TRANSFER OF DIGITAL ASSETS USING BLOCKCHAIN TECHNOLOGY

Surya prakash.C [1], Rohit.S.R[2], Senthil.k[3], Preetha.M[4]

[1,2] Student, Information Technology, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India
[3] Associate Professor, Computer Science & Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India
[4] Professor, Computer Science & Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India

ABSTRACT

In this digital world, maintaining digital assets plays a vital role. The term digital assets refer to the binary data that need to be stored, managed, ingested, organized, and retrieved. In banking sectors, the transaction details of the digital assets are stored in a centralized database and the transaction between two users takes by the arbitrator. These digital assets can be transferred in a secured way by inculcating blockchain technology .Blockchain technology is mainly used for storing the data in a decentralized ledger. The data this are stored in the blocks are immutable in nature. In this work, we have developed Policy Based Access Control which provides flexibility and security for transaction of digital assets.

Keyword : - *Digital Assets Transfer, Block chain Technology, Proof of Delivery, Consensus Algorithm, Smart Contract.*

INTRODUCTION

Blockchain technology is considered as the backbone technology in which the digital assets can be secured by means of digital cryptocurrency. Blockchain technology is used to store the data in a distributed decentralized manner, and hence we could avoid the single point of failure. As the data are stored in a decentralized manner, we could easily recover the data if any failure occurs. One of the emerging and fast developing technology is the blockchain technology and it could be implemented in the banking sectors to address and resolve the pain points in the current banking process. In India, banking industries are facing several issues such as the amount collected by the arbitrators as a service tax, fraudulent attacks on the centralized servers and modification of data by the hackers. The causes for these issues are that the data are stored in a centralized database and also arbitrators are used for validation and verification of user data. As they are validating and verifying, they will collect service tax which is a loss for the recipient. There may be a chance of modifying the data by these arbitrators. Hence banks are adopting new ways to make instant transactions, no fraudulent by the arbitrators, no single point of failure and collection of less service tax when compared with the arbitrators. All these can be achieved by implementing the blockchain technology in banking sectors.

LITERATURE SURVEY

A. THE PAPEER PROOF OF DELIVERY OF DIGITAL ASSETS USING BLOCKCHAIN AND SMART CONTRACTS WAS PROPOSED BY X. PENG

He introduces that the current proof of deliverysystems which are mostly centralized and heavily dependent on a trusted third party especially for payment. Blockchain technology has been used for creating the bitcoin transaction and the transaction details will be stored in a centralized database. Using Ethereum which makes blockchain a programmable distributed ledger, is used to create a POD solution for digital assets. The digital assets have been transferred by using the smart contract in which the Ethereum address has been framed in each andevery block of the blockchain.

B. DIGITAL ASSET MANAGEMENT WITH DISTRIBUTED PERMISSION OVER BLOCKCHAIN AND ATTRIBUTE-BASED ACCESS CONTROL WAS PROPOSED BY YAN ZHU ET.AL

In this paper they had proposed that instead using Transaction Based Access Control they had implemented the concept of Attribute Based Access Control (ABAC). ABAC provides flexible and diverse authorization mechanisms for digital assets, in which the blockchain technology serves as verifiable and traceable medium of access request procedure. There are four types of transactions to describe the TBAC access control procedure, and provides algorithms to subject registration, object escrowing and publication, and access request and grant the permission for transferring the digital assets.

C. LIN GUO YAN ET.AL, DISCUSSED ABOUT BLOCKCHAIN BASED SOLUTION FOR PROOF OF DELIVERY OF PHYSICAL ASSETS LIKE SHIPPED PHYSICAL ITEMS

It uses smart contracts of Ethereum block chain network, in which tracking, tracing activities, logs and events can be done in a decentralized manner with high integrity, reliability and immutability. Thiseliminates the third party like escrow. Tracking of shipped items can be done, which is highly trusted, secure and decentralized. Escrow is a bond or documents kept in thecustody of third party. Anytime, the cancellation of transaction can be done by the user which may result in loss for the admin i.e., the time spent for the verification and validation for that particular transaction.

EXISITING SYSTEM

The existing banking systems are centralized and mostly depends on the trusted third parties for making the transaction between sender and receiver. The existing system uses the arbitrators, in which the extra charges will be collected by those arbitrators from the users. The algorithm used is proof of delivery, this algorithm is mostly used for the transaction of the physical assets. On analysing, the present consensus algorithms are having high computational work. The computation complexity refers to the complexity of the algorithms used for implementation and also the user cannot easily handle the system.

