6G Cellular Networks

Subjects: Computer Science, Cybernetics

Contributor: Adnan Shahid Khan , Zeeshan Ahmad , Jamil Asim , , Mohammed Alqahtani , Mohamed Abbas

There are continued advances in the internet and communication fields regarding the deployment of 5G-based applications. It is expected that by 2030, 6G applications will emerge as a continued evolution of the mobile network. Blockchain technology is one of the leading supporting technologies predicted to provide a secure and unique network to 6G-enabled devices, transactions, and applications. It is anticipated that the 6G mobile networks will be virtualized, have cloud-based systems, and aim to be the foundation for the Internet of Everything.

6G cellular network blockchain technology multifactor authentication technique

1. 6G Cellular Network

1.1. Concept and Development

With the research community involved in discussing possibilities and opportunities that may be opened up with the materialization of 6G technology, most countries in the world are still caught up in the deployment of the 5G technology. However, it is hypothesized by most researchers that 5G and Beyond 5G (B5G) technologies, once fully deployed, will be capable of enabling the Internet of Everything (IoE) to truly take off [1][2], leading to justifying the massive demands for 6G. The sixth generation of wireless technology (6G) will focus on communication between connected machines, i.e., thing-to-thing connection instead of people-to-people links in 1G-4G and people-to-thing communication as in the focus of 5G, as represented in **Figure 1**.

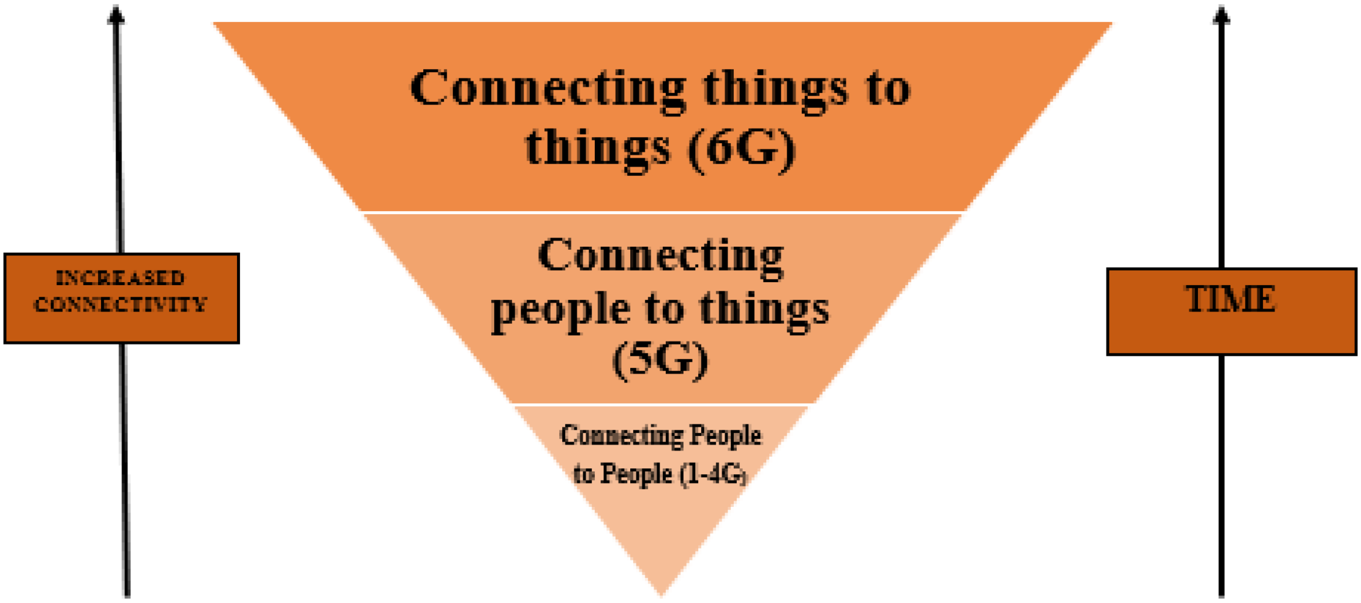
Connecting things to things (6G)
Connecting people to things (5G)
Connecting People to People (1-4G)
INCREASED CONNECTIVITY
TIME

Figure 1. Evolution of Internet.

