# Blockchain in fifth-generation network and beyond: a survey

**Ahmed Shamil Mustafa, Mohammad Abdulrahman Al-Mashhadani, Salah Ayad Jasim, Ahmed Muhi Shantaf, Mustafa Maad Hamdi**
Department of Computer Engineering Techniques, Al-Maarif University College, Al-Ramadi, Iraq

**Article Info**

***Article history:***

Received Dec 27, 2021
Revised Mar 7, 2022
Accepted Apr 4, 2022

***Keywords:***

Fifth-generation
B5G
Blockchain
Wireless communication

**ABSTRACT**

Fifth-generation (5G) technologies enable a wide range of vertical applications by connecting heterogeneous equipment and machines, resulting in significantly improved service quality, increased network capacity, and improved system performance. As a result, the world is shifting to 5G wireless networks. Because 5G has the advantage of supporting various vertical applications, 5G systems must still overcome challenges such as transparency, data interoperability probabilities, decentralization, and network privacy. In this paper, we'll show how blockchain can be used to solve problems in 5G, as well as some of the idea's researchers, have come up with to solve them, like resource sharing, security, and mobility.



***Corresponding Author:***

Ahmed Shamil Mustafa
Department of Computer Engineering Techniques, Al-Maarif University College
Al-Ramadi, Iraq
Email: ahmedshamil90@gmail.com

## 1. INTRODUCTION

Future cellular networks, which are expected to be implemented in the coming years, have the potential to have a wide-ranging and direct impact on consumers and corporate stakeholders. A personalized and sophisticated user-centric value that serves as a path to human connection for more loaded and ever-evolving user needs will be most prominent in the future of fifth-generation (5G) wireless technologies [1]. The strategies mentioned [1], [2] were used to achieve the stated goals, and key technologies included cloud computing, edge computing, and network connectivity. Network slicing, function virtualization, and machine-to-machine communication, as a result, widespread adoption of 5G wireless services raises additional security concerns, particularly in terms of network dependability, data immutability, and privacy.

Integrating multiple technologies to deliver a wide range of services may present significant challenges in terms of security, data integrity, and network resiliency, but integration is required for all disciplines to progress in all fields [3]. As the number of connected devices and data grows, most networks now use a centralized architecture. The 5G ecosystem faces a security risk due to its centralized design. Each device is given a distinct identity, identified, and authenticated. When two devices are near, data transmission must take place over a network. The main issue with this architecture is that it is prone to congestion, outages, and organized attacks that can harm the entire network [4]. One solution to this problem is to employ a decentralized and distributed architecture. Future networks are expected to be mostly made up of networks that aren't controlled by anyone. It helps all the layers of the network work better when they are distributed. This includes the physical, hardware and software layers, and the application layer. As a result, 5G networks will work in a very dynamic and complex environment, with nodes working together to improve their performance and interacting with each other [5].

Although 5G networks are far from autonomous, self-managing, cooperative, or decentralized, and many technologies have advanced. Several internet of things (IoT) use cases, such as device to device (D2D), computation, and storage, necessitate a highly distributed and decentralized architecture. A decentralized network architecture may greatly benefit any collaborative use case [6].

The integration of 5G with blockchain is also anticipated to aid in the development of future mobile services [7]. Gaining greater control of the wireless spectrum would allow for the linking of ever more diverse devices and complicated networks, as well as the integration of a staggering 500 billion mobile devices by 2030. As a vital component of the 5G infrastructure, these ultra-dense small cell networks are capable of providing data rates, and latencies equivalent to radio connections while ensuring stable connectivity in these cases. On the other hand, it provides a foundation for trustworthy and secure interoperation in complex sub-networks. Because diverse devices working together is critical for 5G mobile networks, collaboration is essential. Blockchain technology has the potential to enable large-scale communication while maintaining high security and integrity [8]. Network function virtualization (NFV), D2D communication, and cloud/edge computing are just a few of the new technologies that will be used in 5G. Existing 5G platforms face a significant challenge in keeping the system open, transparent, and safe to ensure the successful implementation of 5G [9]. Blockchain is expected to be a critical tool for meeting 5G system performance requirements while spending the least amount of money and incurring the least amount of operational complexity.

