Lightweight Blockchain of Things (BCoT) Architecture for Enhanced Security: A Literature Review

Aofan Liu   
Xiamen University MalaysiaSelangor, Malaysia

SWE2009510@xmu.edu.my

Hanting Liu  
Xiamen University MalaysiaSelangor, Malaysia  
MEC1909452 @xmu.edu.my

Surma Hia  
University Name  
City, Country  
email address

\*Mahdi H. Miraz  
Xiamen University MalaysiaSelangor, Malaysia  
m.miraz@ieee.org

*Abstract—*Both the internet of things (IoT) and the distributed ledger technology (DLT), more commonly known as blockchain, are two popular emerging technologies of this era. While blockchain offers strengthened security, along with other benefits, it requires peer-to-peer (P2P) nodes for its consensus process. On the contrary, IoT ecosystems inherently consist of many P2P nodes but it is highly critiqued for its lack security measures. Therefore, the fusion of these complementary duos, known as the blockchain of things (BCoT), has become a recent research trend. While the fit is good and the benefits such consolidation can offer are obvious, a lot of challenges are yet to be addressed. Therefore, we have conducted a comprehensive literature review, covering 33 research articles, spanning over the last six years (2016-2021), to report the state-of-the-art research in this domain. We have synthesised the existing literature by comparing, contrasting, resembling as well as critically evaluating them and thus, deduced the current challenges and future research directions, particularly with regards to lightweightness.

Keywords—Blockchain security, Collaborative security, IoT security, Lightweight blockchain of things, Traceability System

# Introduction

As technology has changed the way we live, a multitude of devices connected in the network are providing us ways to communicate between the machine and the people, in our data-driven society [1]. However, the pervasiveness of the internet of things (IoT) device contributes to the privacy and security vulnerabilities. Other vulnerabilities of IoT includes (but not limited to): lack of standardisation, device management, insecure network services and ecosystem interfaces, insecure data transfer and storage, lack of physical hardening, etc. Therefore, such weaknesses of the internet of things are of great concerns, [2], particularly with proliferated use of the IoT as well as the Internet.

On the contrary, Blockchain is an open and transparent database. All data is shared by all nodes and is supervised by all users. Based on the characteristics of this technology centralisation, the application scenarios of blockchain should also be further expanded and can be applied on the Internet of Things [3]. This innovative technology takes trust as its core and promotes the maintenance of security and privacy. This technology which offers the method to address the challenge of IoT technology has consequently formed the lightweight blockchain of things [3]. There are many researchers working on this new technology.

It is essentially a distributed database technology, which does not rely on a central or third-party organisation to ensure the authenticity of the data. The objects stored in the database can not only be "value" such as Bitcoin, but can also store other things that need to be registered. It can be applicable to the area of Certification, traceability, transaction or sharing. More specifically, important industries such as ownership, production process, control signals, copyright and even health records are urgently need this technology [4].

In addition, once the conditions for the realisation of the smart contract are reached, the blockchain system will automatically execute the contract [5], which is a very important feature.

Moreover, M2M (Machine to Machine), which is the essential part of lightweight blockchain of things. It can effectively control and communicate between devices through mobile network. M2M, a technology that transmits data from one terminal to another, that is, the exchange and transmission of information between machines, and the concept of information sharing can be achieved through the transmission and link of network and machine equipment communication. The widely used M2M technology can greatly expand the technological boundary of lightweight blockchain of things.

But most studies in the field of lightweight blockchain of things for enhanced security have only focused on IoT security solutions but few of them are concerning about the commonalites and differences among different solutions [6]. These studies would be more useful if we can give a comparison between these different methods and give out a outlook for future. That is exactly what we are going to do in this paper. By implementing a series of observations, we are able to see the current research results and the trend and future research directions of lightweight blockchain of things. But this is not the end, we still need to conduct further study to ascertain the effectiveness of lightweight blockchain of things. In this article, Our survey is focusing on blockchain security techniques that are designed for IoT.

