Block chain technology for protecting the banking transaction without using tokens

Uma mageshwari J

Computer science engineering. Madha Engineering college, Tamil nadu. India

Abstract

Increasing digital technology has revolutionized the life of people. There are many threats and frauds detected in banking system. A centralized database is used by banking system which makes the attacker easy to get access to data and this makes the system insecure. The drawback of this centralized system can be reduced by reforming the system by implementing blockchain technology without using tokens. Blockchain uses decentralized architecture for storing and accessing data over the database. This reduces attacks on database hacked. Transactions done through blockchain technology are verified by each block in the chain, which will make the transaction more secure and help banking system work faster.

Keywords

Blockchain Technology; Distributed database; Cryptocurrency; Consensus; Security and Protection.

I.   INTRODUCTION

Blockchain was first implemented on Bitcoin cryptocurrency. This technology was first proposed in 2008 to develop bitcoin which is a successful cryptocurrency and executed in 2009.[2] Computerized cash is supported and powered by innovation of Blockchain. Blockchain plays a vital role in affirming and approving exchanges in a digital currency. It has a special structure that does not involve a third person. When a new transaction is requested a new block is created in an existing blockchain by validating that block and thus this chain grows.

Banking as a service requires maintaining and securing customer information to protect it from hackers, which is increasing day by day. In today's world commercial banks has importance in the financial institutions so that data should be able to withstand information leakages and attackers, which provide customers satisfaction and reliable services. For this security purpose, an alternate solution is provided which requires high cost and time, hence its less efficient [1]. Blockchain to serve the customer with a reliable and less time-consuming system. So, the blockchain is a preferred solution.

Peer to Peer network is implemented in the blockchain. The main characteristic of this distributed system includes fault tolerance and extensibility in the blockchain. It is very necessary to protect the geographically decentralized data structure to protect it from data losses, internal failure, and termination of the entire system [1].

To retain consistency in a decentralized system, a blockchain technology is preferred. Blockchain is about advanced data (chunk) put away in an open database (chain). The information is conveyed across numerous PCs, and the entire blockchain is completely decentralized. This implies no individual has command over blockchain, this is an extreme database that controlled and regulated by organizations and different elements.

Blockchain system joins private keys innovations, appropriately arranged and shared records

II.   LITERATURE SURVEY

Natalia A. Popova, Natalia G. Butakova et.al [1] mentioned that the way to improve security and performance regarding transactional information of banks. Entire transaction history can be traced after the generation of a new block. Consensus protocol solves the issues of competitive access. All transactions that are completed are checked by this protocol. The temporary balance conditions of certain transactions are removed. Block hashing uses hash value which is calculated by the Merkle tree.

Satoshi Nakamoto et.al [4] mentioned a peer to peer electronic cash system (Bitcoin). 2016. Online Payments or transaction where directly send from one party to another without going through a financial institution which undergoes peer to peer communication. Digital signatures play a role in protection at a limit. The proposed system uses a verification of data and secure transmission of money through bank validation.

Jesse Yli-Huumo (2016) et.al [6] mentioned the blockchain has Secure Data management technology and a decentralized system. A definition that is constant with the definition of other authors verifies here. It also mentioned several technical limitations and challenges that blockchain technology has. Few identified challenges are multiple chains, wasted resources, usability, throughput, size and bandwidth, latency, security.

Siba (2016) et.al [7] mentioned Public, private & hybrid are the three types of blockchain. A digital ledger that is completely decentralized and can be accessible to any internet user is called public blockchain (Siba, 2016). A private blockchain is wherein the sense that there is a central authority giving permissions control the transaction in the blockchain, which is the main difference between public and private.

Blockchain is a system where there can be no exception because a transaction is wrapped into the blockchain which cannot be hacked. High requirements like reliability and honesty for a business, where they can use blockchain to Attract customers such as cash back. In addition to the distributed functionality that can provide an avoidance to the single point of failure situation. Blockchain faces several problems even if it has a great future.