In the past, a new wireless communication standard emerged after around a decade, and given this trend, it is expected that we would be witnessing 6G around 2030 [3][4][5]. As more and more users are connecting to the internet and using a large number of devices connected to the Internet, big changes and challenges are coming up for internet research. The research communities are already looking towards solutions to the challenges posed by 5G mobile communication. It is expected that many of these challenges will be addressed by the time 6G materializes [6][7].

1.2. Security Needs

While 6G applications and communication technologies will be powerful and a revolution, there will be many specific vulnerabilities [6]. Communication, access control, malicious behavior, authentication, and encryption-related issues will be faced in these applications (see **Figure 2** below). It can be seen in the figure that 6G will support autonomous systems powered by A.I. and ML, multi-sensory X.R. applications built upon molecular communication technology, the THz technology, and the quantum communication technology and distributed ledger technologies that will be mainly developed using blockchains, etc. A.I. technologies and multi-sensory X.R. applications will be susceptible to issues with malicious behavior, encryption, and communication due to heavy data transmissions; however, the blockchains and DLT will be relatively safe as they already implement techniques of multistep or multifactor authentication.

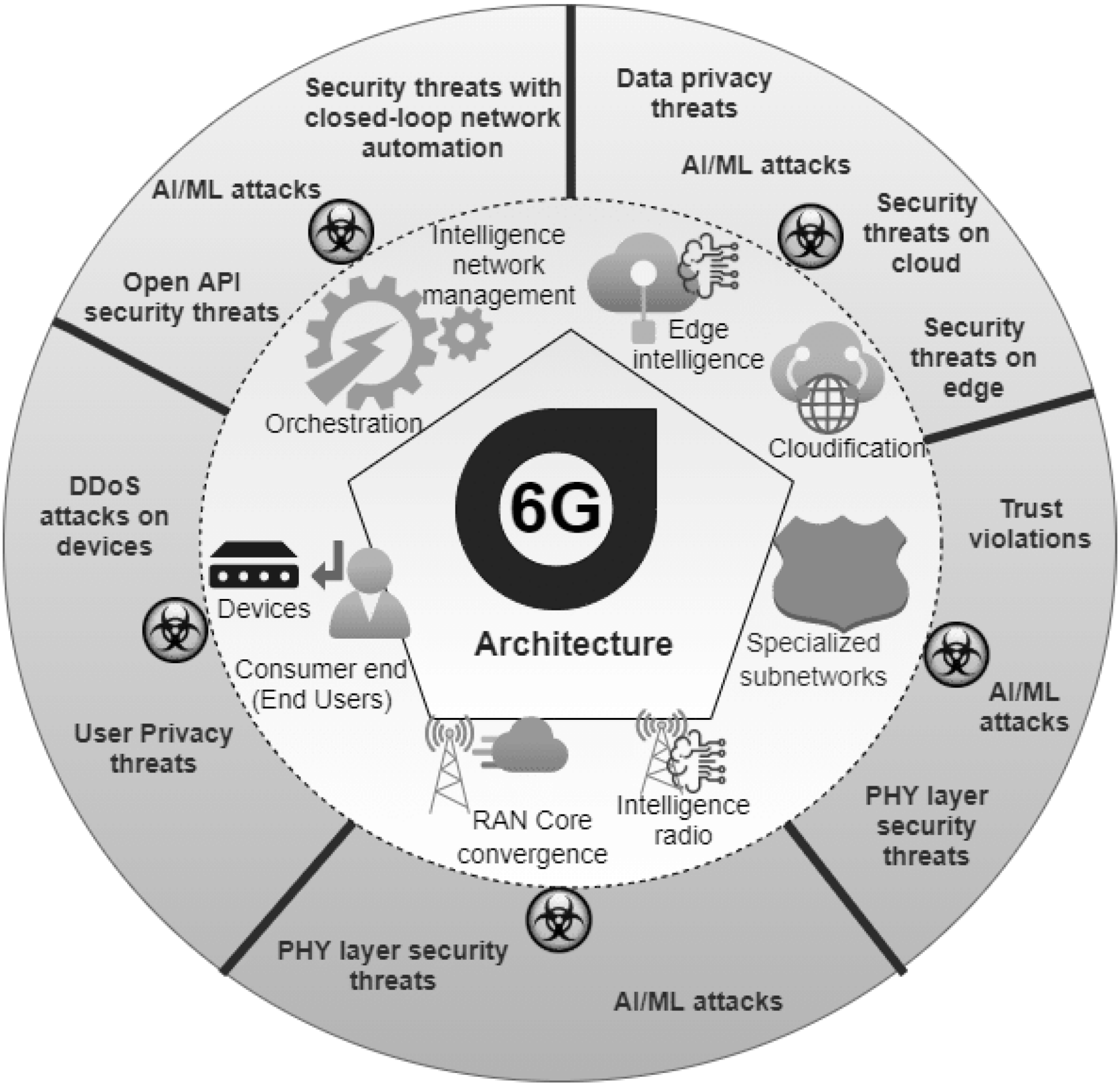

Figure 2. Security and Privacy issues in 6G networks.

2. Blockchain Technology

2.1. What Is Blockchain Technology?

