iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.55106

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: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

Methodology for Securing and Monitoring IoT Devices through Blockchain Technology

Sai Bhaskar Gunisetty

Abstract: ***This paper aims to secure and monitor the IoT devices through blockchain technology. The Internetof Things (IoT) is an essential technology in our daily lives. These devices and sensors are makingour human lives much easier and more comfortable. IoT is a multilayer technology that involves collecting and sharing data via a cloud-based platform. However, these IoT devices are lacking security measures, which makes them vulnerable. Blockchain technology is a decentralized process that is capable of data encryption, auditing, and immutability. It can also help us to solve security issues, especially in IoT devices. Blockchain records digital transactions and prevents them from being duplicated. Nonetheless, adopting blockchain technology for an enterprise network presents challenges. In this paper, we present a new blockchain-based framework for IoT devices in the tollgate plaza system. Our framework is oriented for IoT data and facilitates secure data sharing. Through blockchain, we can quickly improve security measures and network efficiency, which we are affecting with IoT. Additionally, we showcase how to generate hash values to secure data in the network. This application framework developed by using smart contracts that consist of rules and conditions. This paper highlights some IoT issues where blockchain plays a vital role.***
Keywords: Internet of Things, Blockchain, Security, Network, Monitoring, Hashing.

I. INTRODUCTION

Satoshi Nakamoto introduced the first blockchain in 2008. It was a technology that succeeded in securing and managing transaction data. It began with facilitating Bitcoin transactions. Bitcoin and other cryptocurrencies employ blockchain technology. Moreover, blockchain is a decentralized network, and it can record every aspect of the transactions recorded on them. The main advantageof blockchain technology is that their stored data is immutable. One of the significant limitations of the IoT is that it entirely depends on centralized systems that are facing some improper communication problems in the models. IoT devices are connected and authenticated through cloud servers. These cloud servers are capable of ample storage and sufficient processing power. The main difference between a cloud database and blockchain is centralization. However, the data from the IoT devices are recorded and secured in the cloud in a centralized format. When it comes to blockchain, its data is maintained securely by making a copy of records and any changes done so that every user can view the origin of the data. The communication aspect is an essential part of the network, and blockchain is capable of it because they are structured as peer-to-peer networks. The decentralization process of blockchain ledgers shows that the evaluation and storage of the data spread across the devices and are not stored in one central server. In some cases, if the serveris down, then the complete IoT network no longer exists. At this point, blockchain can be beneficial because millions and trillions of IoT devices are connected. By doing this, all these devices can easily communicate with each other without any typical issues. Through this process, we can quickly reduce the cost and scalability of the IoT devices. By using blockchain, we eliminate third parties. Furthermore, blockchain can include collections of different cryptographic algorithms. With the help of such algorithms, we can secure the user's data in the IoT network and make it more confidential. This cryptography serves two purposes: one is to secure the identity of the sender, and the other is to ensure that the previous records do not tamper with the data in the blockchain.

There are different types of hashing algorithms in cryptography for securing data [1]. Some of them are SHA-1, SHA-2, SHA-3, MD-5, etc. In the blockchain, Hashing is used in different ways,like to represent the address and information of a block. Each block connects with the previous block's hash value. Every transaction contains a particular bit of information (amount, address, andtime stamp) that appears in a transaction ID. This transaction ID is a hash value that determines whether the transaction has occurred or not. We should know how the hash values generate for every block. In a blockchain, the first block is called the genesis block, which consists of all the transactions. Once the second block adds, its hash value sums up with the first block's hash value. After this process, a new hash value generates for the second block in the same way whenever a new block adds, the previous block's hash value gets sums up and generates a new one. For this process, we have chosen the Merkle tree concept. The Merkle tree is a part of blockchain technology and provides us with much assistance.

The Merkle tree can generate a unique hash value for different blocks of data in a blockchain. It can also secure a significant component of data and makes the data more efficient. It stores all transactions in a block and verifies whether thetransaction belongs to it or not. A Merkle tree looks similar to a binary tree in the data structure, which consists of children nodes and a parent node. It repeatedly hashes the leaf nodes until it represents the root value. This root value is also called the Merkle root, built using the bottom-upapproach.

