iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5156

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Study of Blockchain Solutions for IoT Issues

Debasis Mahapatra[1], A. Akshay Raja Reddy[2], G. S. Mamatha[3], Kavitha S. N. [4]
[1]*Student,* [2, 3]*Associate Prof.,* [4]*Assistant Prof., Department of Information Science and Engineering, R V College of Engineering, Bengaluru*

Abstract: ***Through the years, the blockchain has procured too much traction from the core technology in place. Blockchain is used in various areas like medical record keeping, equity trading, supply chain, immutable data backup systems etc. The Internet of Things (IoT) deals with the interactions between the present day smart devices to procure data and take decisions usually without user intervention to automate tasks. With such a network of variety of sensors and interconnected electronics, the collection of information in our world can be achieved at a very detailed level. Such digital knowledge will help in delivering services that are advanced in a wide scope of application domains including smart city services and healthcare. This incrementally diverse collection, processing of data related to private lives of people giving rise to serious security and privacy issues. The problem with IoT devise is , lower amount of computing power, limited storage capacity and considerably low network bandwidth. This makes them very likely to get attacked and misused. This paper addresses crucial issues related to the security of IOT and explores ways in which integration of blockchain might solve them. The issues that have yet not been tackled post the implementation of the blockchain have also been stated.***

Keywords: Blockchain, IoT, consensus protocol, smart contracts, immutable ledger

I. INTRODUCTION

IoT has achieved huge adoption due to its integration in cities and homes consided to be smart round the world. IoT is all about collection and processing of user related data. This information can be utilised to provide a range of personalised and sophisticated user services. But at the same time this data can be utilised algorithmically to develop a virtual biography of our doings, revaling behaviour and lifestyle data. The devices in IoT may be controlled remotely over networks that use the standardised communication flows. Connectivity between the systems is increasing with increasing popularity of IoT, and also the complication of computing infrastructure is increasing. This leads to a development of loopholes for the cyber threats. Commonly, the IoT systems are present in unsafe environments. This makes them exposed to the hackers and hence its easy for the information to get altered over network's transmission . So, the data access needs to be seriously looked upon.

This is where blockchain as the technology can be implemented with its features to find a solution to various problems occurring due to the IOT systems.It maintains a distributed store of records called as immutable ledger. In such a ledger, the work can be verified between the nodes of the network derived from the third party. It helps in finding a solution to the issue of having a common point of failure. The records of transaction containing network data are not variable and could be found out from the previous history of the network of IOT systems which fasciliatates in finally gaining public's trust on the network of IOT systems. This trust plays a major part in execution of transactions that are financial and public in nature, leading to the creation of a new land of economy of distribution in the domain of IOT.

II. PROPERTIES OF BLOCKCHAIN

A. *Blocks*

1) *Block Version:* It is used to find the validation rules and structure of data inside block so that computer can read contents of block.
2) *Nonce:* It is an abbreviation for "number only used once," which is a number added to a hashed block in a blockchain. This nonce when rehashed, should meet the difficulty level restrictions. Blockchain miners use computing power to obtain this nonce.
3) *Data:* It contains the root hash of the Merkle tree which is hashed data of the summation of every transaction for that particular block.
4) *Timestamp:* The current time
5) *Previous Hash:* The contents of previous block are hashed using SHA-256 and the hash is stored in the current block as shown in Fig 2.1 to chain it with previous block. The previous hash value of fist block is 0 as there is no block preceding it.
6) *Hash:* The SHA-256 hash of all the contents of the current block.

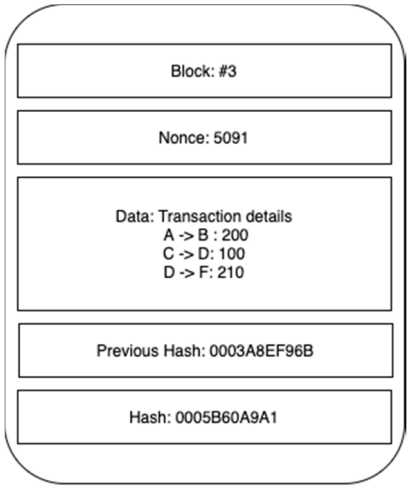


Figure 2.1 Representation of a block

The blockchain is chain of blocks arranged sequentially to possess all the records of transaction occurring in a network of blockchain as an immutable ledger. Its called as immutable as every block is linked to the previous block with its previous hash value as shown in Fig 2.2. So no alterations can be made in any block without recalculating the hash of succeeding blocks. This public ledger has completed transactions that are recorded in a chain of blocks.The sequence of blocks develops as new blocks are added continuously to the chain by different nodes depending on which node mines the target nonce first. Distributed consensus algorithms and public key cryptography are performed for the security of the user. The technology behind blockchain has key features of anonymity , persistent nature ,decentralization and auditability. Having these features, the blockchain could save the budget and increase the effectiveness of the system.

