e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

BLOCKCHAIN BASED DECENTRALIZED TRANSACTION SETTLEMENT SYSTEM

Pratiksha Kale[*1], Sanika Lawande[*2], Komal Malekar[*3], Harshada Mache[*4], Harshit Pawar[*5]

[*1,2,3,4,5]Student, Department Of Computer Engineering, NBNSTIC, Ambegaon BK, Pune, India.

DOI : https://www.doi.org/10.56726/IRJMETS63594

ABSTRACT

Potential threats from viruses, malware, adware and hackers are constant. In the last couple of years, many massive global companies were hacked and compromised. In some cases, this has led to the leakage of confidential and private information, including bank details, addresses, and transactions etc., with a strong security system in place where these things can be stopped before they are close to the data private of the company. This is not only important in terms of confidentiality but also to avoid the expensive fines that are imposed on companies that do not successfully protect customer information. The project is a verification system that verifies the user to access the system only when they have the correct input credentials. The project involves user certificates i.e. Modules. There are many types of security credentials are available. So, in this proposed system we implement custom blockchain for baking security and user authentication purpose. By using this level of authentications there is less chance for hacking and loss of confidential data. Also, in today's scenario safer bank transactions is required as the technology is improved in the field of security. They have also entered the fields like industry medicine telecommunication and home automation etc. Blockchain is basically a distributed ledger. It can store facts like who owns a particular piece of land or say a bond. The technology can be used to keep an immutable record of ownership and enable transaction of the asset amongst distrusting parties.

Keywords: Custom Blockchain, Distributed Ledger, Authentications, Confidentiality, Transactions, Security System, Verification System, Credentials, Baking Security.

I. INTRODUCTION

A blockchain system can be seen as an incorruptible cryptographic database where important and confidential user information is stored. This system is maintained by a network of computers and can be accessed by anyone running the software. Blockchain operates as a pseudo-anonymous system, meaning that while users' identities are not directly revealed, there are still privacy concerns because all transactions are visible to the public. However, it is tamper-proof in terms of data integrity. In order to manage heterogeneous user confidential records across multiple MNC establishments and devices, access control had to be carefully designed. It's important to note that blockchain itself is not intended to be a large-scale storage system. In the context of a secure banking framework, a decentralized storage solution would greatly enhance the limitations of blockchain in this regard. The blockchain network, being a decentralized system, is more resilient compared to centralized systems as there is no single point of attack or failure. However, since all Bitcoin transactions are public and accessible to everyone, there are already existing analytics tools that can identify members within thenetwork based on transaction data.

II. LITERATURE REVIEW

Related Work

1. A Blockchain Based Decentralized Transaction Settlement System in Banking Sector Authors: Sincy Joseph, Smitha Karunan

Published in: 2021

Blockchain, the underlying technology behind Bitcoin, is an emerging technology in industry. Blockchain has the power to reform the existing business processes more democratic, transparent, secure, and efficient. Banking industries are the first movers that capitalize the disruptive potential of this technology.This system completely eradicates the failure of system/data loss/modification of data from the central server. In general, the project aimed to provide a more robust infrastructure for the existing banking network using the

distributed ledger technology.

2. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends Authors'. Zheng, S Xie, H. Wang

Published in: 2017

Blockchain serves as an immutable ledger which allows transactions to take place in a decentralized manner. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome.

This paper presents a comprehensive overview on blockchain technology. In this paper, we present a comprehensive overview on blockchain. We then discuss the typical consensus algorithms used in blockchain. We analyzed and compared these protocols in different respects. Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed.

3. Security Applications and Challenges in Blockchain

Authors: Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, and Wenlin HanPublished in: 2019

Blockchain technology is a highly popular yet highly misunderstood concept that is used today and in future applications. To enhance security and privacy, many applications adopt Blockchain. However, there are intrinsic drawbacks and emerging challenges.

In this paper, we study popular security applications in Blockchain, present their major problems, as well as other challenges in Blockchain which allows future research to be conducted more efficiently.

In this paper, we introduced popular security applications, e.g. Pretty Good Privacy and ProvChain, in Blockchain. We studied the major problems of the applications and discussed how to solve these problems. We summarized other emerging challenges in Blockchain, such as throughput, latency, integration, regulatory, etc. This paper will provide guidance for efficient research in the near future.

