The Role of Blockchain Integration in Edge Computing for 6G IoT: Challenges and Applications

Abdulwadood Alawadhi
InterNetWorks Research Laboratory, School of Computing
Universiti Utara Malaysia
Sintok-Kedah, Malaysia
alawadhi@uum.edu.my

Abdullah Almogahed
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Parit Raja, Johor, Malaysia
abdullahm@uthm.edu.my

Bushra Abdullah Shtayt
Information Technologies Management, Management Technical College of Basra, Southern Technical University
Basra, Iraq
bushra.abdullah@stu.edu.iq

Samera Obaid Barraood
Department of Computer Science College of Computers and Information Technology
Hadhramout University
Hadhramout, Yemen
s.barraood@hu.edu.ye

Mohammad Ibrahim Adawy
Faculty of Information Technology)
The World Islamic Sciences and Education University
Amman, Jordan
Mohammad.adawi@wise.edu.jo

Omar Al-Jamili
School of Computing
Universiti Utara Malaysia
Sintok-Kedah, Malaysia
omaraljamili@gmail.com

***Abstract*—Blockchain is the technology on which cryptocurrencies operate within the 6G Internet of Things. Due to its flexibility, it has received significant adoption in numerous applications as a possible distributed data management solution. Nonetheless, a significant obstacle that impedes blockchain's potential is its constrained scalability, which limits its capacity to facilitate applications requiring frequent transactions. Conversely, edge computing, an innovative technology, addresses the limitations of conventional cloud-based systems by decentralizing cloud functionalities and alleviating problems such as elevated latency and insufficient security. Nonetheless, edge computing presently encounters challenges related to decentralized governance and security. As a result, the integration of blockchain and edge computing within a cohesive framework offers substantial benefits, such as dependable network access and governance, decentralized storage, and computing at the peripheries. This integration effectively mitigates many security problems and guarantees data integrity in edge computing contexts. This article offers a comprehensive analysis of blockchain technology, its attributes, and its relevance in the context of 6G. Additionally, it investigates the amalgamation of blockchain and edge computing, analyzes diverse application cases, and addresses the related issues. Finally, the report delineates contemporary research trajectories and draws conclusions based on the findings.**

Keywords—Blockchain, 6Generation, Edge computing, Internet of things, Application

INTRODUCTION

The sixth-generation (6G) mobile communication technology, which will enable comprehensive interconnectivity through the Internet of Things (IoT) in the future, is the culmination of ongoing advancements in communication technology and scientific research. Anticipated benefits of 6G-IoT networks include unprecedented mobile broadband speeds, minimal communication delays, and extensive device connectivity. Various sectors view 6G-IoT as a catalyst for progress. However, efficiently managing the arge number high-speed data transfers, real-time applications, and networked devices required by 6G-IoT networks presents significant resource challenges. Traditional resource allocation techniques may encounter increased transmission delays. Therefore, the need to optimize resource utilization in 6G-IoT networks to reduce latency has become urgent [1,2].

In the 6G-IoT environment, edge computing enables an edge server near the data generator, including smart homes or sensors/mobile devices, to perform certain data computations. This approach enhances the performance of minimum-latency real-time implementations and consequently alleviates the burden on cloud servers. Autonomous automobiles exemplify real-time edge computing applications prominently [1]. Therefore, it is imperative to modify and optimize these enabling technologies to seamlessly integrate with edge computing. Undoubtedly, edge computing will become a crucial component of the 6G-IoT network. As the edge computing paradigm encompasses interconnected networks and diverse devices, it inherits the traditional security and privacy concerns associated with each technology [2]. Furthermore, these risks are of significant magnitude. Once cloud computing and analytics capabilities are integrated into network edge computing, new security scenarios will emerge that have not been thoroughly investigated. The constraints of memory, power, and processing resources in devices present additional obstacles to edge computing security. Therefore, it is essential to adapt security methodologies to accommodate the limitations of edge design.