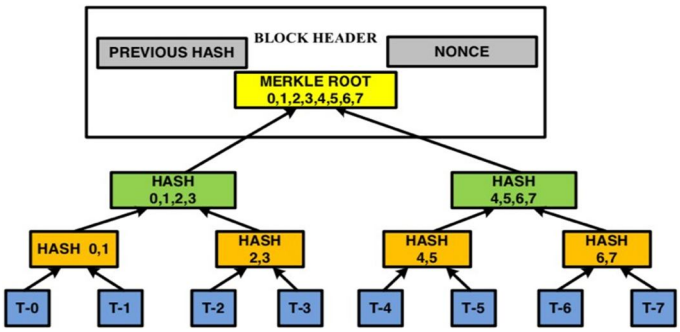


Figure 1: Structure of the Merkle tree

Nick Szabo, is an American cryptographer, scientist, and legal scholar in digital currencies and contracts. Introduced the concept of smart contracts in the year 1994. He described smart contracts as decentralized ledgers that can be executed on their own. Smart contracts can help us solve issues between people (ex: client-server) and create agreements between them. They can help us with banking, transportation, voting, insurance, health care, real estate, etc. These contracts can be converted into code and executed in blockchain platforms. The primary intention of using blockchain is to eliminate third parties between the users while allowing them to communicate with each other. Smart contract is a unique feature of blockchain technology. Even though smart contracts were introduced in 1994, they were not implemented until 2009. These smart contracts are widely used in cryptocurrency like Ethereum.

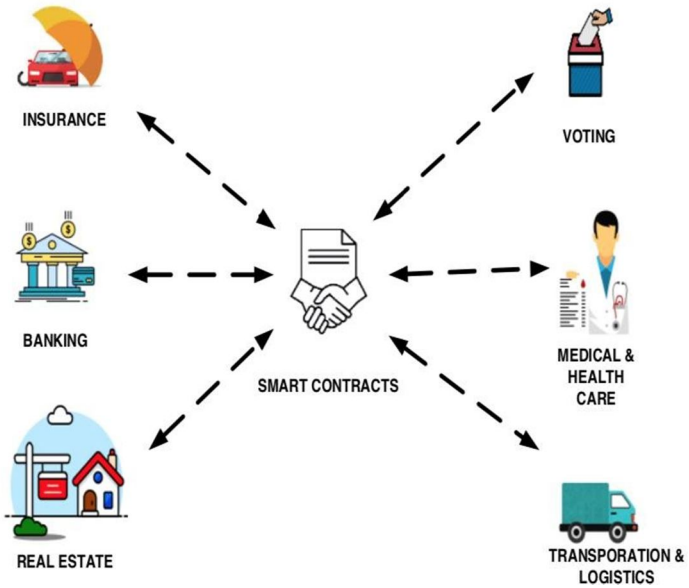


Figure 2: Smart contract in real-time applications

This paper presents the implementation of smart contracts via blockchain technology. Through IoT devices, we can collect and mine data in the blockchain. This process can also help us to accomplish security issues in IoT devices. We may think of how these smart contracts connect toIoT devices, the way they recognize and specialize in computer protocols, that helps to verify andimpose the execution of the contract between the items and devices in the IoT system. By incorporating a real-time scenario, we developed a blockchain framework for IoT devices with a detailed explanation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

II. OVERVIEW OF PROBLEM STATEMENT:

Our discussion of the tollgate plaza system showcases some of its issues. The tollgate plaza system consists of 6-7 tollgates, where each IoT sensor scans the vehicle and records the data in an authorized system. Once the sensor scans the vehicle, it may or may not store data correctly. This kind of issue can eliminate by using blockchain technology. We all know that IoT is one of the most significant ecosystems, which increases its complexity every day. By using IoT devices and networks, we are facing so many security issues and problems because it depends on a centralized model that looks similar to the client-server model. Usually, all these IoT devices are connected through cloud servers and consume more storage capacity. To compensate for these kinds of storage and network issues, we can connect the IoT devices with blockchain technology. In simpleterms, blockchain is a database that maintains and records data even if it proliferates. If someone needs to add data or make changes in the blockchain, all the members in the network need to acceptthose changes before the transaction becomes valid.

However, blockchain could record and store the data, shared between all the IoT devices connected to a network (private/public). Blockchain could prevent suspicious logins and guard against anyone who attempts to modify the records. Trust plays a vital role in blockchain technology. Togain trust between the customer and admin, we use a method called smart contracts. These smart contracts are part of blockchain technology; they eliminate third parties and make agreements between two parties to ensure the transactions are immutable.

