Babylonian Journal of Networking
Vol.2023, **pp**. 82–88
DOI: https://doi.org/10.58496/BJN/2023/010; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Exploring the Role of Block-chain in IoT-Driven Healthcare Solutions

Abeer Mohammed Shanshool,[1,*,]

[1] *National School of Electronics and Communications, Sfax university, Tunisia*.

ARTICLE INFO

Article History

Received 04 Aug 2023
Accepted 05 Oct 2023
Published 25 Oct 2023

Keywords

IoT

BlockChain

Healthcare

Smart Contract

Etherum

ABSTRACT

Due to advances in database hacking, cloud computing, and communication network penetration, current methods are needed to combat IoT threats. This work will leverage blockchains. Blockchains improve transaction speed, accuracy, security, and transparency. The blockchain is expected to make trading stocks, processing payments, managing birth certificates and health information, processing property titles, monitoring digital supply chains, and coordinating the burgeoning IoT simpler, quicker, and cheaper. Blockchain used to protect IoT; research was conducted on blockchain and methods used in the development of data transfer and database security. This study clarifies this technique and what techniques are used with this technology and compares it to previous research that used different protection methods and different directions for investing blockchain in IoT.

1. INTRODUCTION

The healthcare system faced several challenges, including unreadable diagnoses on paper, difficulty accessing patient information by physicians, and space, time, and staff constraints on patient monitoring. As numerous technologies evolve, certain potential exist for improving health care by decreasing some hurdles and delivering more individualized services. In the past decade, health-care companies have used the internet to provide general health information, helping people understand their illnesses. Over 90% of the 5000 American Hospital Association members have websites, with most providing detailed information about their services and facilities [1].

The next technological era is handled by IoT. The IoT revolution is coming after the WWW and mobile internet revolutions of the previous two decades. IoT describes a network where each thing is uniquely accessible, identifiable, and connected to the internet. Many gadgets create, analyze, and communicate privacy-sensitive data. IoT is used in traffic, weather, health, agriculture, smart homes, and more. Each internet layer employs smart IoT devices. These gadgets gather and analyze sensitive data, thus privacy and security are crucial. Lightweight IoT devices have minimal energy footprints [2].

Decentralized architecture was important recently since it's required in many sectors. IoT uses it to solve open challenges, like security. Blockchain was first offered by bitcoin [3]. This peer-to-peer network is open to everyone and does not need personal information for permission. Anyone may be a blockchain component and transact. Public ledger and consensus solve trust and security. Public blockchains like Ethereum and Bitcoin employ PoW [4]. All transactions are validated by unique nodes (miners). For all transactions, participants share a public/private key pair. The public ledger is an immutable chain of transactions, therefore altering any record invalidates the transactions on all peer nodes [5]. Medical IoT is a category of internet-connected gadgets that help healthcare. MIoT is a unique electronic-healthcare technology that uses implanted sensors or tiny wearable devices to monitor patients' physiological parameters and pathology. MIoT is crucial for health assurance and enabling wireless body area networks and implanted medical devices [6].

2. INTERNET OF THINGS AND BLOCKCHAIN

IoT and smart gadgets made ubiquitous computing possible. Over 20 billion IoT devices and smartphones exist. Most situations need IoT-based sensor networks for remote monitoring, while smart gadgets provide real-time video feeds. In addition, IoT applications such diagnostic reporting, body sensing and health-care, monitoring and industrial automation, assets tracking, surveillance and security, telemedicine and consultation, telemetry, and others are advancing rapidly [7]. IoT

*Corresponding author. Email: abeershanshool@gmail.com

is widespread because it can share data across devices, supports heterogeneity, and is easy to use. However, such qualities raise trust, privacy, and security concerns [8]. IoT trust, privacy, and security issues were challenging and crucial, especially in sensitive fields like health-care, economics, military communication, and engineering, due to the absence of audit mechanisms or verification [9]. Since the blockchain allows unreliable entities to communicate information, its fraud protection, authentication, data integrity, and other features solve IoT trust, privacy, and security issues [10].

3. ARCHITECTURE OF BLOCKCHAIN

Although blockchain technology was first utilized to create bitcoins in order to prevent double-spending, it is already being used for other purposes. This research uses IoT as an example. The word "blockchain" is often used to refer to data structures that are periodically mentioned in relation to systems or networks. Furthermore, the blockchain may be described as an ordered list of blocks [11], where each block is made up of a transaction. As seen in Fig. (1), every blockchain block is also linked to the one before it, with each block being composed of a hash from the prior block. As a result, without completely changing the blockchain's contents, the transaction history on blockchains may not be removed or changed. Blockchains are seen as wise against hackers because of this [12].