Tareq Ahram1, Arman Sargolzaei2, Saman Sargolzaei3,4, Jeff Daniels5, and Ben Amaba6 et.al [8] tells about innovation to the blockchain. The efficient use of analytics and cloud technology, mobile, social media, and IoT (Internet of Things), had led the digital world to new creations. A new perspective to security, resiliency, and efficiency are the few terms that are introduced by the blockchain. Blockchain gained huge popularity through bitcoin and formed a foundation for cryptocurrency. A secure way of transaction, goods, services are provided by blockchain technology. Challenges like transaction security, frauds hacker attack blockchain is a quicker and easy chain provider and faster integration with cloud technology and IoT. IBM Blockchain is used for developing and formalizing the healthcare industry. The concepts arepreferable to a huge range of manufacturing industries, government, and finance where efficiency, security, and scalability must meet the needs.

Sachchidanand Singh, Nirmala Singh et.al [10] mentioned the future of financial and cyber security using blockchain technology. This paper explains the need for blockchain and a summary of the working of bitcoin. Financial institutions and the future of banking can be shaped by adopting of Internet of Things (IoT). IoT is a few aspects where the blockchain mainly focuses on. Bitcoin uses hash which is an output of Secure Hash Algorithm 2 (SHA-2). The hashing algorithm converts a huge amount of data into a fixed-length hash value. In public blockchain same hash algorithm is used by a slight variation.

III.BLOCKCHAIN TECHNOLOGY

Blockchain technology is a distributed database which contains information about all the transaction that occurs in the system. It is a type of data structure for storing and transmitting data in packages. These packages are called blocks that are connected to the digital chain.
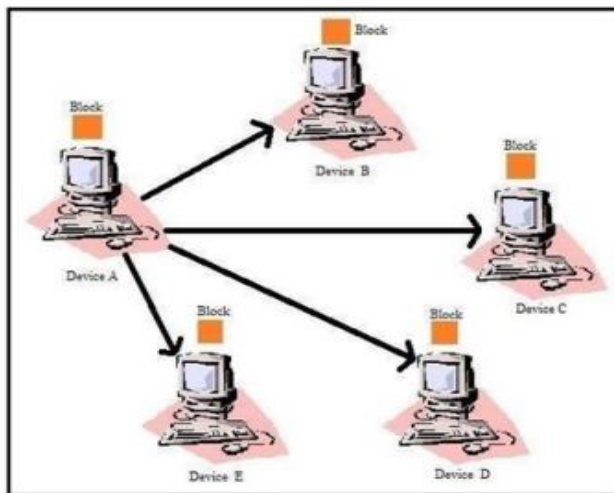
Fig. 1. Information broadcasting in blockchain.

Fig. 1. Represent how the information is distributed by the blockchain over the network which prevents the problem of distributed consensus.

In blockchain each block is verified by consensus of participants before adding it to blockchain. Blockchain is immutable. The reason behind is that once data added in blockchain it cannot be reversible or erased.

The first block created in blockchain is called as genesis block which has no parent and it is parent of all other blocks which are newly added in a blockchain [13].

The consensus protocols are used for adding a new block in blockchain and bring all nodes in agreement i.e. all nodes trust on each other. Suppose one transaction is created and this transaction is broadcasted to every node and new block is created which contains one or many transactions. Each node performs proof-of-work (PoW) for its block. PoW isconsensus mechanism. After performing PoW by a node, block is broadcasted to every node. After validation of block, new block is added in a blockchain [3].

ARCHITECHTURE OF BLOCHCHAIN

The blockchain is sequence of blocks which hold the information about transactions between nodes of a network. Block Header consists of Block version, Merkle tree, Time Stamp, n Bit, Nonce, and Parent Block Hash.

• Block version consist of validation rules to be followed by block.

• Hash values of transactions are calculated by merkle tree.

• Current time is saved in time stamp.

• Target Threshold of a legitimate block hash in n-Bit.

• A varied accessory parameter is called Nonce, a 4- Byte (32 bits) field whose values is adjusted by miners during hash calculation.

• Parent Block Hash indicates the pervious block hash value, where block i-1 is executed, block i is under execution and block i+1 is yet to be executed.

