International Journal of Research in Circuits, Devices and Systems

E-ISSN: 2708-454X
P-ISSN: 2708-4531
IJRCDS 2022; 3(2): 74-80

www.circuitsjournal.com
Received: 09-04-2022
Accepted: 15-05-2022

Akash R
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu, India

Corresponding Author:
Akash R
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu, India

Blockchain for mobile cellular networks: Recent advances and future use

Akash R

Abstract
After the deployment of fifth-generation (5G) wireless networks worldwide it has become common to see people using it in their everyday life. But with pace of our technological developments even 5G network seems slower with time. This caused various researchers to work on sixth-generation (6G) wireless communications to solve this problem. As expected from any form of update in technology, people will always have high hopes for the performance of the newer version. So, 6G networks is expected to accommodate numerous heterogeneous devices and infrastructures with more efficiency and security. The problem comes with the question of how to achieve such an efficient network. After some research by various researchers, it is found that the answer for this question lies in Blockchain technology.
In this review paper, we will see a comparative study of the different methods used by different researcher to achieve an efficient cellular network with Blockchain technology. This paper also discusses about what future such a network holds and the possible problems this network may face in the near future. This paper shall help the researchers working on 6G networks to analyze whether implementing block chain in mobile cellular networks is efficient and also help them to plan ahead on how to deal with the problems in the near future that are discussed in this paper.

Keywords: Cellular network, block chain, future technology, 6G, smart era

1. Introduction
Lately the interest in using Blockchain as a protected and distributed record has expanded drastically. Due to the fact that Blockchain is so secure, it has the potential to grow to be a bedrock of the worldwide record-keeping systems. It was created by unknown persons behind the online cash currency Bitcoin under the pseudonym of Satoshi Nakamoto. Although the main reason for using Blockchain in Bitcoin was about digital currency and distributed exchanges, its application to different frameworks has been broadly increased. It is found by many researchers that telecommunication has likely potential outcomes to profit from Blockchain. The Blockchain can give a dispersed HSS such that the core networks of various operators can utilize it in a secure way. Blockchain can set up helpful trust among discrete organization substances and work with, subsequently introducing another worldview towards 6G. In this review article, we will find out with regards to the impact of blockchain in the headway of cell network advances.
Blockchain is equipped for settling various trust and security related issues in correspondence organizations, working with more productive asset sharing, boosting confided in information association, secure access control and protection assurance, and giving tracing, confirmation and oversight functionalities for 5G and future 6G organizations (Wang, J., Ling, *et al*., 2021) [4].
Blockchains have as of late got expanding consideration as a promising innovation for giving distributed and secure solutions (Zhang, S., Cao, Y., *et al*., 2020) [3]. They are open data sets that ensure information security by em- powering anonymous and dependable exchanges on an immutably distributed ledger record without the assistance of a focal intermediary. (Firdaus, M., & Rhee, K. H., 2020). Every exchange is recorded with a timestamp to be approved by the agreement system before it is put away on a block chain network. Blockchain is secure by design in offering a few elements, like decentralization, recognizability, transparency, and permanent exchanges (Xue, J., Xu, C., & Zhang, Y., 2018).

2. Background

2.1 Blockchain

Blockchain is a particular kind of data set. It contrasts from a common data set in the manner it stores data. Blockchains store information in blocks that are then binded together. As new information comes in it is gone into a new block. When the block is loaded up with information it is anchored onto the past block, which makes the information fastened together in sequential request. Various sorts of data can be put away on a blockchain however the most well- known use so far has been as a record for exchanges. Blockchains can be ordered in two measurements – public and private (Tschorsch and Scheuermann, 2016) [13]. The primary distinction among public and private blockchains lies in verification, for example who can access the blockchain. For the most part, in open blockchains, anybody can join the blockchain, while in private blockchains, the proprietors control the access to the blockchain. Then again, the fundamental contrast among permission less and permissioned blockchains lies in approval, for example who can control the blockchain. Generally, in permission less blockchains, anybody can refresh information in the blockchain, though just approved substances are permitted to take an interest in permissioned blockchains. Remarkably, consortium blockchains are permissioned and semi-private. Contrasted and a private blockchain that is regularly constrained by a solitary proprietor, a consortium blockchain is mutually kept up with by controlled hubs that are from various associations or people. It very well may be viewed as a to some degree decentralized blockchain that can be independent and control- lable while guaranteeing the general security, and it is a reasonable choice for managing multilateral issues and building up trust between numerous gatherings. So, a fitting sort of blockchain is carefully chosen by the particular applications.