# Overview

## Internet of Things (IoT)

At the same time, the Internet of Things, as one of the important ways to transmit Internet of Things information, is the extension and expansion of the Internet to the physical world. The self-organising network composed of computers and sensor networks plays an important role in the real world. Concepts such as Internet of Everything and Internet of nano things are also very popular recently. The relevant attributes of the Internet of Things include concentration, content, collection, computing, communication, and the connectivity of the scene. This method represents the seamless connection between people and objects or between objects and objects and is especially suitable for blockchain technology.

Cyber physical system and IoT are important aspects of industry 4.0. As Miraz once said automation of the complete production ecosystem is the major driver of Industry 4.0. The Industrial Internet of Things refers to the application of the Internet of Things in the industrial field. Industrial Internet of Things has the characteristics of general Internet of Things, but it is not a common Internet of Things application. The interconnection and intercommunication between devices require extremely low latency and high reliability. It has extremely high index requirements for latency and reliability. Need to provide users with millisecond end-to-end delay and nearly 100% service reliability guarantee.

When it comes to the vulnerability, the security of IoT devices can be a tricky problem. In IPv4 network, there are 450 million devices that are accessible. Therefore, there is no denying that to made IoT network become more secure, we need to solve this problem and improve these IoT devices’ security level. The breaking of Wi-Fi Standard WPA is also a serious aspect of its vulnerability. However, this can be solved by using mobile internet connection. With time going on, the network may adapt from Wi-Fi to 5G. Tradition way of hacking such as trojan, DOS and DDOS can bring down IoT devices quickly. We are bound to improve its security.

Below we will discuss the adoption trend of IoT, according to the 2012 NMC report:

1. Internet of Things devices based on RFID technology will become one of the main ways to consider attendance

2. Animal protectors track the whereabouts of marine life, they are in a specific sea water area Establish a network when a creature swims by, the signal receiver can transmit information

3. IoT devices can be used to track the dynamics of laboratory equipment and resources (i.e., IoT can be used in the area of resource management).

## Blockchain and Smart Contract

Under normal circumstances, the blockchain described by researchers is a data structure composed of data blocks in a chronological order similar to a linked list. Since cryptography is used to ensure that it cannot be tampered with and cannot be forged, this distributed decentralised ledger based on the data structure can be stored safely and simply. And there is a sequential relationship between every two transactions, and every transaction in history can be found in the block.

However, this is blockchain 1.0 and it has many problems such as double payment and Byzantine generals’ problem.

The problem of double payment mainly means that a sum of money may be paid twice at the same time. In the traditional financial system where, physical entities are the carrier, such a problem does not exist. Similarly, in a centralised trading system with a third-party authority, such problems can also be easily solved. But in a decentralised ledger, this problem is particularly serious. There is no unified third party to ensure that all institutions keep the same accounts at the same time. Before the data is synchronised, it is difficult for us to prevent the problem of one person spending the money twice at the same time.

Byzantine generals’ problem is also very famous in this field. When the possibility of channel transmission is not 100%, there is basically no absolutely effective way to make all nodes behave in the same way. In other words, the Byzantine Generals problem actually refers to a cluster of n nodes, where any error may occur in t nodes. If n <= 3t, a correct consensus cannot be reached. Most blockchain-based digital currencies use Proof of Work (PoW)to locally solve the Byzantine problem. This approach can partially solve this problem in the Internet world. In addition, there are a few radical representatives who are turning to Proof of Stake (PoS), such as Ethereum.

The concept of smart contract has been used today since Szabo defined the idea of smart contract in 1994. Generally speaking, we can regard vending machines as the simplest smart contract. But now, smart contracts are far more complicated than this. Without covering the trackable and irreversible characteristics of the blockchain, it allows secure transactions between anonymous users in different environments, and can be automatically executed when the conditions are met [7].

When the participants of the smart contract reach it depends on the implementation of the specific smart contract. Generally spe aking, when the participants are committed to the execution of the contract by installing the contract on the contract host platform, the contract is discovered [8].

## Lightweight Blockchain of Things (BCoT)

The design of the block is that it is difficult for the blockchain to make major changes after it is released. Therefore, we need to pay special attention to security. The fusion of blockchain and smart contract is one aspect [9].