Blockchain is widely recognized as a disruptive technology by scholars and companies due to its potential to offer solutions in monitoring, regulating, and, most importantly, ensuring security and reliability in edge computing networks and devices

[3,4]. By combining blockchain technology with edge computing into a unified framework, the 6G-IoT communication environment will provide dependable control and access through the network, distributed computing resources, storage at the edge. Therefore, edge computing enables the secure availability of storage, network administration, and computing capabilities close to the networks' edges [4]. However, this research must address these issues before widespread integration and implementation. We must systematically improve scalability at various levels. Concurrently, we should continue to conduct further research on the emerging security threats that arise from the increased outsourcing of services to the edges. Additionally, the standardization of prices and their interoperability reduces management hassles, especially through the adoption of self-governing mechanisms, but it also introduces new security risks.

The following is a concise overview of the contributions made in this paper: This paper supplies an extensive analysis for blockchain at the 6G-IoT and related technologies, emphasizing key features such as transparency, decentralization, and immutability. Furthermore, it provides a thorough overview of the integration of blockchain technology with edge computing and its related applications. This work has identified the existing obstacles to the integration of blockchain technology with edge computing in the context of 6G-IoT. The remainder of the paper is structured as follows: Section II provides an introduction to the blockchain and its respective technology. Sections III and IV describe the integration of blockchain technology with edge computing and its applications. Section V delineates the obstacles encountered in the amalgamation of blockchain technology with edge computing. Section VI provides the conclusion to this paper.

INTRODUCTION TO BLOCKCHAIN AND TECHNOLOGIES

The blockchain is a decentralized ledger accessible to anybody. In essence, the blockchain functions as a distributed, consolidated, and resistant-to-manipulation database, storing all past transactions and sharing them among parties within a peer-to-peer (P2P) network, as illustrated in Fig 1. A consensus approach verifies or timestamps the hash values in each block of data, and most miners actively participate in authenticating and confirming transactions to link the blocks together in a chain. Miners assign a timestamp and validate the transactions, making them permanently unalterable and resistant to tampering (i.e., immutable) [5].

The integration of elliptical-curve cryptography (ECC) and the secure hashing technique (SHA-256) offers a rigorous confirmation of data authenticity and integrity. Blockchain is a decentralized network specifically created to facilitate secure communication between nodes that lack trust in each other, without the need for a trusted central governance body. A blockchain can be constructed as either a permission (or private) network, which restricts access to a specific group of members, or a permission-less or public network, which allows anybody to participate.

Permission blockchains offer enhanced privacy and improved mechanisms for controlling access [6,7]. The architectural framework of a Blockchain, as shown in Fig. 2, primarily consists of the block header and the block content,

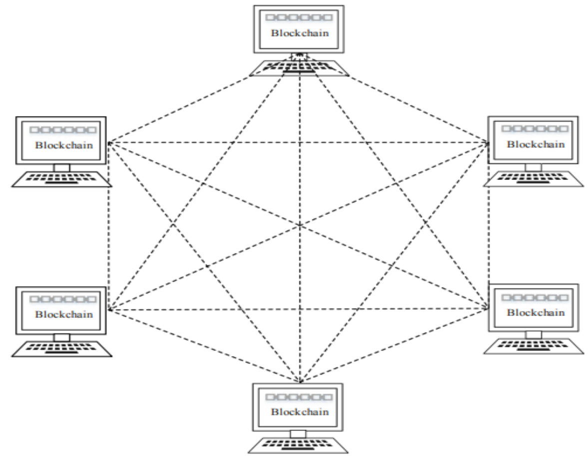

Fig. 1. The architecture of the P2P blockchain network [5].