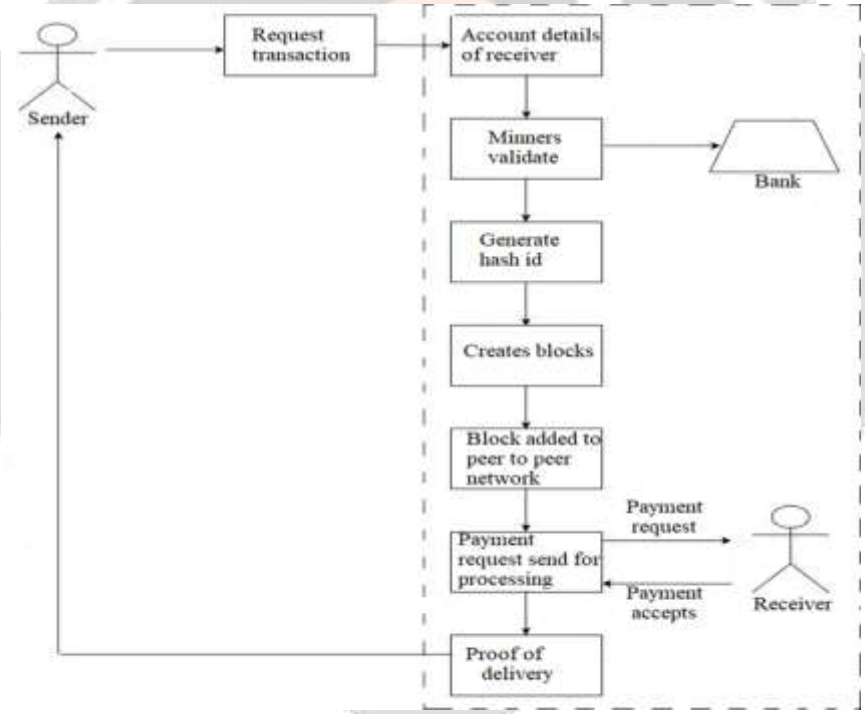
The existing banking systems are centralized and mostly depends on the trusted third parties for making the transaction between sender and receiver. The existing system uses the arbitrators, in which the extra charges will be collected by those arbitrators from the users. The algorithm used is proof of delivery, this algorithm is mostly used for the transaction of the physical assets. On analysing, the present consensus algorithms are having high computational work. The computation complexity refers to the complexity of the algorithms used for implementation and also the user cannot easily handle the system.

PROPOSED SYSTEM

Digital asset transfer refers to the transfer of assets which are in binary form. There are many forms of digital assets, in our proposed system we are transferring the money in a digital form. The system focuses on the transaction of money between sender and receiver without interruption of any arbitrators. The money can be directly transferred from the sender to receiver and thus transaction details are stored by using blockchain technology. The sender sends the request transaction along with this the sender’s account details will be validated by the miners (Not given who is the Miner). The miners validate the details of the sender and receiver from the bank. After validation hash ID is generated by using SHA256 algorithm. After the generation of hash ID, block will be created. The block contains the transaction details. For each transaction, a separate block will be created. Each block will have separate hash ID. These blocks will be added into the peer to peer network. The payment request made by the sender will be send for processing, when the receiver accepts the request then the money will be delivered by using proof of delivery algorithm. If the receiver is not interested in making the payment then he/she can cancel the transaction request and hence payment cannot be made.