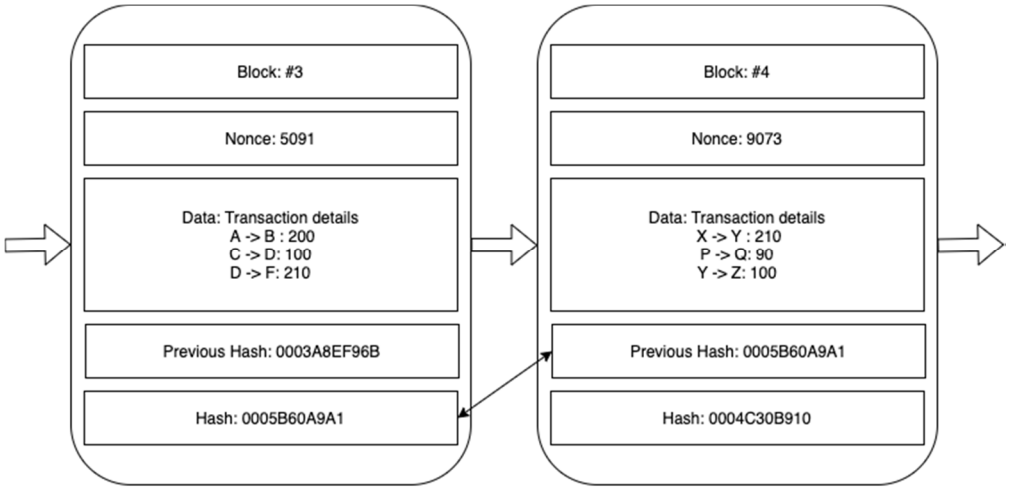


Figure 2.2 Representation of a chain of two blocks

B. Working Of Blockchain Network

The nodes in blockchain perform communication with the flows via a mix of public and private key. The user uses its own private key to sign the transactions digitally and then utilises public key to access the network. The node which makes the transaction broadcasts the transaction which gets signed. All the other nodes in the network of blockchain excluding the node that performs the transaction verify the transaction . All the transactions that are not valid are excluded during this step. In the next step in which all the legitimate transactions are collected over the network nodes into a block during a fixed time and calculates a nonce to generate a hash of the block which matches the target difficulty. This step is called mining. Once a nonce has been found by a node, it does broadcasting of the block to all the nodes that participate as shown in Fig 2.3.

A newly generated block is collected by each node and confirmation is done regarding the authenticity of every transaction and the accuracy of the parent block is declared by using the value of the hash. Once it is confirmed, the nodes will be combined to the block of the blockchain and blockchain is updated. The block that is projected is rejected if it is not confirmed. This brings the existing mining round to an end.

Due to the use of cryptography that is assymetric in nature which contains both the private and public keys that the blockchain technology ensures the elimination of the duplication issue. The private key is kept away from the nodes that are irrelevant. The public key is accessed by all the remaining nodes. Also, the node that does the creation of the transaction signs the transaction which is in broadcast to overall network of blockchain. The transactions are verified by all receiving nodes by the decryption of signature through a public key of node of initialisation. The verification of signature is done to verify the transaction that indicates that the nodes that is initialised is not changed.