Blockchain technology requires blockchain to contribute to nodes in a P2P manner, while IoT technology requires blockchain to ensure security. These two technologies can make up for each other's shortcomings, so the Blockchain of Things was born. But the proof mechanism of PoW based on the workload enables the nodes of the system to finally reach a consensus, and then calculate the final block when it encounters it. At the same time, the calculation action gives a request to the performance of the device. Moreover, the operating speed of the machine and the calculation difficulty of the block are constantly changing.

Because in actual situations, factors such as the number of users, how the users connect to the platform's sensors, and the reliability of the end user's connection to the Internet will affect the stability of the IoT platform. Network problems such as limited bandwidth, excessive delay, and unreliable network hardware can have a significant impact on device performance. Therefore, we need to achieve lightweightness to reduce the burden of equipment [10].

Therefore, lightweightness is an important aspect that we are going to talk here. Because the performance of IoT devices is often very poor, and some even only have sensors, node devices can only perform extensive sensing collection of information and remote-control commands. The nodes of the blockchain often have certain requirements for the storage and calculation of the equipment, because the hash function needs to be calculated. Therefore, lightweightness is very important for fusion of blockchain and smart contract.

# Recent Advances in BCoT Research

Since the concept of lightweight blockchain of things was put forward, academia has carried out many researches on it [11], which also provides a theoretical basis for the wide application of blockchain technology, including but not limited to energy, medical, finance and other disciplines [12]. As bitcoin has gain more and more popularity in recent years, However, generally speaking, people still lack effective corresponding technical solutions and management plans. Although Bitcoin has deprived the government of its coinage rights by technological means in recent years, and has achieved rapid development, the anonymity of its transactions has prevented it from being recognised by most governments. At the same time, although the digital currency derived from blockchain technology has not been recognised by the government in the corresponding field, blockchain technology, an architecture that uses encryption algorithms, time stamps, and consensus mechanisms, has been used in various industries and even government departments. It has a wide range of applications. We need to continue to accumulate experience to break this technical barrier [13].

Most of the application of lightweight blockchain of things can be divided into three structures according to its own characteristics and application scenarios: public chain, alliance chain, and private chain.

A type of blockchain deployment model that allows any node to intervene to participate in reading and writing data is called a public chain, and a blockchain where anyone can view any information on the blockchain is called a public chain. For example, Bitcoin and Ether, which are more familiar to the public, are cryptocurrencies developed using public chain technology.

The private chain is privatised by an organisation and is limited to a single customer or a small number of customers. Each node entering the blockchain network must obtain a corresponding authorisation. A private chain is a blockchain deployment model in which all operations on a blockchain network require the permission of the center and are subject to its constraints and restrictions. The private chain is a relatively centralised decentralised network. The alliance chain is a network between the two using a relatively loose consensus mechanism. The number of nodes is determined in advance, which can increase transaction speed and reduce transaction costs to a certain extent. However, like the private chain, the alliance chain also fails to demonstrate the decentralised characteristics of the blockchain well.

In recent years, the importance of blockchain technology has gradually increased. The following is the work related to the lightweight blockchain of things system in the context of enhanced security, especially in the industrial area and financial area. Mandrita Banerjee proposed a blockchain future for internet of things and suggested several methods that are designed application of IoT [1] which can help to ensure the security and privacy of data. Moreover, he gives out some thoughts on security techniques designed for IoT and related system, which is closely followed by the lack of publicly available. One major drawback of this research is that the researchers pay too much attention to the discussion of the Internet of Things, mainly discussing things in the IoT, but ignoring the lightweight blockchain of things. Ruinian Li’s research are mainly focus on blockchain and edge computing solutions applicable for large-scale of devices. Apart from that, he talked about the security schema for IoT data storage and certificateless cryptography which is very useful in this area. As the first paper tracking and combining the edge computing and certificateless cryptography, this paper is very meaningful.