III. LITERATURE SURVEY

Recently, Lukman A et al. [1] discussed a process in blockchain technology that can manage decentralized ledgers in the oil and gas industries. The transactions that occurred were stored in ablock and secured without any fraudulent activity, modification, and any unauthorized chain participants. To secure the data, they adopted a hashing algorithm called SHA-1. Their work showcased that whenever a transaction occurred, a hash value was generated for the transaction using a public key. The transaction of the block was mined in the blockchain with a hash value, and it could be decrypted by using a private key of the block.

Security is one of the challenging aspects of IoT devices [2]. Data is sensitive in that it carries allthe information of a user. It should be encrypted at least once with two-factor authentication. To solve this problem, they came up with blockchain technology, and they mainly concentrated on securing sensitive IoT data. They created a cluster and selected a leader for it. The clusters optimized the data by using the dragonfly optimization algorithm; this algorithm can be used to find the cluster head or leader. In a blockchain, the transactions are mined in a block, and its hashvalue is generated by using the Merkle root. At the time of encryption, there is a key and a message.This encryption system creates a ciphertext message to be transmitted over unsecured channels with minimized risk.

$$Enc = hash\,(info\ group, hash, public\ key, IP)$$
$$E => m^k \,|\, mod\ info\,|$$
$$D => \_\_mk\_|\, mod\ info\ (E)|\_ * private\ key$$

Public and private keys are needed to decrypt the message. This process helps the IoT devices toenhance accuracy.

Blockchain technology is combined with three components: cryptography, peer-to-peer network, and game theory [3]. Modern blockchain technologies are using ECC to get entirety for its component, which is an asymmetric cryptography process. For hashing the data, they used the SHA-256 hash function.

$$H_B = Hash(H\_A + Info\_Block\_B + Nonce) < Target$$

The above formula is used to generate a hash value for B. They used the previous block's hash value and the B block's information. A nonce is just a value that is used to solve POW (Proof of Work) problems. If any changes are made to the previous block's data, its hash value changes immediately, and the link may be broken. Consequently, the data may not appear concurrently, and it is also a time-consuming process. To solve this, they came up with the Merkle tree process.

By using this process, the data appeared in chronological order. SHA-256 helped them when combining the data, and it also ensured the security of the data in the blockchain. They mentionedthat the encryption occurred by using the ECC methodology. The results showcased that there wasan increase in entirety and transparency for documents.

Rajat Chaudhary et al. proposed a schema for securing energy in the electric vehicles called BEST(blockchain-based secure energy trading) [4]. With this schema, they used blockchain technologyto validate an electronic vehicle's request in a distributed manner. SDN plays a vital role in transferring the vehicle's request to the network controller. Here the network is present but not yet developed, and to increase QOS for the network, they combined it with SDN. Miners used to act as brokers for gaining energy, and they began trading for vehicles.

The POW was sent to all the miners like public auditing, but the miners competed with each other for a hash value. The highesthash value miner receives more energy points. They used the SHA-1 hashing algorithm for the message in the block, and the output was a 160-bit hash. According to the experimental and performance analysis, they observed that it is a lightweight scheme for communication, and therewas an increase of QoS in the network.

Blockchain is a wide range of concepts, which is also introduced in remote patient monitoring [5].With the help of wearable IoT devices, we can get patient records and store them securely in a blockchain. For privacy purposes, they mentioned that only authorized people could access thoserecords. Blockchain is based on the POW concept. They had used the SHA-256 hash algorithm to generate a unique hash value for the data. They also mentioned some of the requirements for their implementation work. For example, they used the digital signature process to ensure that the datawould not be altered and also eliminated the POW process and divided their network into clusters.They used the Merkle tree concept to generate the hash value for every block. For encrypting the data, they came up with ARX algorithms, and then they encrypted the key using the Diffie- Hellman key exchange algorithm.

There are so many hash functions that are superior to SHA-256 [6]. Byoungjin Seok et al. determined that in the context of Industrial IoT (IIoT), as opposed to SHA-256, many hash functions work better while being more lightweight. The authors designed a framework in which their process could change the hash algorithm for mining when adjusting the network traffic. Thelightweight hash functions are QUARK, PHOTON, and SPONGENT; each of these has different security and performance features. We all know that miners try to find nonce, whereas it can generate the hash value that is equal or lower to that network. They also added a hash helper in one of their frameworks to indicate whether the hash function was used or not for that particular block. Using this approach increases scalability in the network.

