Indonesian Journal of Electrical Engineering and Computer Science
Vol. 31, No. 3, September 2023, pp. 1673∼1683
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v31.i3.pp1673-1683

The blockchain internet of things: review, opportunities, challenges, and recommendations

Mahmood A. Al-Shareeda[1], Murtaja Ali Saare[2], Selvakumar Manickam[1]
[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia
[2]Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

Article Info

Article history:

Received Apr 2, 2023
Revised May 9, 2023
Accepted May 19, 2023

Keywords:

BIoT challenges
BIoT recommendations
BIoT review
Blockchain
Internet of things

ABSTRACT

A new technology known as the internet of things (IoT) allows both physical and virtual items to be linked and communicated with one another, creating new digital services that enhance our fineness of sustenance. The IoT system has a number of benefits, but because of its present centralized architecture, there are several problems with regard to data integrity, security, privacy, and single points of failure. The future development of IoT applications is hampered by these difficulties. To tackle these problems, it might be best to integrate the IoT with one of the distributed ledger solutions. The blockchain is one of the most frequent and well-liked varieties of distributed ledger technologies. Numerous advantages can result from integrating blockchain technology with the IoT called blockchain internet of things (BIoT). In this paper, we show a brief overview of blockchain, its components of blockchain, and its features of blockchain. Meanwhile, we describe the architecture of BIoT, issues of BIoT, and BIoT applications. Additionally, this paper provides a future research challenge and open issues.

Corresponding Author:

Selvakumar Manickam
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
11800 USM, Penang, Malaysia
Email: selva@usm.my

1. INTRODUCTION

Internet of things (IoT) adoption will be severely constrained in the future as a result of the inadequacy of conventional security mechanisms alone, such as cryptographic techniques [1], [2]. IoT is predicated on the inherent insecurity of the Internet, where information security was designed as an afterthought, as is obvious by ongoing patches and manual handling [3], [4]. Furthermore, the IoT extends network connectivity and computing capability to objects with low computational capacity, such as sensors and disposable items, enabling these devices to independently produce, distribute, and consume data [5], [6].

Being a distributed, impervious to corruption, and secure ledger Blockchain has the ability to overcome crucial security issues in databases. IoT lawsuits, in particular regarding data reliability and integrity [7], [8]. Blockchain enables software programs to transmit and record transactions and events in a distributed and reliable (peer-to-peer) way. Blockchain is widely utilized in applications and is quickly increasing in popularity. Incorporating distributed storage, digital contracts [9], [10], and smart contracts property [11], [12]. The potential uses of blockchain in the IoT include capturing events (such as moisture, position alters, or temperature) and producing tamper-resistant ledgers that can only be accessed by specific parties, such as certain supply chain participants.

However, none of the previous studies have provided more details and combined two technologies, blockchain and IoT. Additionally, any future efforts to improve the security and permanence of BIoT could look to this paper as a foundational resource. In this study, we examine the main benefits and drawbacks of using blockchain in IoT applications. The most recent Blockchain systems' data formats and consensus mechanisms are examined. The constraints of the available Blockchain technology for IoT applications are highlighted, along with potential future research areas.

The rest of this work is arranged as below. Section 2 shows a brief overview of blockchain, components of blockchain, and features of blockchain. Section 3 describes the architecture of blockchain internet of things (BIoT), issues of BIoT, and BIoT applications. Section 4 and section 5 present a future research challenge and open issues. Section 6 reviews discussion of these related works. Lastly, this paper will concluded in section 7.

2. BLOCKCHAIN

At the end of 1990, up until Szabo invented a decentralized digital currency, the world continued to use centralized architecture, where a single server is required to regulate the treatment and scheduling of jobs. Bitcoin was made available ten years later. Following Satoshi Nakamoto's article in 2009, blockchain technology became widely used [13], [14]. An introduction to blockchain technology is provided in this section.

2.1. A brief overview of blockchain

A number of corporations and scholars have recently become interested in blockchain technology because of all the advantages it offers over current alternatives [15], [16]. To put it simply, a blockchain is a distributed, decentralised, and immutable ledger that keeps track of all transactions ever made within a particular peer-to-peer network [17]-[19]. In order for a transaction to be recorded in the distributed ledger, nearly all devices need to enrol their agreement. There must be a way to reach a consensus. The most common and well-liked consensus mechanisms are proof of work (PoW) and proof of stake (PoS). Each batch of dealings gets its own "block" in the ledger. The blocks in a blockchain are linked to one another using a hash function and a timestamp. A "blockchain" is a series of linked blocks, hence the name. The hash function's primary job is to ensure the integrity of the information contained within a block [20], [21]. Because blockchain technology promotes sharing of data among its users, every node in the network is always up to date with the latest blocks and transactions [22].

