www.ijarp.com ISSN 2456-9992 Page: 01-14

International Journal Advanced Research Publications

Case Study

Volume: 02
Issue: 04

A STUDY OF BLOCK CHAIN CONSENSUS MECHANISMS FOR IOT SECURITY

M. Ragul*[1], Dr. A. Aloysius[2]

[1]PhD Scholar (Full Time), Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli-2, Affiliated to Bharathidasan University, Tamil Nadu, India.

[2]Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli-2, Affiliated to Bharathidasan University, Tamil Nadu, India.

Article Received: 14 March 2026, Article Revised: 03 April 2026, Published on: 23 April 2026

***Corresponding Author: M. Ragul**

PhD Scholar (Full Time), Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli-2, Affiliated to Bharathidasan University, Tamil Nadu, India.

DOI: https://doi-doi.org/101555/ijarp.6753

ABSTRACT

In this technological era, providing network security is a big issue. To provide security to the physical devices connected over the network, Internet of Things is used. That is whenever data is shared over the network, IoT devices ensure integrity of data. So for this additionally, BlockChain(BC) technology helps the IoT devices to enhance security over the network when data is shared. To enhance security over network many algorithms were proposed and used. Since data distribution without loss of integrity is the main goal block chain mechanisms help to provide data security in IoT devices. There are many applications of IoT security like traffic light, automated light, smart parking, smart home access control solution, pollution management etc. in all these wireless network is mandatory as only through wifi the alert message will reach the owner. So when its shared in a network of devices block chain will provide a centralized record of transactions which ensures the data originality. In this paper, the applications of IoT devices, security in IoT devices and some block chain mechanisms are discussed.

KEYWORDS: IoT Security, Applications of IoT, Block Chain, Block Chain mechanisms.

1. INTRODUCTION

1.1 IOT Introduction, Applications and security Issues in IoT

The Internet of Things (IoT) is a system of interconnected gadgets, each of which has a unique identification, gathers, and transmits data automatically across a network. It is difficult to create secure IoT systems and maintain them safe from attackers. IoT is used in many areas but the main demand of the users is about the security. In any internet connected device the main concern should be about security. The security of device, the security of the data transferred, protecting device from various attacks, data integrity, privacy of data are the important things which must be considered primarily. So for this reason, block chain is used in IoT which ensures security.

Applications of IoT devices include smartphones, smart watches and smart homes, smart security cameras, trackers for vehicles, ships and goods, as well as sensors that capture data about industrial machinery that control everything from air conditioning to door locks, track wildlife, monitor traffic congestion and issue natural disaster alerts from a single device [1]. The applications of IoT are shown in Fig1.

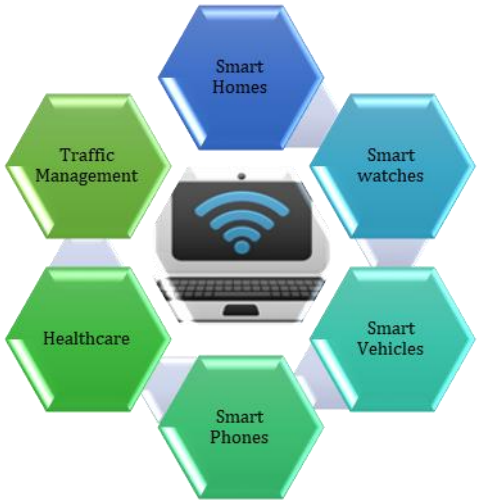

Fig.1 Applications of IoT.

There are some security issues in IoT like confidentiality, integrity, availability, authentication, privacy etc in these IoT devices are shown in Fig.2. Confidentiality refers to securing the data or information from an unauthorized user. Integrity ensures that the data transferred is not altered or modified before reaching the destination. Availability is nothing but the data must not be denied to the intended user when they need it. The user or the source node which is going to access the data is legitimate or not is called authentication. Privacy is

the important thing in a device security. Privacy is the personal data of the person who is sharing it. Hence IoT must be aware of all these to ensure secure transmission.

Fig.2 Security issues in IoT devices.

