Demystifying Blockchain in 5G and Beyond Technologies

Keshav Kaushik

School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
E-mail: officialkeshavkaushik@gmail.com

Received 30 November 2021; Accepted 06 January 2022;
Publication 05 April 2022

Abstract

5G and beyond systems are being built to be prospective by responding to the different needs of a diverse range of applications, which represents a significant departure from this approach. Owing to its openness, encryption techniques, verifiability, integrity, and decentralized design, blockchain has evolved as an important approach. 5G and Blockchain might transform emerging technology. 5G offers consumers high speeds and QoS, while blockchain ensures peer-to-peer trust and privacy. Blockchain is a revolutionary technology having wide range of applications in various domains like Artificial Intelligence, Internet of Things (IoT), Cybersecurity, Wireless networks, 5G and beyond networks, etc. In this paper, the role of Blockchain technology in 5G and beyond networks is discussed. This paper also highlights the various challenges that acts as a hindrance while implementing the Blockchain in 5G and beyond networks. Moreover, the paper also discusses the future aspect of Blockchain in 5G networks.

Keywords: Blockchain, 5G network, networking, IoT, artificial intelligence, smart contracts.

Journal of Mobile Multimedia, Vol. 18_5, 1379–1398.
doi: 10.13052/jmm1550-4646.18513

1 Introduction

Wireless networks of the fifth generation (5G) are being installed all over the globe. By linking heterogeneous devices and machines, 5G advancements aim to serve a wide range of application areas with substantial gains in respect of high quality of service, greater network capacity, and higher system performance. The fourth industrial revolution, often known as Industry 4.0, will be ushered in by 5G technology. Hardware and software advancements are allowing aspects for the Industry 4.0 revolution to take place. However, blockchain is one of the essential technologies in the mobile communications and connectivity field that deserves greater research and development. Blockchain networks allows secure peer-to-peer connection with ground base stations or indeed relay network performance measurements to AI techniques in a self-organizing network configuration to help monitor and optimize radio access structures. Any network adjustments may be done using blockchain-enabled smart contracts or a rules processors in Self-Organizing Networks that was set up when the network was created or changed. The development of a trustworthy billing system will be required for future business strategies based on sharing 5G network resources. In conjunction with existing AI-enabled SON technologies, blockchain-based network slice exchanges and billing systems may assist overcome these obstacles and accomplish the closed-loop automation ideal.

Scientists and groups have identified a variety of security problems with 5G systems, namely decentralization, accountability, data interoperability hazards, and network security concerns. Additionally, traditional solutions may not be enough to cope with 5G's security needs. Because 5G is often implemented in heterogeneous networks with a large number of ubiquitous devices, reliable and autonomous technologies are essential. User equipment might also conduct smooth handoffs between 5G networks and WiFi to obtain the optimal data connection. In purview of managing such a transaction, a bunch of service providers may form a consortium blockchain framework to create an interoperable method of verification and administration of such handoff communication. For many AI algorithms, blockchain may function as a safe storage of data/transactions. The data from which AI learns is only as good as the data from which it learns. Consensus algorithms, the immutability of blockchain transactions, and cryptography-based encryption would all contribute to data integrity and security. The application of blockchain in the healthcare business for securely storing and exchanging patient data is extensively established.

Smart contracts [1] would allow business-oriented applications like as invoicing, by providing an immutable record of a user's interactions with the network (s). It can also manage automatic network resource sharing settlements across multiple telcom networks. Highly distributed architecture and peer-to-peer network properties, blockchain lends itself nicely to decentralized designs. This may be the single most compelling argument for many individuals to assume that blockchain represents a forerunner of a new, more user-centric internet. Users will no longer have to remember several identities, and they will have more control over who they share their data with. People will have a single identify that will allow them to access networks from different operators without being tethered to a single one. Developing a decentralized internet does not seem too far away as carriers move away from fundamental business models and toward MEC-centric ones.

For 5G edge computing use litigation concerning automotive networks, public blockchain models may be employed to facilitate the exchange of vehicular and traffic information. This may be used as a rapid and permanent record for settling claims for vehicle insurance. The requirement for a large network of IoT devices to interact with each other with millisecond responsiveness in situations such as smart buildings and UAV fleets may be met by blockchain-enabled administration and identification of such gadgets. Although the innovation and its prospective applications are exciting, blockchain still has to address the problem of scalability before it can be used effectively in telecom networks. The durability of smart contracts would have to be evaluated on a scale that platforms like Ethereum have never seen before. Interoperability between various blockchain networks or technologies must also be built. The use case of blockchain for automotive insurance settlement is an instance of collaboration between a diverse collection of stakeholders, including as vehicle manufacturers, insurance firms, operators, networking technology suppliers, and regulators. This also illustrates why blockchain applications have not sparked the same level of interest in this area as they have in others, such as financial services. To accelerate innovation on techniques ideally equipped to telecommunication networks, the telecom and networking industry must collaborate with current blockchain platforms like Ethereum.