2.2. Components of blockchain

Compared to current systems, blockchain technology can offer a number of advantages. As shown in Figure 1, the blockchain is made up of a number of fundamental parts, including the block, minor, ledger, transaction, hashing, and consensus procedures. Compared to current systems, blockchain technology can offer a number of advantages [23]. On the other side, the ledger is used to keep track of every transaction that has ever been made by every user that has joined the network. Furthermore, the ledger was divided up among the participating nodes so that every user had a copy of it.

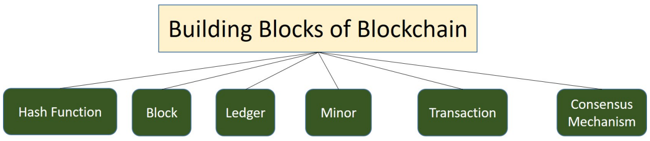

Figure 1. Main components of blockchain

One of the foundational elements of the blockchain is the block. There are a number of transactions in each block. A unique hash value from the block before was stored in the current block to chain the blocks together. This link forms a chain when connected. Each block's content is checked for data integrity using the hash function. To find a block, the minors must solve the hash function, which is essentially a mathematical problem. The hash function's usefulness lies in the fact that it prevents collisions, making it exceedingly hard to produce two digital data sets with the same hash [24].

The simplest unit of procedure or operation is a transaction, which is how a group of transactions is aggregated and stored in a block. Without the majority of the active nodes in the blockchain system recording their approval, a specific transaction cannot be included in the block. For minors, the size of a transaction matters because smaller transactions cost less processing power and are simpler to verify. Minors are machines or agents that try to resolve a challenging mathematical puzzle (usually a hash function) in order to discover a new block. Each node assembles a group of transactions into a block and then performs an operation to determine the block's proof-of-work to begin the process of discovering a new block [25].

2.3. Features of blockchain

For a variety of industries and applications, blockchain can offer a number of benefits. Some of the characteristics of this new technology are similar and include:

- Decentralization: the usual blockchain environment is decentralized, distributed, and based on peer-to-peer (P2P) technology among communicating devices.
- Immutability: the capacity of blockchain to ensure the integrity of transactions by generating immutable ledgers is one of its key features.
- Transparency: blockchain offers a high level of transparency in comparison to the centralized approach, wherever the server of central alone has fully access and control to all information. All nodes have access to all the information about transactions that have ever taken place in their system.
- Better security: the fact that blockchain technology offers better security than current systems is one of its benefits.
- Cost reduction: blockchain technology lowers the expenses associated with installing and maintaining big centralized servers, as opposed to centralized architecture, in which the centralized server must be built using an advanced and full software and hardware networks.
- Anonymity: blockchain gives an anonymous identity to secure the devices' privacy despite using a distributed ledger shared by all users.
- Autonomy: one characteristic that blockchain technology can offer is the capacity for autonomous decision-making.

3. BLOCKCHAIN INTERNET OF THINGS

3.1. Architecture of BIoT

Figure 2 depicts the generalized design for the IoT system network using blockchain as an application. The blockchain layer will be introduced between the communication layer and the application layer for this purpose [26]. The following five sublayers make up the blockchain layer in total:

- Data sublayer: the perception layer sends its IoT data to the data sublayer, which then encrypts and hashes the data using asymmetric cryptography. The blockchain implements its own special form of cryptography and hashing.
- Network sublayer: the network sublayer is atop the communication layer, which uses wired or wireless connections to link together individual nodes (things that make up the IoT).
- Consensus sublayer: in this section, we introduce the layer's consensus algorithm, which may be PoW, PoS, or practical byzantine fault tolerance (PBFT). The primary focus of this layer is ensuring the integrity of each IoT data block.
- Incentive sublayer: this layer describes how rewards will be distributed among the approved users who took part in the mining process.
- Application sublayer: this layer involves a focus on blockchain's potential business uses in settings as varied as supply chain management, the food industry, and the energy sector.

3.2. Issues of BIoT

Applications built on the IoT can benefit from the security and immutability offered by blockchain technology. Using various kinds of encryption and digital signatures, the network traffic of IoT devices is made more secure. Additionally, each participant in the IoT system has a set of public and private keys that they can use to securely change information between any two of the system's nodes.