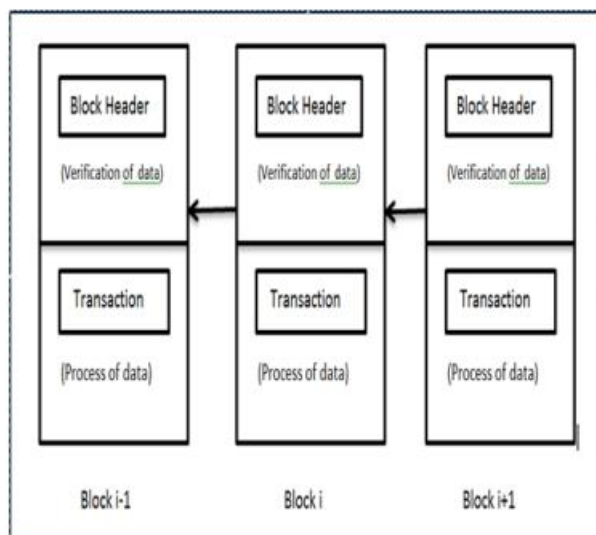Transaction Counter stores the number of transactions that are completed by the block [12].

Fig. 2. Blockchain architecture

A Blockchain is a sort of spreadsheet containing data about exchanges. Every exchange creates a hash. A hash is a series of numbers and letters. Exchanges are entered in the request wherein they occurred. The hash depends on the exchange as well as the past exchange's hash. Indeed, even a little change in an exchange makes a totally new hash. The hubs check to ensure an exchange has not been changed by examining the hash. Each block alludes to the past block and together makes the Blockchain.

IV. PROPORED SYSTEM

In banking system, the centralized database will be replaced by a decentralized system, which will distribute data over the chain.

Banking information system processes and transmits customer's data which consist of account status, history of their transaction which is stored inside their infrastructure. Thus, there is a need to find a way to provide integrity and uniqueness to information that is transferred over banking transactions.

In a Banking System transaction must go through a bank that is why proposed concept excludes the use of miners or tokens. Only bank can add a new block, no one else has an authority to add a block even though they are a part of system. If person A, has to transfer money to person B, then banking system will first verify, validate and record the transaction and then create a new transaction in the block [1]

The system uses SHA-256 algorithm. SHA represents Secure Hashing Function, and 256 communicate the numerical amount of the fixed piece length. This implies the objective is right 256 piece, and as referenced, Bitcoin utilizes a 65-hexadecimal hash value. Using the SHA-256 capacity makes it difficult to copy a hash for creating the hash value for a specific block which is further used for validating the same block. The hashing procedure gathers input information into a fixed size. Hashes recognize, think about, or run figuring against records and strings of information. When endeavoring to add to a degree blockchain, the program must illuminate for the objective hash with the goal for it to arrive at acknowledgment as another block. The validation is done by computer nodes connected in the blockchain. It compares the previous hash value stored in the system with a new hash value of a block. It creates a hash value of data in the block. The length and size of the hash value are the same for all kinds of data.

In the system, in which two people wish to lead an exchange of money, each with a public and a private key, blockchain permits individual A to utilize their private key to merge data in regards to the exchange to the public key of individual B. This data together structures some portion of a block, which contains a computerized signature just as a timestamp and other applicable data about the exchange, yet not the personalities of the people associated with that exchange. That block is then transmitted over the blockchain system to the entirety of the hubs, or other segment portions of the system, which will at that point go about as validators for the exchange of money. Sending of data and approving of block requires enormous measures of figuring power. This is done by miners present in the system which validates the block and then puts it in the block chain, during the time spent blockchain approval, a system who surrenders a little part of their computational force so as to offer assistance to the system accordingly wins a prize.

In Existing System, humans working as miners are rewarded for work. We propose to replace human by a trusted architecture to work as miner, thereby providing a high level of security for the transaction.

Nodes connected in distributed system transfer block to every node that they are connected to. After verification, each block is replicated in system. While transferring a block in highly secured network there is no predetermined path to be followed.

