2021 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA) | 978-1-6654-3610-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/CoNTESA52813.2021.9657112

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

Aofan Liu
Xiamen University Malaysia
Selangor, Malaysia
SWE2009510@xmu.edu.my

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

Mst. Surma Khatun
Russian State Academy
Moscow, Russia
mzsurmahia@gmail.com

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

Abstract—**Both the internet of things (IoT) and distributed ledger technology (DLT), more commonly known as the 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 of 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

I. Introduction

As technology has changed the way we live, a multitude of devices connected in the network now provides us with ways to communicate between the machine and the people, in our data-driven society [1]. However, the pervasiveness of the internet of things (IoT) devices contribute to privacy and security vulnerabilities. Other vulnerabilities of IoT include (but are 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 concern [2], particularly with proliferated use of the IoT as well as the Internet.

On the contrary, Blockchain is an open and transparent database. All the data is shared by all the nodes and is supervised by all the users. Based on the characteristics of this technology decentralisation, 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 and has consequently formed the notion of blockchain of things (BCoT) [3].

Blockchain/DLT is essentially a distributed database technology, which does not depend on a central or third-party organisation to ensure the authenticity of the data. The objects stored in the database can be of any type of data, not only limited to "value" such as cryptocurrency. The application of blockchain has now reached many non-monetary domains such as certification, traceability, transaction, sharing, etc. More specifically, important industries such as ownership, production process, control signals, copyright and even health records, etc., as shown in figure 1, can significantly be benefited from this technology [4].

The implementation of smart contracts on the blockchain is another noteworthy benefit it offers. Once the conditions for the realisation of the smart contract are reached, the blockchain system automatically executes the contract [5], which is a very important feature.

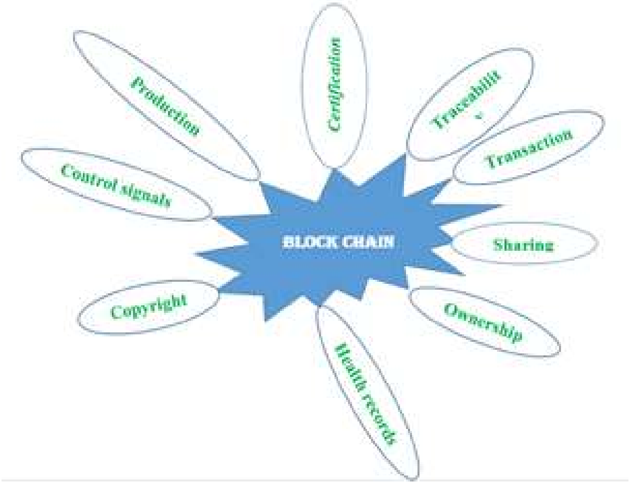

Fig. 1. Non-monetary domains of Block chain

Moreover, Machine-to-Machine (M2M) communication is the essential part of the IoT ecosystem and thus also of blockchain of things (BCoT). It can effectively control and communicate between devices through any wired or wireless networks. M2M communication is a technology that transmits data from one terminal to another, that is, the exchange and transmission of information between machines. Thus, 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

978-1-6654-3610-6/21/$31.00 ©2021 IEEE

greatly expand the technological boundary of blockchain of things.

However, most of the studies, in the domain of blockchain of things for enhanced security, have only focused on IoT security solutions. However, few of them are concerned about the commonalities and differences among different solutions [6]. These studies would be more useful if we can provide with a comparison between these different methods and give out an outlook for the future. In fact, this is the main aim of this review article. By conducting the comprehensive literature review in this domain, we can witness the current research results and trends as well as directions of future research of blockchain of things. In this article, our survey focused on the security aspects of the BCoT. We conclude that further study needs to be conducted to ascertain the effectiveness of lightweight BCoT.

II. Overview

A. *Internet of Things (IoT)*

The Internet of Things, one of the imperative ways of transmitting real-time machine generated information as well as decision making, is the extension and expansion of the Internet to the physical world. The self-organising network composed of computers and sensor networks plays a significant role in the real world. The relevant attributes of the Internet of Things comprise content, concentration, collection, computing, communication as well as 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 systems and IoT are important aspects of industry 4.0. In fact, automation of the complete production ecosystem is the major driver of Industry 4.0 [7]. The Industrial Internet of Things (IIoT) denotes the applications of the Internet of Things in the industrial field. The an IIoT ecosystem, the interconnection and intercommunication amongst the devices require extremely low latency and high reliability. It needs to provide services within millisecond end-to-end delay, with nearly 100% service reliability guarantee.