Which aggregates a comprehensive record of transactions. A version numeral for watch software or protocol upgrades was one of the fields in the block header. Also, the header also includes the transaction count, timestamp, and block size. The Merkle root field was a representation of the hash worth of the exithing transaction block. Merkle tree hashing was routinely employed at distributed systems and P2P networks to achieve efficient data verification. The nonce field facilitates the proof-of-work technique by serving as the test counter worth that generates the hash with leading zerosn [8]. A difficulty target is an appointed quantity of leading zeros used in efforts to ensure block time of roughly 10 minutes for Bitcoin and 17.5 seconds for Ethereum. The difficulty target is again regularly modulable and unless the specific problem demands so, there are extra leading zeros added as better computing hardware is developed. Block time is intentionally established to include the time it takes for blocks to travel to all miners and for all miners to achieve a consensus.

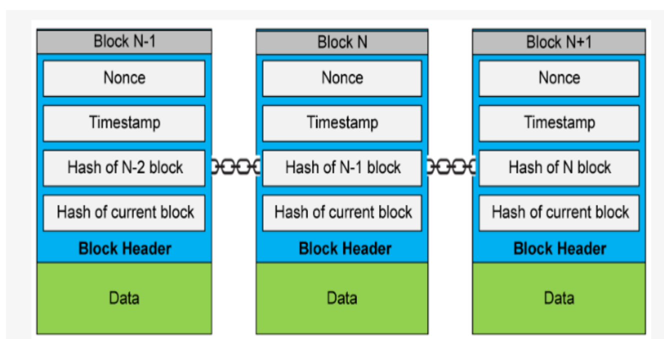

Fig. 2. The Architectural Framework of Blockchain Technology [8].

The fundamental constituents of blockchain technology are cryptography, consensus protocols and smart contracts.

1) *Cryptograph*: An exclusive sequence of numerical values, exclusive to the sender of the information and incapable of counterfeiting by others, constitutes a digital signature [9]. The network produces a matching set of private and public keys randomly for each user. The user exclusively uses the private key for transaction signing.

The network disseminates transactions signed with the private key and then authenticates them using the public key.

2) *Smart Contracts*: Szabo first introduced smart contracts, also referred to as digital contracts or blockchain contracts [9]. These autonomous contracts, encoded as program code and stored on a blockchain, establish the terms of agreement among users in a P2P network. Smart contracts facilitate anonymous transactions between parties, eliminating the need for a third-party authority. Transaction requests or other events trigger the execution of a user's smart contract program.

3) *Consensus Protocols*: A blockchain is comprised of multiple blocks, each containing a set of transactions. These transactions represent the exchange of information, value, or other data among various entities within the computer network. For a block to be deemed valid, it must undergo a consensus process. The prevailing consensus mechanisms in blockchain technology encompass Practical Byzantine Fault Tolerance (PBFT), Proof of Work (PoW), Proof of Storage (PoS), and Proof of Stake (PoS) [9].

The primary factors contributing to the widespread adoption of blockchain technology are its distinctive characteristics, such as transparency, decentralization, and immutability.

- *Transparency*: The blockchain operates on open-source technology, ensuring a consistent level of transparency. This inherent transparency extends to transactions conducted within the blockchain. While the technology and transactions themselves are transparent, they are also securely protected, contingent upon the majority of nodes within the blockchain network supporting any changes. To safeguard user information, we employ sophisticated cryptographic techniques for concealment [8,9].
- *Decentralization*: Before blockchain gained prominence, a centralized governing body was responsible for storing all data and facilitating all interactions with the data. Centralized systems share many drawbacks, including a single point of failure and susceptibility to attacks. By ensuring that every node stores the information, decentralized systems address the limitations of centralized systems [10, 11].
- *Immutability*: Immutability pertains to the inherent characteristic of information stored within the blockchain network, ensuring its unaltered state through consensus mechanisms. This particular attribute of blockchain renders it an ideal solution for various industries, encompassing governance, supply chain management, and finance [8].

INTEGRATION OF BLOCKCHAIN TECHNOLOGY WITH EDGE COMPUTING

Edge computing is a versatile paradigm that enables progress in IoT, 6G, and AI, intending to augment the effectiveness of existing centralized cloud computing. Despite the enhanced data security offered by cloud computing, edge computing encounters several security challenges. These challenges include the authentication of IoT devices and edge servers, as well as safeguarding against malicious attacks. Moreover, the deployment of edge computing in environments lacking adequate monitoring and security measures renders it vulnerable to various harmful attacks, such as jammer attacks, sniffer attacks and distributed Denial-of-Service (DoS) attacks [12, 13].