Contribution of this survey, a research paper that explains how blockchain will be integrated into 5G networks. Unlike any previous survey, this one allows researchers to investigate how blockchain can be applied to 5G networks using an end-to-end research approach. We investigate the benefits and constraints of blockchain application in a dispersed 5G deployment to aid in the growth of 5G system service delivery models. Beyond its current usage, blockchain has new prospects in 5G-related applications such as spectrum management, data interchange, network automation, resource automation, and interference reduction, as well as federated learning and privacy and security risks. Aside from smart cities, smart grids, and unmanned aerial vehicles (UAVs), blockchain's role in 5G IoT networks is addressed through use cases such as smart healthcare, smart transportation, smart grid, and automated vehicle systems. We explain the challenges and unanswered questions that researchers face, as well as the direction of future blockchain-5G research.

Structure of this survey, in this survey paper, the structure is the following, in section 1, we present an introduction of 5G then discuss the integration of services that enable 5G. Section 1 also includes a contribution of this survey paper and the rest paper. Section 2 includes a background of technologies, which means a 5G technology and blockchain. Each technology is described and presented with its features, at the end of section 2 we present a related work of blockchain and 5G. In section 3, we talk about the integration of both technologies together, blockchain and 5G network in detail. Section 4 includes a blockchain with a new generation of network 6G. the last section includes a conclusion of the work.

## 2. BACKGROUND

Two innovative technologies will be on display and discussed, as well as recent advancements in this field. The 5G network will be deployed in many countries beginning in 2020. To meet the demand for the next generation of 5G networks, business, and university researchers are proposing a wide range of emerging technologies. The first segment will contain all the network's components. Blockchain technology has also been implemented, with bitcoin serving as its primary component. Finally, many other researchers have used the tools used in this study. In the case of related work, our goal is to aid 5G technology by implementing blockchain.

### 2.1. Fifth-generation technology

5G cellular networks are now being developed to address the increasing demand for driverless cars and IoT-powered services such as smart home appliances. 3$^{rd}$ generation partnership project (3GPP) released the 5G study in Rel-14 to investigate the possibility of 5G. It is currently projected that 5G specifications would be finished by 2020. We summarize the major needs, architecture, and enabling technologies for 5G in this section.

#### 2.1.1. Cloud/edge computing

In the 5G era, cloud computing was created to meet the ever-increasing demand for resource management, data storage, and mobile sensing. Cloud computing paradigms and virtual compute centers with abundant computing resources could be used to deliver 5G services such as mobility/network management, resource offloading, and sense. Meanwhile, while cloud computing has been identified as a potential path to enabling 5G ecosystems, edge computing has been identified as a viable technology for 5G ecosystem expansion. Edge computing is intended to enable mobile network operators to provide compute and storage services with significantly lower latency [10].

#### 2.1.2. Software-defined networking

Software-defined networking (SDN) is a technique that uses software that may operate on commodity hardware instead of switches or routers to enable users to control the network equipment. Network-wide and in very flexible ways, some various applications and services can be controlled and coordinated by SDN [11]. Separating network administration from the data plane, where a single control plane oversees several devices, allows for a broad variety of network functionalities to be introduced. Network flexibility and centralized control are provided by this split, which also provides the network with global visibility needed to respond swiftly to the changing needs of end-users.

#### 2.1.3. Network function virtualization

SDN and NFV are both components of 5G networks that work well together. NFV allows for the virtualization and operation of entire network operations on cloud infrastructure. Both technologies abstract across the network and are heavily reliant on virtualization. This highlights the parallels between SDN and NFV. The SDN strategy of separating control and forwarding operations as opposed to the NFV strategy of separating both services from the underlying hardware [12].

#### 2.1.4. Device to device

Currently, cellular networks are made up of base stations and connected devices. Communication must take conducted via the base station, even if the two devices are near together. D2D communications improve the cellular network by increasing data speeds at the cell edge. This can be used to create one-of-a-kind applications and services [13], [14].

#### 2.1.5. Network slicing

Network slicing enables the creation of distinct logical networks that are tailored to meet the application-specific quality of service requirements (QoS). The construction of a logical network brings new items and services to the market that can be quickly altered in response to market demands. For example, an augmented reality (AR) network slice may be designed with high throughput and low latency in mind, whereas another slice for massive IoT would require high reliability and security [15].

### 2.2. Blockchain technology

Bitcoin is perhaps best recognized as the platform on which blockchain is built [16]. A blockchain's distinguishing feature is decentralization. This indicates that the database is dispersed and not centralized (i.e., computers). A public blockchain is permissionless, whereas is a private blockchain. Anyone can join a public blockchain and transact while also contributing to the consensus process. Among the most well-known public blockchain applications are bitcoin and Ethereum.