For Bitcoin's situation, blockchain is utilized in a decentralized way so that no single individual or group has control—rather, all clients aggregately hold control. Decentralized blockchains are permanent, which implies that the information entered is irreversible. For Bitcoin, this implies that exchanges are forever recorded and visible to anybody.

2.2 Conventional Mobile cellular networks vs Blockchain assisted cellular networks

The regular cell network designing relies upon a system of fixed base hand- set stations (BTSs) related with the wired focus association. Diverse radio advances for the public security network have been inspected. The typical public security traffic is for the most part light, however when a huge event occurs, the traffic interest at the scene can be essentially heavier than that in a business association. If the cross country public prosperity network accepts a comparative designing as a business association, the sending of BTSs ought to be satisfactorily adequately dense to fulfill the zenith need of public security customer gear (UE), including both routine UE and scene UE. Thus, the cost to manufacture and work a system of fixed BTSs to help the most negative situation traffic is difficult to bear by open security customers and residents. Also, the utilization of the association is low as a rule, in light of the fact that the standard traffic is a ton of lower than the zenith traffic.

The cost of the public security network per unit space of consideration has strong consequences in its gathering and for the most part accomplishment. Plus, it has been recorded that the most generally perceived reason for communication failure is a result of destruction of physical infrastructures. If we simply rely upon the appropriate organization, the network is sensitive, considering the way that it is hard to avoid the real harm on the physical level when a disaster like a earthquake or storm occurs (Chen, X., and Guo, D., 2016) [5].

In the standard plan of organization associations, each admin covers the whole geological space of interest like a country, a domain, etc. Each manager can pass on its own access organization or propose their access network resources with various executives to diminish the system costs. Regardless, satisfying the necessities of 5G by sending dense little cells that has an incredibly low coverage area (i.e., 10-100 m) would be extravagant for admins to cover the whole geological district inside a country. Thusly, to lessen both capital expenses and utilitarian expenses, managers can benefit from each other by separating the inclusion areas. The plan with Blockchain as a SON could be extraordinarily useful at whatever point if used properly. With Blockchain advancement, executives can assist each other by dividing the entire geological district to be covered among all of them and deal various sorts of help to customers from various overseers. Thus, a circulated trade ought to be conceivable among them in a secured environment without the need of any central third person (Mafakheri, B., Subramanya, *et al*., 2018) [2].

3. Integration of the blockchain and cellular networks

3.1. Blockchain-Assisted Information Distribution

With regards to wireless networks, the blockchain can be used to give a disseminated and secure network for cutting edge wireless network by diminishing the managerial cost of the unique access. Blockchains can likewise set up secure and trusted data sharing and resource allocation frameworks in wireless networks (Dai, Y., Xu, *et al*.).

Additionally, by utilizing the MEC structure, blockchains are relied upon to be conveyed to end clients' cell phones. In a framework done by Veeramani UE is used. UE has the ability to lead mining undertakings and take part in the agreement component of the blockchain network. Notwithstanding, as a result of UE asset limitations, these undertakings can be offloaded to local ENs to accomplish better calculation and decrease energy utilization. So, blockchain and MEC empower computational offloading to ENs, while regarding client protection and ensuring exchange security in an appropriated way (Veeramani, K., and Jaganathan, S., 2020) [7].