Some underlying technologies can monitor patient health remotely with the help of wireless bodyarea networks (WBANs) [7]. WBAN plays a vital role in retrieving patients' health records, but there are some privacy and security issues for data storage. To resolve this issue, they came up with a new signature schema with a designated verifier. They used blockchain technology with a DVSSA schema to prevent the data from being modified. The WBAN controller communicates with both the WBAN device and the cloud. In the blockchain, the DVSSA signature is generated to cross-check against the patient's signature. Users need to sign with the DVSSA signature in the cloud before the data transfers to the blockchain. By using this new signature scheme, they ensured that the data is secure and only authorized people could access it.

IoT is moving toward security and scalability challenges [8]. The process of accessing and storingthe data always depends on the IoT infrastructure of the device. Ethereum is one branch of blockchain technology that heightens the security, availability, and privacy of the system. It can also be implemented in a VM called Ethereum virtual machine. Through this, we can access the terminal of IoT devices by using their ABI (application binary interface) and access their files. They used a Rinkeby/ether scan network; for communication purposes, it is like a proof of authority. In the framework, they connected IoT devices and the blockchain by using the gateway.Once the gateway sends the data, it is directly pushed into the Ethereum network for transactions.The transactions get hashed, and it can be addressed by the ether scan network to interact with thedevices.

Blockchain technology prevents modification of the underlying data without any access [9]. In a network, when a node is processed or created, the transactions are verified directly and through other nodes to establish data integrity. For securing the data, they used a hashing algorithm calledSHA-2, which is a one-way function, so the data in the blockchain is secure and complex. With the help of a Merkle tree concept, the data was hashed and added to a block header. As of now, wecan say that SHA-2 is more complex than other hashing algorithms and prevents cyberattacks. Dueto the limitations of IoT nodes, they could not utilize the complete blockchain network in IoT applications. The major advantage of their project is that it can work at the lower layer of the OSImodel through the blockchain.

Blockchain technology is a distributed peer-to-peer network where people can interact with each other without a mediator [10]. In this paper, they discussed how they combined the blockchain andIoT devices and how the services are getting shared in the market with different devices. Privacy is one of the complex issues in blockchain; each member who participated was identified with a hash value or a public key. When a smart contract is deployed, it safely records the hash digest (itcan be centralized or decentralized); these smart contracts automate the task in multiple processes.When all the IoT devices were combined, they showcased the time-consuming workflow and howthey were accomplished cryptographically, which saves time and money.

IV. SECURITY ISSUES AND COUNTERMEASURES

S.NO	ATTACK NAME	PLATFORMS	COUNTERMEASURES	THREAT MODEL
1.	DDoS/ DoS Attack	Blockchain, Miners, Mining Pools	Various Anti-DDoS services are available like Cloud Flare, AWS. PoA protocol offers the best security measures.	Service-Based Attack (Network)
2.	Replay Attack	Blockchain, Mining Pools, Application, Users	By using Chain ID we can detect each transaction.	Identity-Based Attack
3.	Double Spending Attack	Blockchain, Users, Transaction	ENHOBS will alert by checking the input and output of every transaction.	Service-Based Attack (Application)
4.	Sybil Attack	Mining Pools, Blockchain, Wallets, Signatures	Bitcoin Protocol which can select the true chain with the help of PoW.	Identity-Based Attack
5.	Time Jacking Attack	Miners, Mining Pools, Application	Instead of using network time better to use node system time which can restrict the time.	Service-Based Attack
6.	Selfish Mining Attack	Blockchain, Miners, Mining Pools	BIPS will assign various branches to the miners.	Service-Based Attack (Network)
7.	Eclipse Attack	Miners, Users, EVM	Random selections of address and accept the limited number of connections from the same IP address.	Service-Based Attack
8.	Finney Attack	Miners, Mining Pools, Transaction	Multiple confirmations will mitigate the risk and makes the attackers waste their time.	Service-Based Attack

Acronyms:
BIPS - Bitcoin improvement proposals
ENHOBS - Enhanced Observers
POA - Proof-of-Authority
POW - Proof-of-Work

V. MECHANISM

In blockchain technology, hashing plays a vital role in securing data. SHA is one of the most common algorithms that is used in blockchain. It has a unique technique that generates inimitable outputs for every different input [1]. First, we need to send data through the hash function, whichgenerates a unique hash value with a fixed length. Hash functions have several characteristics. For example, they are very deterministic so that for every given input, the same output occurs, and every output that is generated through the hash function is unique. Several authors have proven that it is impossible to get the input from the output. With the help of hashes, we can prevent transactions from being altered, and we can create cryptographic puzzles that can be used during the mining stage. Figure 2 shows some of the popular hash functions and their results. In smart contracts for hashing, it uses a different concept called the Keccak hashing function, which is equalto SHA-3, and for proof of work, it uses Ethash. These two functions are entirely different in the Ethereum process.