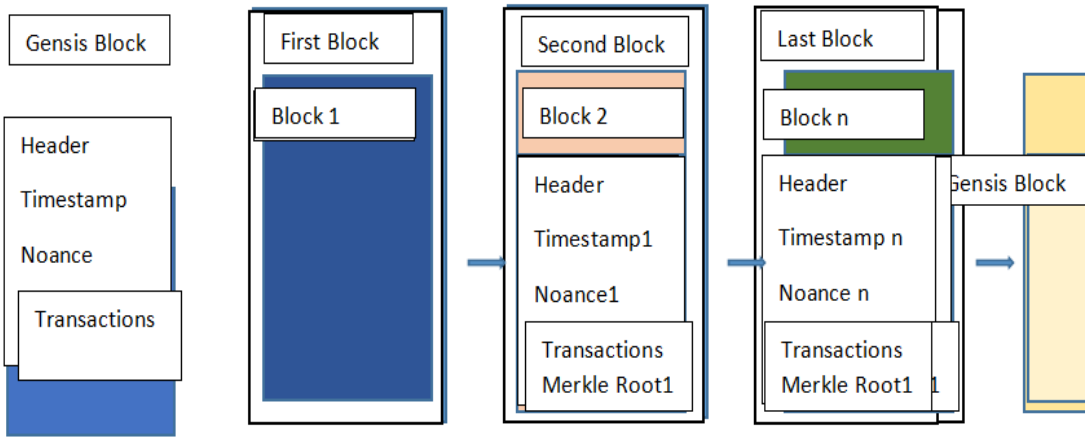

Fig. 1. A blockchain list

3.1 Blockchains have a variety of characteristics.

a. Resilience. While faulty transactions won't be detected by miners, transactions on the blockchain may be confirmed rapidly. Consequently, it is not possible to reverse transactions that have already taken place [13].

b. Auditability. Every blockchain transaction references its predecessor. As a result, every transaction will just need to be monitored and confirmed [14].

c. The decentralized approach. Transaction verification on the blockchain does not need third parties. The consensus method is used in blockchain networks to ensure data consistency [15].

d. The right to remain anonymous. Every user in a blockchain network communicates with others using a created address. Consequently, the interaction doesn't reveal the user's true identify [16].

e. Information structure. The transactions were arranged into blocks and linked together using a cryptographic hashing method that uses previous entry data as input. A secure data chain with unchangeable blocks and no hash invalidation is included in the output [17].

f. Spread out. To eliminate any single point of failure, every network node has a complete duplicate of all the data since the genesis block, which is the first block in the chain.

g. Safety. Cryptographic hash functions guarantee the data integrity of the blockchain. Also, the use of private keys ensures authenticity. If the block is changed, the hash function may change as well, making the block inconsistent with all future chained blocks. Other system nodes may be able to detect this, and the modifications will be rejected [18].

h. Agreement. New entries are being algorithmically vetted by nodes; those that have been approved by the majority of nodes are included in the blockchain.

i. Privacy and transparency. Not only are transactions available to all parties involved, but they are also thought to be traceable back along the chain; all ledger transactions are accessible to all parties. No user identification is visible, even though all participants have complete copies of the database transactions [19].

j. Time stamps. By timestamping, the transaction order accuracy and completeness are guaranteed.

k. Software updates via agreement. Software updates for the blockchain were approved via consensus verification.

l. Disentanglement. Blockchain technology reduces the need for middlemen, lowers overhead expenses, and lessens the risk of a single point of failure.

m. Turing finished. If one had the necessary resources, computational issues were almost entirely solvable; contracts could be written for almost every kind of problem. [20]

In order for service providers to survive, stakeholders must combine a number of qualities (Fig. 2). Ensuring data integrity, or making sure no transactions were carried out, altered, or modified without a network consensus process, is the first and most important attribute. This is often guaranteed inside the company.