The 5G services are used by IoT technology, which takes the advantages of ad-hoc networks for communication. In today's ad hoc networks, the rising need for routing in the sphere of telecommunication is the most essential topic. One of the developing fields that arose from Mobile Ad Hoc Networks is the Flying Ad Hoc Network (FANET). A routing protocol has a significant

issue in determining the most optimum route in any network. Using modified AntHocNet, this study [2] provides a unique routing mechanism for FANET. In comparison to previous heritage best route selection strategies, the ant colony optimization methodology, or metaheuristics in general, has proven improved availability and security. The subject of energy saving in flying-IoT is addressed in this research [3]. This study uses DSDV routing to provide a revolutionary solution for the internet of flying vehicles. The bellman-ford algorithm, which includes routing updates, information dissemination, and the stale approach, is described in ISH-DSDV. In contrast to other modern routing protocols, DSDV achieves the best outcomes. In the case of flying networks, the migratory mobility model is used to test the performance of the proposed scheme.

2 Related Work

5G and Blockchain might revolutionize future technology. 5G offers consumers excellent rates and service quality, whereas blockchain ensures a high degree of peer trust and security. 5G applications have a wide range of requirements in terms of performance, throughput, latency, and other aspects. For dependable and fast connection, 5G is often used in augmented reality, self-driving cars, and other IoT applications. A more sophisticated and effective strategy would be necessary to perform effortlessly and safely in such settings. 5G edge networks can safeguard communications between peripheral entry points, allowing for the creation of a wide range of flexible and configurable applications. Edge networks have the benefit of being the first to integrate other well-known technologies like blockchain and autonomous learning into wireless networks, resulting in enhanced services. The authors [4] offered a smart system that integrates blockchain technology, 5G, and Federated Learning to establish a transaction framework that is both efficient and safe in this article. Federated Learning allows user equipment to train an artificial intelligence prototype without revealing the user equipment's sensitive data to the general public or model suppliers.

Innovative delivery models will be enabled by 5G cellular technology [5], which may worsen security issues. Unlike historical mobile networks, 5G wireless networks will be decentralized and pervasive, with a focus on privacy and security from the standpoint of services. Because there are so many different kinds of devices and so many of them are linked, information security in 5G is more difficult. A significant challenge is how to offer an open information architecture for flexible interference management, data sharing,

and multiuser connectivity, for instance, in order to accomplish ubiquitous 5G service supply while maintaining high data preservation and transparency. To put it another way, prior generations' security designs lack the complexity required to protect 5G networks.

IoT devices are becoming more important in the current day as traditional gadgets grow more autonomous and intelligent. On the one side, high-speed data transmission is a key problem in which a 5G-enabled environment is critical. These IoT devices, on the other contrary, transmit data via protocols based on a centralized design, which may result in data security vulnerabilities. Combining artificial intelligence with 5G wireless networks addresses a number of difficulties, including autonomous robotics, self-driving cars, virtual reality, and security concerns. The system's major objective [6] is to build confidence among network users without relying on third-party authority. Blockchain has emerged as a major technology for maintaining the network's event logs, since it is built on a distributed ledger. For IoT devices, blockchain enables a secure, decentralized, and trustless ecosystem. Nevertheless, connecting IoT with blockchain presents a number of issues, one of which is poor throughput. As a result, blockchains will not be able to provide capabilities for a 5G-enabled IoT network. The blockchain's network is the bottleneck in terms of throughput. The delayed transmission of operations and blocks in the P2P network prevents miners and verifiers from mining and verifying new blocks as quickly as they would like. As a result, the main difficulty with IoT-based blockchains is network scalability. Blockchain has various other applications as well and it can also be aligned with machine learning, pandemic prediction [7], IoT, and cybersecurity. The relevance of blockchain for improving decentralization, confidentiality, and consensus-aware medicinal delivery process by drones is discussed in this study. The authors [8] have gone through the history of blockchain, the 5G-IoT ecosystem, and unmanned aircraft.