When it comes to vulnerability, the security of IoT devices can be of a great concern. In the IPv4 network, there are 450 million devices that are accessible. The IPv4 address space is limited and provision the increased demand of IP addresses for accommodating the growing number of IoT devices. In the recent years, IPv6 has been used in many IoT devices which works pretty well. IPv6 addressing scheme possesses a 128-bit address space, while a 32-bit address space is offered by the IPv4 addressing scheme. IPv6 is thus capable of satisfying the growing demand of IP addresses for IoT ecosystems. Due to the increasing number of connected devices, the IoT networks poses great security and vulnerability concerns. The inherited vulnerabilities through Wi-Fi networks, adopting WPA or other protocol, can be addressed by the utilisation of mobile networks, particularly emerging 5G technology.

B. *Blockchain*

The blockchain is a type of data structure mainly containing mathematically bound data blocks (known as transactions) 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 securely. There is a sequential relationship between every two transactions and every transaction in history can be tracked back in the block. Thus, it provides high level of transparency.

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 problem does not exist. Similarly, in a centralised trading system with a third-party authority is required to solve any such problem. But in a decentralised ledger, this problem is particularly of great concern because there is no unified third party to ensure that all institutions kept the same accounts at the same time. However, to address the double spending problem, blockchain networks deploys the consensus approach, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), etc.

Byzantine Generals problem is also another concern. When the possibility of channel transmission is not 100%, there is no effective way to make all nodes behave in the same way. In other words, the Byzantine Generals problem 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) or other consensus approaches to solve the Byzantine problem.

C. *Smart Contract*

The concept of a smart contract has been in existence since Szabo first defined the idea of a 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 predefined conditions are satisfied [8].

After reaching a smart contract by the participants, execution depends on the implementation of the specific smart contract. With everything taken into consideration, when the participants are committed to the execution of the contract by installing the contract on the contract host platform, the contract is discovered [9].

D. *Lightweight Blockchain of Things (BCoT)*

The design of the block ensures immutability of the ledger. Thus, it is nigh impossible for the blockchain to make any changes after any data is added to the chain/ledger. Therefore, we need to pay special attention to security. The fusion of blockchain and smart contracts is one aspect [10].

Blockchain technology requires p2p participating nodes for the consensus approach which can be sourced from IoT networks. On the contrary, IoT technology requires blockchain to ensure security using smart contracts and principles of cryptography, decentralisation and consensus. Therefore, the fusion of both the blockchain/DLT and the internet of things (IoT), more commonly known as the blockchain of things (BCoT), has emerged. The service offered by BCoT can further be enhanced if combined with other emerging technologies such as smart contracts, artificial intelligence (AI), cloud/edge computing etc.

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 BCoT 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 [11].

Because the performance of IoT devices is often very poor and some even only consist of 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, such as calculation of the hash function. Blockchain can make use of smart contracts to achieve lightweightness through passing much of the IoT device's workload to the smart contracts.

III. Recent Advancements of BCoT Research

Since the concept of blockchain of things was put forward, quite a good number of research has been conducted thus far [12], which also provides a theoretical basis for the wide application of blockchain technology, including but not limited to: energy, medical, finance and other disciplines [13].

Therefore, in recent years, the importance of blockchain technology has gradually increased. The following are the work related to the lightweight blockchain of things system in the context of enhanced security, especially in the industrial area and financial area:

Banerjee *et al.* [1] proposed a blockchain feature for the internet of things and suggested several methods for the application of IoT which can ensure the security and privacy of data. Moreover, they put forward some propositions on the security techniques particularly designed for IoT as well as other related systems. The research of Li *et al.* [13] is mainly focused on blockchain and edge computing solutions applicable for large-scale devices. Furthermore, their article presents the security schema for IoT data storage and cryptography with no certificate.

Song *et al.* [14] has proposed a supply-chain system framework which follows the architecture put forward by Buterin [10]. Rejeb *et al.* [15] suggested that leveraging the internet of things and DLT/blockchain technology has great application prospects in the supply chain. They have also highlighted the limitations and challenges that concern the blockchain of things for a long time.

