Blockchain Algorithm to Fix Transaction, Authentication and Authorization Security Loopholes

Kartik Pandey[1], Nitin Kumar Singh[2] , Dr. Surjeet Balhara[3]
[1,2]*Department of Electronics and Communication Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India*
[3]*Assistant Professor, Department of Electronics and Communication Engineering, Bharti Vidyapeeth College of Engineering, New Delhi, India*

Abstract **- The IoT(Internet of Things)space now a days is one of the most likely innovations of IT field. As the IoT system is integrated on a very large-scale in many forms of design, including smart homes, cities, IoT Vehicles, and so on, it is more insecure due to restricted resources. The conventional user's server architecture has many important limitations to encounter the security demands in IoT devices, such as depending on the trustworthy servers, inability for time- sensitive devices, and huge data maintenance cost. Blockchain network is a decentralized network in which each node has a copy of entire data loop. The blockchain technology is a trustworthy technique for scaling and securing IoT data. Even , still there is not an exact path or technique how blockchain technology can be deployed with IoT devices. A token-based system is implemented for transaction to eliminate these security loopholes and verified the result using transaction summary.**

Index Terms **- Blockchain, Authentication, Security, Cryptography, Decentralization, Immutability.**

1.INTRODUCTION

In[1]recent time, IoT(Internet of Things) has arisen with an end goal of focusing or targeting computerized automated system where all hubs, gadgets and sensors, network are interconnected. IoT has made things much simpler with smart home, smart health, smart agriculture, smart cities and with other smart devices approach. As millions of devices are connected to the consistently developing networks, security and privacy in IoT networks seems to be a main concern in this field. The majority of IoT devices are asset limited and with high cryptographic approaches is challenging in execution and implementation. Latest[2] research work shows that utilizing blockchain in IOT seems to be a way for removing security loopholes. The[3] current IoT environment consist of centralized system in which all the devices are controlled, used and authenticate centrally that raise the adaptability threat Therefore, Blockchain give us a distributed authentication and the executive framework that can validate and authorize the privacy and security of user's data. In Blockchain decentralized node are used which provides automotive security, validation and trust the executive in both distributed and decentralized IoT environment. Blockchain technology ensure that it eliminate the duplicate issue by fetching assistance from a symmetric cryptography process that comprises of a private and a public key. Private keys are stored securely from the other node in the network whereas the public keys are mutually distributed among all the nodes. However, the transactions are digitally signed by the nodes that create the transactions which is broadcast to the entire blockchain networks. All receiving nodes will be verified with the transactions by decryption of the signature with a public key of the processed node. The transactions are verified by the verification of signatures which indicate the initialization of node which is not modified. The main objective of this paper is to implement Blockchain to analyze the prospect of using blockchain in IoT ecosystem for enhancing IoT security and privacy.

2. RELATED WORK

There are many studies on securing of IoT devices using blockchain. In the paper proposed by L. Xu et. al. [11] shows that the IoT devices have loopholes in security shields from which data can be theft by hacking into a IoT network system including sensors,