3.2. Blockchain networking

The huge development of different mobile services requests a huge amount of network resources, e.g., spectra and frameworks, which are for the most part restricted and must be shared for better usage and proficiency (Zhao, Q., and Sadler, B. M., 2007) [8]. However, in practice, resource sharing is frequently deflected by the division among resource hosts, who might need impetus or have cost and security concerns, making coordination and participation between network substances infeasible.

Then again, with the new functionalities of cloud processing, MEC, software-defined networking (SDN) and network functions virtualization (NFV) in 5G frameworks, there are expanding types and amounts of network

resources, e.g., computing and storage resources as well as network slices, which makes resource management and sharing very testing. Blockchain and its innate attributes can successfully advance joint effort and mitigate the trust and security worries among separated network entities, hence prompting more proficient resource sharing as found in Fig. 1.

Fig 1: Resource sharing

3.2.1 Spectrum sharing

There has been concentrated research around applying blockchain to spectrum sharing. Weiss *et al*. (Weiss, M. B., Werbach, K., *et al*., 2019) [9] investigated how to execute spectrum management in mix with blockchain and examined the advantages and disadvantages of various spectrum sharing instruments. Han and Zhu proposed a spectrum sharing framework among network operators dependent on consortium blockchain which ensures reliable privacy and security guarantees.

3.2.2 Computing and storage mechanism

The wide utilization of cloud processing and MEC makes computing and storage capacities significant network resources, which can be proficiently overseen by blockchain (Guo, S., Dai, *et al*., 2019) [14] a blockchain-based calculation offloading framework that upgrades the coordinated effort among entities in sharing computing resources.

3.2.3 Infrastructure of device

Blockchain presents a protected and proficient way of overseeing heterogeneous gadgets and frameworks in 5G and IoT networks. Mafakheri *et al*. (Salsano, S., Samak, T., *et al*., 2018) [2] investigated blockchain to satisfy sovereign, independent and trusted framework partaking in 5G small cell networks. Dong *et al*. (Dong, Z., Luo, F., *et al*., 2018) [16] considered utilizing blockchain as a protected, dispersed cyber infrastructure for the future lattice and proposed a model to enhance energy foundation allotment and further develop energy effectiveness. Huh *et al*. (Huh S, Cho S, *et al*., 2017) [17] proposed a strategy to utilize blockchain to control and arrange IoT gadgets, and attempted the identity management for interconnected gadgets. Novo *et al*. (Novo, O., 2018) [18] introduced a few blockchain-based answers for alleviate the issues related with the administration of various compelled gadgets. In Ref. (Košťál, K., Helebrandt, P., *et al*., 2019) [19], a private-blockchain-based design for the administration and observing of IoT gadgets was presented.

4. Secure access control

The constant densification of wireless networks and expanding heterogeneity of gigantic gadgets bring numerous security dangers to access control in mobile communication systems. In particular, there are mostly three classifications of safety hazard: gadget security hazard brought about by noxious gadget interruption, framework security hazard because of the weak link and information security hazard coming about because of data leakage. Based on its inborn nature, for example, alter obstruction, decentralization and fine-grained auditability, blockchain presents a promising solution for address these security hazards in wireless networks.

4.1 Device access control

Given the large number of different devices in the mobile communication network, there are unavoidably malevolent devices attempting to compromise the security of the framework. A few works have considered utilizing blockchain to prevent such malevolent device (Javaid U, Siang AK, *et al*., 2018) [20] (Pinno OJA, Gregio ARA, *et al*., 2017) [21] (Zhang, Y., Kasahara, *et al*., 2018). Javaid *et al*. (Javaid U, Siang AK, *et al*., 2018) [20] embraced a customized smart contract to safeguard against DDoS attacks and malicious device attacks. Pinno *et al*. (Pinno OJA, Gregio ARA, *et al*., 2017) [21] designed an access control architecture called ControlChain, which gives a safe way of making connections for network entities and relegate them attributes. Additionally, Zhang *et al*. (Zhang, Y., Kasahara, *et al*., 2018) [22] proposed an access control framework containing three smart contracts to securely add, refresh and erase network entity identities.