As it becomes more ubiquitous, blockchain is causing havoc in a variety of industries. The immutability, security, cost cutting, transparency, and quick processing qualities of Blockchain are attracting interest from a variety of application sectors. Several industries have been able to improve their present systems or implement a system architecture change thanks to blockchain technology. Blockchain, for example, has allowed IoT systems to increase their service quality while still meeting their security needs. Several studies are using to provide safe vehicle identification and transference, message authentication, and an indisputable automotive reputation record; blockchain will be used to handle trust in 5G-enabled UAV. Vehicular network systems

involve management for data storage, secure communications operations, and non-interference connections. Blockchain is a good candidate solution for 5G vehicle network systems because of its immutability, tamper-proof nature, and built-in security. A systematic literature review of Blockchain's applicability to 5G vehicle networks, architecture, and technological elements is presented in this study [9]. The authors also explore and emphasize some of the concerns and challenges that come with using Blockchain technology in 5G vehicle networks.

Software-Defined Radio (SDR) allows for path selection for end-to-end application data transmission, enabling unprecedented levels of granular control over what data can and cannot be exchanged. In this study [10], a supportive big data-based "cognitive dynamic origin routing protocol" for cognitive-based IoT networks is presented to simultaneously determine the channel path from source to destination at the network layer. The suggested protocol cognitively DSR with simultaneous channel route entry requirements outperforms the experimental findings. The Internet of flying systems has made great development in recent decades. Several airborne vehicles connect with each other to build ad hoc networks in the air. Flying objects' uneven energy consumption will result in early failed objective and a quick drop in network longevity. This paper [11] demonstrates how to leverage each Unmanned Aerial Vehicle (UAV's) remaining level of energy to assure a high degree of safety while utilizing AntHocNet, an ant-based routing approach. UAVs have lately received considerable attention owing to their efficient constructions, low cost, quick accessibility, and potential to build an ad hoc wireless mobile hotspots. IoT-enabled UAV is a new study [12] subject that leverages location tracking as airborne technology advances. The authors provide an unique approach for detecting interior and open-air three-dimensional (3D) regions of nodes by assessing signal intensity in this paper. A route loss theory and a decision tree deep learning classifier are used in the mathematical formulation.

3 Exposing Blockchain and 5G Technology

Cellular regulations have changed through time, with each generation introducing new services and capabilities in response to market demands. This development was primarily focused on boosting performance, range, and bandwidth. With various technological breakthroughs, the demand has gone without the need for maximum bandwidth to include massive equipment connection and regions that allow high reliability and low bandwidth

transmission. Numerous technological advancements are being implemented into WiFi technology to answer the inadequacies of earlier technologies and to address the demands of various users. Software-Defined Networking (SDN) [13], Network Function Virtualization, cloud computing, and multi-access edge computing are some of the technologies used at various levels in the network. Considering 5G networks must be adaptable and able to grow in the future, such a diverse set of technologies is required. Numerous successful 5G network installations have taken place across practically all continents to test the network's abilities. Nevertheless, combining so many platforms to serve a variety of services poses a number of security, network resilience, and confidentiality, resilience, and data integrity concerns. Several networks now use centralized design, which will not scale effectively as the number of devices and data grows. The 5G ecosystem has centralized design also poses a security risk. The appropriate authentication centre identifies, authenticates, and connects all endpoints. Even though devices are close together, interaction between them must flow via the network. Such a model is vulnerable to congestion, outages, and concerted assaults that might disrupt the whole network's functioning. One answer to this problem is to utilize a decentralized and distributed structure. Future networks, unlike conventional networks, are predicted to be dispersed and decentralized. From the physical layer to the application layer, a dispersed 5G network architecture may provide enormous performance advantages. 5G devices will also function in a robust and tough environment, with multiple devices interacting and cooperating to increase efficiency. Figure 1 shows the applications of 5G technology that is classified into three categories: based on low latency and high reliability, based on IoT devices, based on throughput.

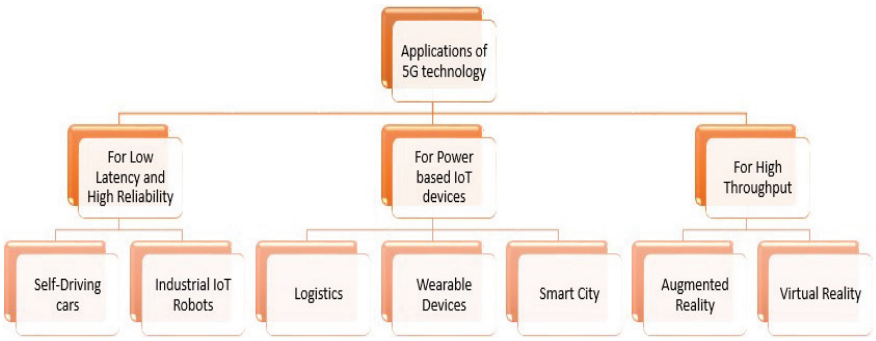

Figure 1 Applications of 5G technology.