Blockchain technology can be claimed to be the most-hyped innovation of the 21st century that was designed to support bitcoin but now powers many business applications and is hyped to be the leading technology for the support of 6G technologies [8][9][10]. Advancements in blockchains are still young and hold the promise of a bright future [11][12][13]. The blockchains can be defined as a digital ledger of transactions (DLT), a database that can store encrypted transaction data in chronological order and chain the data together in the form of blocks [14][15]. Blockchain is used to define a structure of data that can be described as an ordered arrangement of blocks, where each of the blocks contains a small list of transactions and each of the blocks is chained together [16][17][18]. Through these chains, each component of the data can be traced to its source; however, the blockchains cannot be altered, deleted, or replaced without invalidation of the hash chain [16]. Blockchain technology has extensive applications in payment systems and other digital financial or Fintech solutions. Thus, this technology requires strict authentication protocol for managing the safety of the users and transactions [19][20].

2.2. How does Blockchain Work?

This technology, therefore, enables safe transactions between individuals without the fear of government, bank, or other third-party software snooping and stealing the data [21][22]. **Figure 3** maps out roughly how a blockchain works; first, an individual node in a peer network requests a transaction, which is then broadcasted to a P2P network of nodes that authenticates it by verification technique and combines it to other transactions to form an encrypted block of data which is added to an existing blockchain [23][24]. Blockchains can be considered, therefore, as a promising and revolutionary technology for future developments of applications in the 6G network era as it can help in reducing the risks, stamps out frauds, and brings multilayer transparency in any transactions between two nodes in a scalable way, opening up a myriad of application scope and uses.