4.2 System access control

In addition to these malicious device intrusion, the traditional access control systems additionally face the danger of single points of failure because of the way that they depend on centralized entities. Some characteristics like decentralization and joint support in blockchain can promptly forestall the single points of failure. A few scientists have attempted to incorporate blockchain with access control mechanism to tackle this worry (Huh S, Cho S, *et al*., 2017) [17] (Novo, O., 2018) [18]. Ding *et al*. (Ding, S., Cao, J., *et al*., 2019) [23] proposed a quality-based access control scheme for IoT, which uses blockchain to record the distribution of attributes to avoid single points of failure and data altering. Additionally, Xu *et al*. (Xu R, Chen Y, *et al*., 2018) [24] concocted an identity-based robust capability token management strategy, which utilizes smart contracts to register, spread and deny access authorization.

4.3 Data access control

These days, clients have huge worries around information security, while in centralized access control mechanisms information security stays at a low level, as centralized entities might control and leak client information as they wish. A few researches have presented blockchain innovation in access control to address information security issues. Ouaddah *et al*. (Ouaddah, A., Abou Elkalam, *et al*. 2016) [25] understood the security and obscurity of IoT information by sending reasonable access in UTXOs to carry out blockchain-based access control. Besides, Le *et al*. (Le T, Mutka MW, *et al*., 2018) [26] proposed an access control scheme called CapChain, which utilizes the anonymity of the blockchain to conceal key data for information sharing and assignment to guarantee information security. Likewise, Cha *et al*. (Cha, S. C., Chen,

J. F., 2018) [24] implemented a novel blockchain-empowered gateway, which acts as a middle person among clients and IoT devices, subsequently improving information security in IoT access control.

5. Functionalities of Blockchain

With the constant expansion of mobile networks and enhancement of administrations, the requests for data discernibility, device accreditation and data management become earnest, and the basic network data will not be wrongfully gotten to, illegally controlled and erroneously spread. The current countermeasures that utilize third-party servers to give in data storage, device certification and tracking services experience the ill effects of protection and security issues. Blockchain was brought into the world with elements like immutability, openness and transparency and is considered a best solution for these worries.

5.1 Tracing

Blockchain can give a full scope of credible records and security guarantees for tracking network entities through the obligatory activities in consensus mechanisms and smart contracts, which guarantee the uprightness and security of the information and transactions in blockchain. In Refs. (Tian, F., 2018) [28] and (Caro, M. P., *et al*., 2018) [29], blockchain was proposed to upgrade the discernibility of IoT devices. Mitani *et al*. (Mitani, T., and Otsuka, A., 2020) [30] formulated a asset tracing technique in which a blended blockchain structure is taken on. Watanabe *et al*. (Patel, D., Nandi, S., *et al*., 2019) [31] planned another token to improve the traceability of blockchain data. Alkhader *et al*. (Alkaabi, N., Salah, *et al*., 2020) [32] utilized smart contracts to track and oversee industrial transactions in manufacturing.

5.2 Certification

By taking on blockchain, mobile service providers (SPs) can save and certificate devices and data transparently and dependably. Kleinaki *et al*. (Kleinaki, A. S., Mytis-Gkometh, *et al*., 2018) [33] presented a blockchain-based certification service that uses smart contracts to seal biomedical database inquiries and results. Additionally, in Refs. (Kubilay, M. Y., Kiraz, *et al*. 2019) [34], (Wang, Z., Lin, J., 2020) [35] blockchain was proposed to build up the security of device certificates in PKI systems. It proposed a digital certificate system dependent on blockchain, carrying out anti-counterfeiting and verifiable digital certificates. Xie *et al*. (Xie, R., Wang, Y., 2020) [35] planned a blockchain-driven certification system to accomplish proficient and secure declaration queries and approvals.