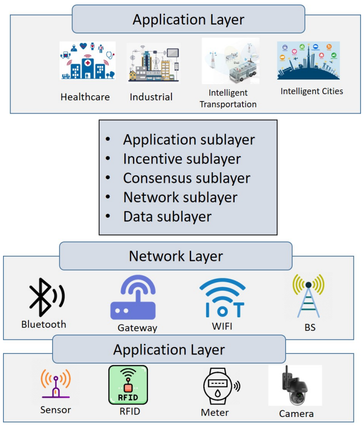

Figure 2. Blockchain internet of things

3.3. BIoT applications

Data is uploaded by a lot of end devices to IoT networks, which are data-centric. Because of this, IoT threats could target both data and devices. Blockchain technology address security issues with end devices as well as sensory data.

a. Correctness of sensory data: IoT-related data, such as sensory data, can be isolated from blockchain-related data, such as account, balance, and transaction fees, in blockchain-powered IoT networks.
b. Malicious behaviors of IoT devices: the following three forms of harmful end-device behaviors in IoT-blockchain can be summed up:
   - Transmitting transactions with forge signatures, which the blockchain system can detect, penalize, and reject.
   - Algorithms that can detect counterfeit information and punish the nodes who originated the transaction are needed to eliminate transactions that have valid signatures but questionable data.
   - Resource consumption, such as denial-of-service (DoS), which can be avoided by transaction fee mechanisms.

4. STATE OF THE ARTS

This section provides the state of the arts, including future research challenges for using BIoT. According to the functions that blockchain performs, this section has divided future research on BIoT use into four aspects: trustworthy third party, data security, access control and automatic payment platforms, as shown in Figure 3. This classification is upper-layer application scenario-focused; we think this is a method that makes sense.

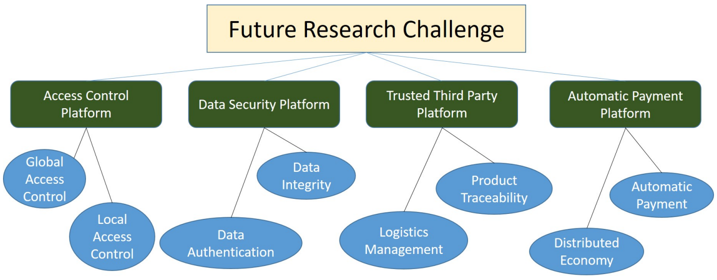

Figure 3. Aspects of future research challenge in state of the arts

4.1. Access control platform

This subsection categorizes this platform into two aspects. We only focus on global access control and local access control. These controls are described as follows.

4.1.1. Global access control

To provide global operations like authenticity, authority, and key management in accordance with the access control policy, the blockchain in the first class, in addition to serving as a distributed ledger, also makes use of intelligent contracts. Ali *et al.* [27] presented a unique decentralized architecture with demands on event and query base permission delegation for permission delegation and access control for IoT applications. Pal *et al.* [28] suggested a blockchain-enabled, identity-less, asynchronous, and decentralized delegation architecture for the IoT. Tapas *et al.* [29] recommended putting access control methods for the smart city application on the blockchain. The goal of this effort was to lower the need for third parties confidence. Zhang *et al.* [30] developed an access control method that can flexibly establish access control policies enabled intelligent contracts for generic IoT applications [16]. Pouraghily *et al.* [31] offered a fascinating IoT access control solution built on a blockchain. They imagined a situation in which the household would give the tenant control of the camera in a rental home. Using an intelligent contract to control the camera's permissions is quite practical. Huh *et al.* [32] presented a remote access control-based IoT device management system. To handle and keep track of the electrical appliances in the house, they developed two smart contracts. Users can send messages to the IoT gadgets in their homes using their mobile phones [33]. Additionally, Outchakoucht *et al.* [34] suggested an access control system for IoT, or the IoT the smart contracts on the blockchain are where the access control method is laid forth. The access control restrictions in the smart contracts were dynamically changed by the introduction of reinforcement learning techniques. Similar to this, several researchers [35]-[39] suggested a blockchain-based IoT access control delegation system.

4.1.2. Local access control

The second class just uses a distributed ledger-based blockchain to hold access and realization rules and keep local authenticity and authority separate from storage. The second group is referred to as local access control. Barger *et al.* [40] suggested that the IoT access control plane be managed using the hyperledger fabric [41]. They disconnect the control plane and data plane by using the cloud object storage to save the elements off-chain. They suggested leveraging blockchain smart contracts to facilitate access control. Andersen *et al.* [42] presented the wireless access vehicular environments (WAVE) access control architecture for use in intelligent city services. The suggested method addresses the issues of out-of-order delegations, heterogeneity, and cross-domain interactions. Shafagh *et al.* [43] presented a distributed access control layer for IoT data sharing based on blockchain technology. The plan also uses the technique of separating the control plane from the data plane. Similar to this, several researchers [11], [44]-[47] designed a blockchain-enabled IoT local access control system.

