the issues outlined in Section II are particularly relevant to industrial settings. Holographic communications for industrial applications, such as remote maintenance or extensive connection of manufacturing equipment, need decentralized structures that are simultaneously reliable [11]. Blockchains may provide these functionalities when incorporated into these applications or use cases. Nonetheless, significant research hurdles persist concerning blockchain-based solutions, including latency and scalability. They provide significant hurdles owing to rigorous performance standards in industrial applications.

These are also applicable to industrial networks and the Internet of Things (IoT) [10].

B. Integrated Environmental Surveillance and Safeguarding

Blockchains provide decentralized cooperative environmental sensing applications that can be implemented on a global scale using 6G technology. These skills may facilitate applications in smart cities, transportation, and environmental conservation for a sustainable economy. Blockchains enable safe data exchange across entities, including IoT devices and businesses.

Extensive reliable sensing and data sharing solutions facilitated by blockchains are essential for environmental monitoring. Additionally, federated and shared learning facilitated by blockchains enhances data analytics and inference procedures for environmental protection in a decentralized fashion.

C. Intelligent Healthcare

Smart healthcare in 6G must advance to address existing challenges in 5G networks. The profound and pervasive integration of blockchains in future networks has the potential to enhance existing healthcare systems and optimize performance via improved decentralization, security, and privacy. The imminent technological difficulty is the question of privacy. Furthermore, the integrity of healthcare data is achievable owing to the immutability feature offered by blockchains. Specifically, user-controlled privacy and safe data storage may be facilitated by blockchains without the need for a centralized trusted third party. In Europe, GDPR rules are significant catalysts that will become more rigorous in the next years. Enhanced decentralization would provide increased security, particularly regarding availability in this vital sector.

D. Decentralized and Reliable 6G Communications Infrastructure and Solutions

A multitude of application potential exists for using blockchains inside 6G infrastructure to enhance performance or facilitate new services and use cases. Specifically, decentralized network management frameworks: The decentralized blockchain-based network administration will enhance resource allocation and improve system efficiency [18].

Blockchain radio access network

One notable breakthrough is the Blockchain Radio Access Network (B-RAN). The use of blockchain inside the network may provide economic incentives and mitigate the overhead costs often associated with centralized systems. The members in the B-RAN network may operate as both access consumers and access providers, while also facilitating the organization of a robust network. This may also lead to the elimination of intermediary third parties and associated security issues.

The incorporation of blockchain into the network may facilitate the sharing of roaming data across diverse parties and networks engaged in wireless communication. The identification of visiting subscribers may be conducted efficiently and expeditiously. The virtual public network of B-RAN offers the necessary security and self-organization, facilitating an open market. Moreover, the collaboration and competition among network members might lead to a reduction in the costs of data access services without necessitating further deployment of radio infrastructure.

5G/6G network advancement

Fifth- and sixth-generation networks are the subject of a major innovation. The 5G network has the potential to revolutionize modern networking and communication. Nguyen (2020) identifies three main features of the 5G

network: enhanced mobile broadband support, ultra-reliable low latency communication services, and massive machine-type communication. Businesses and other sectors may find 5G to be an exciting new frontier for innovation. The quick Nguyen et al. (2020) notes that security risks, data immutability, and privacy difficulties have been brought about by the expansion of the 5G network. From the 2G to the 4G age of networks, several security methods and technologies have been helpful. Security measures included automated repeat requests, forward error correction channel codes, and hybrid methods to automated repeat requests. Nevertheless, innovative and advanced security solutions are required since existing methods cannot guarantee the 5G network's required level of protection (Nguyen et al., 2020).

These days, with 5G and 6G networks everywhere, decentralization, transparency, and immutability are the three most important security features of a security solution. As far as cutting-edge technological developments go, blockchain seems to provide the best chance of meeting the 5G network's security standards. One key component of blockchain technology is its decentralised, peer-to-peer network architecture. New mobile services will improve wireless connectivity throughout the globe as a result of blockchain technology's integration with the 5G network. By 2030, the 5G network hopes to have connected more than 500 million mobile devices, thanks to its ability to handle diverse networks and gadgets. Wireless communication is using blockchain technology to meet the needs of a decentralized security mechanism that is transparent, secure, and imperative in this environment.

Conclusion

The significance of this study lies in the fact that it investigates the possibilities that Blockchain technology presents for 5G and 6G networks. There is a significant improvement in technological advancement brought about by blockchain technology. The combination of this technology with 5G and 6G networks might potentially give a powerful solution. Blockchain technology offers a safe framework for the huge amounts of data that are created by these networks. In order to maximize the synergy that exists between Blockchain technology and the rapidly expanding fields of 5G and 6G, future research should concentrate on the development of scalable Blockchain solutions, the improvement of consensus protocols, and the establishment of interoperability standards of Blockchain.

References

1. Chen, Y., Meng, L., Zhou, H., & Xue, G. (2021). A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. *Wireless Communications and Mobile Computing*, *2021*. https://www.hindawi.com/journals/wcmc/si/481323/
2. A. W. R. Sattiraju and H. D. Schotten, “Performance analysis of deep learning based on recurrent neural networks for channel coding,” in Proceedings of 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2018.
3. J. K. R. Sattiraju and H. D. Schotten, “Machine learning based obstacle detection for automatic train pairing,” in IEEE 13th International Workshop on Factory Communication Systems (WFCS). IEEE, 2017, pp. 1–4.
4. J. L. a. H. S. A. Weinand, M. Karrenbauer, “Physical layer authentication for mission critical machine type communication using gaussian mixture model based clustering,” in IEEE 85th Vehicular Technology Conference (VTC Spring). IEEE, 2017, pp. 1–5.
5. Y. J. S. T. A.S. Khan, K. Balan and J. Abdullah, “Secure trust-based blockchain architecture to prevent attacks in vanet,” Sensors, vol. 19, no. 4954, 2019.
6. Chithaluru, P., Al-Turjman, F., Stephan, T., Kumar, M., & Mostarda, L. (2021). Energy-efficient blockchain implementation for Cognitive Wireless Communication Networks (CWCNs). *Energy Reports*.
7. Ling, X., Wang, J., Bouchoucha, T., Levy, B. C., & Ding, Z. (2019). Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. *IEEE Access*, *7*, 9714-9723. https://ieeexplore.ieee.org/document/8598796?denied=
8. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, *166*, 102693. https://arxiv.org/pdf/1912.05062.pdf

9. P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks," IEEE Communications Magazine, vol. 55, no. 9, pp. 78–85, 2017.
10. V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos, "Blockchain enhanced secret small cells for the 5g environment," in 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019, pp. 1–6.
11. V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5g vehicular networks: Blockchains and content-centric networking," IEEE Vehicular Technology Magazine, vol. 13, no. 2, pp. 121–127, 2018.
12. B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative ddos mitigation with smart contracts," in IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, Cham, 2017, pp. 16–29. O. A. https://ioe.org/, "Internet of everything. (2019). internet of everything (ioe)."
13. M. K. S. R. P. B. B. T. Rana, A. Shankar, "An intelligent approach for uav and drone privacy security using blockchain methodology," in 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2019.
14. Wang, J., Ling, X., Le, Y., Huang, Y., & You, X. (2021). Blockchain enabled wireless communications: a new paradigm towards 6G. *National Science Review*. https://academic.oup.com/nsr/article/8/9/nwab069/6253219
15. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352-375.
16. H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchainbased trusted authentication in cloud radio over fiber network for 5g," in 2017 16th International Conference on Optical Communications and Networks (ICOCN). IEEE, 2017, pp. 1–3.