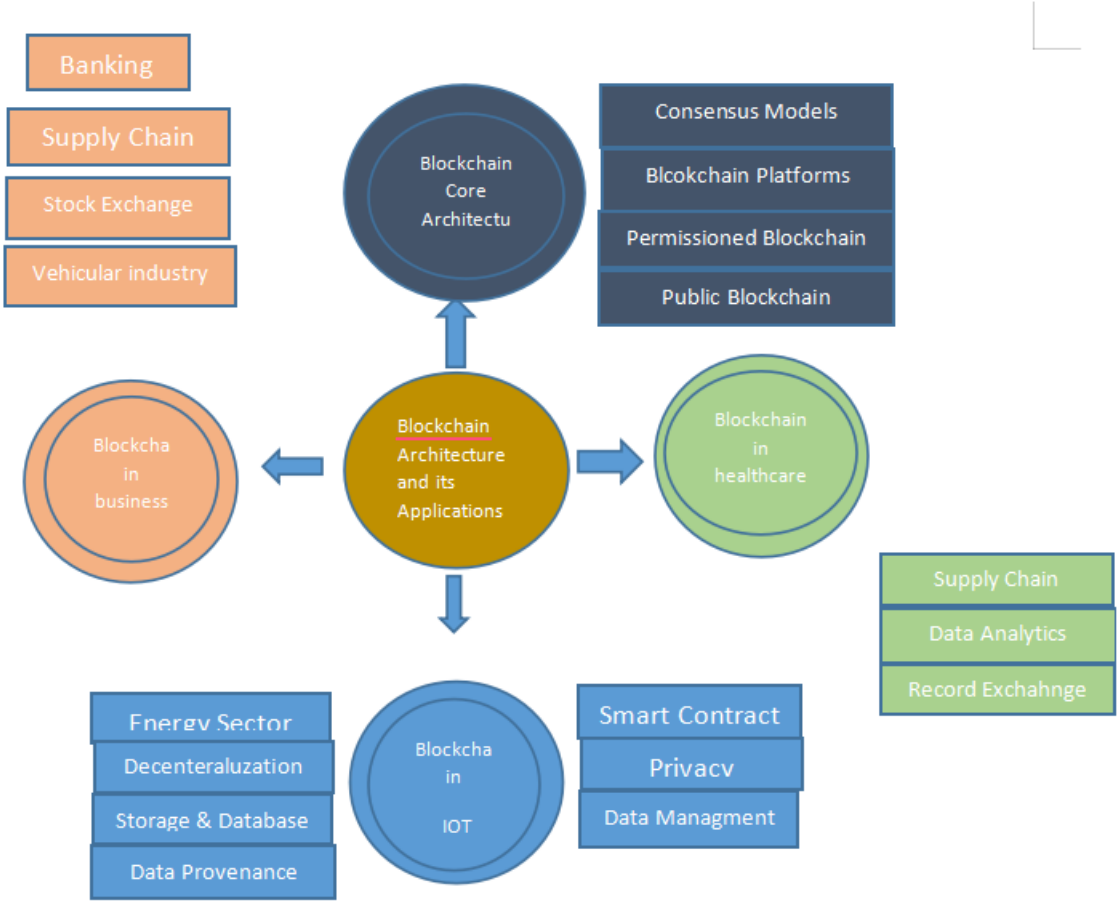

Fig .2.Shows a blockchain architecture and its applications

4. ETHERUM

One of the blockchain systems created by Vitalik Buterin is called Ethereum. A few limitations associated with Bitcoin are also covered. The main benefit of Ethereum is its support for full Turing completeness, which shows that it can keep up with all kinds of computation. Ethereum is further described as a state machine based on transactions. The following are the main and noteworthy components of Ethereum:

a. Money .As intrinsic money on Ethereum, "Ether," or ETH, was used to perform network calculations in a data transfer format.

b. Deal. A signed data package containing messages that will be transmitted from EOA is indicated by a transaction in Ethereum. Additionally, the two sorts of transactions in Ethereum were creating an account and sending a message. In addition, the transaction contains the destination of the message, the sender's signature, the amount of ether and the data that has to be delivered, the number of starts (limit of gas), and the price of gas.

c. The technology used. Ethereum makes use of a wide range of web, client/node, and data storage technologies.

d. Account. Every Ethereum account has a 20-byte address that consists of four parts: contract code, storage, ether balance, and non-cecounter. The two kinds of accounts in Ethereum were Contract Accounts and Externally Owned Accounts (EOA). Additionally, the contract code controlled the contract account, while the private key controlled EOA. The Contract Account is only activated via EOA.

e. The consensus algorithm. In Ethereum, there are three different forms of consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA).