4.2. Data security platform

This subsection categorizes existing research into two aspects. One is to guarantee information authentication; another is to preserve information integrity. These two aspects are described as follows.

4.2.1. Data authentication

A type of data security method known as data authentication identifies the source of the data, its owner, and any modifications made to the data [48]. Ramachandran and Kantarcioglu [49] suggested the use of a mechanism called SmartProvenance to safeguard information authentication. In the suggested system, the data provenance path is recorded on the blockchain. Through a voting smart contract, the data source is chosen. In cloud computing, where users generate data, Liang *et al.* [50] presented a way for tracking where that data originated. They proposed the use of the blockchain as a distributed trust centre and distributed security database, called ProveChain, to protect user anonymity. An alternative approach was suggested by Casado-Vara *et al.* [51] to enhance data quality and false data detection. The layer based edge computing of IoT technology now employs a cooperative approach according to game theory, which lowers the mistake brought on by the IoT sensor. Similar to this, several researchers [52], [53] suggested a blockchain-based IoT data authentication

4.2.2. Data integrity

Data integrity means that there has been no tampering with the data, making it reliable [54]. Yu *et al.* [55] investigated common IoT privacy and security issues and created an approach to link blockchain with IoT, which can offer excellent assurance for IoT data and a variety of functionality and the desired scalability, including authentication, decentralised payment, and other features. Krishnan *et al.* [56] offered an architecture for the information safety preserving of IoT applications, such as a smart city application, that is similar to the usual IoT-cloud architecture. Song *et al.* [57] used hyperledger fabric to safeguard data availability and integrity in the IoT-cloud architecture. The network functions as a separate private network among the cloud and the edge thanks to Fabric's containerization. Liu *et al.* [58] suggested integrating blockchain into the IoT cloud architecture. The distinction is the usage of Ethereum to archive cloud data. Similar to this, several researchers [59]-[63] suggested a blockchain-based IoT data integrity.

4.3. Trusted third party platform

This subsection categorizes IoT-based supply chain solutions. We studied two groups employing blockchain as a reliable third party. These points are described as follows.

4.3.1. Management of logistics

The first is output traceability, and the second is logistical management. The blockchain is primarily utilized in logistics management to combine the essential information from each component of the supply chain, which aids in supply chain management performance analysis. Tijan *et al.* [64] analyzed a variety of instances and the potential and difficulties of using blockchain systems in supply chain management [65]. Hackius and Peterse [66] examined a variety of instances and researched the potential and difficulties of using blockchain systems in supply chain management. Kuhi *et al.* [67] investigated the supply chain management performance metrics paradigm and contrasted the advantages of various blockchain systems as a remedy. Similar to this, several researchers [68]-[71] suggested a blockchain-based logistics management.

4.3.2. Product traceability

Later, smart contracts are utilized to achieve the automation of the parties' transaction operations. The primary function of the blockchain in product traceability is to offer a secure database that can be used to thwart fraud. At the time in 2017, Korpela *et al.* [72] highlighted the status and future development trends of digital supply chains according to the blockchain. Protecting product quality is the goal of product traceability. Blockchain, according to Zhang *et al.* [73] was crucial for supply chain management's quality control. Sidorov *et al.* [74] suggested a reliable, incredibly lightweight, and two-way radio frequency identification (RFID) authentication mechanism. RFID tag authentication is aided by the blockchain, which is also utilized to safely store the tracking information from the tags. Similar to this, several researchers [9], [75]-[77] suggested blockchain-based product traceability.

4.4. Automatic payment platform

4.4.1. Distributed economy

Shahid *et al.* [78] presented a leasing system for the sharing economy. The sharing economy-trust point (SE-TP) concept is put forth in this model. An entity's leasing institution is called SE-TP. Rahman *et al.* [21], [79] suggested a sharing economy service architecture for smart cities that combine blockchain, AI technologies, and edge computing. Al-Shareeda *et al.* [19] and Kaid and Eljazzar [80] investigated how integrating enterprise resource planning (ERP) and blockchain will affect that. Although the many divisions within the supply chain organisation may operate independently of one another [81], frequent information interchange and cash exchanges take place between them. Similar to this, several researchers [82]-[86] suggested a blockchain-based distributed economy.