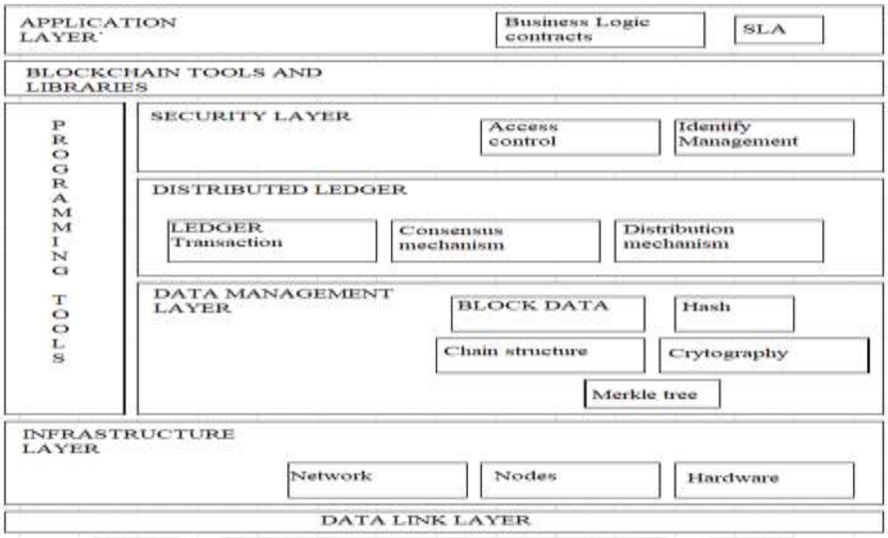
SYSTEM ARCHITECHTURE

The proposed system focuses on transaction of digital asset by using the blockchain technology. The architecture in figure shows the function of the transfer of digital assets using blockchain which is used for the transaction of money and the transaction details are stored in the blocks in a distributed decentralized ledger by using the secured hashing algorithm,



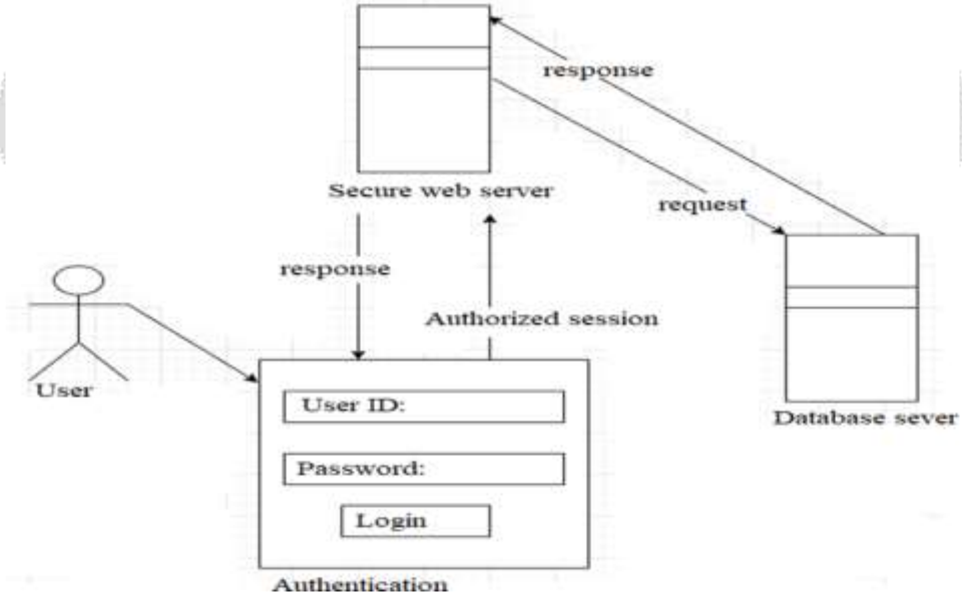
LAYERED ARCHITECTURE

Below diagram depicts the layered architecture of the proposed framework which indicates the organization of the working system. The layers are application layer, blockchain tools and libraries, security layer, data management layer, infrastructure layer, data link layer.



