Received: 13 July 2022 | Revised: 15 August 2022 | Accepted: 15 August 2022
DOI: 10.37917/ijeee.19.1.3 Vol. 19| Issue 1| June 2023

Iraqi Journal for Electrical and Electronic Engineering
Review Article

Open Access

A Review of Blockchain-based Internet of Things

Samaher Ahmed Yousiff *, Raad Abd-Al Hassan Muhajjir
Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq

Correspondence
* Samaher Ahmed Yousiff
Department of Computer Science, College of CSIT,
University of Basrah, Basrah, Iraq
Email: samaheraltumma@gmail.com

Abstract
The use of smart network applications based on the Internet of Things is increasing, which increases the attractiveness of malicious activities, leading to the need to increase the adequate security of these networks. In this paper, the latest recent breakthroughs in blockchain for the Internet of Things are examined in the context of electronic health (e-health), smart cities, smart transportation, and other applications in this article. Research gaps and possible solutions are discussed, such as security, connection, transparency, privacy, and the IoT's blockchain regulatory challenges. In addition, the most important consensus algorithms used in the blockchain have been discussed, including Proof of Work, Proof of Stake, and Proof of Authority, each of which operates within certain rules.

KEYWORDS: Internet of Thing, blockchain technology, consensus algorithm, research gaps.

I. Introduction

Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN) (RFID), and other innovations in other devices that sense, communicate, and act utilizing existing network infrastructure, enhanced by IoT, is used in IoT devices. The Internet of Things (IoT) enables a digitally connected real world in which connected devices can share data, communicate with one another, and control goods remotely over the Internet, potentially without human contact [1].

The development of computer networks, wireless communication, and microelectronic mechanical systems has made WSNs one of the technologies with the quickest growth rates[2].

The "Internet of Things" is a term used to describe a network of connected devices which includes printers, and other internet-connected devices, was one of the attack's beginnings. Mirai virus was used to attack these devices, resulting in Distributed Denial of Service (DDoS) attacks. In 2018, the number of assaults on IoT devices grew, with 32.7 million incidents documented. The key flaw in this situation was their dependence on a centralized cloud architecture as well as the lack of security protocols [3]. Addressing IoT security and privacy issues necessitates investigating and grasping the multiple components of the Internet of Things architecture, identifying vulnerability areas in each section, and finding the proper solutions to detect any vulnerabilities. In October 2016, Dyn Inc., a DNS service, was targeted by a DDoS attack that Tens of millions of IP addresses were affected. The Internet of Things is defined as the meeting of the Internet with the physical world in order to bring about a quantum shift toward a smart, digitally controlled world. As a result of the adoption of IoT technologies, the manner in which people interact with one another, their surroundings, and the environment has been enhanced and transformed [1].

Many of the difficulties connected with the centralized cloud technique might be alleviated by a decentralized alternative based on tamper-proof data sharing on a digital ledger. Every transaction on the chain may be signed, secured, and verified. Editing or removing data blocks kept on the ledger is quite difficult , this technology is called blockchain. Although there are many different blockchain topologies available, they all follow the same core principles [3]:

•Transactions between the parties are signed using cryptography.
• Transactions are recorded using a decentralized approach on a peer-to-peer network on a distributed ledger.
• Agreeing a decentralized strategy.

II. Componant of Internet Of Thing

Before knowing the components of the Internet of Things, it is important to know what the Internet of Things is and what its methodology is. Often known as the Internet of Everything, the Internet of Things is a technological and potentially revolutionary paradigm that explains many technologies, including RFID, short-range wireless communications, and search domains, that can connect actual physical objects from the real world to the Internet. In addition, the methodology of this technology must be known, where data is sent from sensors or devices to the cloud server,

where this data is processed and converted into a language understood by the machine, and after processing the data, the results are converted into a language that the user understands and is sent in the form of a signal, message, or other [4].

Sensors or devices, networking, data processing, and the user interface (UI) are the four primary components of an IoT system, as outlined below as fig. 1 [5]:

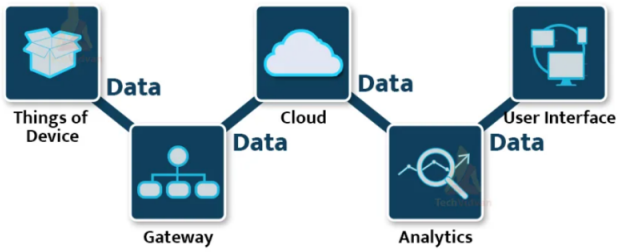

Fig.1 Components of IOT architecture [5].