4.4.2. Automatic payment

A blockchain-based electric vehicle (EV) billing network called IOTA has been proposed by Strugar *et al.* [87]. The M2M unattended electric vehicle purchase transaction is made possible by the platform, which also offers free transaction fees. Pouraghily and Wolf [88] presented a blockchain-based lightweight payment protocol for IoT platforms. To support transactions on low-power devices, they used a ticket-based verification protocol (TBVP). They introduced the contract manager (CM) and the transaction verifier (TV) as two conceptually distinct entities. Wu *et al.* [89] proposed to provide intelligent grid demand side performance using the blockchain. They recorded price and power calculation models on the blockchain, and they utilised intelligent contracts to save transaction information and send assets automatically.

5. RECOMMENDATIONS

In order to create more stable IoT systems using blockchain, this section highlights recommendations.

- Performance of blockchains: both public chains and consortium chains are utilised for IoT applications. In general, consortium chains are more effective than public chains, but they also call for trust presumptions. It is currently unclear how their performance varies with the quantity of nodes, consensus procedures, system conditions, etc. Finding ways to enhance blockchain performance to match IoT technology is also possible after gaining this information.
- The blockchain platform's own security: blockchain is frequently utilised to improve IoT application security. However, the blockchain itself has security vulnerabilities because it is a form of software. In fact, smart contract flaws have already been discovered. Particularly for payment apps as well as other applications, this could have major repercussions. Systematic research is necessary to comprehend the blockchain platform's security.
- Still in its infancy: research studies that demonstrate a topic are the primary works. Building benchmarks for these apps and having actual, larger implementations are both intriguing. Benchmarks are useful for creating blockchain-based IoT apps that are more effective.

6. DISCUSSION

To create blockchain-based access control systems for the IoT, numerous problems must be resolved. Blockchain is now used as a temporary fix for data security. variety of IoT data, like was just discussed. Making these solutions usable requires Future research efforts must address a few issues.

- Performance: as the IoT grows rapidly, controlling IoT devices that develop exponentially is a significant obstacle to blockchain performance.
- User privacy preserving: blockchain relies on consensus to keep a ledger current. The transactions are visible to every node.
- Security: access control-enforcing smart contract security is also a problem.
- The bottleneck of blockchain technology is low throughput, which restricts its use. The amount of managed data for supply chain management may be enormous.
- The challenge of connecting tangible objects with digital ledgers is the problem with asset digitization. The only thing the blockchain can ensure is internal system confidence.
- There is a crucial presumption that sensor information is exchanged and traded in shared economy scenarios for smart cities. The blockchain devices must be as near as feasible to the information source in order to satisfy cross-trust domain transactions of IoT information and cut costs.
- Blockchain invariably causes issues with low throughput in order to seek security and decentralisation. In order to reach consensus, each change to the ledger must be broadcast to the whole blockchain system, which reduces throughput.
- The first focuses on fresh methods for raising performance. Performance is frequently a problem in contemporary blockchain systems, especially for the public chain.
- Enhancing the reliability of data provenance is another research challenge. Blockchain is employed in current research to safeguard provenance data, but in reality, it can't fully ensure the accuracy of the information source, which is input by actual people and organizations.
- It can be hard to ensure the safety of intelligent contracts. A piece of code called a smart contract can run automatically. However, code may also be weak and subject to attack.

7. CONCLUSION AND FUTURE WORK

Given the multiple problems with the centralised IoT design, transforming it into one of the distributed ledger systems may be the best choice. The blockchain is a well-known type of distributed ledger. Decentralisation is used to improve performance and remove a potential weak spot. Additionally, blockchain's tamper-proof and immutability properties improve security and data integrity. BIoT integration can overcome centralised IoT system problems and pave the way for promising future advancements. As a result, the goal of this study was to present an in-depth analysis of how to integrate BIoT technology. The manuscript has gave a thorough demonstration of merging BIoT by highlighting how blockchain addressed IoT hardness after outlining the fundamentals of BIoT. Additionally, recent studies showing the fusion of blockchain and IoT are also discussed. Then, it is addressed how blockchain technology may be used as a service to develop various functionalities for a variety of BIoT applications.

REFERENCES

[1] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," *Sony Corporation*, pp. 7–10, 2008..

[2] Z. G. Al-Mekhlafi *et al*., "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, Mar. 2023, doi: 10.3390/s23073543.

[3] B. Fabian and O. Günther, "Security challenges of the EPCglobal network," *Communications of the ACM*, vol. 52, no. 7, pp. 121–125, Jul. 2009, doi: 10.1145/1538788.1538816.

[4] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 30, no. 2, pp. 778–786, May 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[5] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview." The Internet Society (ISOC), 2015.