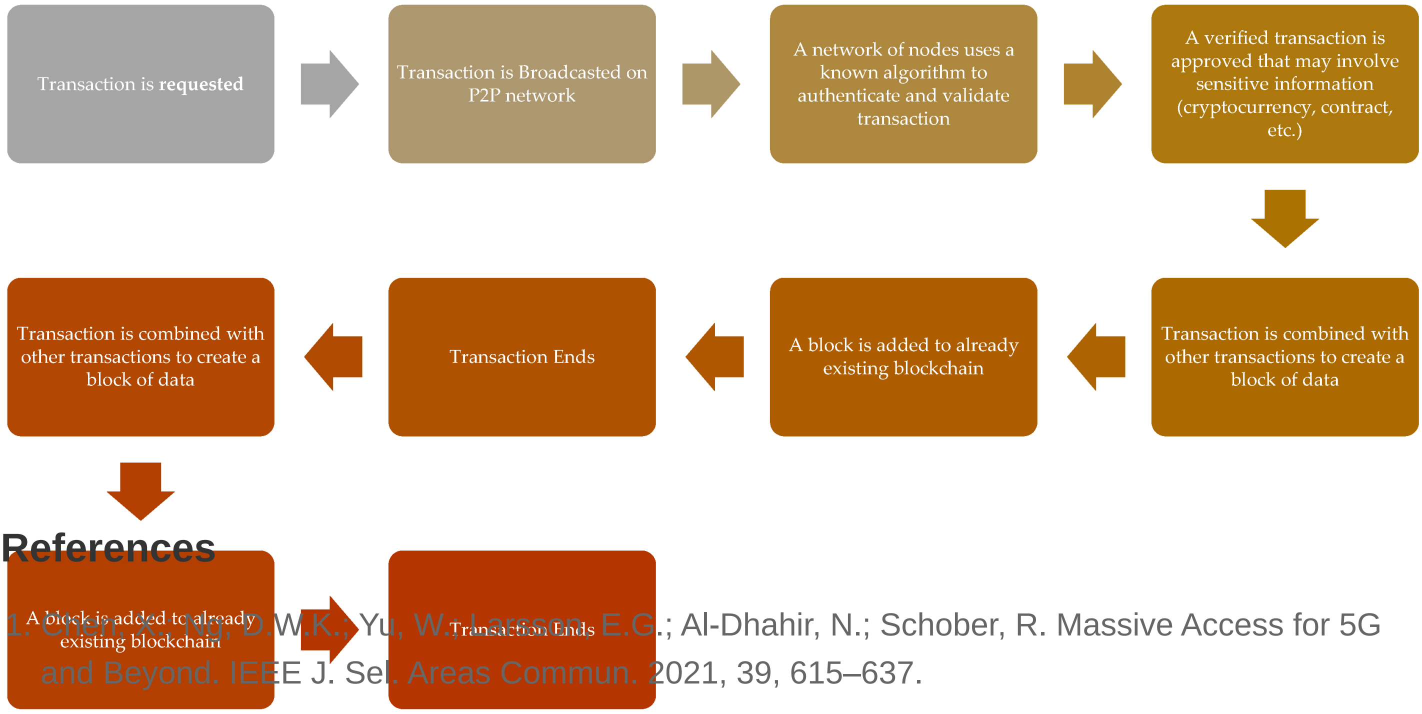
Transaction is **requested**
Transaction is Broadcasted on P2P network
A network of nodes uses a known algorithm to authenticate and validate transaction
A verified transaction is approved that may involve sensitive information (cryptocurrency, contract, etc.)
Transaction is combined with other transactions to create a block of data
A block is added to already existing blockchain
Transaction Ends
Transaction is combined with other transactions to create a block of data
A block is added to already existing blockchain
Transaction Ends

Figure 3. Blockchain Working.

2.3. Benefits of Blockchain

Blockchains are gaining rapid fame due to the importance of record-keeping and storage of transactions and their crucial status for various kinds of businesses [25][26][27]. Blockchains allow efficient processing and faster transactions, saving both time and money [28][29]. Blockchain technology uses a highly secure digital signature feature to ensure that transactions are fraud-free [30]. Blockchains enable decentralized transactions and ensure smoother, safer, and faster transactions as they are carried out with a mutual consensus of users [31][32]. Moreover,

References

1. Chen, X.; Ng, D.W.K.; Yu, W.; Larsson, E.G.; Al-Dhahir, N.; Schober, R. Massive Access for 5G and Beyond. IEEE J. Sel. Areas Commun. 2021, 39, 615–637.
2. Prakasam, P.; Sayeed, S.; Ajayan, J. Guest editorials: P2P computing for 5G, beyond 5G (B5G) networks and internet-of-everything (IoE). Peer-to-Peer Netw. Appl. 2020, 14, 240–242.
3. Routray, S.K.; Mohanty, S. "Why 6G?". arXiv 2019, arXiv:1903.04837v1.
4. Dang, S.; Amin, O.; Shihada, B.; Alouini, M.-S. From a Human-Centric Perspective: What Might 6G Be? Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2020; Preprint November 2019.
5. Milovanovic, D.; Bojkovic, Z. 5G Mobile Networks: What is Next? Int. J. Commun. 2019, 4, 1–5. Available online: https://futurecomresearch.eu (accessed on 25 December 2021).

these systems, enable systematic transactions, events, and payments. The security using blockchains are immutable, i.e., they cannot be changed, deleted, or altered in any way after being recorded since [33]. Hence, in addition to speed and security, blockchains also enable the establishment of trust between users and parties in a transaction [34][35][36].