3.1 Comparative Analysis of Blockchain for 5G Networks Related Papers

This section highlights the comparative analysis of latest papers in the area of Blockchain and 5G. Table 1 shows the major findings of the papers based on some common parameters that are there in the latest papers related to Blockchain and 5G. Based on six important parameters – Blockchain, 5G, AI, IoT, Smart contract, and security, the Table 1 is created to highlight the major findings in the latest related research.

3.2 Blockchain Challenges in 5G and Beyond Networks

Unlike traditional centralized privacy and security solutions, blockchain uses decentralised consensus protocols to validate and verify numerous transactions that are designed to become an essential component of the blockchain platform. In this article [20], the authors reviewed the available literature and then present the fundamental ideas of blockchain and machine learning. Then, in an IoT setting, the authors offered a thorough taxonomy for integrating blockchain and machine intelligence. The authors [21] highlighted 5G communications infrastructure and mobile cloud technologies as potential technologies that may benefit drone-enabled settings while also addressing some of the concerns. The authors also discuss 5G and MEC methods, outlining the current state of the art and attempting to address each of the latter's problems. The authors presented a novel 5G roaming network topology based on a permissioned public blockchain with smart contracts in this paper [22]. During the implementation of 5G networks using the Blockchain, there are various challenges that comes in the path. This section discusses the blockchain challenges in 5G technology.

- Privacy of Data: Companies, organizations, and people are all concerned about data privacy. It is especially important for 5G operators who store sensitive consumer information like as credit card numbers, addresses, subscription and use data, and payment histories. With the implementation of the EU GDPR legislation [23], privacy rules have grown more severe in terms of preserving users' records and information, as well as offering consumers access and ownership over their data. Because blockchain data is irreversible, data kept or published on a blockchain cannot be removed or forgotten. Once it comes to blockchain privacy, however, no personal data should be retained on the blockchain; instead, only references to such information should be maintained.

Table 1 Comparative study of blockchain and 5G related papers

Author	Year	A	B	C	D	E	F	Major Findings
Mistry et al. [14]	2020	✓	✓	✓	✗	✗	✗	This article provides an in-depth analysis of state-of-the-art ideas for blockchain-based industrial automation leveraging 5G-enabled IoT as a basis for applications such as smart cities, home automation, Healthcare 4.0, Smart Agriculture, Autonomous automobiles, and Supply - chain management. By enabling fine-grained decentralized access control, blockchain may change most present and future industrial uses in several areas, according to existing suggestions.
Zhang et al. [15]	2019	✓	✓	✓	✓	✗	✗	In this paper, we provide a customizable and resilient edge service management architecture based on edge intelligence and blockchain technology. Then, we construct a credit-differentiated edge transaction approval framework based on a cross-domain cooperation influenced edge resource scheduling approach. The suggested systems enhance edge service price and capacity significantly, according to numerical data.
Praveen et al. [16]	2020	✓	✓	✓	✗	✓	✓	The authors have listed the precise areas where blockchain might be used to improve the privacy and security of 5G services for consumers in this paper. The present obstacles in 5G rollout and upliftment, as well as associated blockchain-based solutions, are explored. Along with the 5G blockchain application, a methodology for Multi-Operator Network Slicing in 5G is described.

(*Continued*)

Table 1 Continued

Author	Year	A	B	C	D	E	F	Major Findings
Tahir et al. [13]	2020	✓	✓	✓	✓	✓	✓	The authors of this study looked at the current level of Blockchain implementation in 5G technology and considered how it may assist allow multiple services at front, edge, and center by enabling 5G and beyond technical solutions. The authors have proposed a framework for Blockchain applications in 5G networks based on the study and explain numerous difficulties that may be handled via Blockchain integration. A number of field experiments and proofs of concept that use Blockchain to solve the current 5G deployment's problems is also discussed. Furthermore, the authors have highlighted some of the issues that need to be overcome in order to fully realize the promise of Blockchain in networks beyond 5G.
Yue et al. [17]	2021	✓	✓	✗	✗	✓	✓	This article presents a clear and comprehensive overview of current research on decentralizing apps using blockchain in the context of 5G and beyond. It covers five components of reason for decentralizing apps using blockchain and present four burning 5G and beyond issues. Nine essential blockchain modules are highlighted and how these modules might affect decentralization is discussed in detail. The authors also highlighted how decentralization and several desirable blockchain qualities are related.