At point when an exchange is recorded in blockchain, Subtleties of Exchange, for example, value, resources and possession, are recorded, verified and validated in all hubs of system.

V. EXPERIMENTAL SETUP

The proposed system is implemented in NS 2; following are the simulation parameters which are implied on the system.

Table I. Simulation parameters

Configurations Parameters	Values
Simulator	NS 2
Simulation area	1000 m X 1000 m
No. of nodes	1,2,3,4,5,6,7,8,......100
Operation preformed on nodes	10, 20, 30, 40
Source-destination Pairs	4
Packet size	512 bytes
CBR rates	4 bytes
Mobility	RWP
Max. speed (ms)	4–24 ms
Simulation time	600 ms
Channel Type	Wireless Channel
Routing Protocol	SCTP, S-ADHOC, DVR
Transmission Range	250m
Max Packet In Frequency	50

The table defines the configuration parameters that are used for simulation. Here the parameters are examined on the nodes connected in P2P network topology. since it is a public blockchain it can be connected to n number of blockchain, for simulation, results have been evaluated on operation nodes as mentioned in above table. Packet Size defines the size of block transferred in the network.

VI. PERFORMANCE ANAYLSIS

The simulation was performed to test the performance of the existing and proposed work by considering the blocks viz, 10, 20, 30, 40 where the Delay, overhead and throughput was calculated, and the comparison was done for existing as well as for the proposed system. Following are graphs which mention variations with existing and proposed system.

1.   **Delay(ms)** Delay is the time taken by a node to create a new block and validate it in a blockchain. Time taken by the miners to create the blocks and validate them is higher in the existing system than in the proposed system. This is because the existing system requires human interference. Here the delay is calculated in milli seconds.
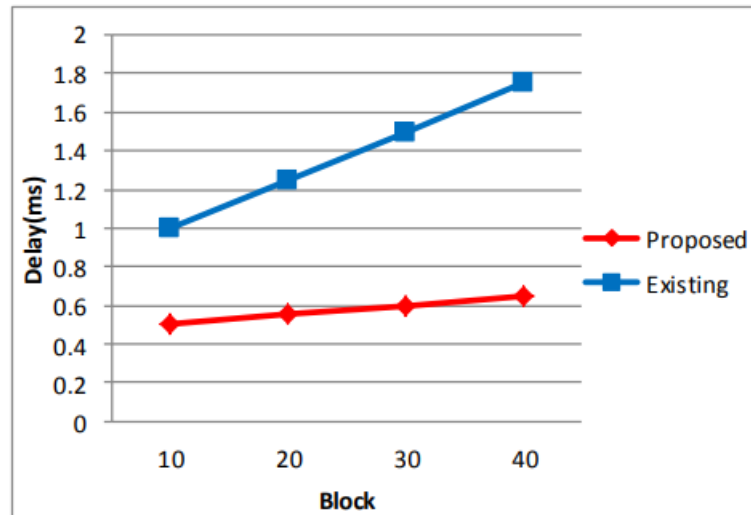
Fig.3 Delay Comparison for Validating Block in Blockchain.

2.

Fig 3 shows a comparison of delay with respect to the existing and proposed model, which stated that the performance of proposed is appreciated.

3. Overhead

Unlike the delay which accounts for single block, the overhead helps us keep track of time lapse of overall blockchain.

In a blockchain, multiple copies of blocks have to be maintained in every system. This results in requirement of high network connectivity. Automation techniques are provided for miners thereby making it easier to share the workload while
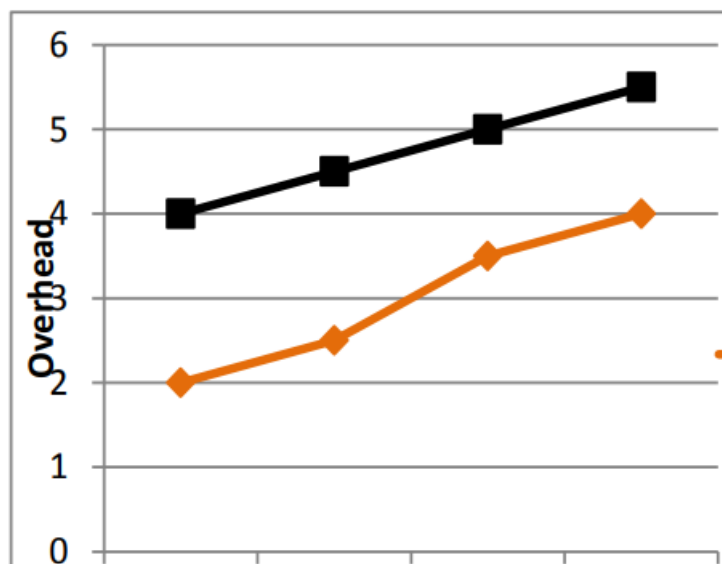
Fig. 4 Overhead Comparison in Blockchain