3. Recent Exploration of MFA Applications and Blockchain Authentication

Blockchain authentication refers to the system developed for increasing the security for the users and it verifies the users and connects it to the resources found on the technologies of digital currency, digital payments, transactions, and cryptocurrencies. The blockchain mainly uses the PKC, public-key cryptography, for the encryption of wallets and also the other places or links of the blockchain where the work of value has been stored. Thus, the authentication requirements for the blockchain increase similarities between the technology itself and the measures taken for securing it [37]. Multifactor authentication is referred to as a process of verification of users through at least two authentication factors [38]. The users can make use of an additional password, flash drive, special software, some particular files, and a flash drive containing important software. The MFA works in such a way that all layers of the verification need to be activated, then the user needs to provide proof of identity through the OTPs, passwords, etc. Although this method is not preferred by most Internet applications due to their security risks, blockchain applications use private keys for the identification of users [39].

There are different methods and techniques for ensuring the safety of the private key. Most of the time, there is a trade-off between security and usability. One of the methods proposes the security key to be placed in a single device without the addition of extra security [40]. However, anyone can access the unprotected device and obtain the keys. Users may use the knowledge of these devices as they need to enable them themselves. Digital wallets are commonly used for storage and access to blockchains [41][42][43][44][45]. They work by encrypting the security key/s by setting up a password. However, the security and key recovery are all challenges as there are numerous attacks on the passwords and security layers applied on the wallets [40]. Another method used for increasing security is using passwords to derive a combination of keys for accessing the information on the blockchains. When following this method, the private key needs to be unlocked so that previously defined passwords can be accessed during the creation of the key. This method is also prone to some disadvantages; one of the main disadvantages is that the user will be unable to change the password. Some devices possess computing capabilities that may be used with blockchain. Although these devices do not possess or support storage and they require zero understanding of the mechanism, it is highly susceptible to malware attacks [46].

Shin et al. [47] proposed a multifactor authentication procedure for WSNs in recent network applications that act in real-time but is found to be vulnerable to the collision of users and desynchronization attacks. Ni et al. [48] presented a service for authentication mechanism for 5G enabled IoT networks using key agreement mechanism by use of an anonymous key. However, after rigorous testing, it was revealed to be a single-level authentication, despite using a complex public key cryptosystem and a single authentication method is not suitable for 5G multiservice systems [49]. A robust MFA protocol was proposed by Huang et al. [50] for systems that use fragile

6. Wang, M.; Zhu, T.; Zhang, T.; Zhang, J.; Yu, S.; Zhou, W. Security and privacy in 6G networks: New areas and new challenges. Digit. Commun. Netw. 2020, 6, 281–291.

7. Li, Y.; Yu, Y.; Susilo, W.; Hong, Z.; Guizani, M. Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions. IEEE Wirel. Commun. 2021, 28, 63–69.

8. Yrjola, S. How Could Blockchain Transform 6G towards Open Ecosystemic Business Models? In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6.

9. Hewa, T.; Gur, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions. In Proceedings of the 2020 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, (6G SUMMIT), Levi, Finland, 17–20 March 2020.

10. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.-T.; Pirttikangas, S. Privacy-Aware Blockchain Innovation for 6G: Challenges and Opportunities. In Proceedings of the 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, 6G SUMMIT 2020, Levi, Finland, 17–20 March 2020.

11. Gürkaynak, G.; Yılmaz, I.; Yeşilaltay, B.; Bengi, B. Intellectual property law and practice in the blockchain realm. Comput. Law Secur. Rev. 2018, 34, 847–862.

12. Teufel, B.; Sentic, A.; Barmet, M. Blockchain energy: Blockchain in future energy systems. J. Electron. Sci. Technol. 2019, 17, 100011.

13. Khan, N.; Abdullah, J.; Khan, A.S. Towards vulnerability prevention model for web browser using interceptor approach. In Proceedings of the 2015 9th International Conference on IT in Asia (CITA), Sarawak, Malaysia, 4–5 August 2015.

14. Peters, G.W.; Panayi, E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking beyond Banks and Money; New Economic Windows; Springer: Cham, Switzerland, 2016; pp. 239–278.

15. Erdem, A.; Yildirim, S.; Angin, P. Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art. In Security, Privacy and Trust in the IoT Environment; Springer: Cham, Switzerland, 2019; pp. 97–122.

