Digitalization and Decentralized Blockchain Technology

DOMKONDAWAR VAISHNAVI , H.No: 21S41D5824,Mtech (Cse), Department Of Computer Science, Vaageswari College Of Engineering Thimmapur,Karimnagar, Telangana, India, Email-Id: vaishnavi.pasnuri5@gmail.com.

Dr.E.Srikanth Reddy , Associate Professor, Department Of Computer Science, Vaageswari College Of Engineering Thimmapur,Karimnagar, Telangana, India,Email-Id: srikanth574@gmail.com.

ABSTRACT

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 timestamps 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.

Index Terms:- Digital signatures, peer-to-peer network, third party, timestamps.

I.INTRODUCTION

1.1 MOTIVATION

The Internet of Things (IoT) represents one of the most significant disruptive technologies of this century. It is a natural evolution of the Internet (of computers) to embedded and cyber physical systems, “things” that, while not obviously computers themselves, nevertheless have computers inside them.With a network of cheap sensors and interconnected things, information collection on our world and environment can be achieved at a much higher granularity. Indeed, such detailed knowledge will improve efficiencies and deliver advanced services in a wide range of application domains including pervasive healthcare and smart city services.

However, the increasingly invisible, dense and pervasive collection, processing and dissemination of data in the midst of people’s private lives gives rise to serious security and privacy concerns.

1.2 PROBLEM DEFINITION

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments.

While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes.

Now-a-days bank account details can be hacked by attacker. Due to sharing of data there will be data security issues raised for user as this data can be misuse by agency peoples or attackers may steal this data.

1.3 OBJECTIVE OF PROJECT

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes.

II.LITERATURE SURVEY

- F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson explains about building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain-based application, which improves the security and decreases the cost of hosting a nationwide election.

- Y. Chang, K. Lin and C. Shen developed a blockchain-based E-marketplace. A decentralized E-marketplace platform utilizing the blockchain technology is implemented. We use the self-enforcement of smart contracts to secure the deposit and process the payment. Each transaction is verified through the blockchain and is recorded to the decentralized ledger. This enables trustless transactions since the smart contract is self-executed. The smart contract is able to perform credible transactions without trusted third parties, and the transactions on the blockchain are trackable and irreversible. Therefore, both the buyer and the seller cannot breach the contract. All processes are recorded on the blockchain including the product launch, purchase, delivery, and payment. It is trackable and could be submitted to courts as electronic evidence to solve the transaction disputes.

- Guo, Y., Liang, C. proposed blockchain technology is a core, underlying technology with

promising application prospects in the banking industry. On one hand, the banking industry in China is facing the impact of interest rate liberalization and profit decline caused by the narrowing interest-rate spread. On the other hand, it is also affected by economic transformation, Internet development, and financial innovations. Hence, the banking industry requires urgent transformation and is seeking new growth avenues. As such, blockchains could revolutionize the underlying technology of the payment clearing and credit information systems in banks, thus upgrading and transforming them. Blockchain applications also promote the formation of "multi-center, weakly intermediated" scenarios, which will enhance the efficiency of the banking industry. However, despite the permissionless and self-governing nature of blockchains, the regulation and actual implementation of a decentralized system are problems that remain to be resolved. Therefore, we propose the urgent establishment of a "regulatory sandbox" and the development of industry standards.

- Ye Guo & Chen Liang described about a new disruptive force of digital technology is changing the business models and increasingly becoming a crucial factor around the world. Blockchain technology is generating significant interest across a wide range of industries in India. As the field of applications for Blockchain grows, industry leaders are customizing and tailoring the technology to fit multiple use cases. The Blockchain technology is responsible for developing a next step in the decentralized approach for creating applications. This paper aims at explaining the architecture of Blockchain Technology as well as how it works. Besides various features of the Blockchain, the benefits derived from it are also discussed. The use cases and Blockchain fit assessment has also been performed for few banking transactions. In the last section we also have a look at the security aspects of the Blockchain.