(*Continued*)

Table 1 Continued

Author	Year	A	B	C	D	E	F	Major Findings
Chaer et al. [18]	2019	✓	✓	✗	✗	✓	✗	In this paper, the authors have examined and emphasized the usage of blockchain in 5G networks. The paper provides a summary of blockchain capabilities, including, decentralized storage, smart contracts, and trustworthy oracles. The possibilities for using blockchain technologies to provide 5G services are discussed in this paper.
Gao et al. [19]	2021	✓	✓	✗	✗	✗	✗	The results in this article are a great starting point for developing a government policy to help with the application and implementation of blockchain-based 5G communication networks for smart cities.

A: Blockchain B: 5G C: IoT D: Artificial Intelligence E: Smart contracts F: Security.

- Reputation and Nomenclature: To manage numerous of the participants and organizations in the blockchain and 5G ecosystems, a decentralized registration procedure with trustworthiness, sustainability, efficiency, and effectiveness is necessary. A system like this might be built using smart contracts and decentralized storage. To connect blockchain IDs, public keys, and identities to real identities for 5G network participants, a decentralized identity registration process is also required. These players must be connected to a decentralized reputation system, which may be developed using smart contracts and will provide aggregated reputation ratings to all stakeholders and oracles based on their previous actions and services. Service users may submit reputation scores to a reputation smart contract, which will aggregate the scores to allow, authorize, and authenticate 5G end users.
- Compatibility: Compatibility across multiple blockchain systems is still a difficult problem to solve. There are several different kinds of blockchain platforms toward which 5G stakeholders may connect currently. It is a significant obstacle that researchers must face and conquer.

Figure 2 Blockchain challenges 5G technology.

- Expandability: In 5G technology [24], payloads and transported data have a goal end-to-end delay of less than 1 millisecond. That strict need necessitates very high - throughput screening configuration and setup operations. To improve the performance of today's public blockchains, researchers are looking at new blockchain topologies, sharing methods, block size increases, and consensus mechanisms.
- Cloud storage cost overhead: Developing and sustaining a private or collaborative blockchain network requires factoring in the price of cloud computing to support the blockchain nodes, which may be expensive if not regulated. Every transaction on Ethereum (an example of public blockchain); must be compensated in gas units. A single unit of gas symbolizes the compute and energy used by mining nodes to leverage the smart contract. The transaction costs are based on the function code that smart contracts will perform. Substantial fees may be charged if smart contract functionalities and its corresponding scripts need a lot of processing or aren't built efficiently.

- Smart Contracts: Mostly on open Ethereum blockchain, there are around 15 million smart contracts in use. The main problem is the conversion of normal contracts into the smart ones for the 5G environment. Especially given the high granularity of IoT devices expected in a typical 5G network. Another point to consider is the legality of the smart contracts in use. In most cases, smart contracts' legal standing is determined by whether or not they are part of a binding contract with a certain jurisdiction. Another significant concern is the safety of smart contract programming. Smart contract code may potentially have defects or vulnerabilities that hackers might exploit. Smart contract code must be safe and devoid of vulnerabilities.
- Compliance: At the regional and international levels, smart contracts and blockchain are currently largely unregulated and does not have any standard to follow. Local and international standards, legislation, and administration are required for widespread use of blockchain in the telecom industries and 5G. Normalization may take place inside telecom industry groups to address telecom-service-specific blockchain solutions, or it can happen independently of other factors.

3.3 Blockchain and 5G: Research Opportunities

The 5G and beyond ecosphere will be marked by a growing number of stakeholders and interconnected products and applications, not all of which will be managed by the same organization. Developing confidence in such a broad and diversified environment is critical to the technology's worldwide acceptance. In this regard, it's critical to address the privacy and security threats posed by this diverse ecosystem. The authors of this article [25] discuss the trust concept and its aspects in 5G and even beyond networks, as well as upcoming trust facilitators and research paths. In addition, the authors developed a blockchain-based data security system to promote data trust in machine learning pipelines. Drones combined with Blockchain and AI technology have the potential to overcome telecommunication security issues. The existing research [26] focuses on 5G-based drone connectivity, and quantum drones applications require a more detailed knowledge of Blockchain and AI opportunities. This article [27] proposes a 5G network ecosystem powered by blockchain-enabled UAVs that can balance network access supply and demand. The system offers dependable and secure decentralized delivery of services and navigation to/from end users.