In the approach of Song *et al.* [14], a supply-chain system framework is proposed which follow the architecture proposed by Buterin [15] who divide the blockchain technology into three, namely public, private and consortium blockchain. The existing body of research of Rejeb [16] suggests that leveraging internet of things and blockchain technology has great application prospects in supply chain. It also talks about the limitations and challenges that concern the lightweight blockchain of things for a long time.

Dorri *et al.* discussed the privacy and security in IoT devices due to their heterogeneity between such a large scale and talk about some solutions proposed by the previous researchers [17]. But it reaches the conclusion that applying the blockchain and internet of things is not straightforward due to the limitation of sensors and microcomputers. And finally suggest a smart home lightweight blockchain of things architecture consisting of smart home, the overlay, and the cloud storage.

Wei attempts to solve the problems using a trust management system in service-oriented IoT which will evaluate the trust worthiness of devices based on their identities [18]. This trust management system can prevent Self-promoting attacks (SPA), Bad-mouthing attacks (BMA) and so on.

Papers from Lin [19] introduces a blockchain based IoT card system whose core function is real-name registration security management consisting of blockchain network infrastructure and point of scale terminal.

The study of Gong set out to investigate the usefulness of BCoT sentry, a system which try to enhance the security by analysing the traffic flow pattern in the peer-to-peer connection network [20].

Ferrag [21] tries to establish a healthcare system with enhanced security in paper “ Blockchain and Its Role in the Internet of Things” which talks about the identification of healthcare field as a subsector of lightweight blockchain of things. Most of its contents are about theory, Due to practical constraints, this paper cannot provide a comprehensive review.

From the above research, we know that the lightweight blockchain is currently being used more and more widely. More scholars are trying to make breakthroughs in related fields, especially in security.

But at the same time, we must also realise that blockchain-related technologies are not omnipotent [22]. Multiple units can be combined into a huge whole to tamper with the data on the entire network. Once the computing power exceeds 51%, it will become an absolute majority is likely to be monopolised by huge interest groups [23]. What we want to achieve is advanced security rather than monopoly. Therefore, we must pay special attention to this.

In the paper of Hickle [24], the application scenarios of various lightweight blockchain of things are depicted in the future, but they are limited by the possible problems of civilian IoT devices, such as poor performance to deploy a block network or insufficient device functions. If we try to solve these problems by improving the performance of the equipment, it will not be widely used because of the high cost.

At present, the requirements for IoT devices based on blockchain technology are higher. However, IoT devices have low power consumption and poor performance [25]. Nodes participating in the network are limited by resources, such as micro-sensors, it is difficult to store and keep accounts, and they cannot undertake consensus tasks [26]. In addition, the consensus node will have a relatively large impact on the performance of the blockchain network. If there are too many nodes. Consensus dissemination will take a lot of time, and in a large amount of data scenario, it is often not able to meet our needs [27].

# Emergning Applications of BCoT

Blockchain, the core of lightweight blockchain of things, was first used as a means of monetary payment that tried to break away from the national credit system, but its application scenarios have gradually increased over time. Now this decentralisation technology which an prevent single point of failure problem[28]. Moreover, its user anonymity is quite suitable for IoT device. This transparent in computing but non-transparent in identification technology can be further extends to the Internet of Things, medicine, and economic fields [29]. Its potential application scenarios even extend to election voting, notarisation, recognition of academic qualifications, network security and so on.

There have been some commercial applications of lightweight blockchain in the world [29]. For example, the energy company LO3 Energy cooperated with Bitcoin company Consensus Systems to establish an interactive grid platform Transactive Grid based on the blockchain system and the Internet of Things technology.

At the same time, the ecology of the lightweight blockchain of things for enhanced security is becoming more complete. For example, a light code environment has emerged [30]. For example, a company called Blockchain of Things, Inc, is providing the draggable editor which can create bitcoin blockchain apps builder. We have face in the face that the prospects of blockchain is becoming more accessible with the improvement of related industries.

At present, commercialisation is not completely perfect. In commercial applications, the lightweight blockchain of things still has a series of shortcomings [25]. The most important and most important issue is the lack of subjects. Because of the anonymity of subjects, we cannot find specific responsible persons and cannot carry out subsequent accountability.