Wireless networks, cloud databases for communication, sensors, data processing software, and interconnected smart devices make up the architecture of IoT systems in most cases. The following components are used by IoT systems to process and exchange data. Smart devices, embedded systems, IoT gateways, Cloud or on-premises data centers [2]. The goals of IoT security are to Detect and eliminate vulnerabilities in IoT components and to make sure all data is collected, stored, processed, and transferred securely. The centralized model of IoT devices which is being used currently is having many security issues. To overcome this issues decentralization must be done. For this a ledger must be there and with the help of that ledger user can give permission to the devices which has been connected remotely to withdraw them anytime from the network.

Hence BC technology is used to do so. In BC technology, there will be a decentralized ledger which is having the data of all transactions in network. So each and every node in the network will have the ledger. As BC is used to ensure security of the devices, cryptography is used to verify the users so that the ledger will not be altered before approval. In [3] addition to IoT, BC can also be used in human-to-object or platform transactions. It is possible to build connected systems for the house using IoT. BC-based IoT applications can be developed by using gateway nodes. Between traditional systems and IoT devices, these gateways act as an abstraction layer. These gateways can communicate with each other to exchange data and can also verify blocks before adding them to the BC network [3].

2. REVIEW OF LITERATURE

Mahdi H. Miraz and Maaruf Ali [9], have presented a sampling of recent research that is representative of the field, starting with the early studies. Various usages of the BC and similar digital ledger technologies along with their applications, impediments, privacy and security concerns were explored. The authors discussed current security issues related to IoT systems. The application of the BC that could eliminate those security concerns inherent in the IoT ecosystem and improved its overall security were investigated by the authors. In [10], Ali Dorri, Salil S. Kanhere, and Raja Jurdak have proposed a lightweight architecture for IoT, that eliminated the overhead of BC. Also they investigated on a smart home application as a case study for broader IoT applications. In order to guarantee a decentralised topology, the suggested design utilised several types of BCs depending on where in the network hierarchy a transaction took place. Qualitative evaluation of the architecture was done.

Sara Koulali and Mostapha Derfouf [11], have explained the most significant IoT-related security issues and a comprehensive approach based on BC was proposed which improved IoT security. Integrating BC in IoT increased trust, security, transparency, and data traceability in IoT applications. In [12], Malak Alamri et al. Internet of things security solutions by integrating IoT applications with BC have explored. They also showed the integration between the BC and Internet Objects provided great features, which could provide significant help to find proper solutions for the Internet objects security challenges. Also they have concluded that BC could be used in the field of encrypted currencies. Yue Wu [13], BC consensus mechanism suitable for lightweight IoT devices was proposed. Diffie–Hellman algorithm was used for key negotiation with BC nodes, sensors, and zones. Machine learning means to identify or eliminate outliers in sensor data before the data uploaded was also introduced.

In [14], Abdul Muneem Khan et al. A safer and more secured IoT model was designed. The security of the Internet of Things (IoT) devices has been improved. Also they have described how a data breach can be a potential threat to individuals. They also provided security and privacy to individuals and kept everyone safe from potential threats. Subhi Alrubei [15], et al. have proposed consensus mechanism based on Proof-of-Authority (PoA) and Proof-of-Work (PoW). They have designed a new consensus mechanism suitable for deployment in IoT-BC systems called HDPoA and they implemented and validated them. In [16], Arshiya S Mohammad et al. The basics of IoT and BC was presented and the integration of IoT and BC was discussed. The authors have also provided some of the recent studies on integration of IoT and BC.

P Arul and S Renuka[17], The BC technology and the basic principle and characteristics of a consensus algorithm for IoT- based e- healthcare system was reviewed. The benefits and difficulties while connecting the BC in IoT was discussed. Various consensus mechanisms had used in BC e-healthcare system were explored. To develop a BC system while involving the existing best suitable consensus algorithm that improved e-healthcare system in a more efficient way was proposed. In [18], Tanweer Alam The author have discussed and presented literature on BC and the IoT. The issues and applications for developing a stable and interoperable communication infrastructure for BC and the IoT were discussed. Also the author examined current BC trends. The integration of BC and IoT architecture was investigated.