validating and creating new blocks.

Fig 4 shows a comparison of overhead with respect to the existing and proposed model, which stated that the performance of proposed is appreciated.

4. Throughput

Throughput is measure of rate of validation of blocks by nodes in a network. In the existing system, humans are miners which take more time, because they have to solve the given mathematical problem to validate and create a new block. In

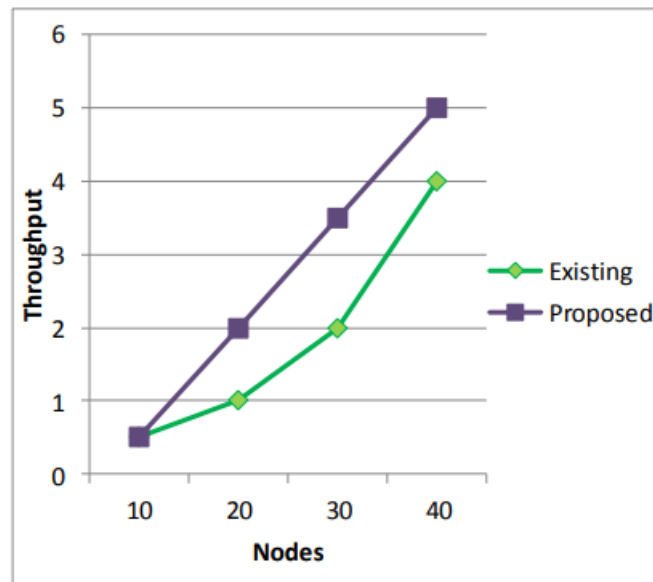proposed system, nodes take lesser time than the existing system

Fig. 5 Throughput comparison in the Blockchain

Fig 5 shows a comparison of throughput with respect to the existing and proposed model, which stated that the performance of proposed is appreciated
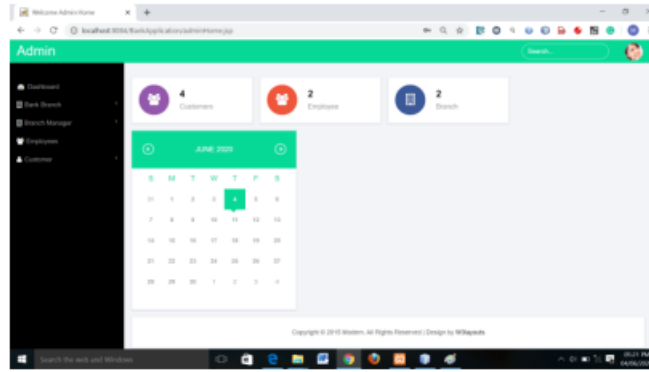
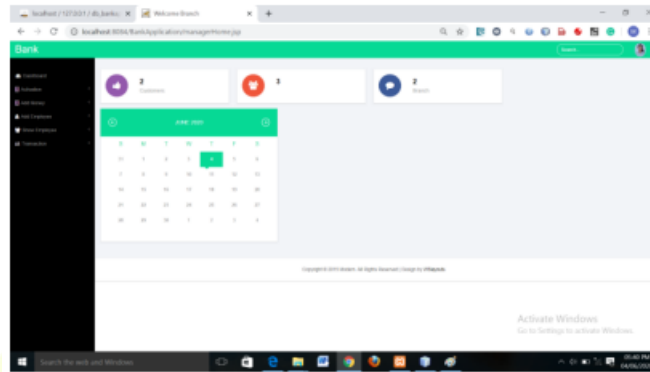## VII. SNEAKPEEKS OF IMPLEMENTATION