The progress made in blockchain architecture has effectively addressed security concerns associated with immutability and resistance to attacks. Additionally, it enables the establishment of a decentralized shared data storage system, fostering a permissionless and censorship-resistant network in edge computing. Blockchain technology has demonstrated its efficacy in facilitating reliable and regulated identity registration and asset ownership tracking, thereby safeguarding transaction integrity in distributed edge computing scenarios, as exemplified by TrustChain. Consequently, the incorporation of blockchain technology into the edge computing layer has the potential to substantially augment network speed [14, 15].

Edge Blockchain: The decentralized edge blockchain is managed locally by each edge server. It facilitates transactions between different edge servers and 6G-IoT devices or solely between IoT devices. These transactions should be clear, logical, and uncomplicated. To ensure this, they must be interchangeable and uniform across the entire blockchain network. Consequently, further design efforts are focused on simplicity, establishing a central context, and maintaining balanced content dispersion. As demonstrated by our findings, networked service platforms have sufficient processing and storage capabilities to accommodate edge computing platforms. Hence, every edge computing system includes storage capabilities along with a management controller to oversee its pool [16, 17]. A crucial aspect of the management controller is its ability to handle transactions originating from Internet of Things devices. Given the resource constraints inherent in IoT devices, such as limited memory, processing power, and storage space, edge computing is employed to store many transactions. 6G-IoT devices generate transactions, which are then forwarded by edge computing to the Internet. These transactions are stacked, encrypted, and digitally signed by the 6G-IoT devices to ensure computer security and privacy. Based on the provided architecture, the edge computers manage the blockchain aspect. They generate blocks of transactions at set frequencies using various consensus mechanisms, including the Proof of Storage [18, 19]. Other edge computers receive these blocks for validation. We distribute the blocks we receive to other edge computers for further verification. This approach guarantees that each edge computer has sufficient resources to support blockchain maintenance. Data rewards are then allocated to the contributing edge computers according to predefined timeframes.

APPLICATIONS OF INTEGRATING BLOCKCHAIN TECHNOLOGY WITH EDGE COMPUTING

Blockchain, a groundbreaking technology, holds significant potential for various applications in the field of edge computing. This section presents a comprehensive compilation of applications that aim to seamlessly integrate blockchain technology with edge computing [20, 21].

A. *Smart Grid:*

Emerging battery energy storage technologies have the potential to facilitate the transition of a significant number of customers into prosumers who utilize renewable energy to generate and store power for edge computing. To achieve this, it is recommended to implement a decentralized database platform known as the smart grid. This platform aims to create an electricity blockchain that is efficient, secure, cost-effective, and sustainable. By adopting this platform, it becomes possible to explore innovative technological solutions and business models for effective energy management[22,23].

B. *Smart Industrial:*

The convergence of blockchain with edge computing provides a safe and cohesive framework for the current data processing, cloud computing, and access control. This configuration facilitates the swift deployment of computing services to edge servers, thereby significantly advancing the growth of industrial IoTs. High-performance computing skills are required for blockchain mining operations, and the deployment of equipment that can achieve this level of computational power is expensive. Hence, migrating mining operations to the edge servers to fully use the constrained computational capabilities of 6G-IoT for mining would be a very attractive approach [24, 25].

C. *Smart Healthcare:*

The advancement of technology has rendered smart healthcare a crucial matter that necessitates improvement in all possible ways. In particular, the utilization of blockchain in integrated edge computing provides extensive control over access, transactions, and storage, thereby guaranteeing the confidentiality of health data. This technology holds the potential to enhance existing healthcare operations [26, 27].