IoT connector and IoT Appliance. S. Singh et. al. [2] proposed that the smart house is also vulnerable which can be attacks by using user's smart phone even if the home gateway system have all controls of exchanging packets to and from the home system. M.A. Ferrag et. al. [12] proposed a method with three different modules to protect user's data privacy and security in smart house. The user's data that is collected by the module collector from the smart house and sends them to the receiver module that store data in two unique data sets. The resultant system module controls the user access to protect data from theft. This method ensures that only the correct user can control and access the data. By using two data sets it is confirmed that connecting different data of a user to each other is not possible. However, this method does not give privacy when the user reveals his data set to a service provider. R. Song et. al. [5]proposed Blockchain - In the recent years, with the rise of Bitcoin, Blockchain is one of the areas where the advancements have boomed exponentially and with rapid developments everyday it has opened a whole new universe for the tech enthusiast and developers that has paved a way for a New World Order in the Digital space. Rapid demand in adoption of blockchain technology, many researchers have proposed different use cases for the new technology. X. Zhu et. al. [18] proposed the insights on the use of security services for current applications, to highlight the state-of-the-art techniques that are currently used to provide these services, to describe their challenges. Z. Deng et. al. [4] proposed many new improvements and advances had also been done. In the sector of healthcare using blockchain which is well mention in the work proposed by Srivastava et al. In the paper by Z. Zheng et. al. [1], a new way for data authentication and authorization was proposed that not only increases the credibility but also suggest new ways of protecting and securing data through blockchain. IoT System and Applications - In previous work by S. Dong et al. [10] shows relationship, investigates challenges in blockchain IoT applications, and surveys the most relevant work in order to analyze how blockchain could potentially improve the IoT. S. Bin et. al. [14] proposed analyses' the security risks of digital wallets in Android, which is the most popular mobile operating system. Not only cryptocurrency wallets but IoT and Blockchain finds its application in Voting System with is brilliantly explained By S. Sankaran et. al. [19] proposed the simple transaction using token method in which transaction is not fully secured from token data of transaction and coins can be easily theft .The token manager used in this study has not have strong algorithm which can be easily hackable. G. Sun et. al. [17]proposed a method with four different steps in which IoT data is processed Which uses a algorithm to covert data in different hash code, which makes data secure from hacker.

3. PROPOSED WORK

This paper proposes a blockchain Ethereum Payment wallet which uses the concept of token for transactions. This implementation of Ethereum Blockchain wallet utilizes smart contract which will enable transaction without instant connection to the internet. The process is divided into four steps. In first step use of internet is required to convert Ethereum coins into token at the token system. The token system initiate the transaction and cover coin into token and provide us a hash key which also contains the information to complete the transaction. After this an offline transaction step will initiate using which the token can be sent to the receiver using secure near field communication. The transaction details and value in the form of encrypted token by the sender is sent to the receiver using near field communication.

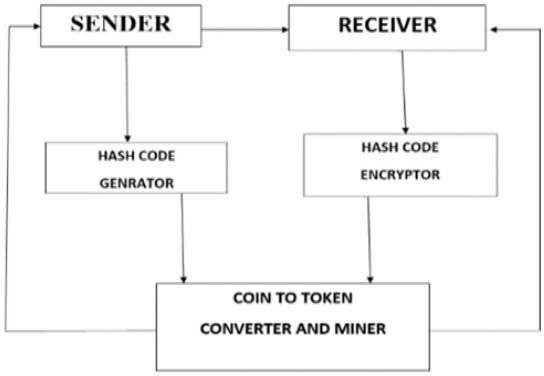

Fig.1 TRANSACTION IMPLEMENTATION

Above Fig.1 is a block diagram of the transaction wallet implementation in which we are converting a crypto coin into a token which is protected by the hash algorithm and coin in the form of token is sent to the receiver. Token contains the transaction information of sender and receiver and it is encrypted by a hash algorithm.

Near Field Communication (NFC)

For [16] transferring the token without using internet there should be a nearby range communication in between the sender and receiver. This process is necessary for the transferring the token under a secure condition that is able to prevent cyber-attacks which makes NFC (Near Field communication) a correct choice. Previously NFC devices are weakly encrypted because of power and computational requirement, making to attacks [15], but now these security issues are eliminated from NFC devices. NFC is a wireless technology with very small range (about 3-4cm) basically consist of two portable devices, connected in a point-to-point configure as shown in Using high cryptographic protocols such as secure socket layer (SSL), NFC devices connection are secured from hacking. An near field communication devices Secures Elements (SE) complimentary attestation and validation for portable devices which is capable of providing a secure on demand access of utilization of NFC-based Host Card Emulation (HCE) . A token is created by a cloud base Trusted Certified Authority (TCA) and stored in a cloud Trust Platform Module (TPM)-based attestation modules on the devices.