5.3 Supervision

Blockchain normally obliges to the prerequisites of data management. It was brought into the world with the capacities of g securing regulatory data and improving the proficiency of management and organization. Lin *et al*. (Lin S, Li J, *et al*., 2018) [35] proposed a blockchain management model for e-government dependent on a threshold ring signature algorithm. Peng *et al*. (Peng, S., Hu, X., *et al*., 2020) [38] proposed a vaccine production supervision mechanism dependent on a two-layer blockchain. Also, Liu *et al*. (Liu, C., Xiao, *et al*., 2018) [39] planned a blockchain-based independent transaction settlement framework for IoT web-based business, which permits all network participants to mutually oversee the settlement interaction.

6. Blockchain Radio Access Network (B-RAN) For 6G

In this segment, we propose B-RAN as a bound together structure of blockchain-empowered wireless communications for 6G networking. Upon the portrayal of the B-RAN worldview for 6G, we have also given a top to bottom conversation on the basic components of B-RAN, including consensus mechanisms, smart contract, trustworthy access, mathematical modeling, cross-network sharing, data tracking and auditing, and intelligent networking in the previous point of this research paper.

The idea of B-RAN offers an original worldview for huge scope, heterogeneous and dependable wireless networks (Ling, X., Wang, *et al*., 2019) [40]. B-RAN goes about as an open and unified system for assorted applications to accomplish resource pooling and sharing across areas and presents an appealing solution for future 6G network. B-RAN joins innately untrustworthy network elements with no mediator and oversees network access, authentication, authorization and accounting through trustful interactions. By means of B-RAN, a MSP is set up to connect different parties and facilitate resource and data sharing in a helpful, adaptable and secure way. B-RAN can't only just dynamically share computing, caching and communicating capabilities, yet in addition convey and spread knowledge across subnetworks. Federated-style learning can additionally optimize under-utilized resource allocation and network services in B-RAN. As a blockchain as-a-administration (BaaS) stage, B-RAN has particular security properties and is relied upon to give improved functionalities of data exchange, privacy protection, tracking, supervision, etc.

7. Potential risks in future

7.1. Alternative history attack

A hacker can dispatch an alternative history attack for double spending by secretly mining an alternative fork, which really uncovered the weakness of distributed frameworks (Nakamoto, S., 2008) [10]. Or he can undermine a confirmed chain accepted by the miner network in case it is adequately fortunate to make longer fraudulent chain. In PoW, if the hacker holds over half of the computational force of the whole blockchain network then it can generally alter a confirmed history successfully.

7.2. Selfish mining

The critical idea of selfish mining is to build an attackers' winning probability by allowing the honest miners squander power on the public chain (Eyal, I., and Emin, G. S. 2014) [11]. At the point when an attacker tracks down a valid block, it keeps mining the following block without delivering the recently created block. Until different miners track down a valid block, the attacker will distribute all blocks recently mined to the network successfully.

7.3. Cryptanalytic attack

On a fundamental level, cryptanalytic assaults (for example key assault and quantum assault) in blockchain mean to break the cryptographic algorithm and uncover its keys. The blockchain foundation can't be isolated from cryptographic algorithms. For instance, Hyperledger Fabric depends on the elliptic curve digital signature algorithm (ECDSA) to create private keys, yet the ECDSA is defenseless against key attacks (Mayer, H., 2016) [12]. Usually, a key attack happens indistinctly on account of the private key leakage weakness

and feeble randomness of key generation. Further, the researchers to refer some interesting articles on Blockchain and its uses in several other sectors (Tyagi *et al*. 2019, 2020, 2021 and 2022) for their future research.