[6] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "Intelligent drone-based IoT technology for smart agriculture system," in *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)*, Nov. 2022, pp. 41–45, doi: 10.1109/ICDSIC56987.2022.10076170.

[7] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: a survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[8] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-fog: a novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, Mar. 2023, doi: 10.3390/math11061446.

[9] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[10] S. U. A. Laghari, S. Manickam, A. K. Al-Ani, M. A. Al-Shareeda, and S. Karuppayah, "ES-SECS/GEM: an efficient security mechanism for SECS/GEM communications," *IEEE Access*, vol. 11, pp. 31813–31828, 2023, doi: 10.1109/ACCESS.2023.3262310.

[11] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and Solutions," Aug. 2016, [Online]. Available: http://arxiv.org/abs/1608.05187.

[12] B. A. Mohammed *et al*., "FC-PA: fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023, doi: 10.1109/ACCESS.2023.3247222..

[13] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system." 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf..

[14] Z. G. Al-Mekhlafi *et al*., "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, p. 872, Feb. 2023, doi: 10.3390/electronics12040872.

[15] A. Back *et al*., "Enabling blockchain innovations with pegged sidechains." 2018, [Online]. Available: https://www.blockstream.com/sidechains.pdf.

[16] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.

[17] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, *Blockchain technology: beyond bitcoin*. 2016.

[18] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, Jan. 2023, doi: 10.3390/math11020399.

[19] M. A. Al-Shareeda, S. Manickam, M. A. Saare, S. Karuppayah, and M. A. Alazzawi, "Detection mechanisms for peer-to-peer botnets: a comparative study," in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, Aug. 2022, pp. 267–272, doi: 10.1109/ICCITM56309.2022.10031860.

[20] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with internet of things: benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, Jun. 2018, doi: 10.5815/ijisa.2018.06.05.

[21] M. A. Al-Shareeda, S. Manickam, M. A. Saare, S. Karuppayah, and M. A. Alazzawi, "A brief review of advanced monitoring mechanisms in peer-to-peer (P2P) botnets," in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, Aug. 2022, pp. 312–317, doi: 10.1109/ICCITM56309.2022.10031721.

[22] H. F. Atlam and G. B. Wills, "Intersections between IoT and distributed ledger," in *Advances in Computers*, Elsevier, 2019, pp. 73–113.

[23] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, Jun. 2017, doi: 10.1016/j.apenergy.2017.03.039.

[24] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for Risk-based access control model for IoT," *Internet of Things*, vol. 6, p. 100052, Jun. 2019, doi: 10.1016/j.iot.2019.100052.

[25] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Dec. 2016, pp. 1392–1393, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[26] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[27] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in internet of things (BACI)," *Computers & Security*, vol. 86, pp. 318–334, Sep. 2019, doi: 10.1016/j.cose.2019.06.010.

[28] S. Pal, T. Rabehaja, M. Hitchens, V. Varadharajan, and A. Hill, "On the design of a flexible delegation model for the internet of things using blockchain," I*EEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3521–3530, May 2020, doi: 10.1109/TII.2019.2925898.

[29] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based IoT-cloud authorization and delegation," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, Jun. 2018, pp. 411–416, doi: 10.1109/SMARTCOMP.2018.00038.

[30] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019, doi: 10.1109/JIOT.2018.2847705.

[31] A. Pouraghily, M. N. Islam, S. Kundu, and T. Wolf, "Poster abstract: privacy in blockchain-enabled IoT devices," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Apr. 2018, pp. 292–293, doi: 10.1109/IoTDI.2018.00045.

[32] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467, doi: 10.23919/ICACT.2017.7890132.

[33] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 29, no. 1, pp. 518–526, Jan. 2022, doi: 10.11591/ijeecs.v29.i1.pp518-526.

[34] A. Outchakoucht, H. Es-Samaali, and J. Philippe, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, 2017, doi: 10.14569/IJACSA.2017.080757.

[35] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: a blockchain-enabled decentralized capability-based access control for IoTs," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1027–1034, doi: 10.1109/Cybermatics_2018.2018.00191.

[36] O. Alphand *et al.*, "IoTChain: a blockchain security architecture for the internet of things," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2018, pp. 1–6, doi: 10.1109/WCNC.2018.8377385.

[37] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the internet of things," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, Jun. 2018, pp. 77–83, doi: 10.1145/3205977.3205993.

[38] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, Dec. 2016, doi: 10.1002/sec.1748.

[39] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[40] A. Barger, Y. Manevich, V. Bortnikov, Y. Tock, M. Factor, and M. Malka, "Shared cloud object store, governed by permissioned blockchain," in P*roceedings of the 11th ACM International Systems and Storage Conference*, Jun. 2018, pp. 114–114, doi: 10.1145/3211890.3211915.