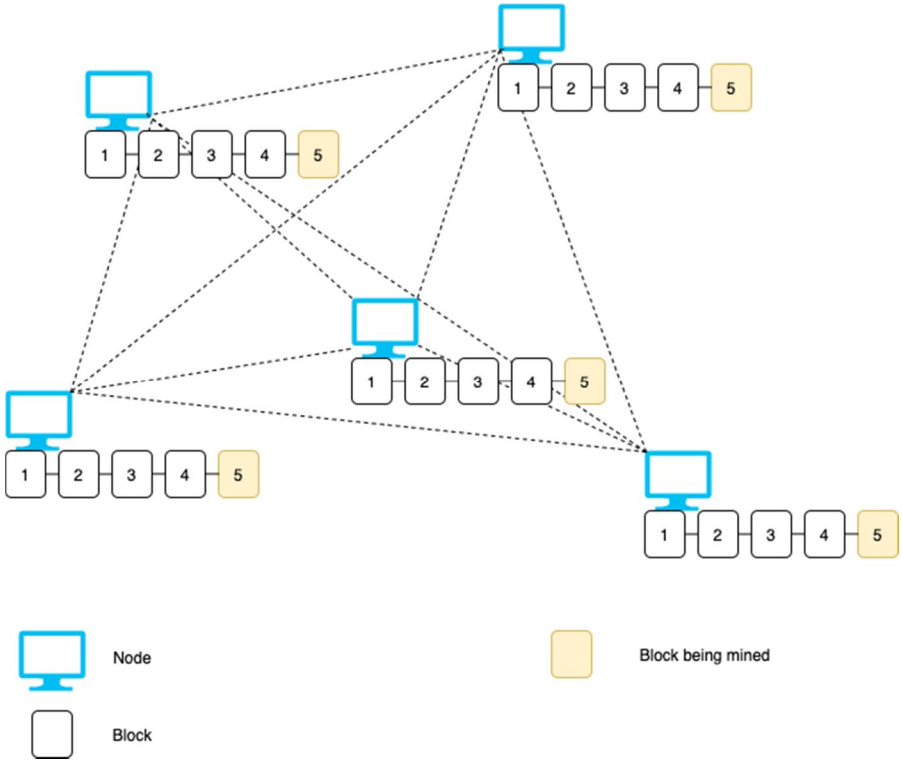


Figure 2.3 Representation of a blockchain network

Secure Hash Algorithm 256 is used as part of work that holds the process of determining data which is hashed along with a nonce to get a target hash . The work that is needed is a lot exponential in nature within the various needed zero bits and is confirmed by executing the hash algorithm. In a network of connected systems of the blockchain, every node implements the proof of performed work of all the mining processes by the increase of the nonce value inside the block until a value is found that fascilitates the block's desired hash bits. The block shall not be changed until not performing the redo of work once the system's effort has been used for the satisfaction of the proof of performed work. Users have the option to share the information among the entities of the third party when IoT is integrated with blockchain. An information access model that is distributed shall be supplied for IoT, that validates the user-data is not allocated to the entities of the corporation that are centralizedl

III. CHARACTERISTICS OF BLOCKCHAIN

A. Decentralised

Transaction is need to be checked via the party that is centrally trusted (like a bank system) in centralized transaction processing environment, resulting in high budget and reduced performance at the point of center. In the blockchain, the other party is not needed anymore in relation to the centralized IoT model. The algorithms referring to the consensues are utilised to maintain the integrity of data and accuracy in blockchain.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

B. Persistence

If a record of transaction is verified by a minder node (nodes that validate the transaction)in a network of blockcain systems, it's duplicate is distributed across the flow and the records is'nt removed or rolled back from the overall implementation of blockchain.

C. Anonymous

In network of blockchain systems, nodes perform interaction with flow of network using the public key that identifies the node in the network of system by maintaining the user's true secret of identity.

D. Secure

With the use of asymmetric cryptographic method, blockchain secures the overall network flow. Public key cryptography or asymmetricity includes two keys, one private and one public key. The node uses the public key to access the blockchain network and uses the private key for signing the transaction it starts. The creator node's identity is verified using its public key.

E. Immutable

For all the nodes that are distributed in the network, the blockchain holds a duplicate of the ledger. This performs help to protect the network from future attacks and failings. If an attacker tries to change any block, the blocks following the attacked block become invalid in every node, which can be then easily identified.