Fig. 6 Homepage of Admin
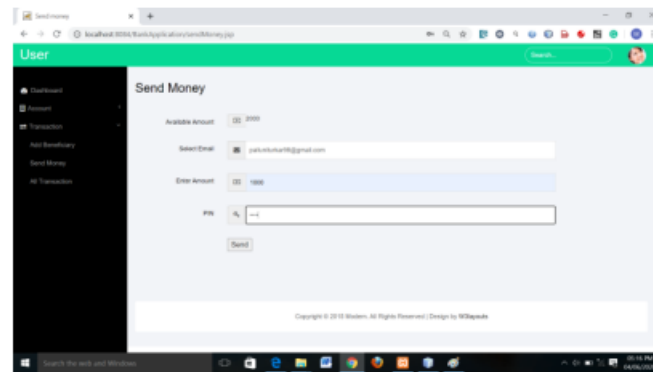

Fig. 7 Homepage of Bank Manager

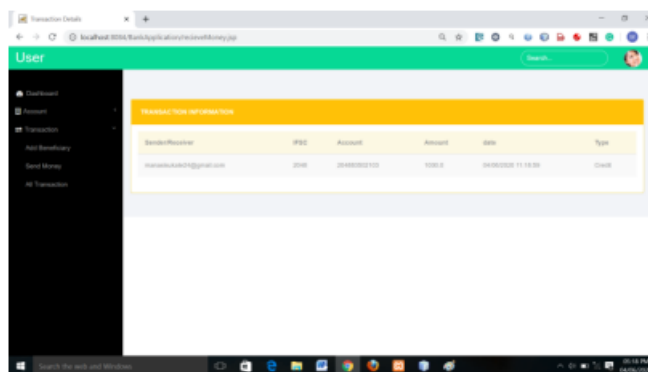Fig. 8 Sending Money to Selected User email-id
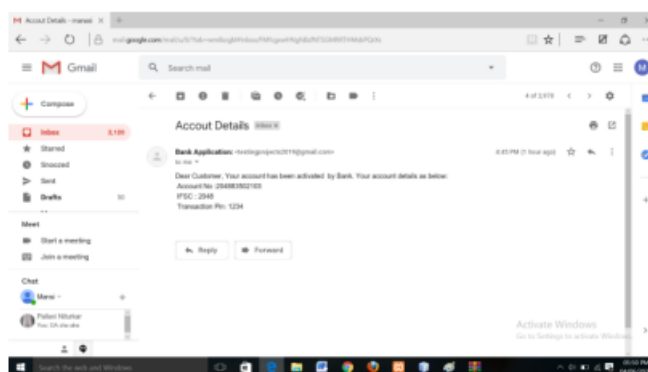
Fig. 9 Transaction Information of User

Fig. 10 Account Details of user for their activated account by bank

VII. CONCLUSION

Finally, the paper concludes that the proposed system defines a security of the system. Blockchain technology is a distributed system that works on total verification and validation of data without consideration of Miners or Tokens. Eliminating use of miners or tokens may lead to create transparent and load free network, which increase in survivability of transaction. By adopting blockchain in the distribution of databases on banking systems one can reduce attacks on the system. Blockchain without tokens plays a vital role in building a system which is more reliable for banking to perform transactions that have to be secure at a very high level.

REFERENCES

[1] Natalia A. Popova, Natalia G. Butakova " Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions",‖ 978-1-7281-0339-6/19/$31.00 ©2019 IEEE.