In addition, blockchain technology has only been around for 9 years and is still in its infancy[31]. We can't even determine what potential problems exist in commercial applications of this technology.

The core function of lightweight blockchain of things is to break trust barriers. This mechanism can achieve trust and self-organisation, and promote the efficient development of business [32] . At the same time, we mainly conduct legality verification based on digital signatures to protect data security.

However, this technology also has certain shortcomings. Blockchain data needs to be synchronised to all nodes on the computing network, which limits the peak value of data processing, and also puts forward higher requirements on database capacity and bandwidth [33]. We need to update Blockchain technology system with shorter intervals. In addition, the fault tolerance challenge of the asynchronous consensus network of the blockchain also needs to pay great attention to [20]. Blockchain technology itself is an asynchronous consensus network. In theory, there is almost no algorithm to ensure that the system can guarantee absolute consensus.

In the end, the combination of blockchain and IoT technology simplifies the handover procedure and greatly increases the reliability of the data on the chain on this platform.

# Future strategies in BCoT:

So far, the previous related research results, application areas and the architecture of BCoT have been provided. Considering the unique features of BCoT, the application can be in various domains, such as healthcare, networks of IoT, inventory control and data storage system. Generally, the primary challenge is how to adapt and improve blockchain technology to maximise the impact of application needs in specific areas. For each direction of application, disparate requirements are raised, customised blockchain implementation needs to be designed for the specific situation. As outlined above, the IoT environment provides comprehensive challenges. In this section, several challenges are analysed and stated below. At present, the security of the code of behaviour of state of the art mainly dependent on exactitude of sophisticated cryptographic computations and puzzles. Currently, the devices involved in such process is considerably constrained by resources. The computation would lay a burden for the devices, that is where lowering the computational requirements is demanded. In addition, the storage limitation is an outstanding challenge as well. In the networks based on blockchain, nodes are ordinarily request the copy of the ledger. The issue with the resource-limited IoT facilities is large quantities of data could not be properly stored. It is worth notice that IoT also face a disadvantage that frequently malicious activities. It is a challenge as well when securing a system with facilities that have limited resource incapable of carrying out heavy-duty calculation. In the meantime, preserving user privacy in interchange links is of necessity. Forming more private IoT networks may resulting in the imperiling of paradigm of decentralised blockchains since the data communication between individuals are confidential. In this section, an overview of other emerging research direction that appropriate for future work to enhance the architecture are included but not limited as followed.

Currently, we mean by monitoring the ability to check which configuration is running. For future work, it could be beneficial to acquire information of the IoT facilities by monitoring in low level instead of examining the running configuration. For example, Zabbix is appropriate to be integrated, which is a mature and effortless enterprise-class open-source monitoring solution for network monitoring. More complex and sophisticated systems could be adopted with the development of technology in the future, and the egression of Notification when there is updated configuration of one device could become available. Streaming message queue applications can be integrated to help update notifications. [32] To further integrate blockchain solutions, a blockchain based PKI such as [33] can be integrated with system instead of traditional PKI based on centralised certification authorities. To achieve a large scale BCoT with a low latency, there should be a hybrid framework that needs to be innovated to combine two or more existing frameworks or a new framework with the revised consensus programme. Excising machine learning techniques in data science to design a new existing consensus method or making improvement is the most promising approach. These machines learning based algorithms can make a difference in ensuring a consensus approach without the need for centralisation or large computing and network overheads [34]

Using different Machine Learning-Based Solutions for Privacy and Security of Block chain in IoT, applying clustering techniques, overcoming technical challenges, strengthening the infrastructure, properly maintaining inter- domain policies and control systems can be future strategies to maintain complicated system of Block chain to solve some limitations come up while using IoT devices i.e., the low computational power, maturity, guidance, practice, storage capabilities, standard etc.

RFID-based locations, barcode-scan events etc devices are used in IoT devices to get information which becomes more useful when they are shared by multiple parties.