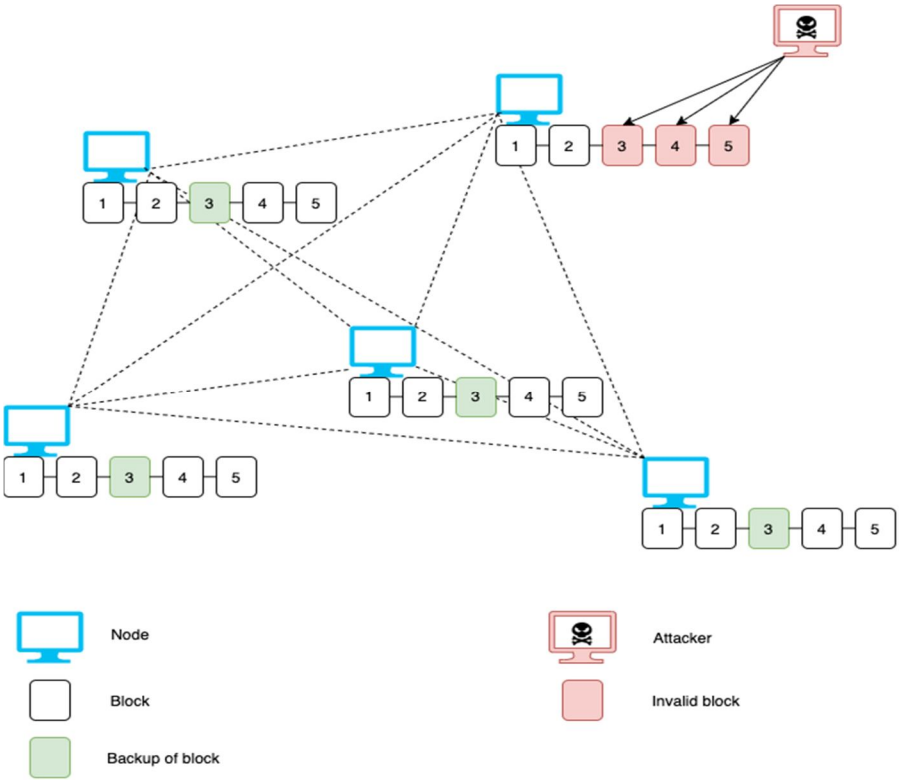


Figure 3.1 Representation of a blockchain under attack

F. Transparent

Changes done on the network of blockchain systems that are public are viewed by all the members. In addition, all transactions are changeable, meaning that they shall note be changed or cancelled.

G. Smart Contract

The smart contract, created by Nick Szabo in 1994, is one of the most powerful elements of the Ethereum. Usage of programs that are referred to uses smart contracts are published that define the rights of access and varied policies. Ethereum supports many other programming languages in writing smart contracts such as Solidity

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

IV. ISSUES FACED WITH IoT DEVICES

A. Privacy Violation

Due to a diversified infrastructure and it's integration in the network, the data stored on a computer is prone to be exposed to the attack by nodes that are compromising and that exist in the network of associated systems. In addition, an infringer could access the information without the approval of the owner.

B. Integrity of data

The intruder may obtain unauthorized access to the network in a model that is centralised (client-server), and modify and forward the original data or information. Middleman procures the data first and pushes the modified data to the receiving side.

C. Unknown Origin of Data

In the world of IoT, it is next to impossible to understand the data's origin, and anyone may alter the data during the transmission.

D. Access conTrol

Access control in the IoT network is among the important problems. In the network of distributed systems it is not easy for the identification of node that is entitled to the access and performing of another job with the data.

E. Single Points Of Failure

Due to presence of a central authority, continuous growth of IoT-based centralized networks may reveal single-point-of-failure. Since the data from the whole network is processed and verified by an authority central to the situation of a malfunction or interruption of the central point in the network

F. Personal Data Misuse

The systems of IoT are nothing but chips and sensors that are collecting and transmitting human, essential data over the internet. The knowledge collected is in storage in every firm's central store. This data reveals users personal information, or information about their digital habits which can be easily taken for misusage. There is a risk of confidentialy, as corporations can manipulate and utilise the data in an illegal manner. PRISM Surveillance System is an example of such abuse of confidentiality.

G. IoT Network Information Sharing

For research purposes, the data that is procured by IoT systems is reported in variation. The data points that have the data loading of network systems or their working logs. Open accessibility of information holds a very important role in maintaining the validation of the methods and studies. Thus, their credibility is important each time such knowledge sets are exchanged openly.

V. HOW BLOCKCHAIN CAN SOLVE THESE ISSUES

A. Privacy Protection

Blockchain network can implement consortium blockchain to provide data protection. Nodes that are in usage for a common purpose form a side chain which is also referred to as a private network. IoT data privately is belonged to each individual sidechain. The nodes that participate in a single sidechain are again not allowed to involve in another sidechain's process of validation.To access the information regarding the consortium blockhain network , the node shall first perform registration and become a piece of the network of sidechain. Preventing of unauthorised access could be fascilitated by the usage of the consortium blockchain.