[2] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" 2017 IEEE 6th International Congress on Big Data

[3] Pasu Poonpakdee∗, Jarotwan Koiwanit∗, Chumpol Yuangyai∗ and Watchara Chatwiriya"Applying Epidemic Algorithm for Financial Service based on Blockchain Technology" 978-1-5386-4956- 5/18/$31.00 ©2018 IEEE

[4] Satoshi Nakamoto " ‖ Bitcoin: A Peer-to-Peer Electronic Cash System"

[5] Soto Méndez Jomar "Current State of Blockchain Technology A Literature Review" Tareq Ahram1, Arman Sargolzaei2, Saman Sargolzaei3,4, Jeff Daniels5, and Ben Amaba6 Blockchain Technology Innovations‖ 2017 IEEE Technology & Engineering Management Conference(TEMSCON).

[6] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE, 11(10), 1– 27.

[7] Siba, T. K., & Prakash, A. (2016). Block-Chain: An Evolving Technology. Global Journal of Enterprise Information System, 8(4), 29–35.

[8] Tareq Ahram1, Arman Sargolzaei2, Saman Sargolzaei3,4, Jeff Daniels5, and Ben Amaba6 ― Blockchain Technology Innovations‖ 2017 IEEE Technology & Engineering Management Conference (TEMSCON).

[9] Sachchidanand Singh, Nirmala Singh ‖ Blockchain: Future of Financial and Cyber Security‖ 463978-1-5090-5256-1/16/$31.00 c˘2016 IEEE ‖ 2nd International Conference on Contemperary Coumputing and informatics (IC3I)

[10] Supriya Thakur Aras, Vrushali Kulkarni,‖ Blockchain and Its Applications – A Detailed Survey ‖ , International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.

[11] Ahmed Ben Ayed,‖ A Conceptual Secure Block Chain-Based Electronic Voting System‖ ,2017 IEEE International Journal of network & Its Applications(IJNSA),03 May 2017.

[12] Huaiqing Wang, Kun Chen and Dongming Xu. 2016. A maturity model for blockchain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z.

[13] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkilic,‖ Towards Secure E-Voting Using Ethereum Blockchain‖ 2018 IEEE.

[14] Ibrar Ahmed, Shilpi, Mohammad Amjad "Blockchain Technology A Literature Survey." ‖ International Research Journal of Engineering Technology (IRJET) Volume:05 Issue:10 | Oct2018.

[15] Fran Casinoa, Thomas K. Dasaklisb, Constantinos Pat sakis "A systematic literature review of blockchain-based applications: Current status, classification and open issues"

[16] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi4, Sooyong Park, Kari Smolander "Where Is Current Research on Blockchain Technology?—A SystematicReview"

[17] Ye Guo , Chen Liang "Blockchain application and outlook in the banking industry"

[18] Gareth W. Peters,Efstathios Panayi "Understanding Modern Banking Ledgers through BlockchainTechnologies: Future of Transaction Processing and SmartContracts on the Internet of Money."

[19] Rohmat Taufiq,Meyliana,Achmad Nizar Hidayanto,Harjanto Prabowo "The Affecting Factors of Blockchain Technology Adoption of Payments Systems in Indonesia Banking Industry " 978-1-5386- 5821-5/18/$31.00©2018 IEEE. ‖2018 International Conference on Information Management and Technology (ICIMTech)

[20] AntonyVigil,PrakarshPathak,ShubhamUpadhyay,DeepankarSingh, Vai bhavGarg "Blockchain Over Transaction System??"978-1- 5386- 4765- 3/18/$31.00 ©2018 IEEE ‖ Proceedings of the International Conference on Communication and Electronics Systems (ICCES2018)

[21] Xin Wang,Xiaomin Xu,Lance Feagan,Sheng Huang,Limei Jiao,Wei Zhao"Inter-Bank Payment System on Enterprise Blockchain Platform"2159-6190/18/$31.00 ©2018 IEEEDOI 10.1109/CLOUD.2018.00085.2018 IEEE 11th International Conference on Cloud Computing.

[22] Lianxiang CUI,Kehong YUAN,Xiaoyu ZHAO,Larry Y. D. MOU"Construction of Elderly Mutual Aid Time Bank Based on Blockchain"2375-0324/19/$31.00 ©2019 IEEEDOI 10.1109/MDM.2019.000-1.‖ 2019 20th IEEE International Conference on Moblie Data Management (MDM).