Participants' permission sets must include a validation method. Understanding blockchain concepts and fundamental properties are critical for unlocking the potential of blockchain in 5G networks. In this introduction, we will first describe the primary components of a blockchain network. Once these concepts are understood, we will demonstrate how immutability, decentralization, transparency, security, and privacy are critical components of blockchain solutions for 5G networks and services [17], [18]. The following is described each characteristic and Figure 1 combines them.

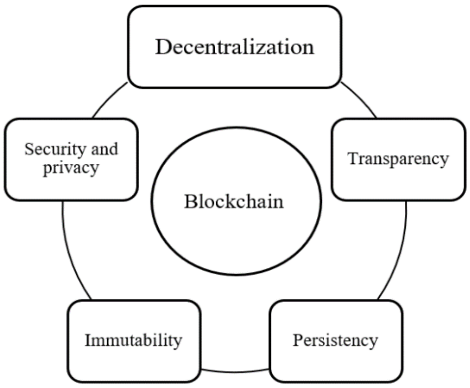


Figure 1. Blockchain characteristics to 5G network [19]

Immutability: once transaction data is saved on a blockchain ledger, it cannot be changed. This is because every block in the chain is hashed and connected in such a manner that entities cannot change or interfere with the information contained inside any given block. A key feature of blockchain technology is data storage and sharing. In 5G applications like secure spectrum sharing, D2D communication, or privacy-preserving network virtualization, this feature supports safe data storage, and transfer. Network operators may use secure communications to perform heterogeneous networking and computing across trustless IoT environments, such as large-scale IoT collaborations or mobile edge/cloud computing [20].

Decentralization: the blockchain is decentralized in the sense that it does not reliant on authority or entity to govern the database. Consensus processes like proof-of-work (POW) are used to keep the database secure. This crucial feature enables data retrieval with great immutability and durability, as well as low latency [20].

Transparency: blockchains, such as the one used for bitcoin, are extremely transparent because all transaction information is available to everyone. By including all network nodes, the company promotes transparency, and which aids in data integrity. Open and fair principles are critical in a 5G environment. Transparent ledger solutions on blockchains may be provided to facilitate open and secure data transfer and payment, with the added benefit of identifying resources and slicing customers. As a result, services like mobile resource trade (e.g., 5G IoT) may be automated on the blockchain using smart contracts, making data exchange more transparent, and reliable for all participants [21].

Security and privacy: one way to ensure the security of the blockchain is to use private and public keys. By using asymmetric cryptography, which involves the use of random strings for key generation, attackers will be impossible to penetrate blockchain security [22], [23]. In addition, immutability, and unanimity in the blockchain resulting in privacy for databases that are kept on the blockchain. Each user can authenticate and maintain their data throughout the network. Data within the block is protected by hashing and mining bottlenecks.

Recently, blockchain has been put to use in real-world 5G use cases via case studies. A blockchain-5G project has been established by China's ministry of industry and information technology (MIIT) to assist Chinese mobile phone manufacturers including China mobile, China unicom, and China telecom is putting blockchain on their current 5G platforms. The initiative is being implemented throughout the country. 5G networks in China earlier this year, China unicorn and Wanxiang blockchain formed a joint venture to implement both blockchain and IoT supply chain technology in China.

## 3. RELATED WORK

Research by Tan *et al.* [24], argues that in 5G-enabled smart cities, an electronic decentralized and blockchain-powered trustworthy service mechanism for the crowdsourcing system is required. The proposal describes a mechanism that follows the nine stages of the crowdsourcing service process sequentially: initialization, task submission, task publication, task reception, scheme submission, scheme arbitration, payment, task rollback, and service compensation. Each stage is executed by an automated smart contract, and payments are sent via blockchain. There are no third-party central institutions involved.

Research by Lee and Ma [25], to address the issue of the key derivation methodology's inability to handle complete forward key separation, a novel solution based on blockchain is used. The author employs blockchain as an authoring platform. Blockchain has a sophisticated approach to dealing with the required transition to 5G with complete forward key separation. The author focused on mobility management in 5G to accomplish this.