The token is used for transactions in between NFC devices. This process can be done without the use of internet. This process is initiated by the sender with an initiation. An acknowledgement notification display the profile details of the receiver and is used to confirm if the token is sent to the right device or not. The receiver device takes the value of token to be transferred. The sender device transfers token after confirming the value of transfer. The receiver device removes the used tokens from sender's device and terminates transaction. The removal of used token is the first measure that is taken to prevent double spending.

Secured Hash Algorithm

This algorithm needs an exponential form within the variety of zero bit which are used to confirm the hash algorithms. In an exceptional blockchain networks, all the existing nodes which are implemented in the blockchain network. This will be used in all the mining process by increasing a nonce value inside the block till the value is established that offer the blocks hash's desirable bit. After the system unit able to fulfill the requirement of PoW (Proof of Work), the blocks cannot be changed till the remake. Blockchains contains a distributed IoT information system that provide user the choice of mutuality the information with other outside entity. The target-area of this process is to give a distributed information access model for IoT, that ensure that the user-data cannot be assigned to centralized entity or corporation as shown in Fig.2 .

Fig.2- Hash algorithm

```
PS C:\Users\DELL\Desktop\Major project file\blockchain> node index.js
smashingCoin mining in progress....
{
    "blockchain": [
        {
            "index": 0,
            "timestamp": "08/05/2022",
            "data": "Initial Block in the Chain",
            "precedingHash": "0",
            "hash": "6fcad691f109b98b7f7fed3099f4dd8822b23b47ed575c1a93eaf0d6b35654c9",
            "nonce": 0
        },
```

```
"index": 1,
"timestamp": "08/05/2022",
"data": {
    "sender": "Kartik",
    "recipient": "Nitin",
    "quantity": 50
},
"precedingHash": "6fcad691f109b98b7f7fed3099f4dd8822b23b47ed575c1a93eaf0d6b35654c9",
"hash": "0000d99813ab308db8f2126fa918d545a8b05c64622454d6b992784a1619386f",
"nonce": 23411
```

Fig.3 . Hash key generated output

In Fig.3 the hash key generated output is shown where the token is converted using secure hash algorithm. For each transaction hash and preceding hash key is generated for each transaction. We have use ganache for generating addresses and Ethereum coin, basically ganache is used for research and development it provides different Ethereum account with private and public key for development purpose.