Low computational power or low cryptographic capabilities impede many IoT devices from mining. Moreover, Block chain needs high storage, high power consumption ability and enough battery life of wireless devices. Small transactions are harder sometimes.

An idea was proposed by some renowned authors of Italy in conference that the actual suitability of Blockchain for the application domains can be altered by social network having reproducible PRNG-base strategy, high usability, low cost, high availability and working by building a meshed chain which can work as lightweight public ledger for easy services, oriented at least to the domain of IoT, and crowdsourcing. It is a kind of pegged sidechains where the data will not be visible which can help to get rid of de-anonymisation attacks. The use of directed acyclic graph of blocks, several validations, secured and private browser strengthen the security.

# Conclusion

This paper surveyed some papers published in the area of lightweight blockchain of things and try to make some simple analysis on these papers. By this survey, researchers can have some basic idea on blockchain technology and internet of things. Moreover, they can know some new research results and progress in this field up to now.

In the first section of the paper, I tried to give an introduction to the two fundamentals of blockchain, the Internet of Things and blockchain technology, and discussed some very important concepts, such as M2M communication.

Next, we deeply studied the technical composition of blockchain technology, such as asymmetric encryption, timestamp server, consensus mechanism, PoW and PoS. In addition, some background knowledge about the Internet of Things is also involved. Through the introduction of these two parts, we try to give readers a certain concept of this field.

In the next part, we discuss some research results in the field of lightweight blockchain of things. Most of them are trying to promote this technology to different fields, such as supply chain, medical. This will greatly improve security in these areas. At the same time, we have briefly discussed some articles.

The fourth section presents the findings of the research, focusing on the recent government and enterprises applying relevant technologies in the business field. In addition, we briefly discussed the possible shortcomings of these application cases.

Researching these papers is of great help in pointing out the direction of our future research. One possible direction to explore is how to deploy blockchain networks on IoT devices with limited resources. Explore whether the blockchain has more suitable mining mechanisms, reward mechanisms, and intelligent algorithms on IoT machines with limited resources and performance. In addition, how to combine the network architecture of a decentralised blockchain with a specific combination of centralised groups such as the government and monopoly industries is also a possible research direction.