8. Conclusion

In this paper, we have known about the impact of blockchain technology in mobile cellular and wireless networks. We have identified the critical trust-related issues in wireless networks that impede the evolution of current 5G networks towards more efficient and secure 6G networks. Upon a brief introduction of the fundamentals of blockchain, we comprehensively investigated the recent research works on applying blockchain to wireless networks from several aspects, including spectral sharing and trusted data interaction. We have also learned about some risks that this could possess in the future.

References

1. Wang J, Ling X, Le Y, Huang Y, You X. Blockchain enabled wireless communications: A new paradigm towards 6G. National Science Review. 2021.
2. Mafakheri B, Subramanya T, Goratti L, Riggio R. Blockchain-based infrastructure sharing in 5G small cell networks. In 2018 14th International Conference on Network and Service Management (CNSM), 2018, Nov, 313-317pp. IEEE.
3. Zhang S, Cao Y, Ning Z, Xue F, Cao D, Yang Y. A heterogeneous IOT node authentication scheme based on hybrid blockchain and trust value. KSII Transactions on Internet and Information Systems (TIIS). 2020;14(9):3615-3638.
4. Xue J, Xu C, Zhang Y. Private blockchain-based secure access control for smart home systems. KSII Transactions on Internet and Information Systems (TIIS). 2018;12(12):6057-6078.
5. Chen X, Guo D. Public safety broadband network with rapid-deployment base stations. In Wireless Public Safety Networks. 2016;2:173-198. Elsevier.
6. Dai Y, Xu D, Maharjan S, Chen Z, He Q, Zhang Y. Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE network. 2019;33(3):10-17.
7. Veeramani K, Jaganathan S. Land registration: use-case of e-Governance using blockchain technology. KSII Transactions on Internet and Information Systems (TIIS). 2020;14(9):3693-3711.
8. Zhao Q, Sadler BM. A survey of dynamic spectrum access. IEEE signal processing magazine. 2007;24(3):79-89.
9. Weiss MB, Werbach K, Sicker DC, Bastidas CEC. On the application of blockchains to spectrum management. IEEE Transactions on Cognitive Communications and Networking. 2019;5(2):193-205.
10. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 2008, 21260.
11. Eyal I, Emin GS. Majority is not enough: Bitcoin mining is vulnerable. In proceedings of the international conference on financial cryptography and data security, Christ Church, Barbados. 2014.
12. Mayer H. ECDSA security in bitcoin and ethereum: A research survey. Coin Faabrik. 2016 June;28(126):50.
13. Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials. 2016;18(3):2084-2123.
14. Guo S, Dai Y, Xu S, Qiu X, Qi F. Trusted cloud-edge network resource management: DRL-driven service function chain orchestration for IoT. IEEE Internet of Things Journal. 2019;7(7):6010-6022.
15. Salsano S, Samak T, dos Santos CRP. 14th International Conference on Network And Service Management (Cnsm 2018) And Workshops.
16. Dong Z, Luo F, Liang G. Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy. 2018;6(5):958-967.
17. Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. In: 19th International Conference on Advanced Communication Technology, Pyeong Chang, Korea. Piscataway, NJ: IEEE Press, 2017, 464-7.
18. Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal. 2018;5(2):1184-1195.
19. Košťál K, Helebrandt P, Belluš M, Ries M, Kotuliak I. Management and monitoring of IoT devices using blockchain. Sensors. 2019;19(4):856.
20. Javaid U, Siang AK, Aman MN, *et al*. Mitigating loT device based DDoS attacks using blockchain. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany. New York: Association for Computing Machinery, 2018, 71-6.
21. Pinno OJA, Gregio ARA, Bona LCED. ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: IEEE Global Communications Conference, Singapore. Piscataway, NJ: IEEE Press, 2017, 1-6.
22. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the internet of things. IEEE Internet of Things Journal. 2018;6(2):1594-1605.
23. Ding S, Cao J, Li C, Fan K, Li H. A novel attribute-based access control scheme using blockchain for IoT. IEEE Access. 2019;7;38431-38441.
24. Xu R, Chen Y, Blasch E, *et al*. Blendcac. A blockchain-enabled decentralized capability-based access control for IoTs. In: IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, Halifax, Canada. Piscataway, NJ: IEEE Press, 2018, 1027-34.
25. Ouaddah A, Abou Elkalam A, Ait Ouahman A. Fair Access: A new Blockchain-based access control framework for the Internet of Things. Security and communication networks. 2016;9(18):5943-5964.
26. Le T, Mutka MW. Cap Chain. A privacy preserving access control framework based on blockchain for pervasive environments. In: IEEE International Conference on Smart Computing, Taormina, Italy. Piscataway, NJ: IEEE Press, 2018, 57-64.
27. Cha SC, Chen JF, Su C, Yeh KH. A blockchain connected gateway for BLE-based devices in the internet of things. ieee access. 2018;6:24639-24649.
28. Tian F. IEEE 2016 13th International Conference on Service Systems and Service Management (ICSSSM)-Kunming, China (2016.6. 24-2016.6. 26). 2016.
29. Caro MP, Ali MS, Vecchio M, Giaffreda R. IoT

Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany). Tuscany, Italy, 2018, 8-9.
30. Mitani T, Otsuka A. Traceability in permissioned blockchain. IEEE Access. 2020;8:21573-21588.
31. Patel D, Nandi S, Mishra BK, Shah D, Modi CN, Shah K, Bansode RS. IC-BCT 2019. Springer Singapore. 2020.
32. Alkaabi N, Salah K, Jayaraman R, Arshad J, Omar M. Blockchain-based traceability and management for additive manufacturing. IEEE access, 8, 188363-188377.
33. Kleinaki AS, Mytis-Gkometh P, Drosatos G, Efraimidis PS, Kaldoudi E. A blockchain-based notarization service for biomedical knowledge retrieval. Computational and structural biotechnology Journal. 2018;16:288-297.
34. Kubilay MY, Kiraz MS, Mantar HA. Cert Ledger: A new PKI model with Certificate Transparency based on blockchain. Computers & Security. 2019;85:333-352.
35. Wang Z, Lin J, Cai Q, Wang Q, Zha D, Jing J. Blockchain-based certificate transparency and revocation transparency. IEEE Transactions on Dependable and Secure Computing. 2020.
36. Xie R, Wang Y, Tan M, Zhu W, Yang Z, Wu J, *et al*. Ethereum-blockchain-based technology of decentralized smart contract certificate system. IEEE Internet of Things Magazine. 2020;3(2):44-50.
37. Lin S, Li J, Liang W. Research on strong supervision algorithm model based on blockchain in e-government. In: 5th IEEE Information Technology and Mechatronics Engineering Conference, Chongqing, China. Piscataway, NJ: IEEE Press, 2020, 345-9.
38. Peng S, Hu X, Zhang J, Xie X, Long C, Tian Z, *et al*. An efficient double-layer blockchain method for vaccine production supervision. IEEE Transactions on Nano Bioscience. 2020;19(3):579-587.
39. Liu C, Xiao Y, Javangula V, Hu Q, Wang S, Cheng X. Norma chain: A blockchain-based normalized autonomous transaction settlement system for iot-based e-commerce. IEEE Internet of Things Journal. 2018;6(3):4680-4693.
40. Ling X, Wang J, Bouchoucha T, Levy BC, Ding Z. Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. IEEE Access. 2019;7:9714-9723.
41. Nair MM, Tyagi AK. Preserving Privacy Using Blockchain Technology in Autonomous Vehicles. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems, 2022, 481. Springer, Singapore. https://doi.org/10.1007/978-981-19-3182-6_19
42. Tyagi AK, Chandrasekaran S, Sreenath N, Blockchain Technology: A New Technology for Creating Distributed and Trusted Computing Environment," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, 1348-1354. doi: 10.1109/ICAAIC53929.2022.9792702.
43. Sheth HSKIAK, Tyagi AK. Deep Learning, Blockchain based Multi-layered Authentication and Security Architectures, 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, 476-485pp. doi: 10.1109/ICAAIC53929.2022.9793179.
44. AK V, AK Tyagi, Kumar SP. Blockchain Technology for Securing Internet of Vehicle: Issues and Challenges, 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, 1-6pp. doi: 10.1109/ICCCI54379.2022.9740856.
45. Pandey AA, Fernandez TF, Bansal R, Tyagi AK. Maintaining Scalability in Blockchain. In: Abraham, A, Gandhi N, Hanne T, Hong TP, Nogueira Rios T, Ding W. (eds) Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems, vol 418. Springer, Cham. https://doi.org/10.1007/978-3-030-96308-8_4
46. Agrawal D, Bansal R, Fernandez TF, Tyagi AK. Blockchain Integrated Machine Learning for Training Autonomous Cars. In: *et al*. Hybrid Intelligent Systems. HIS 2021. Lecture Notes in Networks and Systems, 2022, 420. Springer, Cham. https://doi.org/10.1007/978-3-030-96305-7_4
47. Amit Kumar Tyagi. Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era' Perspective: The Challenges and a Way Forward", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.
48. Amit Kumar Tyagi, Rekha G, Shabnam Kumari. Applications of Blockchain Technologies in Digital Forensic and Threat Hunting, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.
49. Tibrewal I, Srivastava M, Tyagi AK. Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. 2022. https://doi.org/10.1007/978-981-16-6542-4_1
50. Tyagi AK, Fernandez TF, Aswathy SU. Blockchain and Aadhaar based Electronic Voting System," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2020, 498-504pp. doi: 10.1109/ICECA49313.2020.9297655.
51. Amit Kumar Tyagi, Aswathy SU, Aghila G, Sreenath N. AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology IJIN. 2021 Oct;2:175-183.
52. Sawal Neha, Yadav Anjali, Tyagi Amit Kumar, Sreenath N, Rekha G. Necessity of Blockchain for Building Trust in Today's Applications: An Useful Explanation from User's Perspective (May 15, 2019). Available at SSRN: https://ssrn.com/abstract=3388558 or http://dx.doi.org/10.2139/ssrn.3388558
53. Siddharth M. Nair, Varsha Ramesh and Amit Kumar Tyagi, Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications, Book: Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles, 2021, 14pp. DOI: 10.4018/978-1-7998-3295-9.ch012
54. Mishra S, Tyagi AK. Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technology," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, 123-128pp. doi: 10.1109/I-