Sensors or devices are fundamental IoT pieces that collect data from devices with an IP address. These devices can range from simple temperature and humidity sensors in buildings to sophisticated autonomous automobiles. These components primarily gather data in their particular settings, such as temperature or video. These sensors or devices are packaged together instead of working individually. IoT structures are comprised of devices that may gather data from physical settings and communicate it to the IoT ecosystem [6, 7].

Connectivity: LAN, Wi-Fi, satellite, Bluetooth, and cellular infrastructure are all used to link sensors and other devices to the cloud. As a result, to connect with one another, IoT devices use common communication protocols. Bluetooth low energy (BLE) and Wi-Fi, for example, are intended specifically for IoT. The 5G cellular network is projected to assist the IoT by increasing capacity and speed [6, 8].

The development of new technologies, such as edge computing, a new paradigm for dispersed devices, has been forced by the collection of huge amounts of data. Both data and computational power are allocated to where they are required most in edge computing. Any data that the filtered cloud cannot process is transferred closer to the customer, boosting bandwidth and decreasing lag time. These devices or systems process the data, and only the most pertinent information is sent back to the central base for analysis [6, 9].

Data processing: Data is processed with the aid of software once it has been saved in the cloud. This data must be processed, filtered, and analyzed in a specialized manner before it can be of any value. To avoid overburdening the system, zettabytes(10^21) of data are sent via each edge gateway before being processed. By integrating corporate software with cloud data analytics, big data analytics is used to analyze production data at the greatest level possible. IoT data is structured differently and is created in real time. Large volumes of IoT-generated data must be processed, analyzed, and categorized before they can be used in decision making [6, 10].

User interface (UI): The acquired data should also be utilized to inform end users when it has been cleaned and formatted. Users, for example, must be notified when the temperature in cold storage exceeds a certain threshold. This is accomplished through the use of a user interface, which allows end users to examine the acquired data in advance. As a result, depending on the IoT applications, these end users may react to system inputs[6, 11].

III. BLOOCKCHAIN TECHNOLOGY

Blockchains are data structures made up of a series of cryptographically linked blocks. It can be a tamper-proof historical ledger for data and transaction management [12]. Satoshi Nakamoto was the first to propose blockchain, which underpins Bitcoin. Blockchain has been shown to have many essential characteristics, such as security and immutability. As a result, it may be a viable solution for addressing a variety of issues that traditional security systems face, such as centralized systems with bottlenecks and single points of failure, as well as privacy concerns [13]. The structure of the blockchain is depicted in Fig..2 [14].

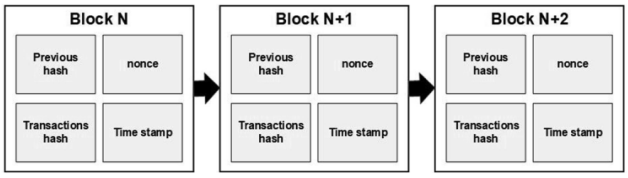

Fig.2 blockchain structure [14].

Blockchain is a technology that is an immutable distributed ledger maintained by a peer-to-peer network. For transactions uploaded to a blockchain network to be valid, network members must come to a consensus on transaction statuses. In addition, it is important to know the methodology of this technique, where transactions are placed in a block with a set of information such as nonce, timestamp, and previous hash, then this information is entered into the hash function for data hashing to be more secure. The node that will add this block to the blockchain is then chosen based on one of the consensus algorithms under specific conditions.[15].

The following are four fundamental properties of blockchains [6] :

Ledger: This is a technicality in which an advertisement is documented to provide a complete value-based history. Unlike traditional databases, blockchains do not have overruns.

• **Secure**: Because blockchains are encrypted, no one can access the information stored on them without permission.

• **shared**: Many people are involved in each record, which clarifies a hub member in a blockchain web.

• **Distributed**: A blockchain can be scattered and can change the number of nodes in a blockchain to increase flexibility and reduce the chances of a successful attack. As Blockchain is a chain of timestamped blocks linked by cryptographic hashes, as the name suggests [16].

A. Hash function

Using preimage as the input and Image as the result, a hash function turns a variable-length input into a fixed-length output. A hash function is a one-way function, which means that identifying its original Image by Image is impossible. The following are the characteristics of the perfect hash function [17]:

1) Accept any preimage length.