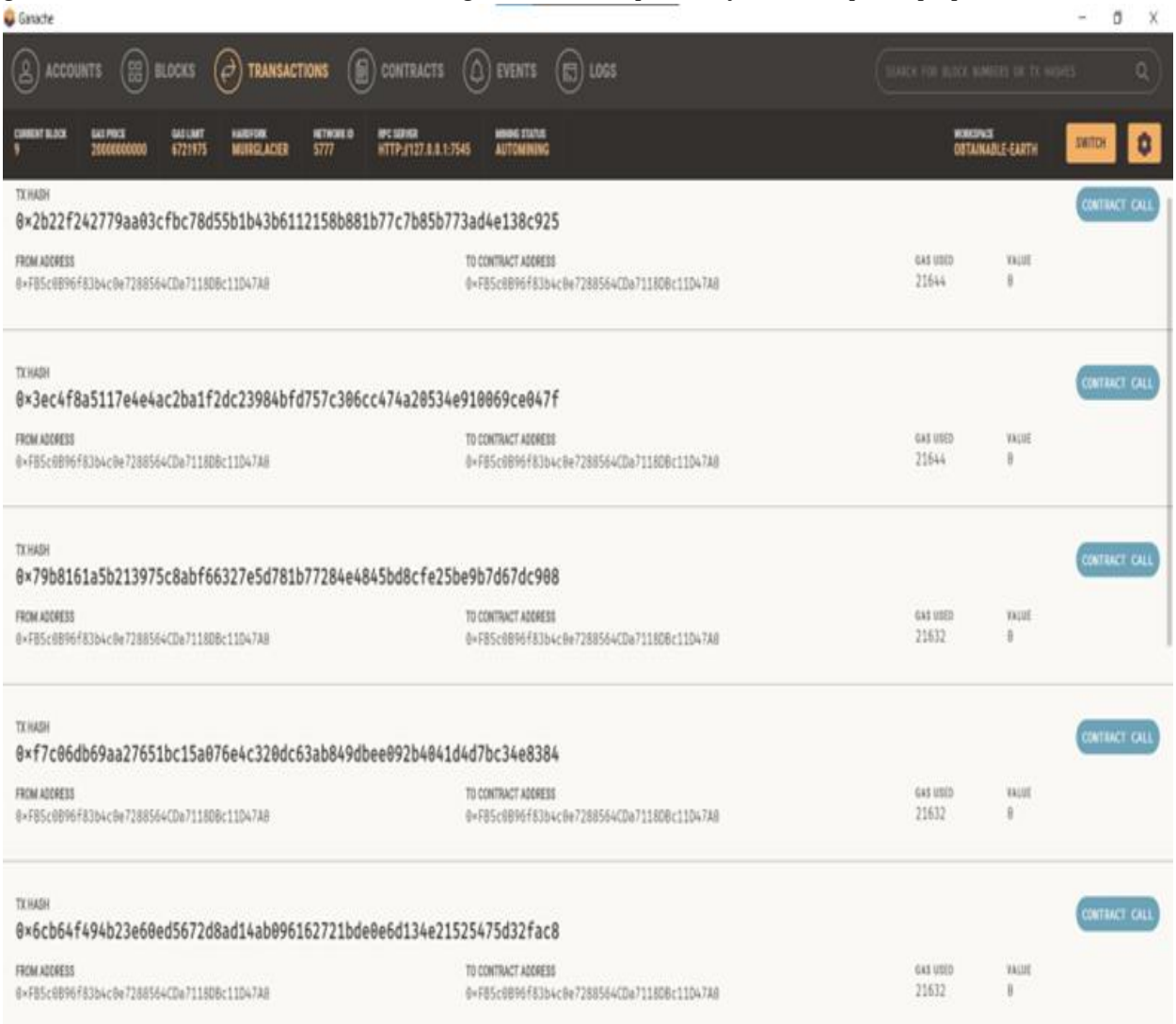

Fig.4 . Transaction summary

We have also provided PoW (proof of work) which provide difficulty of level 4 which is also shown in Fig. 3.In Fig.4 we have shown the transaction summary of our completed transaction using Ethereum coin. The transaction summary is shown in the ganache application which include transaction

addresses, transaction id, PoW (proof of work) that conclude the transaction confirmation with secured process.

5.CONCLUSION

This paper discusses about the different issues that are present in the IoT devices,
many of the issues are related to security. These issues can be eliminated by using blockchain technology in most of the research work as seen in many survey blockchain is appropriate for the IoT devices. The study also include why block chain in IoT networks is necessary and various security issues can be solved using the blockchains technology in IoT networks. To solve the problems that are present in the study shows the measures that can be taken up. We can analyze the reason responsible for lack of security is because authentication does not have the proper proper algorithm. In this work there are many fields that can be improved such as the encryption key or hash key that is generated in the blockchain is not that much secure it can be improved by implementing algorithm mechanisms. Even though authentication that is provided in IoT networks exists many attacks through which the data can be hacked, hence there can be different algorithm that can be implemented in future to surpass this problem.

REFERENCE

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, ‘‘Blockchain challenges and opportunities: A survey,’’ Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2017.

[2] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, ‘‘SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology,’’ Int. J. Distrib. Sensor Netw., vol. 15, no. 4, pp. 1–17, 2017.

[3] X. Jiang, M. Liu, C. Yang, Y. Liu, and R. Wang, ‘‘A blockchain-based authentication protocol for WLAN mesh security access,’’ Comput., Mater. Continua, vol. 58, no. 1, pp. 45–59, 2017.