D. *Smart Home:*

The privacy of home appliances, which transmit a significant amount of home and personal data to centralized databases managed by smart device manufacturers or sellers, may be compromised [8]. In conclusion, the utilization of blockchain technology in edge computing for 6G-IoT provides a transparent and secure alternative framework for managing private data in smart homes [28, 29].

CHALLENGES OF INTEGRATING BLOCKCHAIN TECHNOLOGY WITH EDGE COMPUTING

Blockchain technology introduces innovative concepts and opens up new research opportunities for edge computing. However, it also brings forth significant obstacles that necessitate careful consideration. This section outlines a detailed list of research challenges pertaining to the seamless integration for edge computing with blockchain technologies [30, 31].

A. *Security:*

While blockchain technology provides appealing security characteristics for the distributed processing and storage of data, certain security concerns arise when blockchain is applied to edge computing, particularly in the case of private blockchains. One potential adaptation is the creation of small-scale "white-listed" 6G-IoT networks [32, 33], in which all network nodes have mutual trust and PoW is not necessary. Transmitting transaction data from mobile or IoT devices to edge computing servers can lead to attacks. Establishing a secure and dependable network infrastructure for devices and servers is essential. The potential for DDoS attacks to disrupt the connectivity and operation of edge blockchains must be considered. Additionally, given the reliance of mobile and IoT devices on wireless transmission, the threat of jamming attacks disrupting network data flow should not be overlooked. Furthermore, the susceptibility of edge blockchain to typical 51 percent attacks, in which attackers gain control over the majority of computational power, is a concern due to the limited computing capabilities of mobile and 6G-IoT devices. Their potential inability to rely on expensive external computing services further compounds this risk.

B. *Consensus of the improvement:*

Some of the edge computing applications require the instantaneous conveyance of the processed results to the 6G-IoT devices, like the immediate accident notification in the intelligent transport system ICTS. Currently, mining utilizes such consensus mechanisms, which require the majority of nodes that make up the network to check transactions, an issue that causes considerable latencies. The current consensus algorithms, including the PoW and PoS, are cumbersome for device servers at the LAN level due to the limited storage and computational capacity [34, 35]. The next significant research question for edge computing with blockchain is how to devise new settlement methods that can maintain the real-time demand of deployed applications in place while not incurring excessive latency. Such mechanisms not only protect the blockchain functions but also have the capability to gather data on the devices and servers located at the edge.

C. *Improvements in scalability:*

IoT devices usually have a finite amount of storage, which is a frequent need for blockchain networks. Nonetheless, edge servers may receive D2D transactions and data generated by 6G-IoT devices for processing and archiving. However, the blockchain's smart contract requires all operators to uphold an accurately distributed ledger, and they must periodically track down every transaction recorded in the ledger. As more devices join the network, every participant will create and keep a significant amount of transactions [36, 37]. As a result, servers and 6G-IoT devices must work more efficiently. As a result, increasing the network's overall efficiency becomes difficult, which restricts the scalability of 6G-IoT networks. One of the biggest challenges is scaling the network while using current implementations. Each edge server maintains the decentralized edge blockchain, which records transactions between edge servers and IoT devices, as well as between IoT devices themselves. These transactions must be visible, uniform, and consistent [38].

D. *Standardization of Costs and Interoperability:*

Because of its hierarchical nature, edge computing necessitates the provision of conversion mechanisms via protocols at several layers. Since IoT devices have limited resources, we must use edge servers for mining and transaction data storage. This implies that one or more intermediate-edge servers are required to handle each contact between two 6G-IoT devices. Consequently, well-defined patterns of interaction were necessary for effective data management and interchange. Furthermore, edge computing requires the integration of many application platforms and may need to cooperate in order to offer services [39, 40]. As a result, creating interaction models for a variety of apps running on various platforms is essential. Furthermore, edge servers' limited processing and storage capacity makes it impossible to manage the massive amounts of data produced by 6G-IoT devices. However, this data is too large to be further analyzed and stored locally; hence, it has to be transferred to cloud servers. Thus, to properly deploy intelligent services in networks, it is necessary to establish cost distribution criteria for intelligent settlement of service fees, which smart contracts facilitate.