Authentication and data exchange may be hampered by the drone's accessible and untrustworthy surroundings. To overcome this problem, the authors [28] proposed a blockchain-based data sharing mechanism for 5G flying drones that is both efficient and safe. To secure the confidentiality of instructional problems and data exchange, this architecture uses blockchain and attribute-based encryption. This study [29] proposes a blockchain-based cross-domain authentication mechanism for the smart 5G-enabled Internet of Drones. Not only do centralized authentication techniques have a single point of failure, but they also cannot handle cross-domain identification. A concept for a 'blockchain'-based identification system for drones has been developed to alleviate these restrictions. Due to the evolving nature of the Blockchain and 5G, opportunities available in this domain, some of them are shown various research in Figure 3 below.

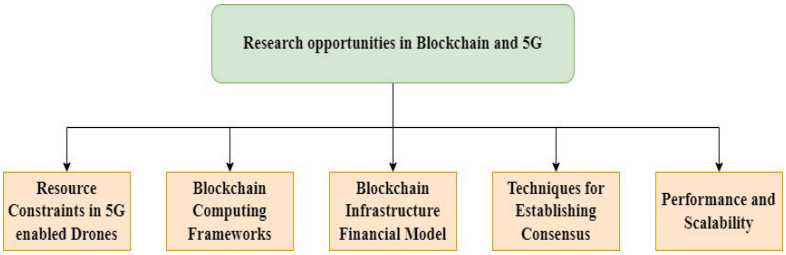

Figure 3 Research Opportunities in Blockchain and 5G.

In a fully decentralized way, the Blockchain has the ability to tackle the numerous difficulties related with 5G, such as authentication, productivity, and strategic planning. Below are some prominent research opportunities available in the domain of Blockchain and 5G.

- Resource constraints in 5G enabled drones: In terms of power [30], dimensions, and mass, the majority of present drones are constrained. Blockchain systems often need encryption and/or consensus techniques; however, drones are usually unsuitable of computing-intensive activities owing to computational restrictions and battery capacity. Furthermore, a swarm of unmanned aerial vehicles (UAVs) can create and/or gather terabytes of data every second, comprising audio and video. It is currently unclear if blockchain's storage capacity can handle such a large amount of data, and whether and how to integrate additional storage facilities with the UAV system is an unanswered question. Drones, on the other hand, are energy-constrained machines that need

energy-efficient alternatives. To deploy blockchain-based drone interactions in the future, the coordination of different computing facilities such as faraway clouds, local edge computers and drones, and other innovations such as routing protocol will become necessary.

- Blockchain computing Frameworks: Many distinct [31] kinds of blockchains have significant computational, memory, and communications needs to provide good security, resulting in excessive delay, wastage, and poor scalability. Furthermore, depending on the application traffic, device mobility, and other factors, various nodes may process millions of transactions per unit time. Current systems, on the other hand, lack the high-efficiency infrastructure required for integrating the blockchain. Conflicts between asset blockchain applications and capacity limits, for example, represent a hurdle to 5G and beyond, as well as blockchain integration.
- Blockchain infrastructure financial model: Blockchain [32] adds a layer of trust to the network, reduces barriers to cooperation, speeds up transaction processing, and offers to develop bigger and more effective ecosystems. Users may instantly achieve a consensus since blockchain offers a trustworthy platform for negotiation, and the negotiation process is substantially expedited. The assurance of formulation and implementation of duties and responsibilities in smart contracts may minimize transaction costs.
- Techniques for establishing consensus: Blockchains like open membership and may be able to support tens of thousands of users. Furthermore, implementing blockchains on a large scale necessitates consensus in order to provide increased variation and to adjust to network latency. As a result, consensus should be developed in accordance with the advancement of DApps. Consensus is far more difficult to design in the environment of blockchain than it is in typical distributed systems. Three elements [33] of the blockchain setup distinguish it from typical distributed systems: open participation, unpredictability and a high number of sensor nodes, and intricacy in game tactics.
- Performance and Scalability: In the combined blockchain-5G ecosystems, despite the advantages of blockchain, performance and scalability difficulties remain important obstacles. Compared to non-blockchain applications, blockchain has a substantially lower throughput. The amount of clones in the networks, as well as performance considerations such as restricted bandwidth, are important scaling obstacles in today's blockchain systems.