16. Khan, N.; Abdullah, J.; Khan, A.S. Defending Malicious Script Attacks Using Machine Learning Classifiers. Wirel. Commun. Mob. Comput. 2017, 2017, 5360472.

17. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaria, V. To Blockchain or Not to Blockchain: That Is the Question. IT Prof. 2018, 20, 62–74.

18. Andolfatto, D. Blockchain: What it is, what it does, and why you probably don't need one. Fed. Reserv. Bank St. Louis Rev. 2018, 100, 87–95.

combinations, based on two, standalone schemes, for authentication; however, these systems are not comprehensive, making them vulnerable to access attacks. Luo et al. [51] presented a flexible 3-factor authentication mechanism for various applications based on 5G multiservice systems. In this system, four different kinds of schemes can be provided for a user to ensure identity authentication and safety. The technique was slightly costly in terms of time efficiency. These issues are addressed by Luo et al. [52], who presented a Service-Based Architecture for 5G multiservice systems that build upon the work of Luo et al. [51] and uses an adaptable and decomposable 3-factor authentication system that can be applied simultaneously to ensure efficiency and speed. The tests on this system showed that it could provide an ideal efficiency in terms of transparency of action, security, and speed. However, further testing and real-time application are required. Wong et al. [53] also presented a 3-factor authentication scheme to ensure a high-security environment for communicating parties and integrates biometrics, password, and smart card authentication into a single system. Multiple server technologies are used to ensure that performance is quick and transparent. However, the technique still poses a communication cost.

There is limited research on the integration of multifactor analysis in blockchain-based applications. However, some papers were reviewed that can be valuable to indicate the benefits of these integrations. Antonio et al. [20] presented a multifactor analysis named 2FA for WordPress pages by using Hydro Raindrop multifactor authentication technology. In this paper, the researcher summarized the use of a blockchain-based two-factor authentication solution by a page on WordPress that contributes to securing user information. The study is not experimental, however, and the entire proposal is based on other theoretical and practical evidence. Overall, it suggested that the use of a decentralized technique provided by the integration of blockchain can enable multifactor and transparent user authentication, strengthening the security of information and the assets of individuals. Several studies also indicate the use of blockchain-based authentication procedures for autonomous vehicles [54][55][56]. In the study by Feng et al. [57], Blockchain-assisted privacy-preserving authentication system (BPAS) is presented to secure the data generated by vehicular ad hoc networks. This technique was proposed for ensuring accuracy as well as trust in the systems. However, there was a lack of support for batch verification in this entry that could provide an optimized verification in the form of blocks of data and hence reduce load on the resource consumption. Kebande et al. [19] also proposed an MFA based on Blockchain technology that proposed the use of an embedded Digital Signature (MFBC_eDS) that was found to be a suitable technique for countering the adversarial attacks on the Internet of vehicles in the past. Alharbi et al. [58] proposed a framework for authentication based on Blockchain technology as they claimed it could add more security to the authentication process. In this framework, the one-time password (OTP) is encrypted and sent to the application/website to complete the authentication process. This system was claimed to be safer than SMS-based authentication mechanisms, but it was less efficient in terms of time efficiency. Wu et al. [59] proposed an out-of-band 2factor authentication mechanism for IoT devices by use of blockchain to enable flexible, secure, and reliable authentication [60][61][62][63][64]. The overheads of blockchain use, however, were high. **Table 1** summarizes all the studies related to MFA and Blockchain.

Table 1. Summary of Reviewed MFA and Blockchain Technology Papers.

19. Kebande, V.R.; Awaysheh, F.M.; Ikuesan, R.A.; Alawadi, S.A.; Alshehri, M.D. A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles. Sensors 2021, 21, 6018.

20. Cardoso, J.A.A.; Ishizu, F.T.; De Lima, J.T.; Pinto, J.D.S. Blockchain Based MFA Solution: The use of hydro raindrop MFA for information security on WordPress websites. Braz. J. Oper. Prod. Manag. 2019, 16, 281–293.

21. Khan, N.; Abdullah, J.; Khan, A.S. A Dynamic Method of Detecting Malicious Scripts Using Classifiers. Adv. Sci. Lett. 2017, 23, 5352–5355.