SMAC47947.2019.9032557.
55. Varsha R, *et al*. 'Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles'. International Journal of Hybrid Intelligent System. 2020 Jan, 1;16(4):223-236
56. Krishna AM, Tyagi AK. Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology, 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, 1-8pp. doi: 10.1109/ic-ETITE47903.2020.332.
57. Deshmukh N, Sreenath AK, Tyagi, UV Eswara Abhichandan. Blockchain Enabled Cyber Security: A Comprehensive Survey, 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, 1-6pp. doi: 10.1109/ICCCI54379.2022.9740843.
58. Tyagi AK, Agarwal D, Sreenath N. Sec VT: Securing the Vehicles of Tomorrow using Blockchain Technology, 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, 1-6pp. doi: 10.1109/ICCCI54379.2022.9740965.
59. Nair MM, Tyagi AK, Sreenath N. The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges, 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, 1-7pp. doi: 10.1109/ICCCI50826.2021.9402498.
60. Tyagi AK, Abraham A. (Eds.). Recent Trends in Blockchain for Information Systems Security and Privacy (1st ed.). CRC Press. https://doi.org/10.1201/9781003139737
61. Tyagi AK, Rekha G, Sreenath N. (Eds.). Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. IGI Global. 2021. http://doi:10.4018/978-1-7998-3295-9