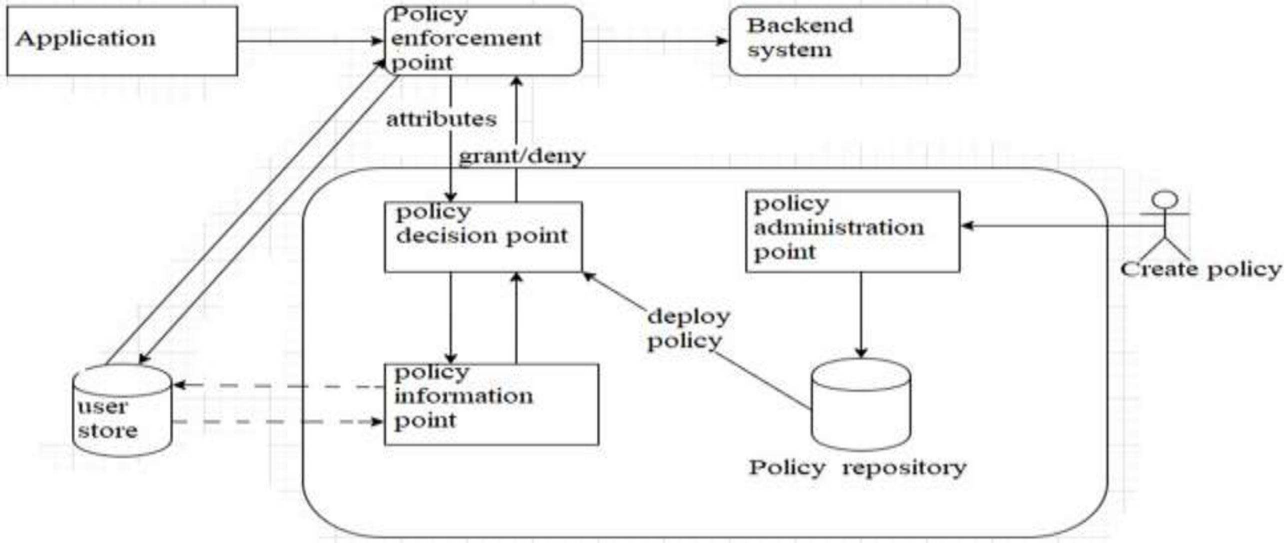
A. USER AUTHENTICATION

In this module, the user is verified based on the transfer of their credentials which is required for the confirmation of the user authenticity. User authentication is used for the interaction between the human to computer. It is the initial stage in which the user enters details and log into the account. The following diagram will explain about the user authentication



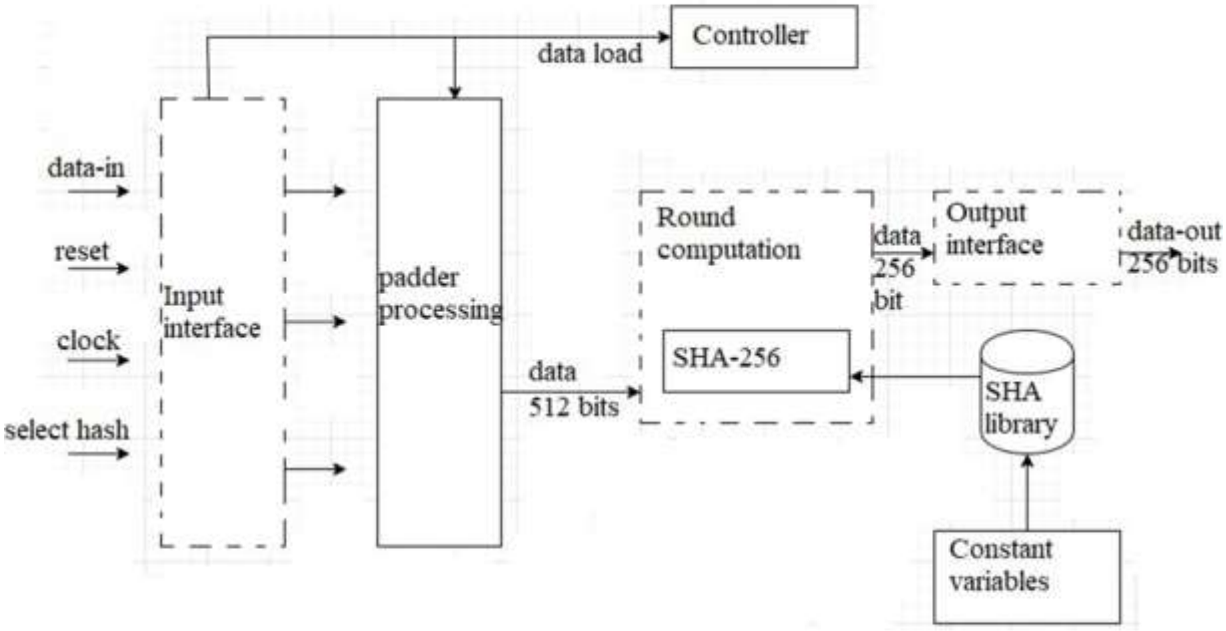
B . POLICY ENFORCEMENT

The deployed policy will be stored in the policy repository. After deploying the policy, the authorization requests are evaluated against the created policy. Now the application comes into consideration. Whenever the sender wants to request for the payment, an authorization request is sent to policy decision point with attributes. The policy decision point receives the attributes and evaluates the policy framed by the sender. The policy framed by the sender is present in Policy decision point. The valuation of the policy is done with the help of policy information point. These attributes and policies are stored in the database of the admin. After validation of the account details of the sender, the policy framed by the sender will be sent to the receiverresearch work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research.