4 Conclusion

The introduction of 5G cellular networking technologies has sparked renewed interest in blockchain's ability to automate numerous cellular network use cases. 5G is projected to open up new market prospects for both small and big businesses. 5G enables much faster Internet transmission rate, lower latency, and indoor and outdoor connectivity in Smart Cities. High dependability, low latency, accurate automated control, safe hidden broadcasting, and evidence traceability are among the particular communication and security needs of the 5G network. By complementing 5G technology, blockchains have enormous potential for upgrading current 5G services and applications. In conclusion, blockchain opens up a plethora of possibilities for supporting 5G technology and new services for 5G systems. In this paper, the role of blockchain in 5G and emerging technologies are discussed along with the future research aspects and challenges. This article also exposes the research opportunities in the domain of Blockchain and 5G.

References

[1] S. Pandita, "Case for Blockchain in 5G: Data Integrity and Security | HCL Blogs," Feb. 25, 2021. https://www.hcltech.com/blogs/case-blockchain-5g (accessed Nov. 23, 2021).

[2] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema, and S. B. H. Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for Flying Ad Hoc Network (FANET)," IEEE Access, vol. 8, pp. 56371–56378, 2020, doi: 10.1109/ACCESS.2020.2981531.

[3] I. U. Khan, M. A. Hassan, M. Fayaz, J. Gwak, and M. A. Aziz, "Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS," Comput. Mater. Contin., vol. 70, no. 2, pp. 3653–3666, 2022, doi: 10.32604/CMC.2022.020697.

[4] S. Rahmadika, M. Firdaus, S. Jang, and K. H. Rhee, "Blockchain-enabled 5G edge networks and beyond: An intelligent cross-silo federated learning approach," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/5550153.

[5] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," J. Netw. Comput. Appl., vol. 166, p. 102693, Sep. 2020, doi: 10.1016/J.JNCA.2020.102693.

[6] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," Trans. Emerg. Telecommun. Technol., p. e4329, 2021, doi: 10.1002/ETT.4329.

[7] K. Kaushik, S. Dahiya, R. Singh, and A. D. Dwivedi, "Role of blockchain in forestalling pandemics," in Proceedings - 2020 IEEE 17th International Conference on Mobile Ad Hoc and Smart Systems, MASS 2020, Dec. 2020, pp. 32–37, doi: 10.1109/MASS50613.2020.00014.

[8] P. P. Ray and K. Nguyen, "A Review on Blockchain for Medical Delivery Drones in 5G-IoT Era: Progress and Challenges," 2020 IEEE/CIC Int. Conf. Commun. China, ICCC Work. 2020, pp. 29–34, Aug. 2020, doi: 10.1109/ICCCWORKSHOPS49972.2020.9209931.

[9] M. Bendechache, T. Saber, G.-M. Muntean, and I. Tal, "Application of Blockchain Technology to 5G-Enabled Vehicular Networks: Survey and Future Directions."

[10] S. Begum, Y. Nianmin, S. B. H. Shah, A. Abdollahi, I. U. Khan, and L. Nawaf, "Source Routing for Distributed Big Data-Based Cognitive Internet of Things (CIoT)," Wirel. Commun. Mob. Comput., vol. 2021, 2021, doi: 10.1155/2021/5129396.

[11] I. U. Khan et al., "Monitoring System-Based Flying IoT in Public Health and Sports Using Ant-Enabled Energy-Aware Routing," J. Healthc. Eng., vol. 2021, 2021, doi: 10.1155/2021/1686946.

[12] I. U. Khan et al., "RSSI-Controlled Long-Range Communication in Secured IoT-Enabled Unmanned Aerial Vehicles," Mob. Inf. Syst., vol. 2021, 2021, doi: 10.1155/2021/5523553.

[13] 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. 115876–115904, 2020, doi: 10.1109/ACCESS.2020.3003020.

[14] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," Mech. Syst. Signal Process., vol. 135, p. 106382, Jan. 2020, doi: 10.1016/J.YMSSP.2019.106382.

[15] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge Intelligence and Blockchain Empowered 5G beyond for the Industrial Internet of Things," IEEE Netw., vol. 33, no. 5, pp. 12–19, Sep. 2019, doi: 10.1109/MNET.001.1800526.

[16] G. Praveen, V. Chamola, V. Hassija, and N. Kumar, "Blockchain for 5G: A Prelude to Future Telecommunication," IEEE Netw., vol. 34, no. 6, pp. 106–113, Nov. 2020, doi: 10.1109/MNET.001.2000005.

[17] K. Yue et al., "A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective," IEEE Commun. Surv. Tutorials, pp. 1–1, Sep. 2021, doi: 10.1109/COMST.2021.3115797.