The article describes how cloud-radio access network (C-RAN) enabled by blockchain (BC-RAN) is used for 5G to stop hostile insider threats, as well as how the size of the blockchain network is increased by the implementation of the practical Byzantine fault tolerance (PBFT) (trust-PBFT) consensus method on the PeerTrust network by Tong *et al.* [26]. In addition, we also suggest a tri-chain blockchain structure for transaction divisions, in which storage is categorized into three distinct blocks. To become participants in PBFT, the algorithm determines the trust value of each node, and the nodes with high trust values are selected. The installation of PeerTrust at the same time results in a new advantage of improving fault tolerance performance more effectively. Since an adjustment mechanism has been added to the algorithm, the malicious nodes' impacts are now restrained by the algorithm.

Research by Yazdinejad *et al.* [27], by combining SDN controllers into a cluster utilizing the unique routing protocol, the author develops a blockchain-enabled, energy-efficient SDN controller architecture for IoT networks. The design minimizes POW and proposes an efficient authentication technique based on distributed trust for resource-constrained IoT devices by using peer-to-peer (P2P) communication between IoT devices and SDN controllers on public and private blockchains. The findings reveal that a cluster-structured routing protocol outperforms existing routing protocols such as EESCFD, SMSN, Ad-Hoc on-demand distance vector (AODV), Ad-Hoc on-demand multipath distance vector (AOMDV), and destination sequenced distance vector (DSDV) in terms of throughput, latency, and energy usage. Traditional blockchain is outperformed by our suggested approach.

Kumari *et al.* [28], proposed a proposal for using a blockchain-enabled UAV software demand infrastructure in 5G for secure communication and network management that was recently published. As a result of using this item, UAV communication services will have these dynamic, flexible, and on-the-fly decision capabilities. UAV architecture provided BC-based software to provide a secure and flexible communication network Gupta *et al.* [29]. The network management system may use flexible and dynamic decision capabilities even in open 5G-enabled UAV networks.

## 4. INTEGRATION OF BLOCKCHAIN AND 5G NETWORK

The integration of blockchain with 5G provides numerous benefits to the network. At first, the blockchain will be used for network management. Second, it aids and manages computing in 5G. Third, in terms of communication, the blockchain enables many services for communication management. Finally, because blockchain is a secure technology, it will provide security and privacy for a 5G network. In this section, we will go over all of the services listed in Table 1.

Table 1. Blockchain keywords in 5G

| | Blockchain for 5G | | | | |
|---|---|---|---|---|---|
| Services | 1 | 2 | 3 | 4 | 5 |
| Network management | SDN | NFV | Network slicing | | |
| Computing management | MEC | Caching of content | Data storage | Distributed computing | Cloud computing |
| Communication management | Spectrum sharing | Infrastructure sharing | D2D | Resource allocation | Interference management |
| Security and privacy | Authentication | Identify as a service | Fraud management | Data privacy | Access control |

### 4.1. Blockchain for network

#### 4.1.1. Software-defined networking

With SDN, network resources may be used more effectively, and new internet protocol (IP)-based services may be rapidly deployed. However, addressing scalability, performance, reliability, and interoperability in 5G networks is feasible by using blockchain. For SDN to be effectively exploited in the 5G and beyond networks, various difficulties must be resolved.

Decentralization: when an SDN controller becomes hacked, it poses a single point of failure since there is only one of them. Distributed SDN architecture development is necessary, especially with capabilities for a backup controller to manage network traffic flow. Reliability, consistency, and interoperability are equally key issues for scalability, and vice versa [29], [30].

Scalability: SDN design employs centralized or partly distributed controllers that connect to various network devices and that operate with the data planes on many devices. when the number of concurrent clients or players increases [30]. Performance-as an SDN deployment is seen more like a network operating system, using a distinct control, and data plane design introduces delay. This might result in excessive latency and degradation of network performance in big networks. Controller reaction time and controller turnaround time.

Security: protecting the controller is critical when it comes to security solutions. The absence of software development standards and rules creates the possibility of security vulnerabilities. Without SDN controllers' approval, third-party providers may enter the network, and make control rules change without permission.Network monitoring: ensuring network data is constantly monitored has the potential to have high overheads that will adversely influence network performance [30].

#### 4.1.2. Network functions virtualization

Virtual machines (VMs) may support virtualization servers, which operate virtual machines to run different operating systems. Cloud infrastructures are commonly shared by tenants in a virtualized environment. The risk of cloud assaults increases in this scenario, resulting in less transparency and responsibility for cloud service providers. In NFV, an attacker may build a VM to carry out a denial-of-service attack that takes place on a separate server [31].