[4] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen, and H. Kim, ‘‘Blockchain-based trusted electronic records preservation in cloud storage,’’Comput., Mater. Continua, vol. 58, no. 1, pp. 135–151, 2018.

[5] R. Song, Y. Song, Z. Liu, M. Tang, and K. Zhou, ‘‘GaiaWorld: A novel blockchain system based on competitive PoS consensus mechanism,’’ Comput., Mater. Continua, vol. 60, no. 3, pp. 973–987, 2018

[6] C. Li, G. Xu, Y. Chen, H. Ahmad, and J. Li, ‘‘A new anti-quantum proxy blind signature for in-enabled Internet of Things,’’ Comput., Mater. Continua, vol. 61, no. 2, pp. 711–726, 2018.

[7] W. Wang and C. Su, ‘‘CCBRSN: A system with high embedding capacity for covert communication in Bitcoin,’’ in Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection. Cham, Switzerland: Springer, 2019, pp. 324–337.

[8] Z. Lejun, Z. Zhijie, W. Weizheng, W. Rasheed, Z. Chunhui, K. Seokhoon, and C. Huiling, ‘‘A covert communication method using special bitcoin addresses generated by vanitygen,’’ Comput., Mater. Continua, vol. 65, no. 1, pp. 597–616, 2019.

[9] S. Li, F. Liu, J. Liang, Z. Cai, and Z. Liang, ‘‘Optimization of face recognition system based on azure IoT edg,’’ Comput., Mater. Continua, vol. 61, no. 3, pp. 1377–1389, 2019.

[10] D.Y. Kim, S. Dong Min, and S. Kim, ‘‘A DPN (delegated proof of node) mechanism for secure data transmission in IoT services,’’ Comput., Mater. Continua, vol. 60, no. 1, pp. 1–14, 2019.

[11] L. Xu, C. Xu, Z. Liu, Y. Wang and J. Wang, ‘‘Enabling comparable search over encrypted data for IoT with privacy-preserving,’’ Comput. Mater. Continua, vol. 60, no. 2, pp. 675–690, 2019.

[12] M. A. Ferrag, A. Derhab, L. Maglaras, M. Mukherjee, and H. Janicke, ‘‘Privacy-preserving schemes fog-based IoT applications: Threat models, challenges and solution’’ in Proc. Int. Conf. Smart Commun. Netw. Technol. (SaCoNeT), Oct. 2020, pp. 37–42.

[13] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, ‘‘A decentralized privacy-preserving the healthcare blockchain for IoT,’’ Sensors, vol. 19, no. 2, p. 326, Jan. 2020.

[14] S. Bin, M. Jiang, N. Cao, Z. Zheng, H. Zhao, D. Wang, and L. Xu, ‘‘Research on public opinion propagation model in social network based on blockchain,’’ Comput., Mater. Continua, vol. 60, no. 3, pp. 1015–1027, 2020.

[15] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, ‘‘Privacypreserving support vector machine training over blockchain-based encrypted IoT data in smart cities,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 7702–7712, Oct. 2020.

[16] R. Song, Y. Song, Z. Liu, M. Tang, and K. Zhou, ‘‘GaiaWorld: A novel blockchain system based on competitive PoS consensus mechanism,’’ Comput., Mater. Continua, vol. 60, no. 3, pp. 973–987, 2020.

[17] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng, H. Zhao, D. Wang, and L. Xu, ‘‘Research on public opinion propagation model in social network based on blockchain,’’ Comput., Mater. Continua, vol. 60, no. 3, pp. 1015–1027, 2020.

[18] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, “Autonomic identity framework for the internet of things,” in Cloud and Autonomic Computing (ICCAC), International Conference on. IEEE,pp. 69–79. 2020

[19] S. Sankaran, S. Sanju and K. Achuthan, “Towards realistic energy profiling of blockchains for securing internet of things,” in 2018 IEEE 2020.

[20] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based storage and sharing of iot data,” in Proceedings of the 2017 on Cloud Computing Security Workshop. ACM, 2020