Nehemiah Adebayo et al. [19], the authors reviewed and concluded that IoT security issues can be solved using BC technology. And they identified that, in the IoT ecosystem and on other platforms with privacy and security issues, BCs offer the advantage of working at both the lower and higher tiers of the communications models, allowing for the mechanism to be used effectively across layers and domains. In [20], Hafiz Abid Mahmood Malik the solution to the problem of security in the network of IoT, based on the idea of implementing the BC in IoT has presented. Also the study contributed to the security of data produced by IoT devices. The approach used in the study could be authenticated by professionals using the system of IoT.

Ms. Ruchi Garg et al. [21], have discussed some of the issues of IoT systems and how BC helped in solving these issues. The authors have addressed the various security issues in IOT. In [22], Abdullah Ayub Khan et al. have done a study on various related literature of BC-enabling industrial Internet of Things and its critical implementation challenging aspects along with the solution. A BC hyperledger sawtooth-enabled framework was proposed. And provided a secure and trusted execution environment. Additionally, they have developed consensus protocols and pseudo-chain codes to enable content broadcasting and transactions on industrial nodes. Bodoor Al-Rayani, Jawaher Al-Harbi, Morooj Al-Ghamdi [23], have presented the benefits of applying BC technology to the Internet of Things. They also described IoT based on BC and enhanced security. The significance of component-based development CBD in IoT-based BC and how it achieved robust security and privacy goals in detail were demonstrated.

In [24], Osama Emam et al. based on the integration of consensus algorithms, a framework for integrating IoT with BC technology that ensures a high level of security and validation process. of BC (PBFT and Tangle) was proposed. Also they have proposed a direction

algorithm to direct IoT transactions. The framed a framework that ensured security, scalability and high performance by optimizing the data transmission overhead and enhanced the validation process by using the proposed direction algorithm with reducing both of the resource utilization and the latency time. They also examined the experimental results and declared that the latency time was reduced.

Fariza Sabrina, Nan Li and Shaleeza Sohail [25], have proposed device identity management approach for BC-based IoT systems that provided data security. Their initial prototype implementation showed that the identity management approach could be implemented in large scale settings. The performance evaluation result showed that the prototype fulfils system requirements. In [26], Haider Dhia Zubaydi, Pál Varga, Sándor Molnár a thorough analysis of cutting-edge BCT and IoT integration strategies, specifically to address certain security issues and privacy related issues was proposed. They highlighted the findings of the study which illustrated different works that addressed the integration of BC technology and IoT to tackle various aspects of privacy and security.

Ali Dorri et al. [27], have outlined the various core components of the smart home tier and the various transactions and procedures associated with it were discussed. They also presented an all-inclusive analysis regarding its security and privacy. Then the simulation results demonstrated that the overheads incurred by the method were low and manageable for low resource IoT devices. In [28], Dr. Sonal Pathak et al. The popular security issues related to IoT-based layered architecture was elaborated. The security prerequisites for IoT alongside existing assaults and dangers faced by IoT devies was outlined. The distributed ledger based BC technology contributed to it was demonstrated.

3. IOT AND BLOCK CHAIN ALGORITHMS

IoT is getting popular in everything and every day the usage of IoT devices is increasing. The security threat to the IoT devices is also increasing day by day. To solve this, the existing methods are not sufficient as the security is not up to the mark. For this reason, BC concept has been introduced which ensures security in IoT based systems. Large amount of data is processed by IoT devices which is easy for vulnerability attacks. For the security of data, BC tracks whether the data collected by the sensors is prone to any alteration or duplication. BC technology enables coordination between devices, and track millions of connected devices and processing transactions[4].

3.1 Blockchain Technology Architecture

A BC is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the BC. BC technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. It is a method of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated. Typically, this storage is referred to as a digital ledger. It creates a decentralized system and removes the indulgence of central servers and provides peer-to-peer interaction. It creates a fully transparent and open to all database, which brings transparency to the governance and elections. Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering[5,6].

Hence, the information the digital ledger contains is highly secure[5,6]. There are 4 basic elements in bc they are, consensus, contract, ledger, cryptography. Consensus provides the proof of work and it checks the activities in the network. The participants in the network is verified and authenticated using smart contract. The complete details of transactions happen in the network will be given in the ledger. Cryptography is responsible for providing security to the information that is shared in the network. The structure of block chain is shown in fig.3.