2) For identical preimages, the calculated Image is identical.

3) The length of any preimage Image is fixed, and it can be computed quickly.

4) Exhaustion is the only method to discover the preimage through the Image.

5) Finding another preimage that corresponds to the estimated Image of a particular preimage is tricky.

6) There is no connection between the photographs before and after the change; even minor changes in the preimage cause big changes in the image.

B. Algorithm of Consensus

On the blockchain, consensus methods ensure that each new block added to the network is the only version of the truth. All nodes in a distributed/decentralized computer network agree. Consensus algorithms are critical for blockchain networks because they ensure the integrity and security of these distributed computing platforms [3]. There are many important consensus algorithm in blockchain:

Proof of Work (PoW): It was the first method utilized to reach a worldwide consensus[18]. Within Blockchain architectures, The PoW has traditionally been the most popular means of achieving a consensus. By seeking for hash functions with a difficulty proportional to the network's processing power, PoW makes it challenging to construct a legal block and link it to a Blockchain. You must revalidate any future blocks after changing a block. The older the block being updated is, the more validations are necessary When only a few miners or groups of miners are capable of generating new blocks every ten minutes, even a newly validated block update is costly[3].

Proof of Stake (PoS): After criticism of PoW, an alternative technique called proof of stake was devised (PoS). PoS substitutes a random selection process for computing activity, with the probability of successful mining proportional to the number of validators. The stake nodes' investment in the system, i.e., coin ownership, affects the chance of generating a block.

Proof-of-Authority(PoA): In response to the risks involved with Proof-of-Work, it was first proposed as an addition to the Ethereum blockchain for checking internet usage. The core tenet of Proof-of-Authority is that only selected, trusted nodes are allowed to create new blocks. Despite centralizing the blockchain's overall membership, it's ideal for small networks and test nets [19].

C. The types of Blockchain Technology

The two most frequent types of blockchain [20] are public and private.

1-Public blockchain, which means that all network users can observe transactions, but the identities of the nodes who initiate them are hidden [1]. It's a decentralized peer-to-peer network that's not controlled by a single entity [21]. In Fig. 3 describes the Public Blockchain [22].

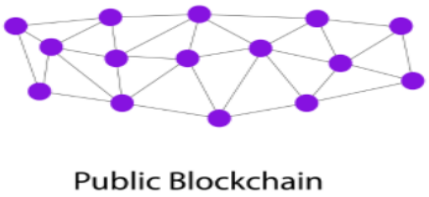

Fig 3. Public Blockchain Network for IoT [22].

2- Private blockchain: A permissioned blockchain [20, 23] sets a list of rights that players with specified characteristics must have to operate within the network. The block creation is controlled by a single entity that owns this kind. Organizations typically utilize a private blockchain to record transactions or distribute data to a small group of users [1]. In fig.4 describe the Private Blockchain [22].

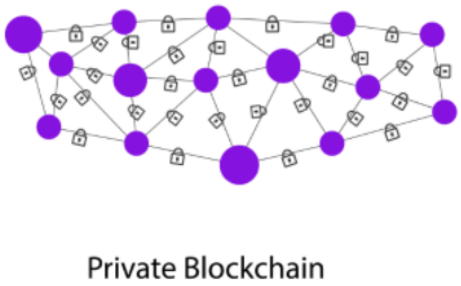

Fig 4. Private Blockchain Network for IoT [22].

3-Consortium Blockchain**:** It is a semi-decentralized kind in which the blockchain network is managed by multiple organizations. It differs from the private blockchain, which is controlled by a single entity. More than one entity operates as the authority to do mining or exchange information in this type of blockchain. Blockchains are employed in a variety of industries, including banking and government agencies [24]. In fig.5 describe the Consortium Blockchain [22].

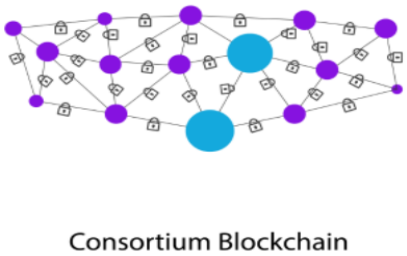

Fig 5. Consortium Blockchain Network for IoT [22].