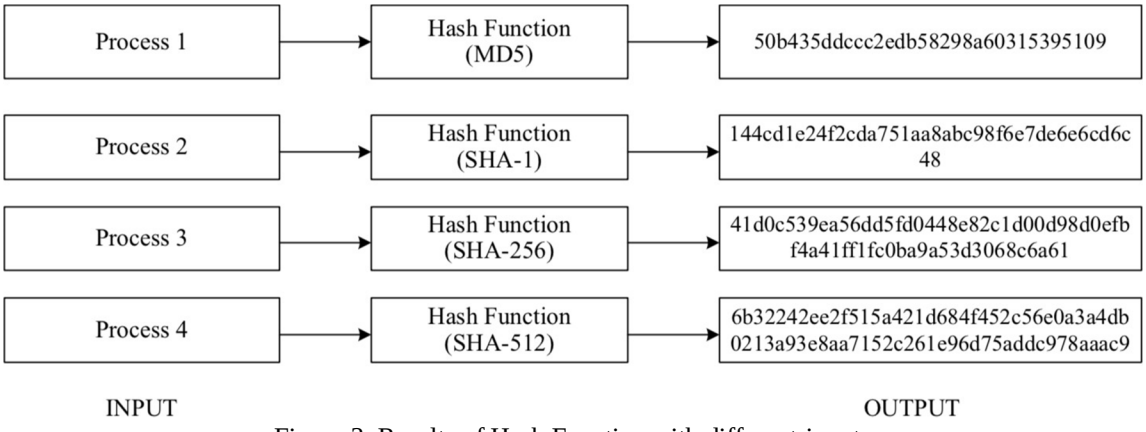


Figure 3: Results of Hash Function with different inputs

In general, smart contracts are agreements between two parties in the form of a computer code [2]. They are part of a blockchain, stored in a public database and cannot be changed. Blockchain handles the transactions that occur with smart contracts. They automatically implement once an agreement encounters, where there is no interference of a third party. This blockchain technology decentralizes smart contracts so that they act as trustless. If a hacker wants to hack the blockchainor smart contracts, he must have at least more than half of the nodes (computers).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

We are saying that with the help of smart contracts and blockchain, we can live in a world where we are free from third parties and intermediaries. By using smart contracts, both parties understandtheir conditions, and it helps them to improve their relationship. It quickly detects if any changes occur between the parties. By using these blockchain ledgers, we can decrease the time required for the devices to exchange information.

Figure 4 describes the connection process of IoT and smart contracts and how they are communicating with each other through a network. When a vehicle passes through a tollgate, the RFID sensor scans the vehicle's data and validates whether the vehicle is registered or not. For thisvalidation process, the RFID sensor sends the data to the authentication system and cross-checks whether the vehicle's data register with RTO's data or not. It is an entirely remote process, and forsecurity purposes, we have added a gateway from system to server and a firewall from server to RTO's database. It notifies if the vehicle is registered or not. Admin controls the above process, and only authorized people can access it. The administrator gathers the data from the IoT devicesand shifts them to the database. This data registers in the blockchain via the smart contract function.If the customer wants to access the sensor data, he must request it directly from the admin via a smart contract. With the help of the blockchain, all the data and contracts store simultaneously, and only an admin has access to it. After receiving the request, the admin and customer must cometo an agreement, where a smart contract generates and mines in the blockchain. The data stored inthe server are mined in the blockchain too. The customer receives a notification from the blockchain after the data is ready.