For these difficulties, blockchain technology has shown to be an effective tool. Incorporating its irreproducibility, integrity, and non-repudiation features, blockchain makes it possible for NFV networks to take place in three primary ways. First, blockchain technology empowers VNF orchestration with greater orchestration, network management, and overall system reliability. The second method, the network operations, and system integrity are protected against both internal attacks and external threats, such as malicious VM modifications and distributed denial-of-service (DDoS) assaults, through the use of blockchain technology. In the final analysis, blockchain technology can execute system auditing and monitoring of system status while the network is in contact. To help with the aforesaid difficulties, we are reviewing the recent breakthroughs in blockchain application for NFVs [32].

#### 4.1.3. Network slicing

A network slice is a network that is entirely separated into end-to-end logically isolated segments, each of which has 5G devices. The most difficult task associated with network slicing is dealing with different levels of service needs for various subslices. Proper isolation across slices requires a wide variety of basic concerns, such as assured QoS, resource usage, billing rules, and security. An network slicing brokering (NSB), using blockchain, is suggested in [33].

### 4.2. Blockchain for computing

The edge network's networking capabilities can be improved thanks to blockchain. The blockchain is used in [34] to construct a distributed and trustworthy authentication system so that devices situated at the edges of IoT systems may be sure of the reliability of their authentication and exchange of information. The user identity information may be safely maintained in the system while authentication data and user access information are linked to the blockchain, which also tracks actions of mobile terminals (devices) without the need of a central authority.

Blockchains have recently been used to provide security in cloud-based 5G networks. BlockONet, created by [35], is a framework aimed at better enabling the 5G network fronthaul in terms of both connectivity and security. Using blockchain in cloud-RAN 5G network offers two major advantages. Decentralized, fair agreement with a consensus platform in the core network. Single point failure bottlenecks are eliminated, and the system's confidence is greatly improved.

Blockchain has shown to be the most suitable platform for this variety of dynamic, dispersed, and heterogeneous 5G networks. Also, it monitors all the transactions to determine current market values, helping end-users, and network providers. A permissioned content caching solution for edge networks based on deep reinforcement learning [36]. Content caching is done on cars safely and reliably while maintaining the blockchain on base stations. Proof-of-utility-based consensus (PoU) is suggested for reaching an agreement as additional base stations are installed.

### 4.3. Blockchain in communication

In this subsection, we will present a method of integration of blockchain in 5G in terms of communication management. The service of blockchain will include the following: infrastructure, spectrum, D2D, resource, and interface. Infrastructure: there may be resources owned by other parties such as the base station provider and the spectrum provider that are available to the network operator. All the desired qualities, such as confidentiality, immutability, auditability, and transparency, are simultaneously guaranteed. While network operators can rapidly locate and use resources (infrastructure and spectrum) with the least cost, service offerings may be offered openly and with transparency, ensuring customers have an idea of where their requests are met from start to finish [37].

Spectrum: while 5G networks will advance the state of the art, significant physical restrictions such as spectrum limits hinder operators from taking full use of these new technologies. Network spectrum shortage causes a slower rate of bandwidth improvement, as well as poor service quality [38]. To have single-point failure bottlenecks in such centralized designs puts the whole spectrum sharing network at risk if the authority is attacked or is out of service [39]. To construct spectrum sharing and management models with greater security and better performances, such as reduced latency and greater throughput, the blockchain may be used. The proposed use of blockchain is for wireless spectrum management and has these advantages [40].

D2D: a D2D network access control mechanism is described in [41] using a blockchain (CSI). The criticality of the CSI in providing the necessary resources to enhance the QoS of the user, as well as network performance, can't be underestimated. The malicious node may increase its CSI to gain more network resources, and that will impede the QoS of the legal users. The framework is built using a consensus process and saves the output on two blockchain: one that keeps track of the certified/true CSI and one that keeps track of the counterfeit/false CSI.

Access management: blockchains may help in 5G wireless access technology deployments and end-user equipment (UE) and IoT device connectivity via seamless access across a variety of networks. When you enter a geographical coverage region for the network, the UE may choose to connect using several technologies, for example, 5G, long-term evolution (LTE), and wireless-fidelity (Wi-Fi). Only when network operators can manage multiple access nodes and procedures will they be able to provide network access via numerous technologies, a key characteristic of 5G technology [42].