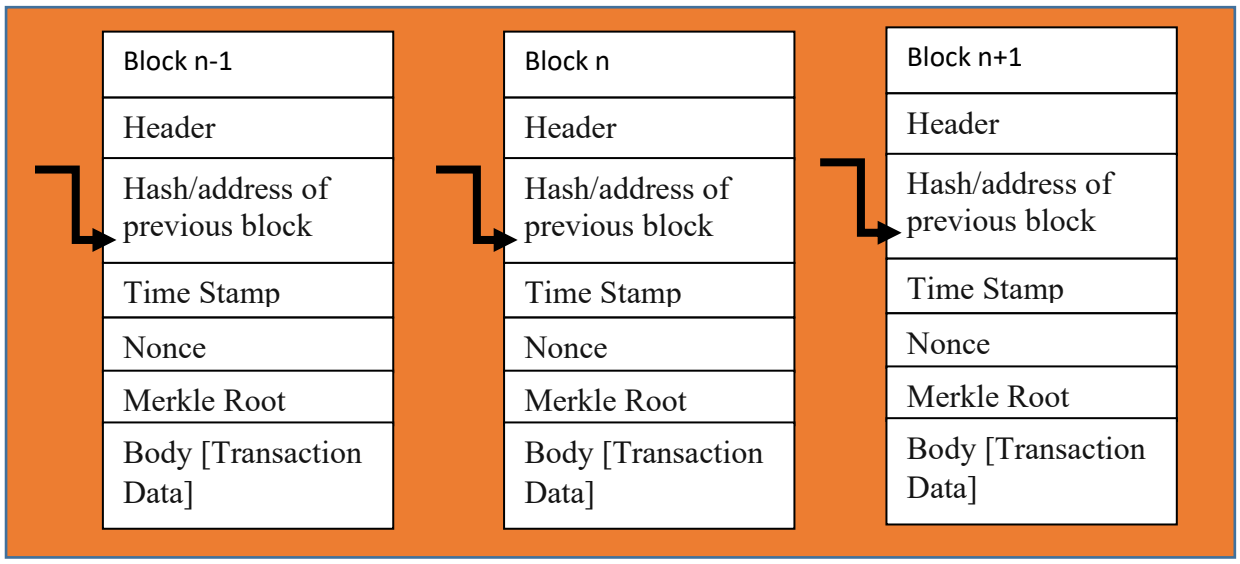

Fig.3 Structure of Blockchain.

The block starts from and goes on till n-m, n, ….., n+m. The header is used to point the specific block as it has the information of all the blocks. The address of the previous block or the hash value of the previous block will be stored in this block. The timestamp holds

information like time and date of creating digital documents which is assigned by verifying the data which enters the block. The nonce is nothing but a number which is used only once. It creates the proof of work for the block as the invalid nonce will be eliminated. Merkle root is similar to data structure tree which holds many blocks of data. All the transactions in the block will be stored in merkle root. Also it facilitates the users by allowing them to verify the transaction that is to be added in the block or not. There are some important characteristics that bc possess. They are, decentralization in which third party authentication is not required, validating and ignoring the invalid transactions is the key characteristic called persistency. In this the transactions in the network cannot be deleted. For securing the data in the block it uses cryptography.

3.2 Types of Block chain

Blockchain technology provides data integrity, eliminates data duplication and increase security using cryptography. A BC ledger can be shared, but not altered. If some data is altered, all blocks will be alerted and will know which block made the attempt. There three main types of bc. They are, public, private and consortium BC which is shown in fig.4