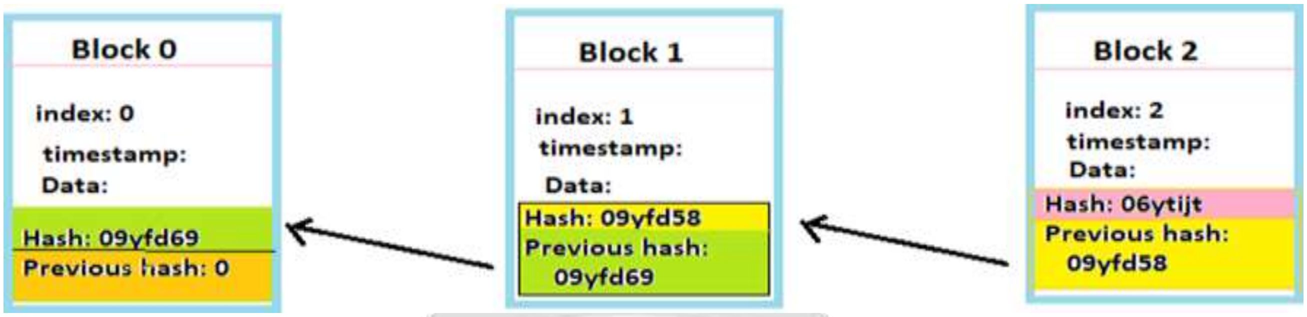
C.HASH ID GENERATION

In this module hash ID will be generated based on the account details of the user. The sender initially sends the policy along with the account details. These accounts must be validated. This validation is done by certain nodes which are called as miners. The miners collect the account details from the bank and validates. After the validation, the encryption process will take place. The encryption can be done in many ways but a strong encryption is needed in this blockchain technology



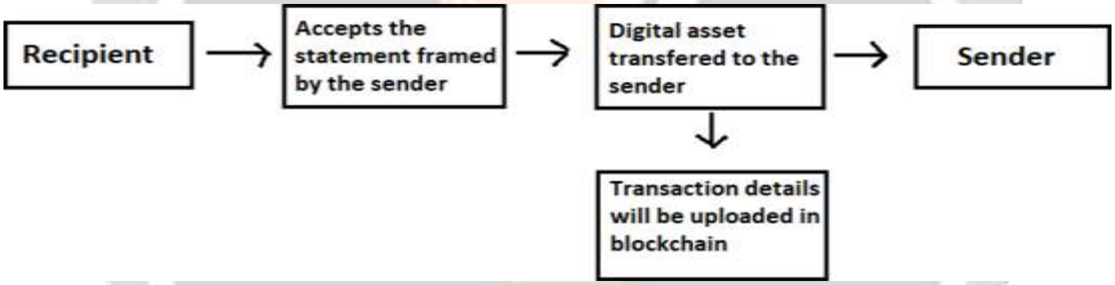
D.BLOCK CREATION AND VERIFICATION

In this module the blocks are created after the hash id generation. The hash id acts as the identity for each block in the blockchain. These blocks will be interlinked to form a peer to peer network. In a blockchain, nearly 210,000 blocks (about four years) can be created and blocks need to be verified. The verified blocks are added to the distributed ledger(record). In the chain, the first created block is referred as the genesis block. The genesis block will have the block number, time stamp (time and date of block created), data, hash value of that block and previous block's hash value.



E.CONSENSUS ALGORITHM

Consensus algorithms are widely used in blockchain as it is a distributed decentralized network. As in the blockchain, there is no centralized party required hence the verification and validation is completely done by using the consensus algorithm. Hence in the blockchain network, the consensus algorithm is considered as the core part.


Recipient
Accepts the statement framed by the sender
Digital asset transfered to the sender
Sender
Transaction details will be uploaded in blockchain

ALGORITHM US

1. ALGORITHM -SECURED HASHING ALGORITHM

INPUT: The details of the receiver has to be entered. PROCESS:

1 Initially the has been entered.

2 Input interface : It transforms the input data into binary code that are acceptable to a computer.

3 Padding process: the input data are split into blocks of fixed size. The last block may be small so it is extended until it reaches the fixed size (448 mod 512)

4 Round computation: It is the function used in the rounds of encryption.

Function round means same function applied many times over. We do this to intention slow down the calculation.