[41] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, Jan. 2014, doi: 10.1016/j.jnca.2013.02.036.

[42] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, "Wave: a decentralized authorization system for IoT via blockchain smart." 2017.

[43] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, Nov. 2017, pp. 45–50, doi: 10.1145/3140649.3140656.

[44] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.

[45] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications," *Sustainability*, vol. 14, no. 23, p. 15900, Nov. 2022, doi: 10.3390/su142315900.

[46] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: a secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, p. 155014771984415, Apr. 2019, doi: 10.1177/1550147719844159.

[47] J. Wan, J. Li, M. Imran, D. Li, and Fazal-e-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, Jun. 2019, doi: 10.1109/TII.2019.2894573.

[48] P. Buneman, S. Khanna, and T. Wang-Chiew, "Why and where: a characterization of data provenance," in *Database Theory — ICDT 2001. ICDT 2001. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, 2001, pp. 316–330.

[49] A. Ramachandran and M. Kantarcioglu, "SmartProvenance," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, Mar. 2018, pp. 35–42, doi: 10.1145/3176258.3176333.

[50] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.

[51] R. Casado-Vara, F. de la Prieta, J. Prieto, and J. M. Corchado, "Blockchain framework for IoT data quality via edge computing," in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*, Nov. 2018, pp. 19–24, doi: 10.1145/3282278.3282282.

[52] F. Angeletti, I. Chatzigiannakis, and A. Vitaletti, "Privacy preserving data management in recruiting participants for digital clinical trials," in *Proceedings of the First International Workshop on Human-centered Sensing, Networking, and Systems*, Nov. 2017, pp. 7–12, doi: 10.1145/3144730.3144733.

[53] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, Jul. 2018, doi: 10.1007/s10916-018-0982-x.

[54] D. E. Denning and P. J. Denning, "Data security," *ACM Computing Surveys*, vol. 11, no. 3, pp. 227–249, Sep. 1979, doi: 10.1145/356778.356782.

[55] 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, Dec. 2018, doi: 10.1109/MWC.2017.1800116.

[56] K. N. Krishnan, R. Jenu, T. Joseph, and M. L. Silpa, "Blockchain based security framework for IoT implementations," in *2018 International CET Conference on Control, Communication, and Computing (IC4)*, Jul. 2018, pp. 425–429, doi: 10.1109/CETIC4.2018.8531042.

[57] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized IoT networks," in *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, Jun. 2018, pp. 169–174, doi: 10.1109/SYSOSE.2018.8428720.

[58] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *2017 IEEE International Conference on Web Services (ICWS)*, Jun. 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.

[59] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[60] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in *CEUR Workshop Proceedings*, 2017, vol. 1816, pp. 146–155.

[61] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019, doi: 10.1109/TII.2019.2893433.

[62] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure FaBric blockchain-based data transmission technique for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019, doi: 10.1109/TII.2019.2907092.

[63] 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 Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020, doi: 10.1109/TII.2019.2936278.

[64] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustainability*, vol. 11, no. 4, p. 1185, Feb. 2019, doi: 10.3390/su11041185.

[65] M. A. Al-Shareeda and S. Manickam, "MSR-DoS: modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks," *IEEE Access*, vol. 10, pp. 120606–120615, 2022, doi: 10.1109/ACCESS.2022.3222488.

[66] N. Hackius and M. Petersen, "Blockchain in Logistics and supply chain: trick or treat?," in *Hamburg International Conference of Logistics (HICL) 2017*, 2017, vol. 9783745043, no. April, pp. 1–18, doi: 10.15480/882.1444.

[67] K. Kuhi, K. Kaare, and O. Koppel, "Ensuring performance measurement integrity in logistics using blockchain," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, Jul. 2018, pp. 256–261, doi: 10.1109/SOLI.2018.8476737.

[68] Y. Fu and J. Zhu, "Big Production enterprise supply chain endogenous risk management based on blockchain," *IEEE Access*, vol. 7, pp. 15310–15319, 2019, doi: 10.1109/ACCESS.2019.2895327.

[69] S. S. Arumugam *et al.*, "IOT enabled smart logistics using smart contracts," in *2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS)*, Aug. 2018, pp. 1–6, doi: 10.1109/LISS.2018.8593220.

[70] J. Li, F. Qu, X. Tu, T. Fu, J. Guo, and J. Zhu, "Public philanthropy logistics platform based on blockchain technology for social welfare maximization," in *2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS)*, Aug. 2018, pp. 1–9, doi: 10.1109/LISS.2018.8593217.