B. Data Integrity

The network of blockchain systems is a peer-to-peer one, where every nodes possesses the similar file record. When there is an initiation of a transactoin, the node that initiates signs the transaction with it's own private key and the pushes it for the sake of confirming of other involved nodes.

All the remaining minder nodes are involved in the process of invalidation, and want to find the nonce. The node that initially detects a nonce is needed to verifiy and gain a reward. Additionally, the freshly generated block will be transmitted to remaining network-wide nodes. After the record has been loaded into blockchain it cannot be changed or removed.

C. Trusted Data Origin

Inorder to monitor the informatin among the network of systems , each IoT device is associated with a unique Id. Data obtained from a computer is labeled with its name, and the data is sent to the entire network after computing a hash on the data. This is the basis for trustworthy sources of data.

D. Access Control

Blockchain applications can be built by using smart contracts, in which different policies and access rights are specified. For example, If the temperature exceeds 80 C, processors need to enter the energy-saving mode.

E. Fault Tolerance

Accidentally, the systems are of decentralised nature are very less likely to malfunction as they depend on several individual components. The network of blockchain systems is a peer-to-peer decentralized network, in which each system has the similary duplicate of a record which is why a single node failure has none of the effects over the network. Thus network of blockchain systems prevents a common point-of-failutre.

F. Personal data Protection

The unethical usage of data that is personal with blockchain could be prohibited. As the blockchain P2P storage devices , all the jobs performed on the data related to the network can be verified and registered. The goal is facilitate storage that is decentralised wherever the operators oversee their data as an option to any intermediate authority that is centralised. Therefore, anonymity is generalized to several rates where 'Consortium blockchain' is adviced for the systems implementing IoT.

G. IoT network Information Sharing

As the rate of transfer of knowledge on the IoT network increases, the fundamental storage costs will rise as well. In this way, the information is retained in sources that are at distance and an archive that is centralised is maintained that contains the references to those sources in isolation. In addition Blockchain is used to preserve knowledge set RIM (Reference Integrity Matrix).
Since the Blockchains have Immutability functionality, and RIM accessibility for all Blockchain IoT network apps, RIM Integrity was assured. Whenever a necessary information collection originates, its validity could be checked by the comparision of variations of its RIM on the network of blockchain systems.

VI. PROBLEMS WITH IMPLEMENTING BLOCKCHAIN

As blockchain is a network of distributed system, to secure the privacy, anonymity is of importance. Blockchain in an appropriate manner offers pseudo anonymity so that users shall not possess a real world identification. Users possess a public key that is utilised in performing transactions over the network. A user could be identified using this ID through a mix of these Ids and associating IP addresses. In addition, if a user utilises more than a single Public Key, this could be tracked from testing whether the varied addresses are belonging to the same person. Future job is the answer to the much desired anonymity.