##### References

1. M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," Digital Communications and Networks, vol. 4, no. 3, pp. 149-160, 2018, doi: 10.1016/j.dcan.2017.10.006.
2. 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, 2019.
3. W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain Technology for Applications in Internet of Things—Mapping From System Design Perspective," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8155-8168, 2019, doi: 10.1109/jiot.2019.2925825.
4. Y. Liu, K. Wang, Y. Lin, and W. Xu, "$\mathsf [4] $: a lightweight blockchain system for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3571-3581, 2019.
5. D. Svetinovic, "Blockchain Engineering for the Internet of Things," presented at the Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, 2017.
6. X. Wang et al., "Survey on blockchain for Internet of Things," Computer Communications, vol. 136, pp. 10-29, 2019, doi: 10.1016/j.comcom.2019.01.006.
7. B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," Information and software technology, vol. 51, no. 1, pp. 7-15, 2009.
8. C. Hart, "Doing a literature review: Releasing the research imagination," 2018.
9. V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.
10. E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. d. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," Security and Communication Networks, vol. 2018, pp. 1-27, 2018, doi: 10.1155/2018/9675050.
11. W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," Journal of Industrial Information Integration, vol. 15, pp. 21-28, 2019, doi: 10.1016/j.jii.2019.05.002.
12. L. Ismail, H. Hameed, M. AlShamsi, M. AlHammadi, and N. AlDhanhani, "Towards a Blockchain Deployment at UAE University," presented at the Proceedings of the 2019 International Conference on Blockchain Technology, 2019.
13. Q. Song, Y. Chen, Y. Zhong, K. Lan, S. Fong, and R. Tang, "A Supply-chain System Framework Based on Internet of Things Using Blockchain Technology," ACM Transactions on Internet Technology, vol. 21, no. 1, pp. 1-24, 2021, doi: 10.1145/3409798.
14. A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management," Future Internet, vol. 11, no. 7, 2019, doi: 10.3390/fi11070161.
15. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," presented at the Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 2017.
16. L. Wei, J. Wu, and C. Long, "Blockchain-Enabled Trust Management in Service-Oriented Internet of Things: Opportunities and Challenges," presented at the 2021 The 3rd International Conference on Blockchain Technology, 2021.
17. M. Lin and H. Han, "A Blockchain-based Flexible Traceability System for IoT Cards," presented at the 2021 The 3rd International Conference on Blockchain Technology, 2021.
18. L. Gong, D. M. Alghazzawi, and L. Cheng, "BCoT Sentry: A Blockchain-Based Identity Authentication Framework for IoT Devices," Information, vol. 12, no. 5, 2021, doi: 10.3390/info12050203.
19. M. A. Ferrag, L. Maglaras, and H. Janicke, "Blockchain and Its Role in the Internet of Things," in Strategic Innovative Marketing and Tourism, (Springer Proceedings in Business and Economics, 2019, ch. Chapter 119, pp. 1029-1038.
20. T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979-33001, 2018, doi: 10.1109/access.2018.2842685.
21. A. Sultan, M. A. Mushtaq, and M. Abubakar, "IOT Security Issues Via Blockchain," presented at the Proceedings of the 2019 International Conference on Blockchain Technology, 2019.
22. 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.
23. W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "New Blockchain-Based Architecture for Service Interoperations in Internet of Things," IEEE Transactions on Computational Social Systems, vol. 6, no. 4, pp. 739-748, 2019, doi: 10.1109/tcss.2019.2924442.
24. C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things," presented at the Proceedings of the Third ACM Workshop on Attribute-Based Access Control, 2018.
25. 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, 2016, doi: 10.1007/s12083-016-0456-1.
26. 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, 2018, doi: 10.5815/ijisa.2018.06.05.
27. Z. Baozhi, Y. Junyan, L. Rongsheng, and S. Shanting, "Research on the Application of Blockchain technology in Ubiquitous Power System Internet of Things," presented at the Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, 2019.
28. S. Cho and S. Lee, "Survey on the Application of BlockChain to IoT," in 2019 International Conference on Electronics, Information, and Communication (ICEIC), 2019: IEEE, pp. 1-2.
29. M. Hammoudeh, I. Ghafir, A. Bounceur, and T. Rawlinson, "Continuous Monitoring in Mission-Critical Applications Using the Internet of Things and Blockchain," presented at the Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, 2019.
30. M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "Blockchain-based Data Provenance for the Internet of Things," presented at the Proceedings of the 9th International Conference on the Internet of Things, 2019.
31. L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture," IEEE Network, vol. 34, no. 1, pp. 16-23, 2020, doi: 10.1109/mnet.001.1900103.
32. Košťál, K., Helebrandt, P., Belluš, M., Ries, M., & Kotuliak, I. (2019). Management and monitoring of IoT devices using blockchain. Sensors, 19(4), 856.
33. Yakubov, A.; Shbair, W.M.; Wallbom, A.; Sanda, D.; State, R. A blockchain-based PKI management framework. In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6. [CrossRef]

Uncategorized References

[1] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks,* vol. 4, no. 3, pp. 149-160, 2018, doi: 10.1016/j.dcan.2017.10.006.

[2] 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, 2019.

[3] W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain Technology for Applications in Internet of Things—Mapping From System Design Perspective," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8155-8168, 2019, doi: 10.1109/jiot.2019.2925825.

[4] Y. Liu, K. Wang, Y. Lin, and W. Xu, "$\mathsf {LightChain} $: a lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 6, pp. 3571-3581, 2019.

[5] D. Svetinovic, "Blockchain Engineering for the Internet of Things," presented at the Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, 2017.

[6] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Computer Communications,* vol. 136, pp. 10-29, 2019, doi: 10.1016/j.comcom.2019.01.006.

[7] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 254-269.

[8] D. C. Donald and M. H. Miraz, "Multilateral transparency for securities markets through DLT," *Fordham J. Corp. & Fin. L.,* vol. 25, p. 97, 2019.