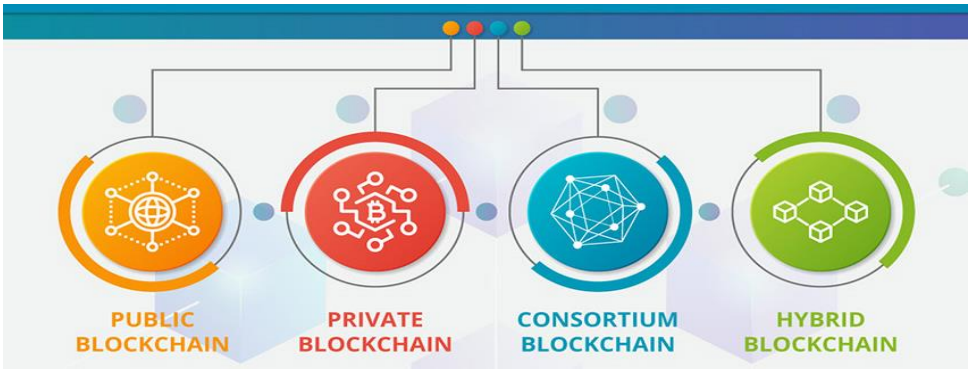

Fig.4 Types of Blockchain.

3.2.1 Public or permission-less blockchain

The public or permission-less BC is completely decentralized, the central authority manages all of the chain's blocks, and it has access to and control over the ledger. Data on the BC is accessible at all times and is not restricted to specific individuals. Because of nobody dealing with it independently then there is exciting reason need to get consent to get to the public BC. A public BC is an idea where anybody is allowed to join in the center exercises of the BC network. In the network or chain, any individual can set their own node or block. All blocks are connected in a peer-to-peer fashion after a node or block settles in the chain of blocks [5, 7].

A copy of that data is created if the block is attacked, and only the block's original author can access it. A BC network that does not require permission to participate is known as a public network. The majority of cryptocurrencies are managed by consensus algorithms or rules on a public BC. Anybody can peruse, compose, and review the continuous exercises on a public BC network, which assists with accomplishing oneself deciding, decentralized nature frequently approved when BC is examined. Because it is impossible to change data once it has been validated, data stored on a public BC is safe [5,7].

3.2.2 Private or permissioned Blockchain

Unlike public BCs, private or permissioned BCs are run by the organisation that owns the network. A dependable individual is in charge of managing the BC; they will decide who has access to the private BC and manage the network's access permissions. While gaining access to the private BC network, there may be some limitations. Organisations can restrict who has access to BC data using a private, or permissioned, BC. Specific sets of data can only be accessed by users who have been given permission. A BC with permissions is Oracle BC Platform. Access to a private BC is restricted to miners. It operates based on restrictions and permissions that set limits on network involvement. Only the parties involved in a transaction will be aware of it, and other stakeholders won't have access to it. Because of the way it operates based on permissions it is also known as a permission-based BC [5,7].

3.2.3 Consortium Blockchain

Between public and private BCs, there are consortium BCs. Organisations created them, and nobody outside of those organisations is allowed access. All businesses between organisations participate equally in consortium BCs. They don't permit access from the consortium's or organisations' network. In a consortium BC, as opposed to a private BC, approval is granted by the government and a number of organisations. Because consortium BCs are more decentralised than private BCs, the privacy and security of the blocks are increased. Those who favour private BCs linked to the block network of governmental organisations. A BC network where a predetermined group of nodes or a predetermined number of stakeholders tightly regulate the consensus process [5,7].

3.2.3 Hybrid Blockchain

It is the combination of the private and public BC. Permission-based and permissionless systems are used. Transactions and records in a hybrid BC are not public but can be verified when needed, this can be done by allowing access through a smart contract. The confidential information can also be verified even if it is hidden. The transactions cannot be altered even though the data is private. A user will have full access to the network once they join the

network. The identity of the user is kept secret until they join the transaction. Only after joining the network the identity of the user will be revealed.

3.3 Consensus Mechanism

In a BC[8], each participant shares the exact same copy of the network transactions, which helps them stay synchronized and connected. Achieving a decisional condition where all network members concur is known as consensus. A consensus mechanism or method is needed in the system to prevent centralization and member conflicts. A consensus technique can be used to maintain network synchronisation in a democratic setting. Each participant in the network has an equal say in choices thanks to decentralisation. As a result, guidelines must be set for network users (also known as nodes) to make new changes to the system with consensus worldwide. In a decentralised network, the consensus process serves to spread the right to update as well as to validate the change across a number of independent nodes. in the network equally.

3.4 Types of Consensus Mechanisms

There are different consensus mechanisms. They are proof of work, proof of stake, proof of capacity, proof of elapsed time, proof of importance, proof of activity, proof of authority, proof of burn, delegated proof of stake.