5 Output interface: the output generated will be an hash value which is considered as the hash id for the blocks.

2. ALGORITHM – BLOCK CREATION

```

Create GenesisBlock() {

return newBlock(0, “01/01/2020” , “Genesis block” , “0”)

}

#append blocks return self.chain[-1] add Block (new Block)
{
newBlock.previousHash=self.getLastBlock().hash
newBlock.hash=newBlock.calcHash() self.chain.append(newBlock)
}

```

CONCLUSIONS

Blockchain technology is one of the technologies in which the trust can be achieved by securely storing the data in a decentralized distributed ledger. It also allows us to verify the information without the interference of the third party. The data can be only appended in the blocks of blockchain and hence the data cannot be modified. The data that are appended in the blockchain are verified and validated and then stored in the distributed ledger. These data are stored in a decentralized form and hence there is the possibility of recovering the data when its lost. As we know blockchain is a open distributed ledger it is resistant to modification of data of information and hence our proposed system was designed as the open distributed ledger and hence all the data can be stored in the blockchain and hence modification of data cannot takes place and if modification occurs it could be easily identified.

ACKNOWLEDGEMENT

We would like to thank all our faculties, friends and family members who have directly and indirectly helped in easy completion of our project. Special thanks to Dr.K.Senthil, Associate Professor And Dr. M. Preetha, Professor, Department of Computer Science and engineering, Prince Shri Venkateshwara Padmavathy Engineering college, Chennai, Tamil Nadu, India for guiding us in completing this project successful.

REFERENCES

[1] X. Peng, “Proof of Delivery of digital Assets using blockchain and smart contracts”, IEEE conference, vol.3 issue-8, 2019, pp. 1-11.

[2] Yan Zhu et.al, “Digital asset Management with distributed permission over blockchain and Attribute-based access control”, journal, vol.5 issue-7, 2018, pp. 1-18.

[3] Lin guoyan, “Blockchain based solution for proof of delivery of physical assets like shipped physical items”, journal, vol.2 issue-10, 2019, pp. 1-23.

[4] WenAn Tan, Yong sun, Ling Xia Li, Tong Wang, “Blockchain-based proof of delivery of physical assets with single and multiple transporters”, journal, vol.7 issue-4, 2016, pp. 1-10.

[5] Tianwei zhang and Rudy T. Lee , “Blockchain Future of financial and cyber security” , journal, vol-4 issue-12, 2018, pp. 1-7.

[6] Mouad zouina, Benaceur outtaj, “Towards a distributed token based payment system using blockchain technology”, IEEE conference, issue-8, 2019, pp. 1-10.

[7] Tong wu, Xiubo liang, “ Exploration and practice of inter-bank application based on blockchain”, journal, vol.3 issue-5, 2017, pp. 1-6.

[8] Qixia, Emmanuel boateg sifah, Ke huang, Ruidong chen, “Secure payment routing protocol for economic systems based on blockchain”, journal, vol.4, 2018, pp.1-5.

[9] Simanta ,Shekhar sarmah, “Application of blockchain in cloud computing”, journal, vol.8 issue-12, 2019, pp.1-7.

[10] I.M.Bach, B.Mihaljevic, M.Zagar, “Comparative analysis of blockchain consensus algorithms”, journal, vol.5 issue-9, 2018, pp.1-6.

[11] Haya R.hasan, Khaled salah, “Blockchain based solution for proof of delivery of physical assets”, journal, vol-2 issue-4, 2018, pp.1-16.

[12] Jing Zhong wang, Mengru li, Chao wang, “A blockchain based privacy preceрving incentive mechanisms in crowdsensing applications”, vol.4, 2018, pp.1-12.

[13] Sachidanand singh, Nirmala singh, “Blockchain future of financial and cyber security”, journal, vol.3 issue-8, 2016, pp.1-5.

[14] Haya r.hasan, Khaled salh, “Blockchain based proof of delivery of physical assets with single and multiple transporters”, IEEE conference, issue-4, 2015, pp.1-13.

[15] Weili chen, Zibin zheng, Elithngai peilin zheng, “Exploiting blockchain data to detect smart ponzi schemes on Ethereum”, journals, vol.8 , 2019, pp.1-12.

[16] Prachmawari, Jtarigen, C Gingting, “Acomparative message digest and SHA256 algorithm”, journal, vol.6, 2017, pp.1-7.