[9] M. H. Miraz and M. Ali, "Blockchain enabled smart contract based applications: Deficiencies with the software development life cycle models," *arXiv preprint arXiv:2001.10589,* 2020.

[10] I. Ayres and R. Gertner, "Filling gaps in incomplete contracts: An economic theory of default rules," *The Yale Law Journal,* vol. 99, no. 1, pp. 87-130, 1989.

[11] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. d. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Security and Communication Networks,* vol. 2018, pp. 1-27, 2018, doi: 10.1155/2018/9675050.

[12] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *Journal of Industrial Information Integration,* vol. 15, pp. 21-28, 2019, doi: 10.1016/j.jii.2019.05.002.

[13] L. Ismail, H. Hameed, M. AlShamsi, M. AlHammadi, and N. AlDhanhani, "Towards a Blockchain Deployment at UAE University," presented at the Proceedings of the 2019 International Conference on Blockchain Technology, 2019.

[14] Q. Song, Y. Chen, Y. Zhong, K. Lan, S. Fong, and R. Tang, "A Supply-chain System Framework Based on Internet of Things Using Blockchain Technology," *ACM Transactions on Internet Technology,* vol. 21, no. 1, pp. 1-24, 2021, doi: 10.1145/3409798.

[15] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper,* vol. 3, no. 37, 2014.

[16] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management," *Future Internet,* vol. 11, no. 7, 2019, doi: 10.3390/fi11070161.

[17] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," presented at the Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 2017.

[18] L. Wei, J. Wu, and C. Long, "Blockchain-Enabled Trust Management in Service-Oriented Internet of Things: Opportunities and Challenges," presented at the 2021 The 3rd International Conference on Blockchain Technology, 2021.

[19] M. Lin and H. Han, "A Blockchain-based Flexible Traceability System for IoT Cards," presented at the 2021 The 3rd International Conference on Blockchain Technology, 2021.

[20] L. Gong, D. M. Alghazzawi, and L. Cheng, "BCoT Sentry: A Blockchain-Based Identity Authentication Framework for IoT Devices," *Information,* vol. 12, no. 5, 2021, doi: 10.3390/info12050203.

[21] M. A. Ferrag, L. Maglaras, and H. Janicke, "Blockchain and Its Role in the Internet of Things," in *Strategic Innovative Marketing and Tourism*, (Springer Proceedings in Business and Economics, 2019, ch. Chapter 119, pp. 1029-1038.

[22] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access,* vol. 6, pp. 32979-33001, 2018, doi: 10.1109/access.2018.2842685.

[23] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IOT Security Issues Via Blockchain," presented at the Proceedings of the 2019 International Conference on Blockchain Technology, 2019.

[24] 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.

[25] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "New Blockchain-Based Architecture for Service Interoperations in Internet of Things," *IEEE Transactions on Computational Social Systems,* vol. 6, no. 4, pp. 739-748, 2019, doi: 10.1109/tcss.2019.2924442.

[26] C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things," presented at the Proceedings of the Third ACM Workshop on Attribute-Based Access Control, 2018.

[27] 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, 2016, doi: 10.1007/s12083-016-0456-1.

[28] 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, 2018, doi: 10.5815/ijisa.2018.06.05.

[29] Z. Baozhi, Y. Junyan, L. Rongsheng, and S. Shanting, "Research on the Application of Blockchain technology in Ubiquitous Power System Internet of Things," presented at the Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, 2019.

[30] S. Cho and S. Lee, "Survey on the Application of BlockChain to IoT," in *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, 2019: IEEE, pp. 1-2.

[31] M. Hammoudeh, I. Ghafir, A. Bounceur, and T. Rawlinson, "Continuous Monitoring in Mission-Critical Applications Using the Internet of Things and Blockchain," presented at the Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, 2019.

[32] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "Blockchain-based Data Provenance for the Internet of Things," presented at the Proceedings of the 9th International Conference on the Internet of Things, 2019.

[33] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture," *IEEE Network,* vol. 34, no. 1, pp. 16-23, 2020, doi: 10.1109/mnet.001.1900103.