22. Vishwa, A.; Hussain, F.K. A Blockchain based approach for multimedia privacy protection and provenance. In Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 18–21 November 2018; pp. 1941–1945.

23. Meunier, S. Blockchain 101: What is blockchain and how does this revolutionary technology work? In Transforming Climate Finance and Green Investment with Blockchains; Academic Press: Cambridge, MA, USA, 2018; pp. 23–34.

24. Pilkington, M. Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations; Xavier, F., Zhegu, O.M., Eds.; Edward Elgar Publishing: London, UK, 2015; pp. 225–253.

25. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. 2018, 57, 2117–2135.

26. Xiaolong, H.; Huiqi, Z.; Lunchao, Z.; Nazir, S.; Jun, D.; Khan, A.S. Soft Computing and Decision Support System for Software Process Improvement: A Systematic Literature Review. Sci. Program. 2021, 2021, 7295627.

27. Kersten, W.; Blecker, T.; Ringle, C.M. Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proc. Hambg. Int. Conf. Logist. 2017, 23, 533.

28. Zubair, S.; Fisal, N.; Abazeed, M.B.; Salihu, B.A.; Khan, A.S. Lightweight distributed geographical: A lightweight distributed protocol for virtual clustering in geographical forwarding cognitive radio sensor networks. Int. J. Commun. Syst. 2015, 28, 1–18.

29. Niranjanamurthy, M.; Nithya, B.N.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. Cluster Comput. 2019, 22, 14743–14757.

30. Faroukhi, A.Z.; El Alaoui, I.; Gahi, Y.; Amine, A. An Adaptable Big Data Value Chain Framework for End-to-End Big Data Monetization. Big Data Cogn. Comput. 2020, 4, 34.

31. Lin, W.; Yin, X.; Wang, S.; Khosravi, M.R. A Blockchain-enabled decentralized settlement model for IoT data exchange services. Wirel. Networks 2020, 1–15.

Study	Technologies Mentioned			Advantage/Contribution	Disadvantage/Gap
	MFA	BC	3/4/5G		
[50]	✓		✓	A robust and effective system for fragile communications between two nodes.	Vulnerable to access attacks.
[48]			✓	The authentication mechanism for 5G enabled IoT networks in the form of a service.	Not an MFA-based technique.
[51]	✓		✓	The flexible 3-factor authentication mechanism for various kinds of applications that are based on 5G multiservice systems.	Costly in terms of time efficiency.
[47]	✓		✓	Provides a multifactor authentication procedure for WSNs in recent network applications and may be extendible to future network advancements such as 6G.	Vulnerable to the collision of users and desynchronization attacks.
[53]	✓		✓	Multiple server technologies are used to ensure that performance is quick and transparent.	Technique still poses a communication cost as it integrates biometrics, password, and smart card authentication.
[52]	✓		✓	An adaptable and decomposable 3-factor authentication system that can be applied simultaneously to ensure efficiency and speed.	Further testing and real-time application are required.
[20]	✓	✓	✓	Hydro Raindrop multifactor authentication technology to conduct 2FA for WordPress.	Not experimental in nature.
[57]	✓	✓	✓	BPAS for ensuring accuracy as well as trust in the systems.	A lack of support for batch verification for an optimized verification in form of blocks of data and hence reduce the load on the resource consumption.
[19]	✓	✓	✓	Embedded Digital Signature-based MFA suitable technique for countering the adversarial attacks.	Overheads are high.
[58]	✓	✓	✓	More security to the authentication process as compared to SMS-based authentication protocols.	This system was claimed to be safer than SMS-based authentication mechanisms, but it was less efficient in terms of time efficiency.
[59]	✓	✓	✓	Flexible, secure, and reliable authentication.	The overheads of blockchain use, however, were high.

Int. J. Adv. Comput. Sci. Appl. 2018, 9, 298–304.

44. Aqeel, S.; Khan, A.S.; Ahmad, Z.; Abdullah, J. A comprehensive study on DNA based Security scheme Using Deep Learning in Healthcare. EDP Audit. Control. Secur. Newsl. 2021, 1–17.

45. Ahmad, Z.; Khan, A.S.; Shiang, C.W.; Abdullah, J.; Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. 2020, 32, e4150.