Dorri *et al.* discussed the privacy and security in IoT devices due to their heterogeneity in such a large scale deployment and synthesised the solutions proposed by the previous researchers [16]. They reiterate the fact that applying the blockchain and the internet of things together is not very straightforward due to the limitation of sensors and microcomputers. They proposed a smart home lightweight blockchain of things architecture consisting of smart home, the overlay and the cloud storage.

Wei *et al.* attempted to solve the trust problems using a trust management system in service-oriented IoT which will evaluate the trustworthiness of devices based on their identities [17]. This trust management system can prevent bad-mouthing attacks (BMA), self-promoting attacks (SPA) and so forth.

Lin and Han [18] introduced 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 *et al.* investigated the usefulness of BCoT sentry, a system that tries to enhance security by analysing the traffic flow pattern in the peer-to-peer connection network [19].

Ferrag *et al.* [20] tries to establish a healthcare system with enhanced security focusing on the identification of the healthcare field as a subsector of blockchain of things.

While we see a great research interests in the domain of BCoT, particularly in the recent past years, as evident by the aforementioned section of the literature survey, we must also realise that blockchain-related technologies are not omnipotent [21]. 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 that is likely to be monopolised by huge interest groups [22]. We need to bear in mind that what we want to achieve is advanced security rather than monopoly. Therefore, we must pay special attention to this.

Huckle *et al.* [23], depicted various scenarios with regards to the future application of blockchain of things are . However, they are limited by the possible problems of civilian IoT devices, such as poor performance to deploy a block network or insufficient device functions.

At present, the requirements for IoT devices based on blockchain technology are higher. However, the IoT devices have low power consumption and poor performance [24]. Nodes participating in the network are limited by resources, such as micro-sensors. Therefore, it is difficult to store and keep accounts as well as to undertake consensus tasks [25]. 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. In a large amount of data scenario, it will often not be able to meet our needs [26]. Therefore, the lightweight aspect of BCoT needs to be further researched.

IV. Emerging Applications of BCoT

Blockchain was first used as a means of monetary payment that was aimed to challenge the traditional banking system. However, its application has spread beyond cryptocurrencies, over the period of time [27]. The decentralization aspect of this technology eliminates the single point of failure (SPF) problem[28]. Moreover, its user anonymity is quite suitable for IoT devices. This transparent in computing but non-transparent in identification technology can be further extended 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, securities settlement and so forth.

There have been some commercial applications of blockchain of things in the real world scenario [29]. For example, the energy company, LO3 Energy, established an interactive grid transactive platform based on the blockchain system and the internet of things technology.

In commercial applications, the blockchain of things still has a series of shortcomings [25]. The 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. These further leads to some legal and regulatory concerns.

In addition, blockchain technology has only been around for approximately 13 years and is still in its infancy[30]. We can't even determine what potential problems exist in commercial applications of this technology.

The core function of blockchain of things is to break trust barriers [31]. 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 the nodes on the computing network, which limits the peak value of data processing and also puts forward higher requirements on the database capacity and bandwidth [33]. We need to update the 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.

The combination of blockchain and IoT technology simplifies the handover procedure and greatly increases the reliability of the data on the chain.

V. FUTURE CHALLENGES AND RESEARCH DIRECTIONS OF BCOT

So far, the previous related research results, application areas and the architecture of BCoT have been presented, in the aforementioned sections. Considering the distinctive attributes of BCoT, the application can be used in various domains, such as healthcare, networks of IoT, inventory control, data storage systems, etc. 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 is mainly dependent on the exactitude of sophisticated cryptographic computations and puzzles. The devices involved in such a process are considerably constrained by resources. The computation would lay a burden for the devices that is where lowering the computational requirements, i.e., the lightweightness, is demanded. In addition, the storage limitation is an outstanding challenge as well. In the networks based on blockchain, all the nodes ordinarily store a copy of the ledger. The issue with the resource-limited IoT facilities is that the large quantity of data cannot be properly stored. In the meantime, preserving user privacy in interchange links is extremely important. Forming more private IoT networks may result in the imperilling of the paradigm of decentralised blockchains since the data communication between individuals is confidential.

In the following paragraphs of this section, an overview of other emerging research directions to enhance the BCoT architecture is presented.