VI. SCENARIO

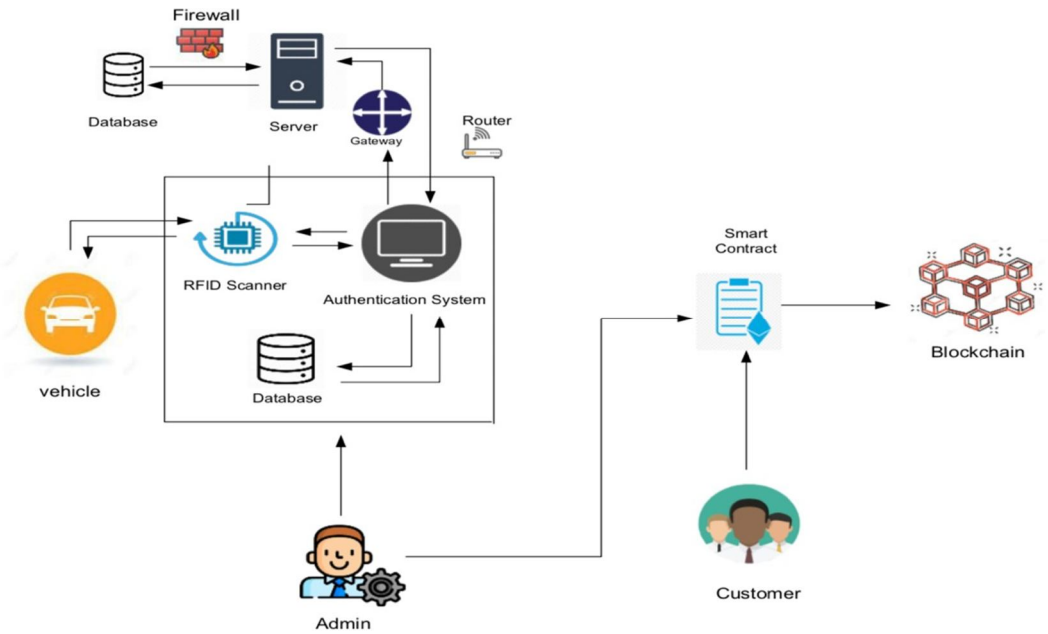


Figure 4: Connection of IoT and Smart contracts

Usually, we need to know the real-time working process of the blockchain and smart contracts. We picked one concept on the tollgate plaza system to explain the scenario. Here, our main motiveis to monitor IoT devices and secure the data through blockchain technology. For the real-time experience of the blockchain, we chose Ganache software and developed an application frameworkfor enrolling the data. Metamask played a crucial role in creating a private network for the blockchain. It helped us to associate with the blockchain network and interact with smart contracts.In our scenario, IoT sensors scan the vehicle's data and store it in a particular tollgate system.

Let us think of a tollgate plaza having 6-7 gates; each gate has an IoT sensor. These 7 gates' data gets stored in the merchant's or admin's database. Every tollgate connects to a network, and an admin controls it. The data gets stored in every block through the node. Here, the node is just an IoT sensor, and for experimental purposes, we created different nodes in our blockchain. When a transaction has occurred, the people in the network gets notified through Metamask. It helps with authentication purposes; only registered and authorized people can access it. People in the networkneed to accept the transaction for verification purposes. During the transaction, the admin gets notified with the Block ID, transaction address, and the cost of the transaction in Ethereum (ether).

When a new member enters a network, the admin generates a unique hash address and assigns himsome controls over the data. Here, each member receives separate controls, and some of them might have the same. Each IoT sensor is a node, and each tollgate center represents a block. In a state, all these tollgates are different blocks, and it creates a chain among them. Here we are usinga concept called Merkel Root for generating a hash header for the blocks. The data collected by the members gets stored in all the blocks chronologically, and the admin can directly access it through the network. Here the admin and members communicate with each other by a one-way hash function. Let us discuss how we are using smart contracts.

They are used to communicate between two parties without any help of a middleman. For example, two members, A and B, have different commitments and controls. These commitments are just agreements in a computer program. If A wants to communicate with B, he receives details of A, and it notifies that A is going to approach him. Here, B can provide or decline permission. Once A is communicates with B, then B hides all his personal information and shows the rest of the datato A. The blockchain mines these contract creations/transactions via smart contracts. This transferred data is in hash form. In Smart contracts, every transaction carries out the agreements between two nodes or blocks; all these things depend on the transaction and data needs. Sometimesthe blocks fail to meet the expectations, and the agreement compromises which leads to a lack of trust that is solved by smart contracts, we can define some rules between the organizations in the form of code. In our scenario, all rules and penalties are not predefined by smart contracts, but wecould apply them in the form of codes. However, we were performing some tests on our project. We observed a delay in the blockchain when mining the transaction.