- T. Wu and X. Liang, implemented a blockchain techonolgy.Blockchain is considered as the important technological innovation behind Bitcoin system. It facilitates the transaction payment process by creating a decentralized, general ledger to improve regulatory capacity and remove unnecessary intermediaries. At present, the blockchain technology has been employed in the financial industry for a wide range of experimental application and exploration. In this paper, we firstly analyze the principle architecture and the technical characteristics of blockchain. Then its current research achievements and application scenarios are introduced. Finally, the application of blockchain in China Foreign Exchange Trade System is designed and explored. Combining with the credit matching trading system X-Swap, an inter-bank application based on the blockchain technology is implemented.

III. EXISTING SYSTEM

Now a days the transactions are being processed using Cheques, Net Banking and payment Wallets. Payment wallet transactions involves third party of government.

These transactions allows centralized platform means power and rights are not to be equally distributed among all the participants in a system.

Performing transactions through Cheques, Net banking and payment Wallet Entail the receiver effectively authorizing the seller to "Pull" a payment from their account, passing through several financial intermediates in the process.

In this type 1of transaction, it is necessary to provide personal identification information such as your name and address and this type of transactions are stored physically in a wallet.

DISADVANTAGES OF EXISTING SYSTEM:

- ❖ These transactions offer less security.
- ❖ There is a need of documentation.
- ❖ Due to the involvement of third party there is a problem of "Double spending".
- ❖ It is not cost effective.

IV PROPOSED SYSTEM:

In this project an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.

In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes

ADVANTAGES OF PROPOSED SYSTEM:

- Block chain transactions offers more security.
- There is no need of documentation.
- It is cost effective.
- Unlimited transactions in a limited span of time.
- No need of involvement of third party.

V. SYSTEM DESIGN

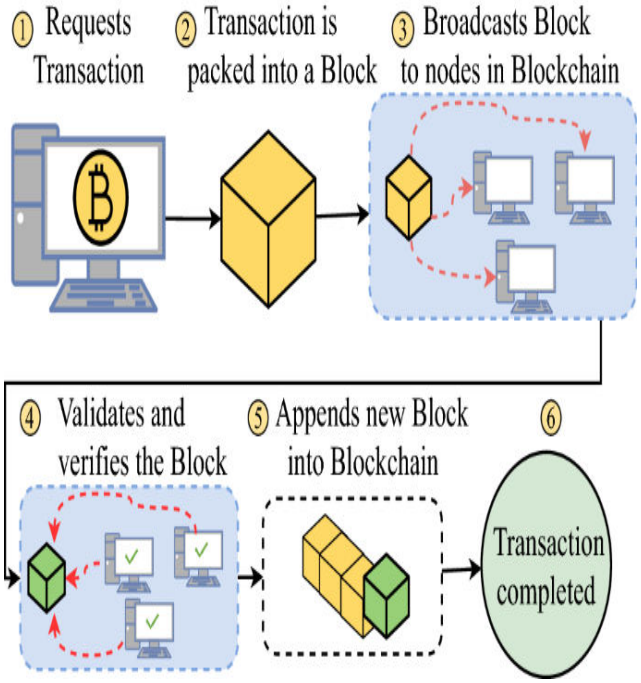


Fig1: Architecture of system.

VI.MODULE DESCRIPTION:

. This project consist of 4 modules

Peer Module: Peer Module using this module we will add peer details to application

Block Module: Block Module using this module we can add peer to block

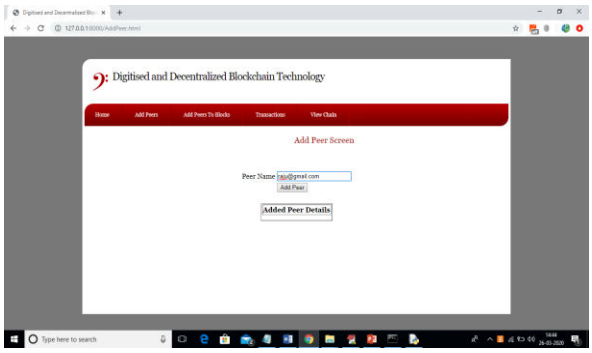
Transaction Module: one peer can transfer coin to other peer

Chain module: if transaction completes and hash code validated then transaction will be added to chain module.

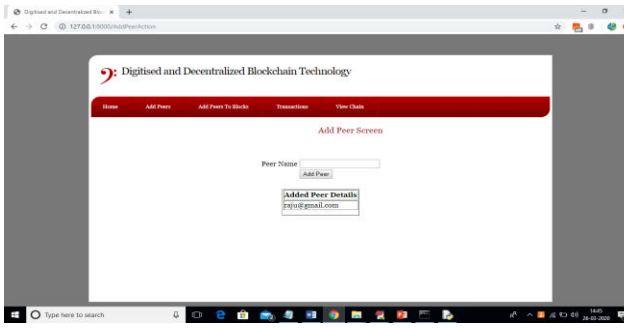
VII. RESULT:

First screen

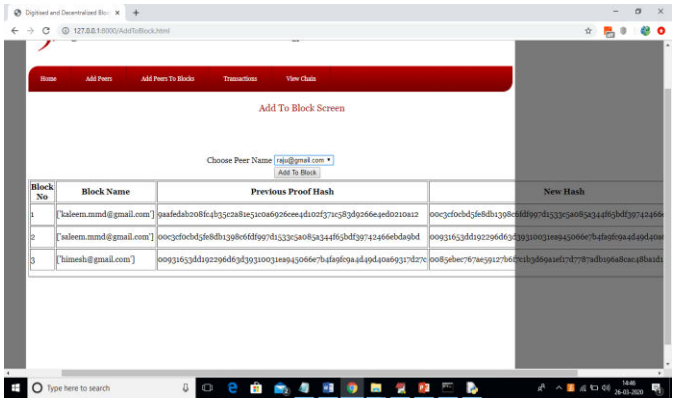
In above screen click on 'Add Peers' link to add new peer details



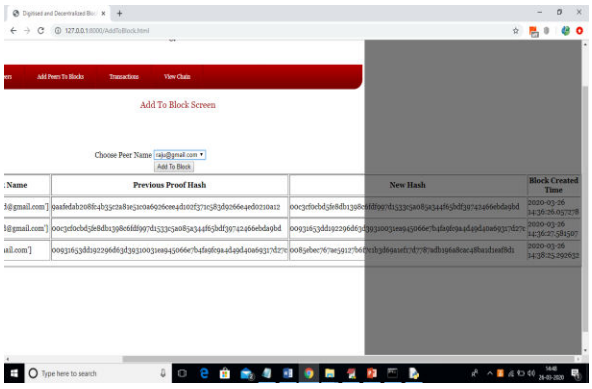
In above screen I am adding new peer as 'raju@gmail.com' and the entry will be available here till it added to block and after adding to block entry will be deleted from peer screen. Now click on 'Add Peer' button to get below screen



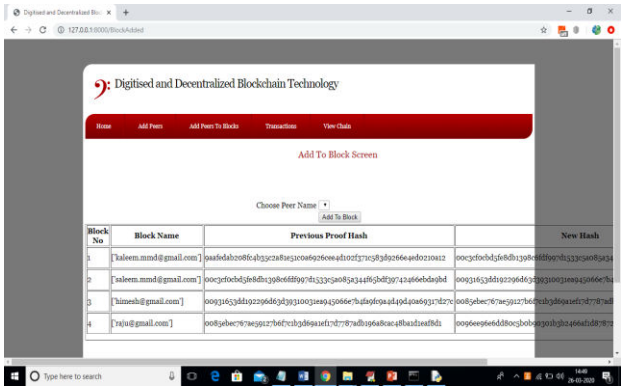
In above screen we can see newly added peer details showing in above screen table. Now click on 'Add Peers To Blocks' link to add this peer to block chain.



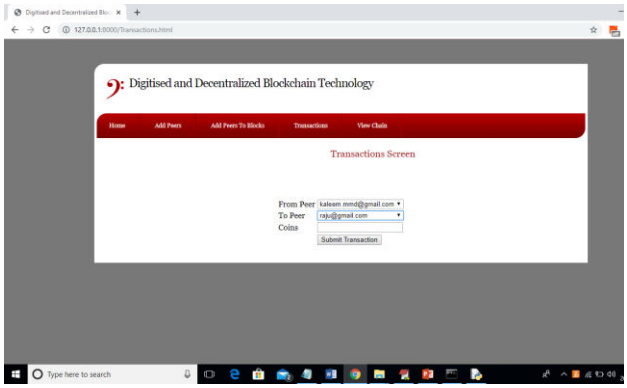
In above screen all added peers to block chain will be displayed here with their old and new hash code as proof of work. We can see in above screen New Hash of first row is match with previous hash of second row and goes on till transaction executed successfully with hash validation. Scroll above screen to view created date also.



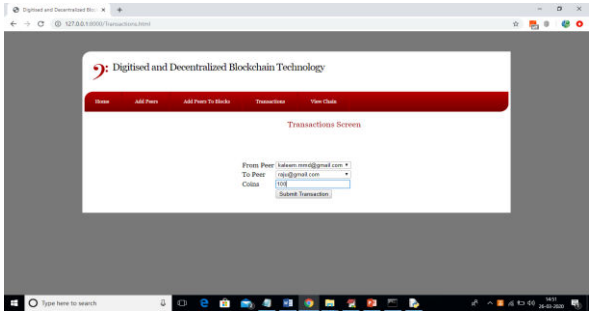
Now we can select new peer name from drop down box and click on 'Add to Block' button to add new peer to new block



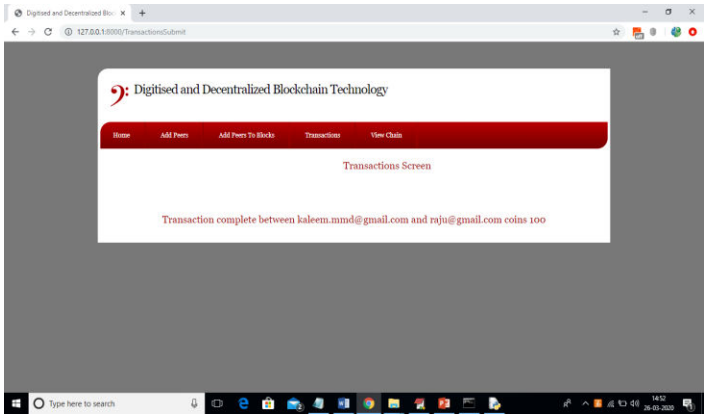
In above screen new peer also added to block and once it added then that peer will be removed from drop down box. Now click on 'Transactions' link to perform transaction between block chain users.



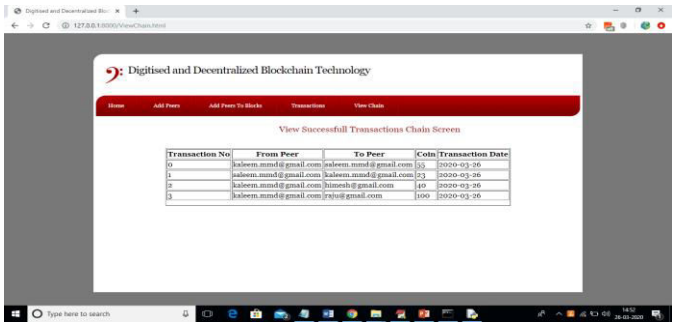
In above screen from peer and choose desire to peer from drop down box and then enter amount and click on 'Submit Transaction' button to transfer fund



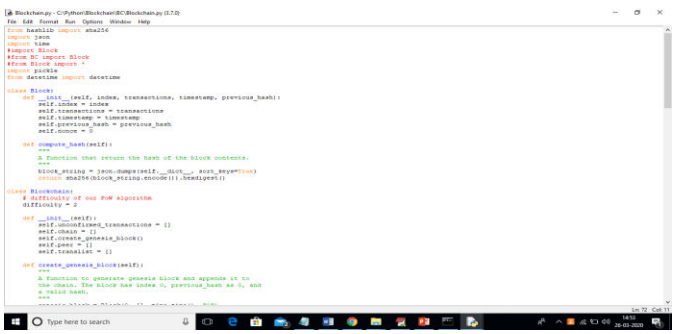
In above screen I am sending 100 coins and after transaction complete will get below screen

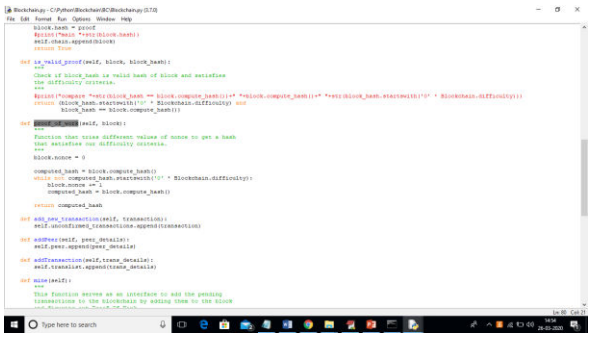


Now click on 'View Chain' link to view all transactions details



In above screen from block chain we can retrieve all transaction details. Below block chain code use to validate transactions





In above screen is_valid_proof and proof_of_work functions validate all transactions with old and new hash c

VIII. CONCLUSION

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending.

To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.The network is robust in its unstructured simplicity. Nodes work all at once with little coordination.

They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis.

Thus, to overcome the mentioned disadvantages of the traditional centralized banking system, blockchain technology can be used.

IX. FUTURE ENHANCEMENT

Blockchain provides a secure and intrusion free environment for all the transactions occurring between the nodes. This helps in reducing the transaction fee and time, which is significant in traditional banking systems. Also, as this technology is under development, there can be multiple advancement in the future.

X. REFERENCES

[1] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[2] Y. Chang, K. Lin and C. Shen, "Blockchain Technology for eMarketplace," 2019 IEEE International Conference on Pervasive Computing and Communications

Workshops (PerCom Workshops), Kyoto, Japan, 2019, pp. 429-430, doi: 10.1109/PERCOMW.2019.8730733.

[3] I. Ahmed, Shilpi, and M. Amjad, “Blockchain Technology A Literature Survey,” Oct 2018 Volume: 05 Issue: 10 International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056.

[4] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[5] S. Aich, S. Chakraborty, M. Sain, H. Lee and H. Kim, "A Review on Benefits of IoT Integrated Blockchain based Supply Chain Management Implementations across Different Sectors with Case Study," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South), 2019, pp. 138-141, doi: 10.23919/ICACT.2019.8701910.

[6] Guo, Y., Liang, C. “Blockchain application and outlook in the banking industry,” Financ Innov 2, 24 (2016). https://doi.org/10.1186/s40854- 016-0034-9.

[7] T. Wu and X. Liang, "Exploration and practice of inter-bank application based on blockchain," 2017 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, 2017, pp. 219-224, doi: 10.1109/ICCSE.2017.8085492.

[8] S. Ma et al., "Nudging Data Privacy Management of Open Banking Based on Blockchain," 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), Yichang, China, 2018, pp. 72-79, doi: 10.1109/I-SPAN.2018.00021.

[9] N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 2019, pp. 1764-1768, doi: 10.1109/EIConRus.2019.8657279.

[10] ” Application of Blockchain Technology in Banking & Finance” by TealShah, Shailak Jani.