IV. BLOCKCHAIN IN IOT

Because ecological monitoring software's potential is comprised of a cost-effective ability to construct and handle a wider range of data with greater resolution, wireless sensor networks (WSNs) are constantly used by the scientific community, these systems are regarded as an important part of ubiquitous computing [25]. In the process of connecting devices with sensors surrounding the Internet and facilitating access to information, exchange, and processing of required data from anywhere in the world and at any time via ready-made software platforms via the Internet [26], the Internet of Things has become a supporter of many areas. Decentralization, anonymity, persistency, and auditability are some of the properties of Blockchain [27]. Remember that Blockchain's unique properties offer a possible solution to IoT security issues. Decentralization, resilience, security, and identity management are all improved in IoT systems. As a result, the Blockchain can serve as a secure foundation for IoT networks. The majority of Blockchain participants must validate transactions before they can be approved and added, to the public ledger that is distributed, ensuring public visibility as well as visibility. Furthermore, there is no centralized authority for transaction approval or establishing precise communication or service access requirements for participants. Therefor is increased and widespread trust because most participating IoT network devices must agree to confirm transactions [13]. In fig.6 explains an IoT data transaction and how it can be secured using Blockchain.

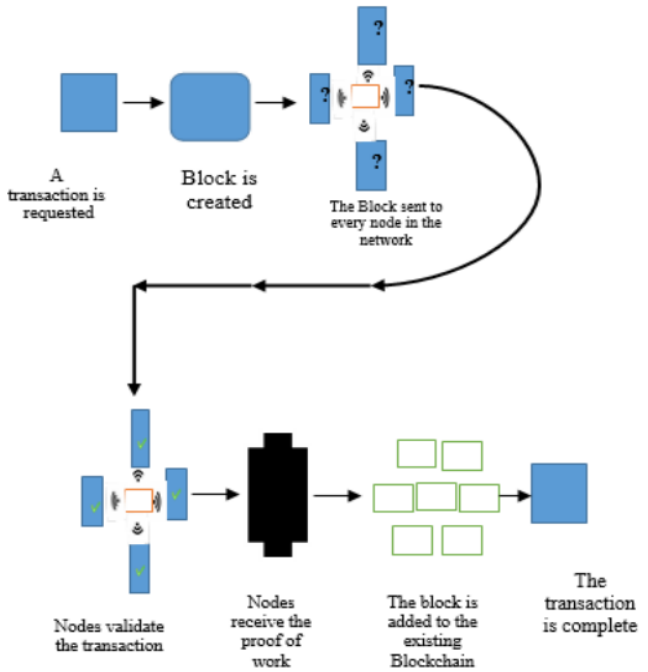

Fig 6. How Blockchain work [13]

Since the Internet of Things is a central network and transmits important and sensitive information, the issue of security is one of the most important issues that must be addressed in this network, and one of the most important techniques used to solve the issue of security is the Blockchain technology. Where the data is transferred from the Internet of Things to the Blockchain network through the application of the API and using the consensus algorithms used in this technology. Then the data is stored in the form of blocks, and after verifying its validity by the nodes participating in the network, this block will be added to the Blockchain after it is fragmented data via the hash function.

Among the most important advantages of using the blockchain with the Internet of things are:

1- Making the Internet of Things more secure, because the Blockchain is a decentralized network, so the process of penetrating it is difficult.

2- It is more private, so it is preferred to be used in many companies and institutions.

On the other hand, there are some disadvantages in integrating the Blockchain with the IoT, the most important of which are:

1- It needs high computing power.

2- It needs continuous energy because its work depends on the Internet, and in the event of any disconnection of the Internet, it leads to some problems.

V. RESERCH GAP AND SOLUTION

IoT technology has aided industrial automation and digitization in the manufacturing sector., Several innovative Internet of Things apps has improved manufacturing infrastructure quality, flexibility, and scalability, cutting errors, saving money, and improving the performance and security of manufacturing and industrial operations. [28, 29] that come to me when I think about The majority of modern IoT systems store and process sensor data in a centralized data center, which is susceptible to data breaches, single points of failure, and malicious assaults like DDoS and Sybil. [28-30]. This leads to service outages and a flood of sensor data, outweighing the IoT system's significant benefits. Furthermore, When IoT devices exchange data, data interception is a possibility, raising concerns about the collected data's reliability. The idea of combining blockchain and IoT has recently acquired a lot of traction among researchers who want to take advantage of it.