3.4.1 Proof of Work (PoW)

For a stakeholder node to be granted the right to add new transactions to the BC, they had to provide proof that the work had been completed and submitted by them. Here, miners (or block adders) must perform complex mathematical operations to get the correct hash by altering the block's nonce. The chance to add his block to the network is given to the miner who discovers the hash below the required level of difficulty. hence accepts the award. It uses powerful calculation to arrive at a consensus in a way that is puzzle-friendly. Then, already existing network users who made valid transactions in the block that the miner added[5,8].

3.4.2 Proof of Stake (PoS)

PoS[5,8] consensus does away with PoW's high energy need. In order to be chosen for adding a block, validators (or miners) in a proof-of-stake (PoS) network must stake part of their earned currencies. Another popular consensus method is proof of stake, which emerged as a low-cost, low-energy-consumption substitute for the PoW algorithm. It is not a network's initial consensus algorithm. It can only be put into practise after a network has a sufficient number of participants (or nodes).

3.4.3 Proof of Capacity (PoC)

Sharing of memory space among BC network nodes is made possible by Proof of Capacity (PoC). In a decentralised network, PoC mines a block using the disc or storage space. At the moment, the miner merely uploads to the network the calculated files of potential hashes. The adding and validating of a block of transactions is accelerated via PoC. It trades disc space for the computation factor. The proof-of-concept encourages miners to compile a list of every potential nonce and block hash before beginning the actual mining[5,8].

3.4.4 Proof of Elapsed Time (PoET)

The PoET[5,8] method is based on time-lottery principles. Each miner receives a random distribution of waiting times. The first node to wake up has the opportunity to add its block to the network during the miner node's waiting period. It uses cryptography to encrypt the passage of time in order to come to an agreement without using a lot of resources. A new block is then added after the block has been verified by network validators.

3.4.5 Proof of Importance

Based on importance scores, PoI selects one block harvester from among all participants. It seeks to do away with preferences for wealthy players in PoS consensus. The importance score will be impacted by your network reputation as well as the transaction quality.

3.4.6 Proof of activity

Proof of activity (PoA) is a combination of PoW and PoS algorithms [5,8]. The miners must first complete the challenging math in order to add an empty block with header information and a reward address. A technique called Proof of Activity combines proof of stake. In the majority of proofs of activity agreements, miners compete to create new blocks in exchange for rewards in the form of tokens. Contrarily, the blocks are empty templates with the transaction title and block reward address included in them rather than actual transactions. The information in the transaction title is used to choose a validator node at random to sign the block and confirm it to the BC ledger. Only token holders are eligible to serve as validators.

3.4.7 Proof of Authority

Private or authorised BC networks use the Proof of Authority (PoA) consensus protocol. In contrast to proof-of-stake BCs, proof-of-authority BCs force validators to risk their social capital. BCs require validators to risk their financial resources in order to guarantee legal acts. BCs, on the other hand, require potential network validators to make large financial investments in the network in addition to staking their reputation with numerous proofs of authority. This enables the network to reward honest nodes who are willing to commit for the

long term while eliminating would-be validators with murky or dubious objectives. The reputation of the miner or other network user who wants to add a new block of transactions is crucial to PoA[5,8].

3.4.8 Proof of Burn

By transferring some of their funds to an unspendable account, PoB enables miners to contribute their block[5,8]. Burning the coins refers to the action of transferring your earned currency to a bonded account. PoB permanently removed the burned coins from use in normal transactions. As a result, they can no longer be spent even by their owner. A miner's chances of uploading his fresh block of transactions to the network increase as he burns more bitcoin. The miner gains virtual mining rights by burning currencies.

3.4.9 Delegated Proof of Stake(DPoS)

Because DPOS makes it simpler to scale up networks and also increases security and decentralisation by making those networks more difficult to attack or compromise than other types of consensus mechanisms like POW (Proof-of-Work) or POS (Proof-of-Stake), it is growing in popularity. The opportunity for one delegate to add its block is then given based on a random selection. Here, network users cast their coins as votes for the reliable delegates. DPOS employs a significantly more decentralised method in instead of a single node validating each block. There are numerous nodes on the network in a DPOS system that can approve transactions and add new blocks. Because only one miner can create a block at a time in bitcoin or ethereum, there is no need for miners in those systems. Anyone can create new blocks with DPOS as long as they receive a sufficient number of votes from other network users[5,8].