46. Espitia, A.; Ortega, K.; Romero, E.; Jaramillo, I. Authentication and digital signature USB device for telemedicine applications. In Proceedings of the 7th International Caribbean Conference on Devices, Circuits and Systems, ICCDCS, Cancun, Mexico, 28–30 April 2008.

47. Shin, S.; Kwon, T. A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. IEEE Access 2020, 8, 67555–67571.

48. Ni, J.; Lin, X.; Shen, X.S. Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT. IEEE J. Sel. Areas Commun. 2018, 36, 644–657.

49. Ahmad, Z.; Khan, A.S.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.; Tarmizi, S.; Rodrigues, J. Anomaly Detection Using Deep Neural Network for IoT Architecture. Appl. Sci. 2021, 11, 7050.

50. Huang, X.; Xiang, Y.; Bertino, E.; Zhou, J.; Xu, L. Robust Multi-Factor Authentication for Fragile Communications. IEEE Trans. Dependable Secur. Comput. 2014, 11, 568–581.

51. Luo, Y.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. DIAM: Diversified Identity Authentication Mechanism for 5G Multi-Service System. In Proceedings of the 2019 International Conference on Computing, Networking and Communications, ICNC 2019, Honolulu, HI, USA, 18–21 February 2019; pp. 418–424.

52. Luo, Y.; Li, H.; Ma, R.; Guo, Z. A Composable Multifactor Identity Authentication and Authorization Scheme for 5G Services. Secur. Commun. Netw. 2021, 2021, 6697155.

53. Wong, A.M.-K.; Hsu, C.-L.; Le, T.-V.; Hsieh, M.-C.; Lin, T.-W. Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks. Sensors 2020, 20, 2511.

54. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors 2019, 19, 4954.

55. Khan, A.S.; Ahmad, Z.; Abdullah, J.; Ahmad, F. A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. IEEE Access 2021, 9, 87079–87093.

56. Khan, A.S.; Iqbal, A.M. Mobile Multihop Relay WIMAX Networks: A Security Perspectives; Universiti Malaysia Sarawak: Sarawak, Malaysia, 2018.

57. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. IEEE Trans. Ind. Inform. 2020, 16, 4146–4155.

58. Alharbi, E.T.; Alghazzawi, D. Two Factor Authentication Framework Using OTP-SMS Based on Blockchain ScaleUp View project Workflow Execution Time Predictions in Distributed Systems View project. Trans. Mach. Learn. Artif. Intell. 2019, 7, 17–27.
59. Wu, L.; Du, X.; Wang, W.; Lin, B. An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. In Proceedings of the International Conference on Computing, Networking and Communications, Maui, HI, USA, 5–8 March 2018; pp. 769–773.
60. Saqib, R.M.; Khan, A.S.; Javed, Y.; Ahmad, S.; Nisar, K.; Abbasi, I.A.; Haque, M.R.; Julaihi, A.A. Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security. Intell. Autom. Soft Comput. 2022, 32, 1633–1647.
61. Javed, Y.; Khan, S.; Khan, A.S.; Qahar, A.; Abdullah, J. Preventing DoS Attacks in IoT Using AES Static Analysis of Web Applications View project Cloud Robotics View project Preventing DoS Attacks in IoT Using AES. J. Telecommu-Nication Electron. Comput. Eng. 2018, 9, 3–11. Available online: https://www.researchgate.net/publication/322243661 (accessed on 29 December 2021).
62. Javed, Y.; Khan, S.; Khan, A.S.; Qahar, A.; Abdullah, J. EEoP: A Lightweight Security Scheme over PKI in D2D Cellular Networks. J. Telecommun. Electron. Comput. Eng. (JTEC) 2017, 9, 99–105. Available online: https://jtec.utem.edu.my/jtec/article/view/3191 (accessed on 29 December 2021).
63. Khan, N.; Ahmad, F.; Khan, S.; Abdullah, J.; Khan, N.; Julahi, A.A.; Tarmizi, S. Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks. IJCSNS Int. J. Comput. Sci. Netw. Secur. 2017, 17, 357.
64. Khan, A.S.; Lenando, H.; Abdullah, J.; Fisal, N. Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. J. Teknol. 2015, 73, 75–81.