To solve the aforementioned concerns, hybrid architectures are being developed. Differences in mining rates and resource capacity imbalances between IoT devices and blockchain nodes make integrating blockchain technology into IoT applications difficult. These problems must be resolved. According to experts, autonomous agents are used in many IoT ecosystems, including healthcare, smart cities, smart homes, and electric energy commerce[31, 32]. An agent is a self-contained entity that uses sensors or data from the Internet of Things to function in place of users. Wearable sensors, cellphones, network devices, and portable computers all contribute to the huge volumes of data generated by the Internet of Things (IoT) ecosystem. Users may not always be able to deal with the onslaught of information [33]. As a result, self-contained businesses must monitor and analyze data from a wide range of IoT devices. The autonomous agent is a proactive body that can detect

and act on crucial sensor data activities without the need for human interaction [31]. Machine learning and artificial intelligence technology are widely used to create an autonomous agent that can comprehend data pouring from sensors or online sources and make decisions on its own [34].

Luo et al. [35] introduced a decentralized electricity market system based on blockchain and governed by several participants. This system is made up of two layers: a top layer that uses multi-agents to negotiate electricity trading contracts, as well as a bottom layer that settles contracts via a blockchain network. To address the scalability issue in blockchain-based designs, Qayumi et al.[36] called for multi-agent architectures, although they did not explain how this could be accomplished. Smart contracts were proposed by Norta et al.[37] for cross-organization collaboration They talked about how non-repudiating features can be achieved via a blockchain smart contract. These activities, on the other hand, are still in development and will be improved in the future. Bilal et al.[38] for the home management system, this study built a novel optimization technique as well as a cloud device architecture. This research proposes a two-level communication strategy between microgrids in the event of a failure in cloud-level communication. The authors of [39] suggested software defined networking SDN, fog computing, and a distributed blockchain-based cloud architecture model. At the network's edge and in the distributed cloud, the approach sought to manage raw IoT data streams effectively. Three layers make up the model: distributed cloud based on blockchain, SDN controller network for fog nodes based on blockchain, and IoT devices.

A. Security

An information system must traditionally meet three conditions to be secure:

• Confidentiality is one of the most important aspects of any business. Unauthorized access to the most sensitive data should be avoided.

• Integrity and reliability It ensures that unauthorized parties cannot change or delete data. It's also common to include the requirement that if an authorized person corrupts the data, the modifications should be reversible.

• Availability. When necessary, data can be accessed.

In terms of confidentiality, the section dealing with transaction data is linked to their privacy, which was previously discussed. In terms of the architecture that supports the stored data, current IoT applications tend to centralize communications in a server, a farm of servers, or the cloud. Such an approach is viable as long as the administrators of the centralized infrastructure can be trusted and the system stays secure against external and internal threats [16].

Blockchain technologies, on the other hand, for example, are decentralized, which implies that even if one node fails, the system as a whole should continue to function. In terms of integrity, it's worth noting that the foundations of a blockchain are built to hold data that can't be changed (or is extremely expensive to do so) after it's been saved. However, it should be noted that there have been times in the past when this principle has been disregarded. In 2014, for example, the money exchange network MintPal informed its users that a hacker had stolen roughly 8 million Vericoins, or roughly 30% of the platform's total coins, in an unresolved incident. The Vericoin team elected to hard fork the blockchain to avoid investor money being lost and an actor controlling 30% of the coin's proof-of-stake network capacity, reversing the harm (a hard fork is a permanent divergence from the previous version of the blockchain). As a result, while many websites claim that blockchains provide permanent storage for data that can't be modified, this is only true in the most severe cases. In IoT applications, data integrity is equally crucial, and it's often provided by third parties. To reduce the need for third-party trust, [16] presents a blockchain-based data integrity service platform for cloud-based IoT applications.

The third aspect of security is availability, which is the easiest to achieve with blockchains because they are built to be distributed systems, allowing them to function even while particular nodes are under attack. However, numerous types of attacks can risk availability [16]. A 51-percent assault (also known as a majority attack) is the most dangerous type of attack, in which a single miner can take control of the entire blockchain and make any transaction they choose. Although data is available in this situation, the attacker who controls the blockchain may be able to prevent transactions from taking place. This type of assault also compromises data security [16]. Several techniques to ensure security for BIoT applications have been proposed. Some have used machine learning techniques, while others have used more traditional methods [40].

B. To address the issue of connection

On a peer-to-peer blockchain network, all nodes stay connected to the network and use standard protocols to operate independently.