Interference: interference has been shown in tests to have a significant impact on wireless network performance. There will be several challenges associated with 5G networking because each network operator will have to collaborate with other network operators to organize the network. Furthermore, developing cooperative strategies that reward and penalize dynamically is extremely difficult. Some of these issues may be addressed by distributed interference management on the blockchain. This also applies to the authors of [43], who created a distributed coordination protocol using blockchain-enabled distributed coordination.

### 4.4. Security and privacy

Two of the most critical challenges in an open and decentralized network with billions of devices is privacy and security. Fan *et al*. [44] suggested blockchain-based methods to create mutual trust between users and content providers in order to overcome privacy challenges that develop in content-centric mobile networks. Material producers are benefiting from the adoption of blockchain technology to govern and protect their content. Using blockchain, it keeps track of the actual storage locations of the data on the cloud.

Chen *et al*. [45] described an authentication mechanism for ultra-dense networks. The idea of trusted APs group (APG) built utilizing blockchain is presented instead of employing on-hand authentication for each handover. In order to generate the APG chain, the PBFT consensus procedure is used.

Blockchain-based keyless signature infrastructure (KSI) is gaining broad recognition as a way to assure data integrity [46]. All data requests with blockchain-based KSI are hashed and timestamped in the Merkel tree. It is usual to discover and store data pieces using a Merkle tree, which is a binary hash tree. The Merkle tree is ordered chronologically in the timestamps to protect data from modification. For data integrity and data management, an IoT-enabled KSI proposed in [47] is built on blockchain.

## 5. BLOCKCHAIN IN B5G/6G

The issues, observable to human beings, that would arise with 6G have been discussed by Aazhang *et al.* [48]. Also, as shown in research by Biral *et al.* [49], many hurdles face M2M communications. In Table 2, we summarize the challenges of the new generation. Reseach by Xu *et al.* [50], blockchains are used as the information backbone of a local resource management system, which has consumers and producers from an open, transparent market broken down into individual sections to make information available, and improve transaction speed. Blockchain implementation future use-cases were thought to be possible through the use of 6G resource management, spectrum sharing, and compute and energy trading. Furthermore, we have already discussed a number of specific blockchain applications and how they improve wireless networks today.

Table 2. Challenges of the new generation 6G

| Main Item | Sub Item | Definition |
|---|---|---|
| Massive connectivity | Scalability | Future industrial ecosystems will have billions of devices linked and controlled. |
| | Real-time communication | Autonomous vehicles and AR-assisted healthcare use cases |
| | Higher throughput | 5G and beyond are applied to mission-critical systems, all the subsystems must be connected concurrently. |
| | Synchronization | For time-critical industrial applications, synchronization is necessary. |
| Security requirement | Confidentiality | The potential of future computer infrastructures such as the IoT increases the number of vulnerable areas presented by wireless connections. |
| | Integrity | The systems need authorized users to access and change the data as it is being sent, or moving. |
| | Availability | A higher number of networked devices coupled with the sophistication of 5G ecosystems means an explosion in the ecosystem's complexity. |
| | Authentication and access control | The data must be protected by the access control measures both while it is moving and after it has arrived at its destination. |
| | Audit | In order to examine the behavior of network tenants, an audit is necessary. |
| Higher data consumption | | The expectation in the future network is a dramatic increase in data rates. |
| Device resource restrictions | | While the computational and storage limits are expected to reduce the algorithms' capabilities, they will not have a significant impact. |

## 6. CONCLUSION

Following the adoption of the blockchain in various industries, the interest became more and more interest in the field, several studies have investigated how blockchain can apply to 5G networks. Due to the scattered and decentralized structure of future 5G networks, network management, and security challenges will become more widespread and harder. The interest in the blockchain has become more effective, due to the concept of the blockchain in the process of management, decentralization, abbreviation, and the conclude contracts between the two parties, the real motive behind the use of the blockchain in the 5G. In this paper, we presented a set of reviews that support the possibility of using the blockchain in 5G in the field of phone communications and others, and the success in solving many problems that the 5G was suffering from due to its widespread, overlap, safety, and so on. In this research, we explored the huge potential of blockchain in management and it has a high ability to spread fifth-generation technology around the world efficiently and a high ability to connect widespread and heterogeneous devices.