In the future, it could be beneficial to acquire information about the IoT facilities by monitoring at a low level instead of the current approach 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 an updated configuration of any device becomes 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 the system instead of traditional PKI based on centralised certification authorities. To achieve a large-scale BCoT with 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 program. Excising machine learning techniques in data science to design a new existing consensus method or make improvement could be a promising approach. These machine learning-based algorithms can make a difference in ensuring a consensus approach without the need for centralisation or large computing and network overheads [34].

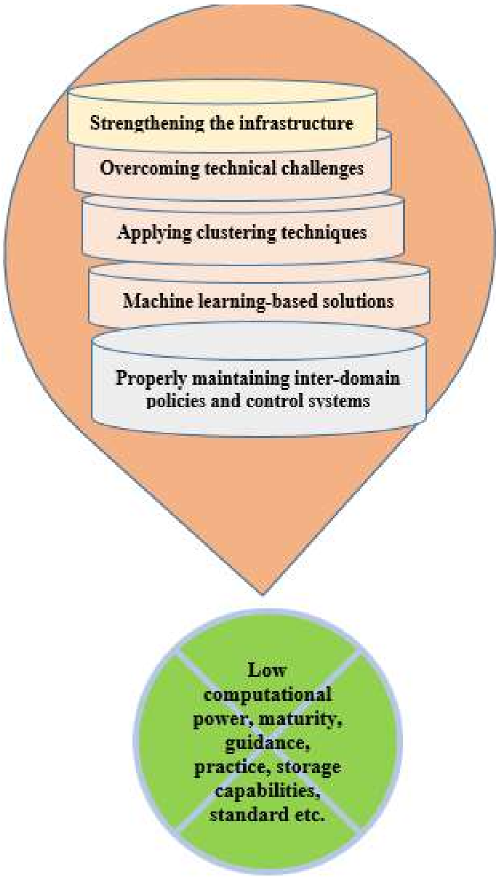
Strengthening the infrastructure
Overcoming technical challenges
Applying clustering techniques
Machine learning-based solutions
Properly maintaining inter-domain policies and control systems
Low computational power, maturity, guidance, practice, storage capabilities, standard etc.

Fig. 2 Key future strategies for complicated blockchain systems.

Using different machine learning-based solutions for privacy and security of blockchain 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 the complicated system of blockchain to solve the limitations that come up while using IoT devices i.e., the low computational power, maturity, guidance, practice, storage capabilities, standard, etc. Figure 2 demonstrates the key future strategies which will be required for maintaining complicated blockchain systems.

Low computational power or low cryptographic capabilities impede many IoT devices from mining. Moreover, Blockchain needs high storage, high power consumption ability and enough battery life for wireless devices. Therefore, conducting significant research on novel lightweight solutions for BCoT is a must.

Actual suitability of blockchain for the application domains can be altered by a social network having reproducible PRNG-base strategy, high usability, low cost, high availability and working by building a meshed chain which can work as the lightweight public ledger for easy services, oriented at least to the domain of IoT and [35]. It is a kind of pegged sidechain 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 can further strengthen the security standard.

VI. Conclusion

In this paper, we have presented the literature survey results covering the recent articles and projects within the domain of blockchain of things – a fusion of the blockchain or distributed ledger technology with the internet of things (IoT). Our survey covered the recent advancement in the domain of BCoT as well as the current and future challenges it holds. Future research directions were also provided. We conclude that significant research still needs to be conducted, particularly for appropriate lightweight solutions to address the impediments of BCoT.

Acknowledgment

This research work was financially supported by the Ministry of Higher Education (MoHE), Malaysia (Grant No. FRGS/1/2021/ICT08/XMU/02/1) as well as Xiamen University Malaysia Research Fund (Grant No. XMUMRF/2021-C8/IECE/0025).

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] M. Miraz, M. Ali, P. Excell and R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", 2021.

[8] 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.

[9] C. Hart, "Doing a literature review: Releasing the research imagination," 2018.

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

[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] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] Košťál, K., Helebrandt, P., Belluš, M., Ries, M., & Kotuliak, I. (2019). Management and monitoring of IoT devices using blockchain. Sensors, 19(4), 856.

[34] 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.

[35] B. Lashkari, J. Rezazadeh, R. Farahbakhsh and K. Sandrasegaran, "Crowdsourcing and Sensing for Indoor Localization in IoT: A Review", IEEE Sensors Journal, vol. 19, no. 7, pp. 2408-2434, 2019. Available: 10.1109/jsen.2018.2880180 [Accessed 3 December 2021].