VII. RESULTS

Figure 5 Smart Contract Address

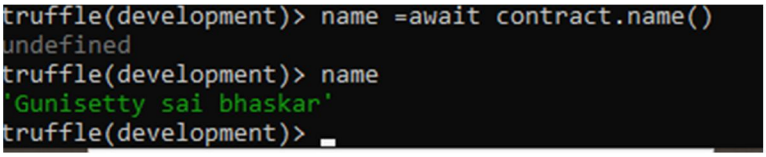


Figure 6 Smart Contract Name

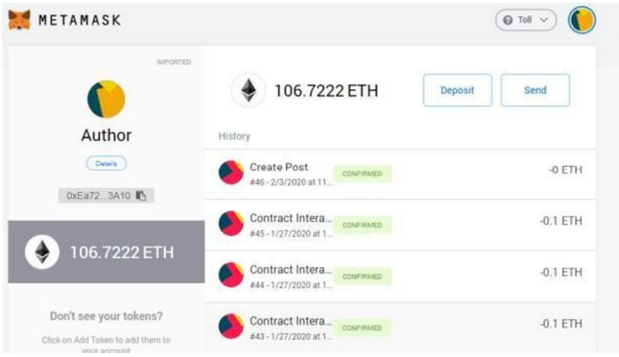


Figure 7 Smart Contract Creation and Interaction

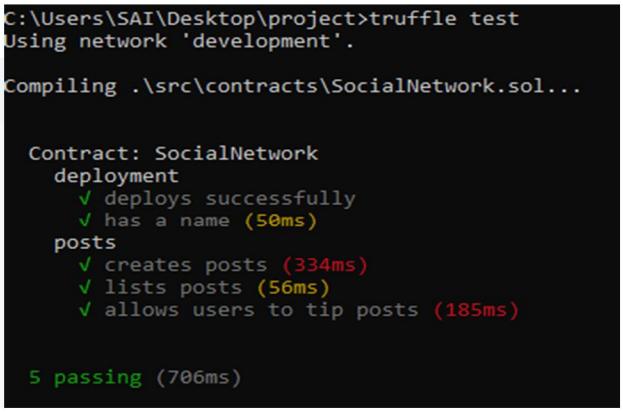


Figure 8 Truffle Test

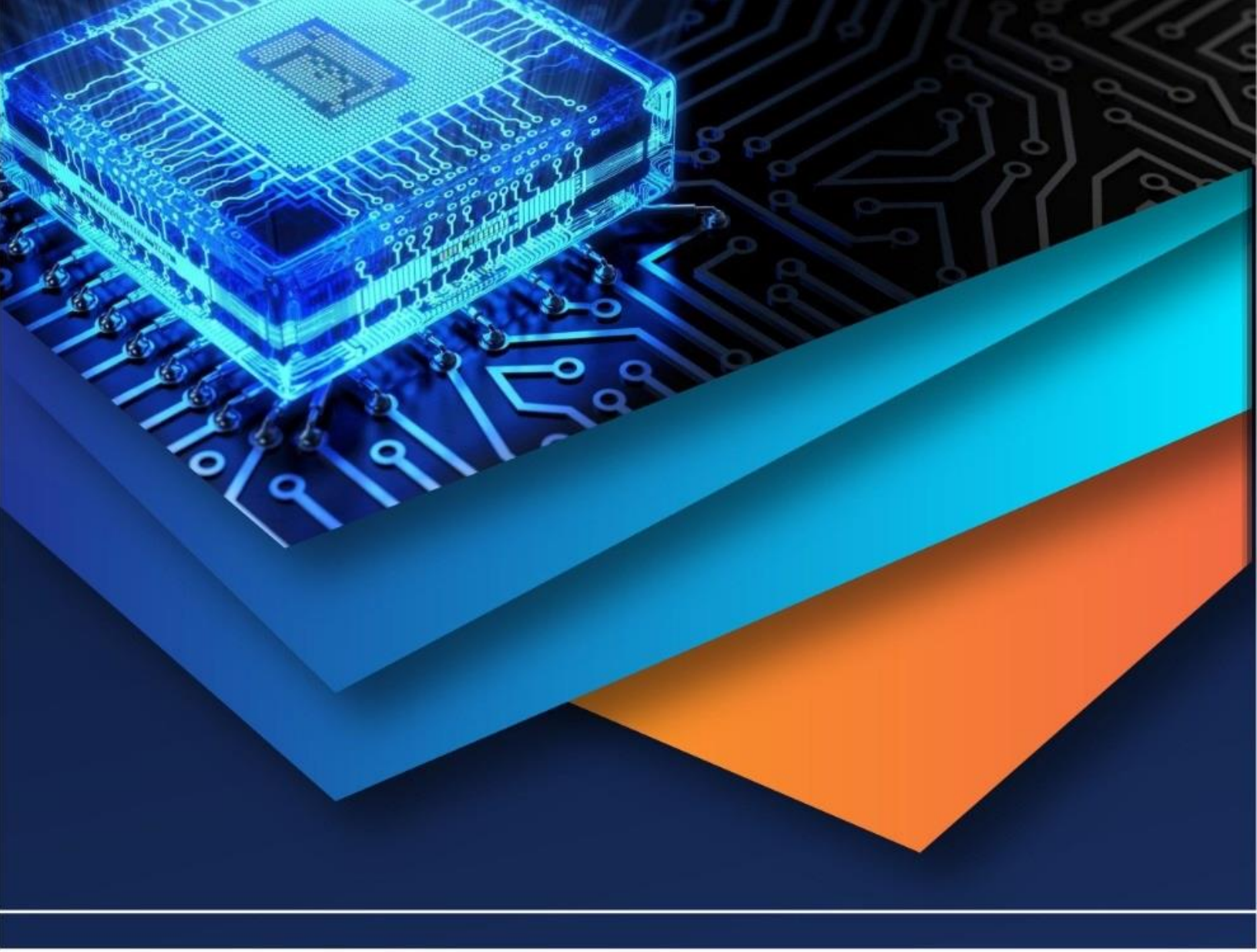
These above figures explain the process of smart contract creation and their interaction with different nodes. We have created our application framework, and these figures are our performance analysis. They are specific Truffle commands where we can get our results. Here, Figure 5 depictsthe smart contract address; the developer creates smart contracts, are mined in the blockchain after their creation. Figure 6 depicts the smart contract name, where it easily recognizes the names andaddresses that can be created only once. Figure 7 depicts the logs of different posts and interactionsof the users in Metamask via the blockchain; Metamask gives us a detailed explanation and the cost of every transaction in ethers. Figure 8 depicts the Truffle test; it is one of the critical points where we can see if the posts were created and deployed.