5. LITERATURE SURVEY

Ref.	Concept	Type of Security	Goal of Study	Conclusion
[25]	Move security information across the blockchain network	The RSA Cryptosystem	implemented across enterprises that depend on strict security transferring media data, such as documents, music, video, and photos, in a way that maximizes communication security	Any kind of file may be sent by utilizing Base64 encoding to transform it into a text file. RSA was used to encrypt the raw text because of its advantages in terms of the co-factoring required to crack it.
[26]	From blockchain to a network of health applications	Intelligent contracts	adapted blockchain models suitable for IoT devices	The solutions increase the security and anonymity of IoT transactions and application data across the blockchain-based network..
[27]	Data security and information security, along with a blockchain-based solution.	Hashing value	Boost cloud computing security	Information must be stored in the cloud so that it is easily accessible from anywhere at any time.
[28]	Data safely using blockchain technology that has been tailored.	constructing a general hierarchical IoUT and keeping track of its structure Blockchain for securing IoUT data storage.	Ensuring the privacy, security, and low computing costs of data conveyed by hierarchical sensor networks remains a problem.	The simplicity of the architecture for monitoring IoUT data is shown by performance analysis as well as mitigation related to security threats analysis.
[29]	Digital Health Record	Hashing value	designed to facilitate information exchange with other healthcare providers and organizations	encouraging the growth of broader health-care ecosystems, including both contemporary and traditional ideas
[30]	These systems include the industrial, health, and other systems.	new Proof of Block & Trade (PoBT) consensus method that is lightweight	IoT networks served as the foundation for efficient and intelligent corporate operations.	lowering the processing time required via peers and enabling high transaction rates for Internet of Things devices with limited resources
[31]	blockchain to guarantee the distributed nature proposed by IoT	Access control in the Internet of Things (IoT) by proposing a dynamic, completely distributed security policy.	featuring a centralized design and operating without transferring access control management to network nodes from a central source	supplying a security policy that is dynamic, self-adjusting, and optimal.
[32]	blockchain technique to provide a decentralized, secure, and privacy-preserving machine learning system,	Using a pseudonym to conceal one's true identity	creating a blockchain-based, decentralized stochastic gradient descent (SGD) method to train a generic predictive model.	Creating a system of expanded differential privacy that offers robust privacy protection
[33]	Permit peers to trade directly as consumers and producers of data on the blockchain network.	An encryption method and smart contracts were used to regulate users' access rights.	using a blockchain-related decentralization feature to eliminate centralized platforms	The CP-ABE method is used to address issues related to access control and data security in traditional data distribution systems.

[34]	systems for quantum signatures	intelligent contracts	enhancing blockchain smart contract security performance against quantum assaults	For decentralized dispersed business applications, it is more suitable.
[35]	A novel incentive system that takes into account the effort made by healthcare practitioners to both generate new blocks and preserve medical information.	intelligent contracts	Enhancing current systems to offer safe, compatible, and effective medical records for patients, healthcare providers,	In terms of reaction time, throughput, and communication overhead, the outcomes show how well the plan works to manage a large data volume with little delay.
[36]	Enhances the individual's access to quality as well as inexpensive health-care services	Protocols	Reducing medical errors, improving the safety of patients, and optimizing the health-care processes.	Integrating multi-agent as well as RFID technologies into IoT platform for health-care.
[37]	describing the potential decentralized sharing of genetic data with blockchain technology in public health surveillance.	Data sharing	facilitating communication between several parties that share data, however we were concerned concerning their privacy .	Protecting sensitive data and maintaining privacy are important considerations. Decentralization of organizational infrastructures also helps to eliminate gaps in data exchange.
38	describing ModelChain, a revolutionary system that uses blockchain technology to enable machine learning with privacy preservation.	Hashing function	creating a unique proof-of-information method to ascertain the online learning process's order.	The technology of blockchain solves the privacy-preserving health-care predictive modeling tasks and increasing interoperability

6. CONCLUSION

Numerous features that blockchains provide, like immutability, decentralization, and transparency, may be used to improve health-care interoperability. Nevertheless, the body of current research offers few or no standards or best practices for developing or assessing blockchain-based health applications. In order to close this gap, the research that was presented provided a set of assessment criteria from both a technical and domain standpoint for evaluating health care when using this new technology. These measures may also be used as a starting point for the creation of future applications in the same field. Future research endeavors will include expanding this study to investigate alternative suitable assessment measures and verifying our findings via the use of tangible blockchain-based health-care use cases. Additionally, this study's findings suggest that there are other ways to enhance blockchain security.

Conflicts Of Interest

The paper explicitly states that there are no conflicts of interest to disclose.

Funding

The acknowledgments section of the paper does not mention any financial support from institutions or sponsors.

Acknowledgment

The author acknowledges the support and resources provided by the institution in facilitating the execution of this study.

References

[1] A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," Trans. Emerging Telecommun. Technol., vol. 32, no. 10, p. e4333, 2021.

[2] T. Saravanan, A. Ambikapathy, A. Faraz, and H. Singh, "Blockchain and big data for decentralized management of IoT-driven healthcare devices," in Convergence of Blockchain, AI, and IoT, CRC Press, 2021, pp. 57–81.

[3] J. Indumathi et al., "Blockchain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (bc iomt u 6 hcs)," IEEE Access, vol. 8, pp. 216856–216872, 2020.

[4] J. Becker et al., "Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency," in The Economics of Information Security and Privacy, Springer, 2013, pp. 135–156.
[5] Y. Liu et al., "A blockchain-empowered federated learning in healthcare-based cyber physical systems," IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2685–2696, 2022.
[6] Alexander, "Electronic health records implementation with blockchain, BPM, ECM, and platform," Samarin.Biz, Geneva, Switzerland, Tech. Rep., 2016.
[7] J. Wang et al., "Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network," Inf. Sci., vol. 617, pp. 133–149, 2022.
[8] K. R. Darshan and K. R. Anandakumar, "A comprehensive review on usage of Internet of Things (IoT) in healthcare system," in Proc. Int. Conf. Emerg. Res. Electron. Comput. Sci. Technol., 2015.
[9] K. R. Qasim and S. S. Qasim, "Encrypt medical image using Csalsa20 stream algorithm," Jinu. M, Thankamma. P. George, NA Balaram, Sujisha. SS 2. Profile of Burn Deaths: A Study Based on Postmortem Examination of Burn Cases at RNT, vol. 20, no. 3, p. 569, 2020.
[10] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. 2016 IEEE 18th Int. Conf. e-Health Netw. Appl. Serv. (Healthcom), 2016, pp. 1–3.
[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[12] C. Qu, M. Tao, and R. Yuan, "A hypergraph-based blockchain model and application in Internet of Things-enabled smart homes," Sensors, vol. 18, no. 2784, 2018.
[13] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," Sensors, vol. 18, no. 2575, 2018.
[14] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," J. Med. Syst., vol. 40, no. 218, 2016.
[15] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," Sensors, vol. 18, no. 4215, 2018.
[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. 2017 IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), Kona, HI, USA, Mar. 2017, pp. 618–623.
[17] M. Mettler, "Blockchain technology in health-care: The revolution starts here," in Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016.
[18] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of, IEEE, 2016, pp. 1–6.
[19] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in Proc. IEEE Technology & Engineering Management Conference (TEMSCON), June 2017.
[20] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," IEEE Access, vol. 6, pp. 9917–9925, 2018.
[21] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," IEEE Trans. Smart Grid, pp. 1–1, 2018.
[22] N. Zhumabekuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," IEEE Trans. Dependable Secur. Comput., pp. 1–1, 2016.
[23] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.
[24] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," IEEE Access, pp. 1–23, May 2018.
[25] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey," Sensors, vol. 18, p. 2575, 2018.
[26] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," Published: 15 January 2019.
[27] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017, pp. 618–623.
[28] M. Mohan, B. J. Nirmal, R. Sophie Angela, R. Nivetha Angel, and A. Joseph Praveen, "Securing patient Health Record in Blockchain With Abe Access Control," vol. 02, issue 06, June 2020.

[29] S. Biswas, K. Sharif, and F. Li, "PoBT: A Light Weight Consensus Algorithm for Scalable IoT Business Blockchain," IEEE Internet of Things Journal, DOI 10.1109/JIOT.2019.2958077.
[30] A. Outchakoucht, H. Es-Samaali, and J. P. Leroy, "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 7, 2017.
[31] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When Machine Learning Meets Blockchain: A Decentralized, Privacy-preserving and Secure Design," in 2018 IEEE International Conference on Big Data (Big Data).
[32] H. Bowen, Y. Li, F. Li, X. Dong, and P. Chen, "Blockchain-based Access Control Data Distribution System," in 2019 IEEE 5th International Conference on Computer and Communications.
[33] Z. Cai, J. Qu, P. Liu, and J. Yu, "A Blockchain Smart Contract Based on Light-Weighted Quantum Blind Signature," Oct. 4, 2019.
[34] E. Y. Daraghmi, Y. A. Daraghmi, and S. M. Yuan, "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management," DOI 10.1109/ACCESS.2019.2952942.
[35] C. E. Turcua and C. O. Turcua, "Internet of Things as Key Enabler for Sustainable Healthcare Delivery," in The 2nd International Conference on Integrated Information, 2013.
[36] J. L. Bellod Cisneros and F. M. Aarestrup, "Public Health Surveillance using Decentralized Technologies," Blockchain in Healthcare, ISSN 2573-8240.
[37] T. T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks," 2018.