[18] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: Opportunities and challenges," 2019 IEEE Globecom Work. GC Wkshps 2019 – Proc., Dec. 2019, doi: 10.1109/GCWKSHPS45667.2019.9024627.

[19] F. Gao, D. L. Chen, M. H. Weng, and R. Y. Yang, "Revealing development trends in blockchain-based 5g network technologies through patent analysis," Sustain., vol. 13, no. 5, pp. 1–24, 2021, doi: 10.3390/su13052548.

[20] A. Miglani and N. Kumar, "Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review," Comput. Commun., vol. 178, pp. 37–63, Oct. 2021, doi: 10.1016/J.COMCOM.2021.07.009.

[21] T. Han et al., "Emerging Drone Trends for Blockchain-Based 5G Networks: Open Issues and Future Perspectives," IEEE Netw., vol. 35, no. 1, pp. 38–43, Mar. 2021, doi: 10.1109/MNET.011.2000151.

[22] 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 Commun. Mag., vol. 59, no. 3, pp. 77–83, Mar. 2021, doi: 10.1109/MCOM.001.2000857.

[23] C. Lima, "Blockchain-GDPR Privacy by Design How Decentralized Blockchain Internet will Comply with GDPR Data Privacy," 2018.

[24] "5G Vision – The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services." https://espas.secure.europarl.europa.eu/orbis/document/5g-vision-5g-infrastructure-public-private-partnership-next-generation-communication (accessed Nov. 29, 2021).

[25] C. Benzaid, M. Z. Farooqi, C. Benzäıdbenzäıd, and T. Taleb, "VEND-NET: Vehicular Named Data Network View project Secure Time Synchronization in Wireless Sensor Networks View project IEEE NETWORK MAGAZINE 1 Trust in 5G and Beyond Networks," doi: 10.1109/MNET.011.2000508.

[26] A. Kumar et al., "Survey of Promising Technologies for Quantum Drones and Networks," IEEE Access, vol. 9, pp. 125868–125911, 2021, doi: 10.1109/ACCESS.2021.3109816.

[27] M. Aloqaily, O. Bouachir, A. Boukerche, and I. Al Ridhawi, "Design Guidelines for Blockchain-Assisted 5G-UAV Networks," IEEE Netw., vol. 35, no. 1, pp. 64–71, Mar. 2021, doi: 10.1109/MNET.011.2000170.

[28] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Netw., vol. 35, no. 1, pp. 130–137, Mar. 2021, doi: 10.1109/MNET.011.2000223.

[29] 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 Things J., 2021, doi: 10.1109/JIOT.2021.3113321.

[30] Y. Wu, H. N. Dai, H. Wang, and K. K. R. Choo, "Blockchain-Based Privacy Preservation for 5G-Enabled Drone Communications," IEEE Netw., vol. 35, no. 1, pp. 50–56, Mar. 2021, doi: 10.1109/MNET.011.2000166.

[31] T. Maksymyuk et al., "Blockchain-Empowered Framework for Decentralized Network Management in 6G," IEEE Commun. Mag., vol. 58, no. 9, pp. 86–92, Sep. 2020, doi: 10.1109/MCOM.001.2000175.

[32] J. Backman, S. Yrjola, K. Valtanen, and O. Mammela, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," Jt. 13th CTTE 10th C. Conf. Internet Things – Bus. Model. Users, Networks, vol. 2018-January, pp. 1–8, Jul. 2017, doi: 10.1109/CTTE.2017.8260929.

[33] M. Vukolićvukolić, "Rethinking Permissioned Blockchains," Proc. ACM Work. Blockchain, Cryptocurrencies Contract., doi: 10.1145/3055518.

Biography

Keshav Kaushik is working as an Assistant Professor in the School of Computer Science at the University of Petroleum and Energy Studies, Dehradun, India. He is an experienced educator with over 7 years of teaching and research experience in Cybersecurity, Digital Forensics, the Internet of Things, and Blockchain Technology. Mr. Kaushik received his B.Tech degree in Computer Science and Engineering from the University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak. In addition, M.Tech degree in Information Technology from YMCA University of Science and Technology, Faridabad, Haryana. He has published 20+ research papers in International Journals and has presented at reputed International Conferences. He is a Certified Ethical Hacker (CEH) v11, CQI and IRCA Certified ISO/IEC 27001:2013 Lead Auditor, and Quick Heal Academy certified Cyber Security Professional (QCSP). He acted as a keynote speaker and delivered 50+ professional talks on various national and international platforms. He has edited more than 8 books with reputed publishers.