## ACKNOWLEDGEMENTS
Authors thanks Al-Maarif University College for supporting.

## REFERENCES
[1] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Physical Communication,* vol. 18, pp. 64-84, 2016.
[2] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE access,* vol. 3, pp. 1206-1232, 2015.
[3] N. Kamaruddin and A. Wahab, "Effective tocotrienol dosage traceability system using blockchain technology," *Bulletin of Electrical Engineering and Informatics,* vol. 9, pp. 1670-1676, 2020.
[4] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustainable Cities and Society,* vol. 63, p. 102364, 2020.
[5] A. AHAD and K. I. AHMED, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," 2020.
[6] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu*, et al.*, "Survey on blockchain for Internet of Things," *Computer Communications,* vol. 136, pp. 10-29, 2019.
[7] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics,* vol. 9, p. 1338, 2020.
[8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials,* vol. 21, pp. 858-880, 2018.
[9] M. Chaudhry, "Joint ieee spectrum and comsoc talk, test and measurement virtualization and blockchain: Enablers for 5G networks," ed: Nov, 2018.
[10] A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future generation computer systems,* vol. 29, pp. 1278-1299, 2013.
[11] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE,* vol. 103, pp. 14-76, 2014.
[12] B. Yi, X. Wang, K. Li, and M. Huang, "A comprehensive survey of network function virtualization," *Computer Networks,* vol. 133, pp. 212-262, 2018.
[13] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A survey of device-to-device communications: Research issues and challenges," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 2133-2168, 2018.
[14] M. Waqas, Y. Niu, Y. Li, M. Ahmed, D. Jin, S. Chen*, et al.*, "A comprehensive survey on mobility-aware D2D communications: Principles, practice and challenges," *IEEE Communications Surveys & Tutorials,* vol. 22, pp. 1863-1886, 2019.
[15] A. Nakao, P. Du, Y. Kiriha, F. Granelli, A. A. Gebremariam, T. Taleb*, et al.*, "End-to-end network slicing for 5G mobile networks," *Journal of Information Processing,* vol. 25, pp. 153-163, 2017.
[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," ed, 2008.
[17] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang*, et al.*, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access,* vol. 7, pp. 22328-22370, 2019.
[18] W. Mougayar, *The business blockchain: promise, practice, and application of the next Internet technology*: John Wiley & Sons, 2016.
[19] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications,* p. 102693, 2020.
[20] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187,* 2016.
[21] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Communications Surveys & Tutorials,* vol. 21, pp. 1676-1717, 2018.
[22] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Communications,* vol. 25, pp. 12-18, 2018.
[23] O. M. Osman, M. E. A. Kanona, M. K. Hassan, A. A. E. Elkhair, and K. S. Mohamed, "Hybrid multistage framework for data manipulation by combining cryptography and steganography," *Bulletin of Electrical Engineering and Informatics,* vol. 11, pp. 327-335, 2022.
[24] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A Blockchain-empowered crowdsourcing system for 5G-enabled smart cities," *Computer Standards & Interfaces,* vol. 76, p. 103517, 2021.
[25] H. Lee and M. Ma, "Blockchain-based mobility management for 5G," *Future Generation Computer Systems,* vol. 110, pp. 638-646, 2020.
[26] W. Tong, X. Dong, Y. Shen, and J. Zheng, "BC-RAN: Cloud radio access network enabled by blockchain for 5G," *Computer Communications,* vol. 162, pp. 179-186, 2020.
[27] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Transactions on Services Computing,* vol. 13, pp. 625-638, 2020.
[28] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," *Computer Communications,* vol. 161, pp. 304-323, 2020.