CONCLUSION

This study provides a comprehensive analysis of blockchain technology and its distinguishing features within the context of the 6G-based IoT. Additionally, the early-stage integration of blockchain technology into edge computing shows promise in streamlining edge computing and facilitating decentralized data management. It is widely believed that incorporating blockchain technology effectively addresses various security concerns and data anomalies. This study investigates the integration of blockchain technology with edge computing, its applications, and the associated challenges. The findings of this study will serve as a comprehensive guide for future directions, as this model is expected to play a crucial role in shaping the future of the blockchain and computing landscape.

REFERENCES

[1] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," IEEE Vehicular Technology Magazine, vol. 14, p. 28–41, 2019.

[2] F. R. Yu, "From information networking to intelligence networking: Motivations, scenarios, and challenges," IEEE Netw., vol. 35, no. 6, pp. 209–216, Nov./Dec. 2021.

[3] A. Alawadhi and A. Almogahed, "Recent Advances in Edge Computing for 6G," in 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), 2022.

[4] M. B. Mollah et al., "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," IEEE Internet Things J., vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[5] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," J. Netw. Comput. Appl., vol. 166, Sep. 2020, Art. no. 102693.

[6] A. Alawadhi, M.H. Omar, A. Almogahed, N. Nordin, S.A. Alqahtani, and A.M. Alamri "DNBP-CCA: A Novel Approach to Enhancing Heterogeneous Data Traffic and Reliable Data Transmission for Body Area Network," Comput. Mater. Contin., vol. 79, no. 2, pp. 2851-2878. 2024.

[7] Jiang, Z. Pang, M. Luvisotto, R. Candell, D. Dzung, and C. Fischione, "Delay optimization for industrial wireless control systems based on channel characterization," IEEE Transactions on Industrial Informatics, pp. 1–1, 2020.

[8] A. Almogahed, A. Amphawan, F. Mohammed, and A. Alawadhi, "Performance improvement of mode division multiplexing free space optical communication system through various atmospheric conditions with a decision feedback equalizer," Cogent Engineering, 2022.

[9] W. Wang et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," IEEE Access, vol. 7, pp. 22328–22370, 2019.

[10] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1214–1229, Apr.–Jun. 2021.

[11] L. Nkenyereye, J. Y. Hwang, Q.-V. Pham, and J. S. Song, "Virtual IoT service slice functions for multiaccess edge computing platform," IEEE Internet Things J., vol. 8, no. 14, pp. 11233–11248, Jul. 2021.

[12] A. Alawadhi, A. Almogahed, and M. H. Omar, "A Survey on IEEE 802.15. 7 MAC Protocols for Visible Light Communication" in: 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), IEEE, 2023.

[13] S. U. Rehman, S. Ullah, P. H. J. Chong, S. Yongchareon and D. Komosny, "(Visible light communication: a system perspective—overview and challenges)," Sensors, vol. 19, p. 1153, 2019.

[14] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for IoT-based energy management in smart cities," IEEE Netw., vol. 33, no. 2, pp. 111–117, Mar./Apr. 2019.

[15] A. Alawadhi, A. Almogahed, F. Mohammed, B. Ba-Quttayyan, and A. Hussein, "Improving Performance Metrics in WBANs with a Dynamic Next Beacon Interval and Superframe Duration Scheme," Heliyon, vol. 10, no.2024.

[16] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1392–1431, 2nd Quart., 2020.

[17] D. Xu, T. Li, Y. Li, X. Su, S. Tarkoma, and P. Hui, "A survey on edge intelligence," 2020, arXiv: 2003.12172.

[18] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," IEEE Netw., vol. 34, no. 1, pp. 8–14, Jan./Feb. 2020.

[19] A. M. Alawadhi, M. H. Omar, and N. Nordin, "IEEE 802.15.4 MAC protocol optimization in body sensor networks: a survey, outlook and open issues," International Journal of Communication Networks and Distributed Systems, 2023, DOI: 10.1504/IJCNDS.2022.10047499.