BC technology offers an innovative approach to achieve confidentiality in IoT security. BC uses cryptography to secure data on the network. Each transaction on the BC encrypted, and only authorized parties can access the information using their private keys. This ensures that sensitive information is kept confidential and can only be accessed by those with the appropriate permissions. By using cryptography to protect data on the network, BC can provide improved confidentiality. Using a distributed ledger that is verified and updated by multiple network nodes, it is able to maintain data integrity. By providing a transparent and auditable record of all network transactions, it can provide accountability. Therefore, for enhancing IoT security, BC use the cryptographic algorithms.

4. CONCLUSION

In this paper, the IoT security, issues in IoT devices and the solution for those issues has been discussed. The BC technology has taken and a brief survey has been done on the techniques and types of BC mechanisms. Further the work can be extended with the help of cryptographic algorithms for security purpose.

ACKNOWLEDGEMENT

The authors thank, DST-FIST, Government of India for funding towards infrastructure facilities at St. Joseph's College (Autonomous), Affiliated to Bharathidasan University Tiruchirappalli – 620002.

REFERENCES

1. https://www.imperva.com/learn/application-security/iot-internet-of-things-security/
2. https://www.apriorit.com/white-papers/513-iot-security
3. https://originstamp.com
4. https://www.chakray.com/blockchain-iot-security/
5. https://www.geeksforgeeks.org/blockchain-to-secure-iot-data/
6. https://www.simplilearn.com
7. https://www.oracle.com
8. https://www.shiksha.com
9. Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2018.
10. Ali Dorri, Salil S. Kanhere, and Raja Jurdak, "Blockchain in Internet of Things: Challenges and Solutions",
11. Sara KOULALI and Mostapha DERFOUF, "BLOCKCHAIN BASED APPROACH TO IMPROVE IoT SECURITY", International Journal of Recent Scientific Research, 2022.
12. Malak Alamri, NZ Jhanjhi, Mamoona Humayun, "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review", IJCSNS International Journal of Computer Science and Network Security, 2019.
13. Yue Wu et al., "Consensus Mechanism of IoT Based on Blockchain Technology", Hindawi Shock and Vibration, 2020.
14. Abdul Muneem Khan et al., "Secured Internet of Things (IoT) Model using Blockchain", BRAC University, 2020

15. Subhi Alrubei et al., “Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm”, White Rose Research, 2021.
16. Arshiya S Mohammad et al., “Integration of IoT and Blockchain”, www.techniumscience.com, 2021.
17. P Arul and S Renuka, “Blockchain technology using consensus mechanism for IoT-based e-healthcare system”, IOP Conf. Series: Materials Science and Engineering, 2021.
18. Tanweer Alam, “Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges”, https://www.mdpi.com/journal/computers, 2022.
19. Nehemiah Adebayo et al.,” Blockchain Technology: A Panacea for IoT Security Challenge”, EAI Endorsed Transaction, 2022.
20. Hafiz Abid Mahmood Malik et al.,” Resolving Security Issues in the IoT Using Blockchain”, https://www.mdpi.com/journal/electronics, 2022.
21. Ms. Ruchi Garg et al.,” Secure IoT via Blockchain”, IOP Conference Series: Materials Science and Engineering.
22. ABDULLAH AYUB KHAN et al.,” Internet of Things (IoT) Security With Blockchain Technology”, IEEE ACCESS, 2022.
23. Bodoor Al-Rayani, Jawaher Al-Harbi, Morooj Al-Ghamdi, “Enhancing Security of IoT by Using Blockchain”, Open Access Library Journal, 2022.
24. Osama Emam, Hanan Fahmy, Menna Mamdouh, “Securing IoT Systems using Blockchain Algorithms”, Communications on Applied Electronics (CAE), 2020.
25. Fariza Sabrina, Nan Li, Shaleeza Sohail, “A Blockchain Based Secure IoT System Using Device Identity Management”, https://www.mdpi.com/journal/sensors, 2022.