IoT devices are theoretically more prone to security breaches because of the nature of blockchain networks [32, 41]. In the settings of Ref. [42]. Smart Agent, which employs many security mechanisms to protect IoT devices from hackers, connects IoT devices to the blockchain. By focusing on Gateway services, The structure of a centralized IoT network increases the likelihood of many security vulnerabilities, including data fabrication, manipulation, and illegal access to devices [43]. Gateway services are frequently used to connect IoT equipment in smart homes to the internet and users. As a result, the smart home Gateway should include centralized systems that are both efficient and dependable. Uddin et al. [42] aided in the creation of a blockchain-based system for securely tracking smart homes and cities. Fig. 6 [32] depicts the article's smart agent and blockchain components. contained a network management module that used sign encryption to protect user data and ensure user privacy.

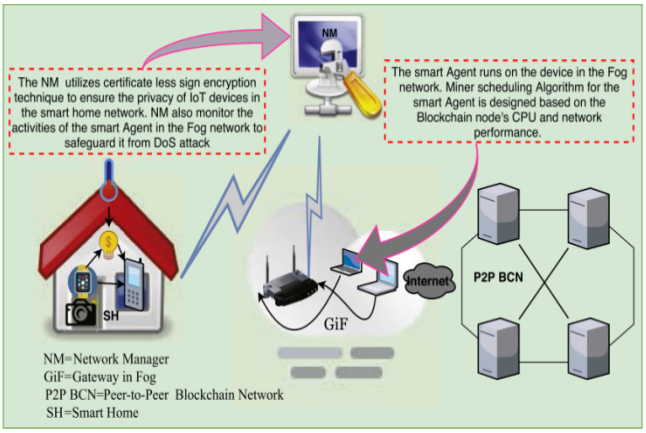

Fig. 6 . A smart home monitoring architecture based on blockchain technology [32].

C. *Ensuring both transparency and privacy*

There is a risk of data leakage when information is processed on blockchain nodes due to the fact that unencrypted data is shared and accessible by several nodes The employment of homomorphic encryption technology in the blockchain computer architecture provides for secure data storage as well as the protection of user privacy when mining[32, 44]. Homomorphic encryption, in combination with blockchain-based eHealth in a decentralized paradigm, can secure a patient's privacy[44]. The current COVID-19-related global health concern necessitates tracking positive COVID-19 patients without relying on centralized authority, tamper-proof data interchange, or privacy protection while collecting individual and healthcare institution data, so a homomorphic encryption-compatible consensus strategy must be devised. The COVID-19 pandemic's essence can be discovered in nature[45]. COVID-19 issues can be solved using distributed ledger technologies like blockchain, although user privacy cannot be guaranteed. Decentralized COVID-19 tracing apps may be constructed without the need for a centralized authority to gather and communicate user data safely and privately, blockchain technology and federated machine learning [46]. Federated learning [47] is a machine learning technique that involves training an algorithm on a distributed network of decentralized nodes or servers that do not share local data samples with a centralized server.

D. *To deal with the IoT's blockchain regulatory issues*

Blockchain offers a wide range of uses in finance, economics, and other fields, and law because of its accuracy and security properties.

Following the ransom are attack on the New York Times and the BBC earlier this year, the US Congress is looking into blockchain technology as a viable cyber-defense tool. Nonetheless, because blockchain is currently mostly unregulated [48], its abuse in underground trading networks, such as the now-defunct Silk, has resulted in many controversies. Traditional legislation is difficult to control blockchain due to its decentralized character, according to Filippi et al.[49]. Laws, on the other hand, can be enacted via smart contract technology, which translates them into blockchain code. A smart contract on the blockchain can be used to make the law a product. Within the knowledge-driven economy, Pokrovskaia et al.[50] stressed the need for a tax, finance, and social control system. They emphasized the importance of establishing an effective regulatory framework for blockchain and fog computing. Effective governance and monitoring are required for the long-term viability and adaptation of blockchain technology. For adequately controlling any uses in cyberspace, Lessig [51] outlined four methods: the law, social standards, and financial resources. These four techniques can be utilized to effectively regulate blockchain-based IoT applications. Currently, blockchain applications are uncontrolled. Blockchain may be tracked and regulated with IoT application-oriented smart contracts.

VI. Future Direction

Despite recent advancements in integrating BIoT and solutions, numerous areas still require further investigation. To develop BIoT applications and solutions, as well as make deployments safe and scalable, more study and analysis are required in numerous areas. One such field is privacy and security-based solutions for IoT applications. Although some of the security and privacy applications of BIoT have previously been investigated in this study, testing the consensus methods used in a private blockchain and applying them to a government institution such as a power utility would be helpful.