[20] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," IEEE Trans. Syst., Man, Cybern., Syst., vol. 50, no. 1, pp. 43–57, Jan. 2020.

[21] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[22] A. Alawadhi, A. Almogahed, and E. Azrag, "Towards Edge Computing for 6G Internet of Everything: Challenges and Opportunities," in: 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), IEEE, 2023, pp. 1–6.

[23] D. Nagothu, R. Xu, S. Y. Nikouei, and Y. Chen, "A microserviceenabled architecture for smart surveillance using blockchain technology," in Proc. IEEE Int. Smart Cities Conf. (ISC2), Kansas City, MO, USA, 2018, pp. 1–4.

[24] A. Alawadhi, A. Almogahed, R. B. Ahmad, S. O. Barraood, O. Al-Jamili, and M. I. Adawy "Improving Packet Delivery Ratio through Duty Cycle Control in Heterogeneous Visible Light Communication," in 2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA). IEEE, 2024.

[25] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," IEEE Access, vol. 7, pp. 18611–18621, 2019.

[26] D. Bruneo et al., "An IoT service ecosystem for smart cities: The SmartME project," Internet Things, vol. 5, pp. 12–33, Mar. 2019.

[27] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," Future Gener. Comput. Syst., vol. 86, pp. 650–655, Sep. 2018.

[28] A. Almogahed, M. Omar and N. H. Zakaria, "Recent Studies on the Effects of Refactoring in Software Quality: Challenges and Open Issues," in 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2022.

[29] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, “PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities,” Comput. Security, vol. 88, Jan. 2020, Art. no. 101653.

[30] B. W. Jo, R. M. A. Khan, and Y.-S. Lee, “Hybrid blockchain and Internet-of-Things network for underground structure health monitoring,” Sensors, vol. 18, no. 12, p. 4268, 2018.

[31] A. Almogahed, A. Amphawan, and F. Mohammed, "Design of 7× 2.5 Gbps decision feedback equalization scheme for mode division multiplexing over free-space optics under diverse atmospheric turbulence," Optical Engineering, vol. 61, no. 5, p. 056102-056102, 2022.

[32] P. V. Klaine, L. Zhang, and M. A. Imran, “An implementation of a blockchain-based data marketplace using Geth,” in Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Serv. (BRAINS), 2021, pp. 15–16.

[33]

[34] R. M. A. Latif, M. Farhan, O. Rizwan, M. Hussain, S. Jabbar, and S. Khalid, “Retail level blockchain transformation for product supply chain using truffle development platform,” Clust. Comput., vol. 24, no. 1, pp. 1–16, 2021.

[35] A. Almogahed, M. Omar, N. H. Zakaria and A. Alawadhi, " Software Security Measurements: A Survey," in 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), 2022.

[36] A. Alawadhi, R. B. Ahmad, A. Almogahed, and A. Abrar, "Deep learning techniques in mobile edge computing for internet of medical things," in 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA). IEEE, 2023.

[37] M. Alamri, N. Jhanjhi, and M. Humayun, “Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review,” Int. J. Comput. Sci. Netw. Security, vol. 19, pp. 244–258, May 2019.

[38] D. C. Nguyen et al., “Enabling AI in future wireless networks: A data life cycle perspective,” IEEE Commun. Surveys Tuts., vol. 23, no. 1, pp. 553–595, 1st Quart., 2021.

[39] A. Alawadhi, M. H. Omar, and N. Nordin, "A Survey on IEEE 802.15.4 MAC Protocols for Body Sensor Networks," in 6th International Conference on Internet Applications, Protocols and Services. NETAPPS 2020, 2021, pp. 109 -114.

[40] X. Xu, Z. Zeng, S. Yang, and H. Shao, “A novel blockchain framework for industrial IoT edge computing,” Sensors, vol. 20, no. 7, p. 2061, 2020.