VII. FUTURE WORK

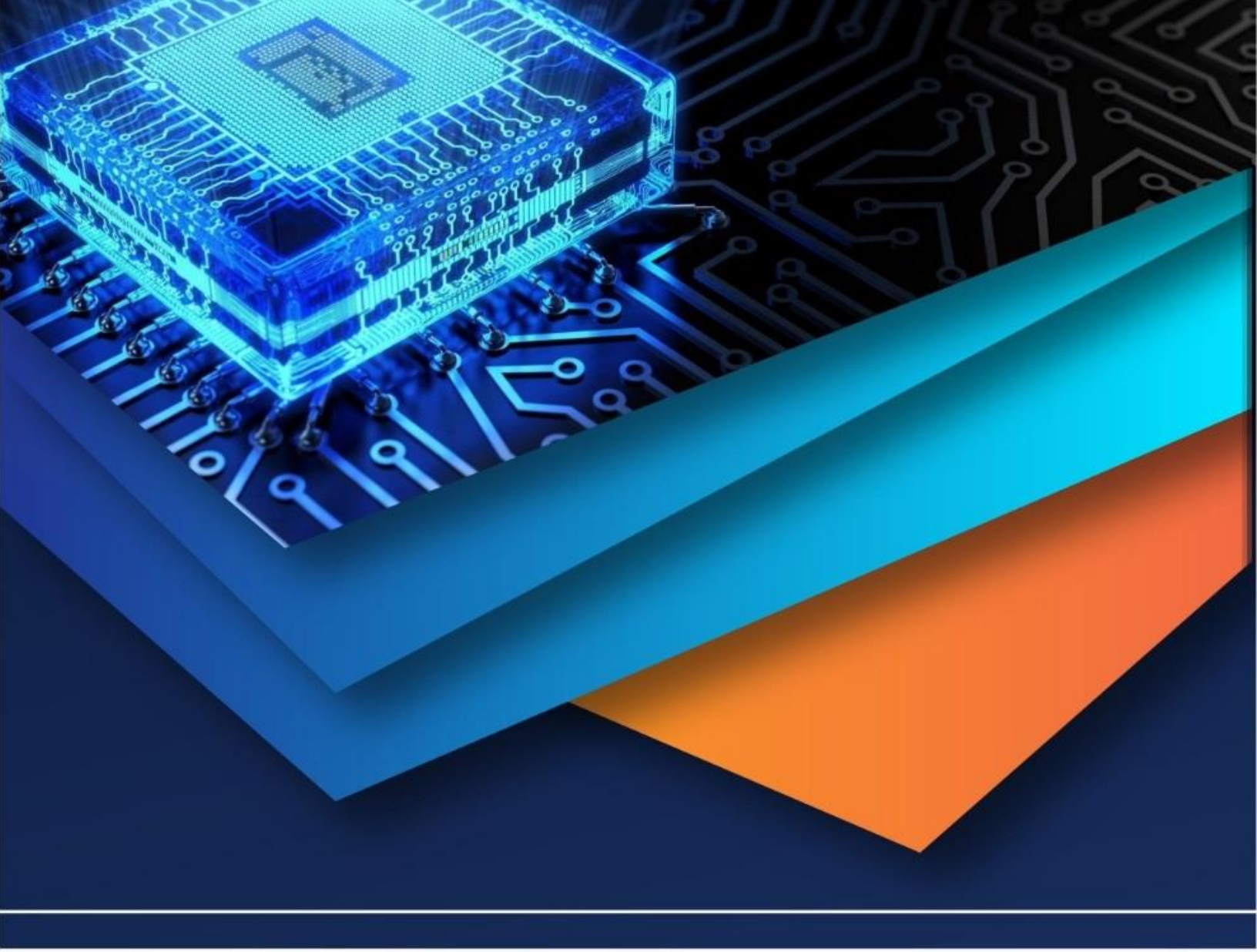
We further aim to simulate such IoT systems using blockchain and monitor the impact on security. These observations might help us explore and discover new merits that blockchain brings to the table or may be find out limitations of blockchain beyond all its benefits that a theoretical approach may not be able to shed light upon.

VIII. CONCLUSION

This paper targets to present the Internet of Things and Blockchain literature review and discusses problems relevant to an environment involving the IoT systems. IoT is upcoming potential technology, with the advent of network that is high-speed and smart network apps. IoT systems are unfortunately vulnerable to threats and are prone to being misused by attackers. In this paper, such order is illustrated in the varied features of network of blockchain systems to eliminate problems in IoT. In addition, problems that aren't resolved after blockchain deployment are highlighted.

REFERENCES

[1] T. Sureshkumar and D. Vijayakumar, "Security in IoT Networks Using Blockchain Technology", Journal of Advanced Research in Dynamical and Control Systems, vol. 12, no. 1, pp. 74-79, 2020. Available: 10.5373/jardcs/v12i1/20201010.
[2] H. Malviya, "How Blockchain Will Defend IOT", SSRN Electronic Journal, 2016. Available: 10.2139/ssrn.2883711.
[3] M. Miraz, "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies", SSRN Electronic Journal, 2019. Available: 10.2139/ssrn.3464085.
[4] D. Minoli, "Special Issue of the Elsevier IoT Journal on Blockchain Applications in IoT Environments", Internet of Things, p. 100149, 2019. Available: 10.1016/j.iot.2019.100149.
[5] "Blockchain-enabled multimedia in industrial IoT", Multimedia Tools and Applications, 2020. Available: 10.1007/s11042-019-08541-w.
[6] J. Veuger, "Convergence Blockchain, AI en IoT", Research & Development in Material Science, vol. 12, no. 1, 2019. Available: 10.31031/rdms.2019.12.000777.
[7] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security", Internet of Things, vol. 1-2, pp. 1-13, 2018. Available: 10.1016/j.iot.2018.05.002.
[8] R. Thakore, R. Vaghashiya, C. Patel and N. Doshi, "Blockchain - based IoT: A Survey", Procedia Computer Science, vol. 155, pp. 704-709, 2019. Available: 10.1016/j.procs.2019.08.101.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY