OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

BANKING SYSTEM USING BLOCK CHAIN TECHNOLOGY

[1]Akhilesh Behera, [2]Disha Pujar, [3]Varsha Gaikwad, [4]Aniket Ramgir, [5]Prof. Vaishali Bhorde

[1, 2 ,3, 4]UG Student, Department Of Computer Engineering, JSPM ICOER Wagholi, Pune

[5]Professor, Department Of Computer Engineering, JSPM ICOER Wagholi, Pune

akhileshbehera74@gmail.com[1], dishapujar14@gmail.com[2], varsha.gaikwad1085@gmail.com[3], ramgiraniket@gmail.com[4]

Abstract: Increasing digital technology has revolutionized the life of people. The banking system in today's world is open to threats of fraud and cyber-attacks. Since todays banking system is built on centralized databases, it is easy for an attacker to penetrate in any such database which will easily compromise all the information and data of the customers of the bank. This vulnerability of today's banking system can be reduced by re-building the banking systems on top of block chain technology, which will remove the centralized database architecture and decentralize the data over the block chain, thus reducing the threat of database being hacked. Since the transactions over the block chain technology is verified by each and every nodes of the chain, it will make the transactions more and more secure thus making the overall banking system faster and secure.

Keywords*: - Cyber Security, Block Chain, Banking System.*

I INTRODUCTION

One of the essential issues that the banking segment is confronting today is the expansion in misrepresentation and digital assaults. Presently, the greater part of managing an account frameworks are based on a centralised database, which makes them more defenseless to digital assaults as all data is put away locally in one place. Additionally, numerous banking frameworks are obsolete and are, in this manner, more helpless against new types of digital assaults. By building new managing an account frameworks over block chain innovation, the possibility for extortion and information burglary can be decreased generously as the disseminated record innovation secures records; it stores, scrambles and checks each and every piece of information in an exchange. Accordingly, should any information rupture or false movement happen, it would be made promptly evident to all gatherings who have consent to get to the exchange information on the record.

II RELATED WORK

1. Satoshi Nakamo to Bitcoin: A Peer-to-Peer Electronic Cash System

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network time stamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2.Christopher D. Clack, Smart Contract Templates: foundations, design landscape and research directions.

In this position paper, we consider some foundational topics regarding smart contracts (such as terminology, automation, enforceability, and semantics) and define a smart contract as an agreement whose execution is both automatable and enforceable. We explore a simple semantic framework for smart contracts, covering both operational and non-operational aspects. We describe templates and agreements for legally-enforceable smart contracts, based on legal documents. Building upon the Ricardian Contracttriple, we identify operational parameters in the legal documents and use these to connect legal agreements to standardized code. We also explore the design landscape, including increasing sophistication of parameters, increasing use of common standardized code, and long-term academic research. We conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates.

3.EppMaaten, Towards remote e-voting: Estonian case

This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

4.Paul Gibson, A review of E-voting: the past, present and future

Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades.

5. Muhammad Ajmal Azad, M2M-REP: Reputation of Machines in the Internet of Things 2017.

The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam, malware, viruses etc, but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collaborative reputation system that calculates trustworthiness of machines in the IoT- based machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation system for the decentralized IoT environment, this paper present sanovelM2M-REP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way.

III PROPOSED SYSTEM

In the proposed system, the traditional architecture followed by banks which consists of a centralized database will be removed. The data will be largely distributed over the block chain which will make the banking systems decentralized. This will not only make the data ore secure but also will remove the power centralization. The transactions over the block chain will be in form of encrypted tokens which will be verified by each nodes on the block chain. To make any transaction valid, the nodes of the block chain will have to give the proof of the processing it has done in order to verify the transaction. That proof will be taken in terms of the amount of processing done. The above mentioned transaction system has two benefits. Firstly it will make the transactions faster by removing the intermediate processes employed in the normal transactions and secondly it will become nearly impossible for an individual to hack the system as it will require a huge amount of processing power which no one has.

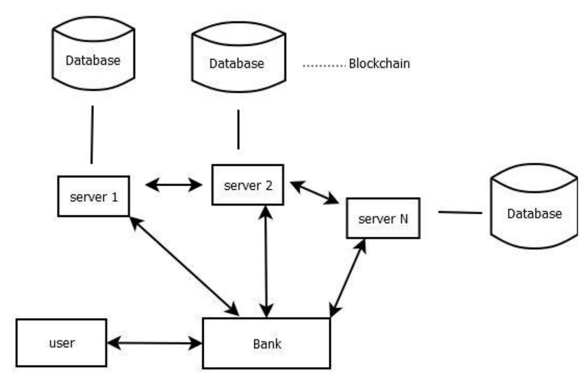

FIGURE 1: SYSTEM ARCHITECTURE

IV MATHEMATICAL MODEL

Let S be the whole System,

Set S = {I, P, O} Where,

Input (I) represented as: I = {I0, I1, I2, I3, I4}

I0 = User Registration Details

I1 = User Login

I2 = Transaction Id

I3 = User transaction amount

I4 = User transaction

Process (P) represented as: P = {P0, P1, P2, P3, P4}

P0 = Login by user-side

P1 = Approval of login

P2 = visual cryptography

P3 = block chain

P4 = user transaction process

Output (O) represented as: O = {O0, O1, O2, O3}

O0 = show user details

O1 = receiver id

O2 = user transaction successful

O3 = view balance

V PROPOSED SYSTEM ALGORITHM

Input: a set N of users in the network

Input: a blockchain called B, bn is the last block on the blockchain

Input: T, the deadline of transaction

1. While Current Time() < T
2. Foreach $n \in N$
3. numOfTransaction ← Dotransaction();
4. Foreach numOfTransaction ∈ Transaction
5. transactionmax ← compare(numOfTransaction);
6. m ← SelectMiner();
7. bn+1 ← GetTrans(α);
8. B’ → AddBlock(m, B, bb);
9. Foreach $n \in N$
10. Broadcast (n)

VI RESULT

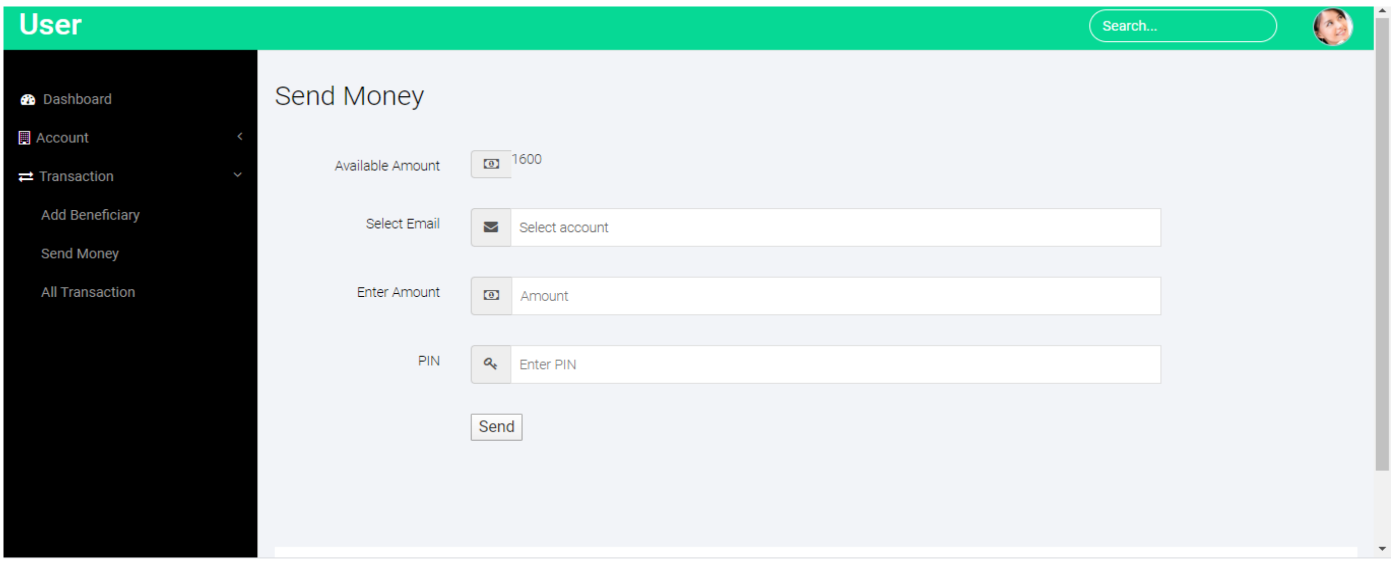

Fig 6.1: Send Money

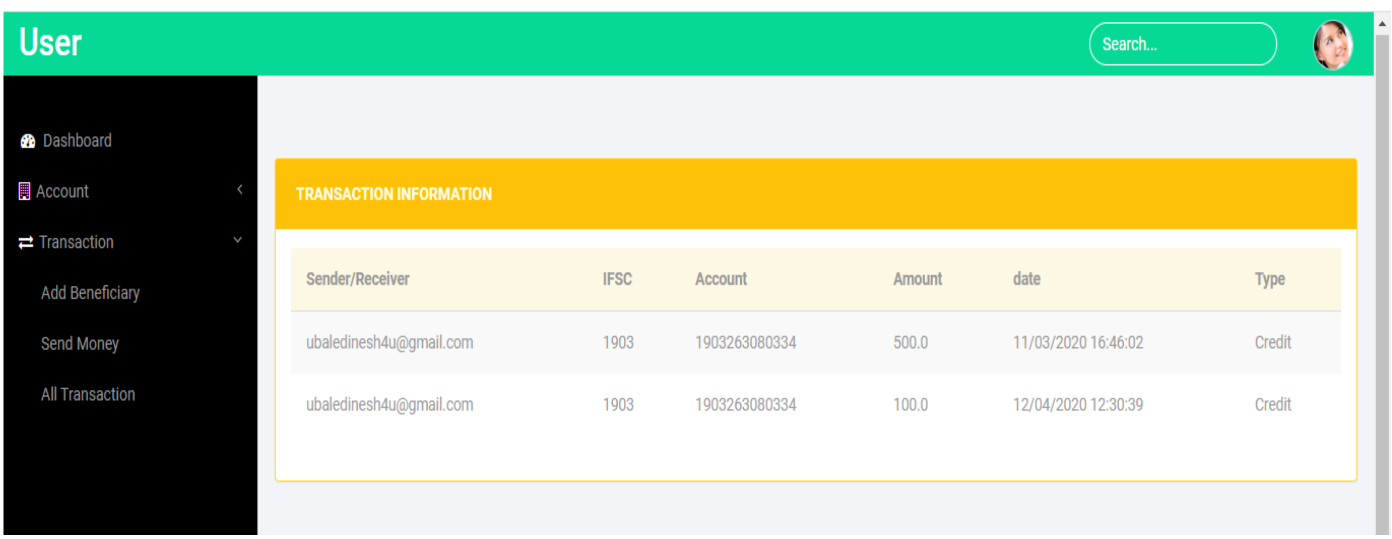

Fig 6.2: Transaction Information

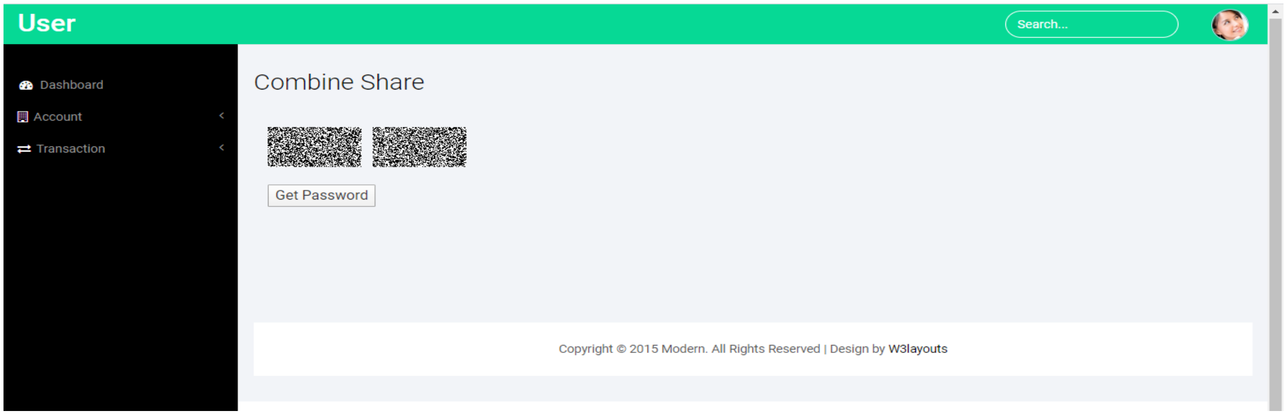

Fig 6.3: Combine Share

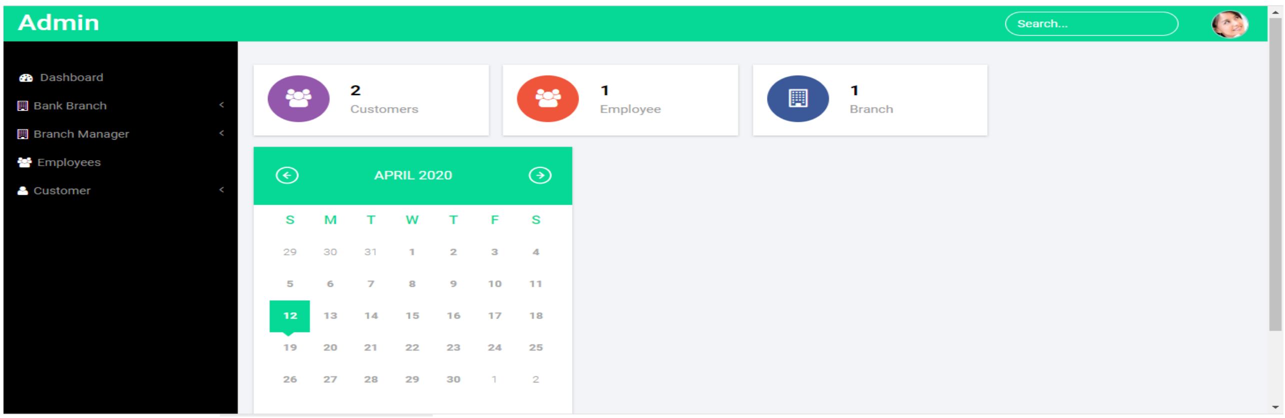

Fig 6.4: Admin Home Page

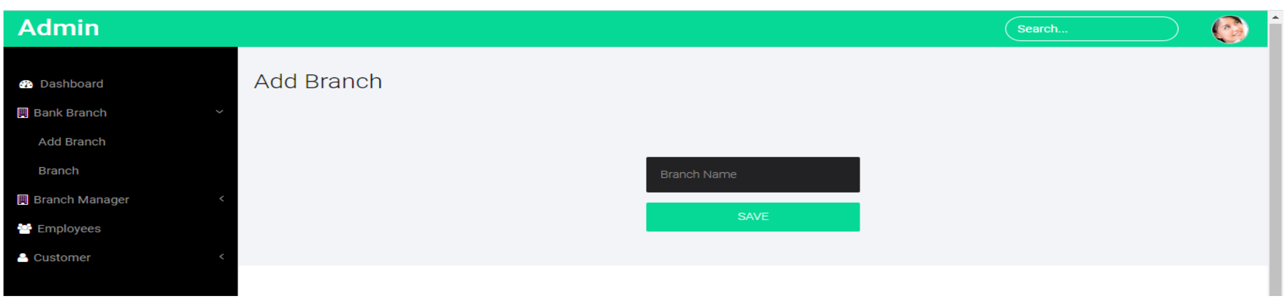

Fig 6.5: Add Branch

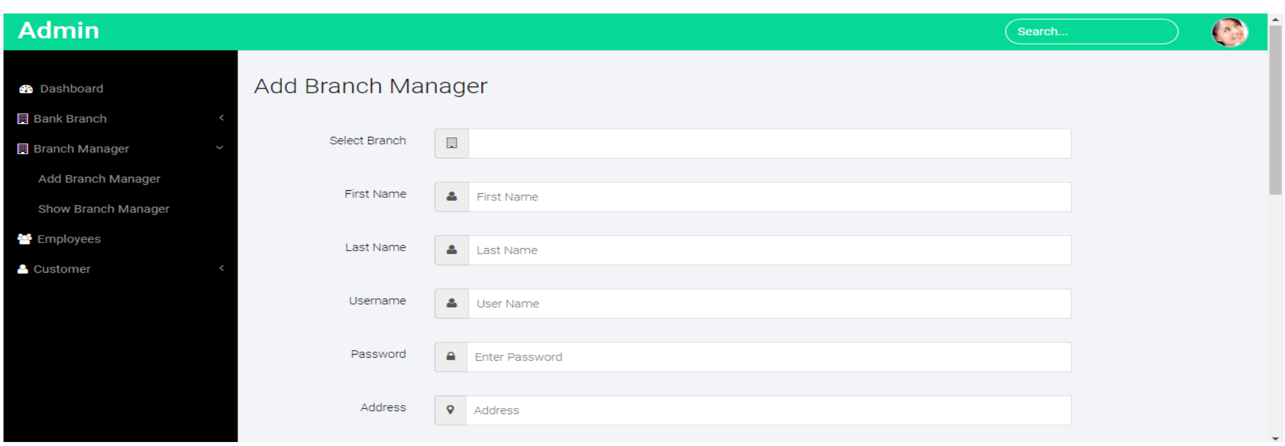

Fig 6.6: Add Branch Manager

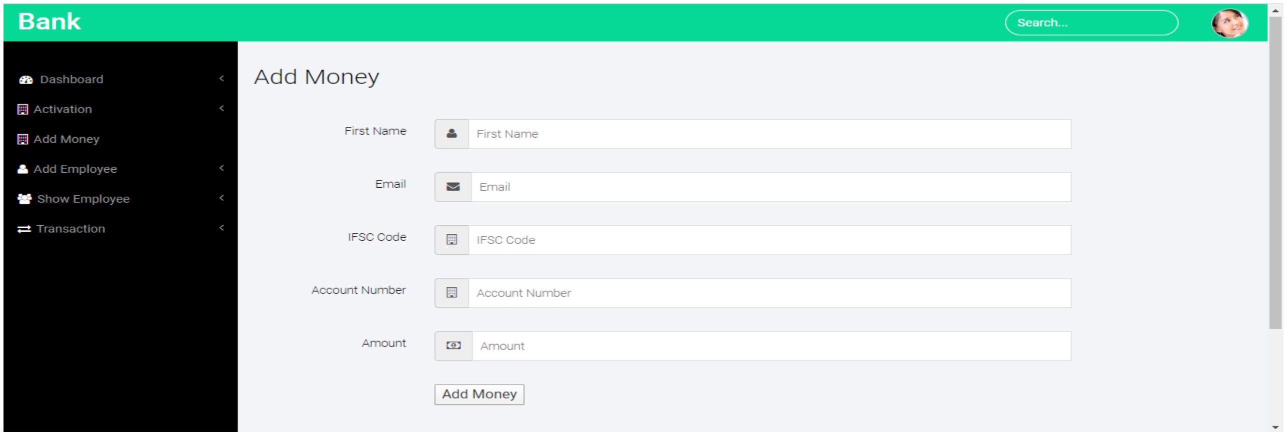

Fig 6.7: Add Money

VII APPLICATIONS

There are many applications that help users to monitor their running activities.

- Thissystemisalsousedforcorporatecompaniestoconducttheir electionsfor different posts such as the presidential election, manager election etc.
- Online social network
- Financial services
- Enterprise transformation.

VIII CONCLUSION AND FUTURE WORK

The proposed system designed to provide a secure data and a trustworthy banking system. Block chain itself has been used in the bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on banking systems one can reduce the cheating sources of database manipulation.

REFERENCES

1. Ahmed Ben Ayed, “A Conceptual Secure Block Chain-Based Electronic Voting System”,2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.
2. .Rifa Hanifatunnisa, Budi Rahardjo, “Blockchain Based E-Voting Recording System Design”,IEEE 2017.
3. Kejiao Li, Hui Li,Hanxu Hou, Kedan Li,Yongle Chen,” Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain”, 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.
4. Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkilic,” Towards Secure E-Voting Using Ethereum Blockchain”,2018 IEEE.
5. 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.
6. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram,Konstantinos Markantonakis,” E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy”,IEEE 2018,03 July 2018.
7. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan,” Secure Digital Voting System based on Blockchain Technology”,IEEE 2017.
8. 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
9. Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online]https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
10. Prakash K. Ukhalkar, Dr. Rajesh N. Phursule , Dr Devendra P Gadekar, Dr Nilesh P Sable. (2020). Business Intelligence and Analytics: Challenges and Opportunities. International Journal of Advanced Science and Technology, 29(12s), 2669-2676
11. Zyskind et. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Securityand Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http://dx.doi.org/10.1109/SPW.2015Jianliang Meng, Junwei Zhang,Haoquan Zhao, “Overview of the Speech Recognition Technology”, 2012 Fourth International Conference on Computational and Information Sciences.