VII. Conclusion

The research was looked at from a variety of perspectives, including IoT, blockchain technologies, and privacy issues. Despite this, several technological and security challenges related to the Internet of Things remain unresolved. This review article discusses some barriers to implementing blockchain technology in the IoT space, as well as how they are being overcome. Existing blockchain and IoT articles are examined for a variety of characteristics to show their strengths and weaknesses. A detailed discussion of blockchain components and numerous conventional consensus processes are also included in this paper. In addition, this review, a detailed explanation of the Internet of Things, its methodology and components, as well as an explanation of Blockchain technology and how to deal with the Internet of Things is given so that it is clear and understandable compared to previous works.

Conflict of Interest

The authors have no conflict of relevant interest to this article.

References

[1] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance

performance and eliminate challenges," *IEEE Access,* vol. 9, pp. 54478-54497, 2021.
[2] M. M. Saleh, "WSNs and IoT Their Challenges and applications for Healthcare and Agriculture: A Survey," *Iraqi Journal for Electrical & Electronic Engineering,* 2020. DOI: 10.37917/ijeee.sceeer.3rd.6
[3] A. Pieroni, N. Scarpato, and L. Felli, "Blockchain and IoT convergence—a systematic survey on technologies, protocols and security," *Applied Sciences,* vol. 10, no. 19, p. 6749, 2020.
[4] S. Merzouk, A. Cherkaoui, A. Marzak, and S. Nawal, "IoT methodologies: comparative study," *Procedia Computer Science,* vol. 175, pp. 585-590, 2020.
[5] TeachVidvan, "Architecture of IoT," 2022. [Online]. Available: https://techvidvan.com/tutorials/architecture-of-iot/.
[6] I. Al_Barazanchi *et al.*, "Blockchain Technology-Based Solutions for IOT Security," *Iraqi Journal For Computer Science and Mathematics,* vol. 3, no. 1, pp. 53-63, 2022.
[7] S. Khan *et al.*, "Utilizing manufacturing variations to design a tri-state flip-flop PUF for IoT security applications," *Analog Integrated Circuits and Signal Processing,* vol. 103, no. 3, pp. 477-492, 2020.
[8] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "IoT-BSFCAN: A smart context-aware system in IoT-Cloud using mobile-fogging," *Future Generation Computer Systems,* vol. 109, pp. 368-381, 2020.
[9] I. F. Akyildiz and A. Kak, "The Internet of Space Things/CubeSats: A ubiquitous cyber-physical system for the connected world," *Computer Networks,* vol. 150, pp. 134-149, 2019.
[10] B. Shang, S. Liu, S. Lu, Y. Yi, W. Shi, and L. Liu, "A cross-layer optimization framework for distributed computing in IoT networks," in *2020 IEEE/ACM Symposium on Edge Computing (SEC)*, 2020: IEEE, pp. 440-444.
[11] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview," *Computers & Electrical Engineering,* vol. 87, p. 106776, 2020.
[12] M. J. Baucas, S. A. Gadsden, and P. Spachos, "IoT-based smart home device monitor using private blockchain technology and localization," *IEEE Networking Letters,* vol. 3, no. 2, pp. 52-55, 2021.
[13] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Sensors,* vol. 22, no. 3, p. 1094, 2022.
[14] M. T. Al Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT networks," *Egyptian Informatics Journal,* 2022.
[15] S. K. Lo *et al.*, "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access,* vol. 7, pp. 58822-58835, 2019.
[16] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access,* vol. 6, pp. 32979-33001, 2018.
[17] H. Zhang, W. Lang, C. Liu, and B. Zhang, "A blockchain-based security approach architecture for the Internet of Things," in *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2020, vol. 1: IEEE, pp. 310-313.
[18] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Secure information networks*: Springer, 1999, pp. 258-272.
[19] C. Natoli, J. Yu, V. Gramoli, and P. Esteves-Verissimo, "Deconstructing blockchains: A comprehensive survey on consensus, membership and structure," *arXiv preprint arXiv:1908.08316,* 2019.
[20] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?," *International Journal of Production Economics,* vol. 211, pp. 221-236, 2019.
[21] W. Mougayar, *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.
[22] Komodo, "4 Types of Blockchain Technology Explained," 2021 July,28. [Online]. Available: https://komodoplatform.com/en/academy/blockchain-technology-types/.
[23] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and informatics,* vol. 36, pp. 55-81, 2019.
[24] M. Wazid, A. K. Das, S. Shetty, and M. Jo, "A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things," *IEEE Access,* vol. 8, pp. 88700-88716, 2020.
[25] B. N. Alhasnawi, B. H. Jasim, and B. A. Issa, "Internet of things (IoT) for smart precision agriculture," *IJEEE,* vol. 16, pp. 28-38, 2020.
[26] J. A. AL-Hammoudi and B. H. Jasim, "Design and implementation of monitoring and warning (IOT) system for electricity poles," *Iraqi Journal for Electrical And Electronic Engineering,* 2020.
DOI: 10.37917/ijeee.sceeer.3rd.15
[27] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications,* vol. 125, pp. 251-279, 2019.
[28] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged decentralized IoT eHealth framework," *Internet of Things,* vol. 9, p. 100159, 2020.
[29] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications,* vol. 25, no. 6, pp. 12-18, 2018.
[30] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against

sybil attacks," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, 2008: IEEE, pp. 3-17.
[31] R. J. Tom, S. Sankaranarayanan, and J. J. Rodrigues, "Agent negotiation in an iot-fog based power distribution system for demand reduction," *Sustainable energy technologies and assessments,* vol. 38, p. 100653, 2020.
[32] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in iot: Challenges and solutions," *Blockchain: Research and Applications,* vol. 2, no. 2, p. 100006, 2021.
[33] J. K. M. Verame, "Helping users adopt and delegate agency to autonomous agents in everyday life," University of Southampton, 2018.
[34] D. Calvaresi, A. Dubovitskaya, J. P. Calbimonte, K. Taveter, and M. Schumacher, "Multi-agent systems and blockchain: Results from a systematic literature review," in *International conference on practical applications of agents and multi-agent systems*, 2018: Springer, pp. 110-126.
[35] F. Luo, Z. Y. Dong, G. Liang, J. Murata, and Z. Xu, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Transactions on Power Systems,* vol. 34, no. 5, pp. 4097-4108, 2018.
[36] K. Qayumi, "Multi-agent based intelligence generation from very large datasets," in *2015 IEEE International Conference on Cloud Engineering*, 2015: IEEE, pp. 502-504.
[37] A. Norta, A. B. Othman, and K. Taveter, "Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration," in *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, 2015, pp. 244-257.
[38] B. N. Alhasnawi, B. H. Jasim, P. Siano, and J. M. Guerrero, "A novel real-time electricity scheduling for home energy management system using the internet of energy," *Energies,* vol. 14, no. 11, p. 3191, 2021.
[39] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *Ieee Access,* vol. 6, pp. 115-124, 2017.
[40] C. Nartey *et al.*, "On blockchain and IoT integration platforms: current implementation challenges and future perspectives," *Wireless Communications and Mobile Computing,* vol. 2021, 2021.
[41] F. Ellouze, G. Fersi, and M. Jmaiel, "Blockchain for internet of medical things: A technical review," in *International Conference on Smart Homes and Health Telematics*, 2020: Springer, pp. 259-267.
[42] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged task migration in body area sensor networks," in *2019 25th Asia-Pacific Conference on Communications (APCC)*, 2019: IEEE, pp. 177-184.
[43] K. Gu, L. Yang, and B. Yin, "Location data record privacy protection based on differential privacy mechanism," *Information Technology and Control,* vol. 47, no. 4, pp. 639-654, 2018.
[44] R. Shrestha and S. Kim, "Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities," in *Advances in Computers*, vol. 115: Elsevier, 2019, pp. 293-331.
[45] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE access,* vol. 8, pp. 90225-90265, 2020.
[46] A. Hard *et al.*, "Federated learning for mobile keyboard prediction," *arXiv preprint arXiv:1811.03604,* 2018.
[47] J. Xie *et al.*, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 393-430, 2018.
[48] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance,* 2017.
[49] S. Hassan and P. De Filippi, "The expansion of algorithmic governance: from code is law to law is code," *Field Actions Science Reports. The journal of field actions,* no. Special Issue 17, pp. 88-90, 2017.
[50] N. N. Pokrovskaia, "Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation," in *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*, 2017: IEEE, pp. 709-712.
[51] L. Lessig, "The law of the horse: What cyber law might teach," *Harv. L. Rev.,* vol. 113, p. 501, 1999.