[71] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: a lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018, doi: 10.1109/ACCESS.2018.2875782.

[72] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Hawaii International Conference on System Sciences (HICSS)*, 2017, pp. 4182–4191, doi: 10.24251/HICSS.2017.506.

[73] Y. Zhang, X. Xu, A. Liu, Q. Lu, L. Xu, and F. Tao, "Blockchain-based trust mechanism for IoT-based smart manufacturing system," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1386–1394, Dec. 2019, doi: 10.1109/TCSS.2019.2918467.

[74] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains," *IEEE Access*, vol. 7, pp. 7273–7285, 2019, doi: 10.1109/ACCESS.2018.2890389.

[75] J. Li and X. Wang, "Research on the application of blockchain in the traceability system of agricultural products," in *2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC)*, May 2018, pp. 2637–2640, doi: 10.1109/IMCEC.2018.8469456.

[76] Y. Cao, F. Jia, and G. Manogaran, "Efficient traceability systems of steel products using blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6004–6012, Sep. 2020, doi: 10.1109/TII.2019.2942211.

[77] M. Westerkamp, F. Victor, and A. Kupper, "Blockchain-based supply chain traceability: token recipes model manufacturing processes," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1595–1602, doi: 10.1109/Cybermatics_2018.2018.00267.

[78] M. R. Shahid, S. Mahmood, S. Hafeez, B. Zahid, S. Jabbar, and R. Ashraf, "Blockchain based share economy trust point," in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, Jul. 2019, pp. 1–5, doi: 10.1145/3341325.3342026.

[79] 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, doi: 10.1109/ACCESS.2019.2896065.

[80] D. Kaid and M. M. Eljazzar, "Applying blockchain to automate installments payment between supply chain parties," in *2018 14th International Computer Engineering Conference (ICENCO)*, Dec. 2018, pp. 231–235, doi: 10.1109/ICENCO.2018.8636131.

[81] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 9, pp. 113226–113238, 2021, doi: 10.1109/ACCESS.2021.3104148.

[82] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, Jul. 2017, doi: 10.1007/s12083-016-0456-1.

[83] J. Sun, J. Yan, and K. Z. K. Zhang, “Blockchain-based sharing services: what blockchain technology can contribute to smart cities,” *Financial Innovation*, vol. 2, no. 1, p. 26, Dec. 2016, doi: 10.1186/s40854-016-0040-y.

[84] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, “Internet of things, blockchain and shared economy applications,” *Procedia Computer Science*, vol. 98, pp. 461–466, 2016, doi: 10.1016/j.procs.2016.09.074.

[85] A. U. Mentsiev, E. R. Guzueva, S. M. Yunaeva, M. V Engel, and M. V Abubakarov, “Blockchain as a technology for the transition to a new digital economy,” *Journal of Physics: Conference Series*, vol. 1399, no. 3, p. 033113, Dec. 2019, doi: 10.1088/1742-6596/1399/3/033113.

[86] H.-T. Wu, Y.-J. Su, and W.-C. Hu, “A study on blockchain-based circular economy credit rating system,” in *Security with Intelligent Computing and Big-data Services*. SICBS 2017. Advances in Intelligent Systems and Computing, Cham: Springer, 2018, pp. 339–343.

[87] D. Strugar, R. Hussain, M. Mazzara, V. Rivera, I. Afanasyev, and J. Lee, “An architecture for distributed ledger-based M2M auditing for electric autonomous vehicles,” Apr. 2018, [Online]. Available: http://arxiv.org/abs/1804.00658.

[88] A. Pouraghily and T. Wolf, “A lightweight payment verification protocol for blockchain transactions on IoT devices,” in *2019 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2019, pp. 617–623, doi: 10.1109/ICCNC.2019.8685545.

[89] X. Wu, B. Duan, Y. Yan, and Y. Zhong, “M2M Blockchain: the case of demand side management of smart grid,” in *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Dec. 2017, pp. 810–813, doi: 10.1109/ICPADS.2017.00113.

BIOGRAPHIES OF AUTHORS

Mahmood A. Al-Shareeda obtained his Ph.D. in advanced computer network from University Sains Malaysia (USM). He is currently a postdoctoral fellowship at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security. He can be contacted at email: alshareeda022@usm.my.

Murtaja Ali Saare is an assistant professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master’s degree in information technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph.D. at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work inreputablescopus indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sa-uc.edu.iq.

Selvakumar Manickam is currently working as an associate professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, internet of things, industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.