[29] R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and 5G integrated softwarized UAV network management: Architecture, solutions, and challenges," *Physical Communication,* p. 101355, 2021.
[30] G. Lakhani and A. Kothari, "Fault administration by load balancing in distributed SDN controller: A review," *Wireless Personal Communications,* vol. 114, pp. 3507-3539, 2020.
[31] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, "Network function virtualization in 5G," *IEEE Communications Magazine,* vol. 54, pp. 84-91, 2016.
[32] E. Ak and B. Canberk, "BCDN: A proof of concept model for blockchain-aided CDN orchestration and routing," *Computer Networks,* vol. 161, pp. 162-171, 2019.
[33] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1-7.
[34] D. Garcia-Roger, S. Roger, D. Martín-Sacristán, J. F. Monserrat, A. Kousaridas, P. Spapis, *et al.*, "5G functional architecture and signaling enhancements to support path management for eV2X," *IEEE Access,* vol. 7, pp. 20484-20498, 2019.
[35] H. Yang, Y. Wu, J. Zhang, H. Zheng, Y. Ji, and Y. Lee, "BlockONet: blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul," in *Optical Fiber Communication Conference*, 2018, p. W2A. 25.
[36] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," *IEEE Transactions on Vehicular Technology,* vol. 69, pp. 4312-4324, 2020.
[37] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: opportunities and challenges," in *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1-6.
[38] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, and B. Ottersten, "Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 674-707, 2017.
[39] F. Hu, B. Chen, and K. Zhu, "Full spectrum sharing in cognitive radio networks toward 5G: A survey," *IEEE Access,* vol. 6, pp. 15754-15776, 2018.
[40] M. B. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Transactions on Cognitive Communications and Networking,* vol. 5, pp. 193-205, 2019.
[41] D. Lin and Y. Tang, "Blockchain consensus based user access strategies in D2D networks for data-intensive applications," *IEEE Access,* vol. 6, pp. 72683-72690, 2018.
[42] H. Klessig, D. Öhmann, A. I. Reppas, H. Hatzikirou, M. Abedi, M. Simsek, *et al.*, "From immune cells to self-organizing ultra-dense small cell networks," *IEEE Journal on Selected Areas in Communications,* vol. 34, pp. 800-811, 2016.
[43] A. El Gamal and H. El Gamal, "A single coin monetary mechanism for distributed cooperative interference management," *IEEE Wireless Communications Letters,* vol. 8, pp. 757-760, 2019.
[44] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain‐ based efficient privacy preserving and data sharing scheme of content‐ centric network in 5G," *IET communications,* vol. 12, pp. 527-532, 2018.
[45] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5G ultra-dense network based on block chain," *IEEE Access,* vol. 6, pp. 55372-55379, 2018.
[46] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless signatures' infrastructure: How to build global distributed hash-trees," in *Nordic Conference on Secure IT Systems*, 2013, pp. 313-320.
[47] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm," *IEEE Network,* vol. 32, pp. 112-117, 2018.
[48] B. Aazhang, P. Ahokangas, and L. Lovén, "Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper)," *Oulu, Finland: 6G Flagship, University of Oulu,* vol. 1, 2019.
[49] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digital Communications and Networks,* vol. 1, pp. 1-19, 2015.
[50] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digital Communications and Networks,* vol. 6, pp. 261-269, 2020.


## BIOGRAPHIES OF AUTHORS

**Ahmed Shamil Mustafa** received his Master of Communication and Computer Engineering from Universiti Kebangsaan Malaysia (UKM), Malaysia in 2015. Currently serving as a lecturer in the Department of Computer Engineering Techniques at Al Maarif University College. He is highly interested in communication, computer engineering, VANET, and digital signal processing (DSP). He can be contacted at email: ahmedshamil90@gmail.com.

**Mohammad Abdulrahman Al-Mashhadani** was born in Iraq. He received his Ph.D. degree from the Belarussian Technical State University, Belarussian. He is currently a lecturer in the computer engineering Department, Al-Maarif University College. His research interests include system analysis, DSP, data processing, and control system. He can be contacted at email: mar@uoa.edu.iq.

**Salah Ayad Jassim** was born in Ramadi, Iraq, in 1990. He received a B.S. degree from Al-Anbar University, Electrical department, Ramadi in 2013 and an M.S. degree from the University of Technology, Baghdad, in 2016. He is currently pursuing a Ph.D. degree with the Department of Electrical and Electronic Engineering, Sudan University for science and technology. He can be contacted at email: salahayadvip@uoa.edu.iq.

**Ahmed Muhi Shantaf** was born in Al-Anbar, Iraq. He received a master's degree in electrical and Computer Engineering in 2020/06/03 from Turkey, Altinbas University. He is looking to develop his skills to work in the interest area of Ad-Hoc networks, security, and the design algorithms in a network. He is currently a lecturer in the computer engineering department at Al-Maarif University College. He can be contacted at email: ahmedmuhi89@gmail.com.

**Mustafa Maad Hamdi** was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College, Iraq and the M.Sc. degree in Communication and Computer Engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing a Ph.D. degree in the Department of Communication Engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include wireless and mobile communications, VANET, MANET and satellite communication, and cryptographic. He can be contacted at email: meng.mustafa@yahoo.com.