VIII. CONCLUSION

In this paper, we developed a new application framework for securing and monitoring IoT devices through blockchain technology. This blockchain helps us to improve IoT devices and deliver better accuracy. The blockchain system has a distributed peer-to-peer communication network where it helps to interact with different peers securely. These IoT devices help us to make contact with the physical world. However, when combining all these devices through the blockchain, it automatesto achieve significant time and cost savings. The integration of IoT and the blockchain can improve security. Our framework permits efficient access control and data sharing through different IoT devices. The evaluation results of our framework are promising. We are currently processing our implementation to build several IoT applications in the future.

REFERENCES

[1] Ajao, L.A., Agajo, J., Adedokun, E.A. and Karngong, L., 2019. Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry. J—Multidisciplinary Scientific Journal, 2(3), pp.300-325.
[2] Maseleno, A., Othman, M., Deepalakshmi, P., Shankar, K. and Ilayaraja, M., 2019. Hashfunction based optimal block chain model for the Internet of Things (IoT). In Handbook of Multimedia Information Security: Techniques and Applications (pp. 289-300). Springer, Cham.
[3] Son, K.T., Thang, N.T., Dong, T.M. and Thanh, N.H., 2019. Blockchain Technology forData Entirety. Science Research, 6(6), p.68.
[4] Chaudhary, R., Jindal, A., Aujla, G.S., Aggarwal, S., Kumar, N. and Choo, K.K.R., 2019. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportationsystem. Computers & Security, 85, pp.288-299.
[5] Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R., 2019. A decentralized privacy-preserving healthcare blockchain for iot. Sensors, 19(2), p.326.
[6] Seok, B., Park, J. and Park, J.H., 2019. A Lightweight Hash-Based BlockchainArchitecture for Industrial IoT. Applied Sciences, 9(18), p.3740.
[7] Ren, Y., Leng, Y., Zhu, F., Wang, J. and Kim, H.J., 2019. Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network. Sensors,19(10), p.2395.
[8] Mehedi, S.T., Shamim, A.A.M. and Miah, M.B.A., 2019. Blockchain-based security management of IoT infrastructure with Ethereum transactions. Iran Journal of ComputerScience, 2(3), pp.189-195.
[9] Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internetof Things, 1, pp.1-13.
[10] Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smart contracts for theinternet of things. Ieee Access, 4, pp.2292-2303.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY