Lightweight Blockchain of Things (BCoT) Architecture for Enhanced Security: A literature review

line 1: Given Name Surname   
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address

line 1: Given Name Surname  
line 2: *dept. name of organization*  
*(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address line 1: Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address

line 1: Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address line 1: Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address

line 1: Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address

*Abstract*—As the concepts of blockchain and the Internet of Things are more and more popular in the field of civil and military, many researchers want to do research on blockchain based adaptive IoT application for enhanced security. In this field, there is a lack of a concise and effective literature review for them to quickly enter. We are trying to give a extensively review on the current prominence lightweight blockchain of things for enhanced security by researching 65 papers spanning over 10 years. The research to date has tended to focus on solutions rather than comparison between different solutions., In particular, we first give a rough introduction to the background of blockchain and the Internet of Things and core technologies related to these two fields such as asymmetric encryption. Next, we talk about some newly published papers in these areas and make some comments on them. Finally, based on the research results of these papers, and we discuss some possible research directions in the future.

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

# Introduction

As technology have changed the way we live, a multitude of devices connected in the network are providing us ways to communicate between machine and people in our data-drive society [1]. However, the pervasiveness of internet of things device undoubtfully gives the privacy and security some vulnerabilities. Weaknesses on the internet of things such as poor privacy and security vulnerabilities are getting more concerned [2].

Meanwhile, 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 centralization, the application scenarios of blockchain should also be further expanded and can be applied on the Internet of Things [9]. 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 organization 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 realization 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 commonalities 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

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 decentralized 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.

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-organizing network composed of computers and sensor networks plays an important role in the real world. Concepts such as Internet of Everything and Internet of nanothings 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.

Before the emergence of this new technology, many researchers were studying technical problems related to digital currency. But compared to the previous solutions, for blockchain technology, its biggest innovation is to solve the two major problems of digital currency: the double payment problem and the Byzantine general 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 centralized trading system with a third-party authority, such problems can also be easily solved. But in a decentralized 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 synchronized, it is difficult for us to prevent the problem of one person spending the money twice at the same time.

The system stamps each transaction with the correct time stamp to prove that the transaction did occur at this moment and the ownership of the funds in the transaction has been transferred. At the same time, this transaction record will be broadcast to all nodes. In most cases, only more than half of the nodes have recorded the transaction before we consider the transaction successful. In this way, when the previous fund owner uses the funds again, an error will be reported, thereby solving the problem of double payment. In addition, each block will also be stamped with the correct time stamp, thus forming a correct linked list that develops in chronological order. To put it simply, timestamp, a tool originally used internally by the supply, becomes very effective when combined with the broadcast mechanism. In the blockchain network, the difficulty of changing a record will increase with the increase of time, and the difficulty of tampering will increase with the increase of the running time of the system.

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 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. Find a reasonable hash block value through continuous and time-consuming and resource-consuming calculations. At the same time, with the development of real-world technology and the design of rules, the operating speed of the machine and the calculation difficulty of the block are constantly changing. In any case, a node can find this value through a lot of calculations. Compared with the proof-of-work mechanism, the proof-of-stake mechanism requires only a small amount of calculation to maintain the normal operation of the blockchain. The amount and time of currency holdings can determine the distribution method of the following blocks. However, this distribution method is not perfect. It is difficult to determine the value of the block that does not consume a lot of resources and time. At the same time, this method will also cause the strong to be stronger and the weak to be weaker.

In addition, there are several technologies that have been widely used in blockchains. The Merkle tree, a tree based on data hash invented by Ralph Merkle, is used in distributed systems, P2P applications, or districts. The block chain is widely used. Merkle trees are widely used in verification and file comparison. It has the following characteristics. First of all, its data structure is a binary tree or multi-tree. Secondly, each of its leaf nodes contains data blocks with hash values. The non-leaf node is the hash value of all its child nodes. Especially in a distributed environment, Merkle trees will greatly reduce the amount of data transmission and the complexity of calculations.

# Research Status

Since the concept of lightweight blockchain of things was put forward, academia has carried out many researches on it [10], which also provides a theoretical basis for the wide application of blockchain technology, including but not limited to energy, medical, finance and other disciplines [11]. 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 recognized by most governments. At the same time, although the digital currency derived from blockchain technology has not been recognized 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.

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 privatized by an organization and is limited to a single customer or a small number of customers. Each node entering the blockchain network must obtain a corresponding authorization. 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 centralized decentralized 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 decentralized 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 give 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 Qun Song [13], a supply-chain system framework is proposed which follow the architecture proposed by Vitalik Buterin [9] who divide the blockchain technology into three, namely public, private and consortium blockchain. The existing body of research of Abderahman Rejeb [14] 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.

Ali Dorri and others 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 [15]. 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.

Lijun 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 [16]. This trust management system can prevent Self-promoting attacks (SPA), Bad-mouthing attacks (BMA) and so on.

Papers from Meiyu Lin [17] 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 Liangqin Gong set out to investigate the usefulness of BCoT sentry, a system which try to enhance the security by analyzing the traffic flow pattern in the peer to peer connection network [18].

Mohamed Amine Ferrag [19] 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 realize that blockchain-related technologies are not omnipotent [20]. 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 monopolized by huge interest groups [21]. What we want to achieve is advanced security rather than monopoly. Therefore, we must pay special attention to this.

In the paper of Steve Hickle [22], 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 [23]. 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 [24]. 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 [25].

# Application status

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 decentralization technology which an prevent single point of failure problem[26]. 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 [27]. Its potential application scenarios even extend to election voting, notarization, recognition of academic qualifications, network security and so on.

There have been some commercial applications of lightweight blockchain in the world [27]. 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 [28]. 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, commercialization is not completely perfect. In commercial applications, the lightweight blockchain of things still has a series of shortcomings [23]. 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[29]. We can't even determine what potential problems exist in commercial applications of this technology.

.

# Conclusion

This paper surveyed some papers published in the area of lightweight blockchain of things and try to make some simple analysis on this 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 decentralized blockchain with a specific combination of centralized 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.