4. Blockchain-enabled decentralized time banking for a new Social Value System (2019)**Authors: X. Lin, R.Xu, Y.Chen and J.K.Lum*

Time Banking is a generalized exchange economy not based on money, but values everyone's contribution on the same scale, the time expended. In this paper a BLockchain ENabled Decentralized Time Banking System (BlendTBS) is proposed to build a trustful, dynamic and respectful community. People in this community are encouraged to be engaged in mutual serving relationships. In this position paper, we proposed to develop and apply BlendTBS, a blockchain-enabled decentralized time banking system, to explore a better understanding of a social value system in the context of exchanging economies. Consequently, the BlendTBS system will encourage the residents in the communities to behave nice and make the entire community more trustworthy and safer.

5. Blockchain and smart contract for digital certificate (2018)**Authors: J. Cheng, N. Lee, C. Chi and Y. Chen*

Smart contracts are the main feature of Ethereum, a blockchain platform founded in 2015. A smart contract is "a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain".

In this paper using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

6. Performance Analysis of Consensus Algorithms in Private Blockchain (2018)**Authors: Y.Hao, Y.Li, X. Dong, L. Fang and P.Chen*

This paper proposes a method to evaluate the performance of consensus algorithms in private blockchain platforms of Ethereum and Hyperledger Fabric. Through quantitative analysis of latency and throughput, we obtain the performance evaluation results of consensus algorithms with different numbers of transactions. The results show that the consensus mechanism induces a performance bottleneck.

The results show that Hyperledger's PBFT algorithm outperforms Ethereum's PoW algorithm in terms of average throughput and average delay. In addition, both in Ethereum and Hyperledger Fabric, the existence of

consensus mechanisms causes performance bottlenecks in both platforms, due to the nature of exchanging security for performance. Another study result indicates that the performance difference of the two consensus algorithms increases as the number of transactions increases.

7. Decentralized secure money transfer using blockchainAuthors: Suganya, T.Vignesh, A. Kumar*

Published in 2018.

The purpose of this paper is to create a list of blocks each block to connect the previous block to some previous key to connect to find the next key to-do the transaction.

This project concludes that money transfer will be securely stored in the block chain. In this type of block chain, all users will know every transaction. It must be decentralized transfer No third party included in this transaction.

The beautiful web page also shows the transaction of money.

By using the block chain technology method, the participating parties can be confident that transferring amounts at both ends of the agreement will be upheld and the transfer values agreed upon are attainable.

8. Decentralizing Privacy: Using Blockchain to Protect Personal Data** Authors: G. Zyskind, O. Nathan and A in the Pentland*

Published in 2015.

The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data.

Bitcoin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger.

In this paper, we describe a decentralized personal data management system that ensures users own and control their data. We implement a protocol that turns a blockchain into an automated access- control manager that does not require trust in a third party.

9. Blockchain Over Transaction System**

Authors: A. Vigil, P. Pathak, S. Upadhyay, D. Singh and V. Garg*

This paper intends to draw a representation of blockchain transactions over a peer to peer network, representing the change in the newly developed network and solution over obsolete banking technology.

This paper will draw clarity over the transaction by blockchain system and methods.

The paper concludes the functioning of transaction system over the obsolete which has been developed from over the years by a system, which has been developed and transformed by the given the fundamentals of blockchain, which was formed in the earlier of the time but can be used as an undivided tool for generating a corruption-free environment also it saves major problems of centralization of the network and involving consensus of the total derived system.

10. InterBank Payment System on Enterprise Blockchain Platform** Authors: X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao and W. Zhao*

The real-time gross settlement (RTGS) system is the current infrastructure for inter-bank payment and settlement. All payments.

III. MOTIVATION

Potential threats from viruses, malware, adware and hackers are constant. In the last couple of years, many massive global companies were hacked and compromised. In some cases, this has led to the leakage of confidential and private information, including bank details, addresses, and transactions etc., with a strong security system in place where these things can be stopped before they are close to the data private of the company. This is not only important in terms of confidentiality, but also to avoid the expensive fines that are imposed on companies that do not successfully protect customer information. The project is a verification system that verifies the user to access the system only whenthey have the correct input credentials.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

IV. OBJECTIVE

- To implement a decentralized application and designed an online banking security system based on Custom blockchain.
- To address the feature of this technology which is it is incorruptible, encrypted, and trackable and permits data synchronization.
- To improve the efficiency of operations at each stage. Improving transaction speed and latency than traditional banking.
- To reduce the server downtime or to make it effectively zero with the distributed blockchain.
- Proposed system addresses the system, saves on time, cuts management costs, prevents authentication forgery, and provides accurate and reliable information on banking systems.
- Proposed system provides thread protection over various Viruses and Malwares with theblockchain.

V. PROBLEM STATEMENT

The Indian banking system is the most complicated bank payment system in this world. It is based on a real time gross settlement system Which follows a central server mechanism where all the personal information of account holders, bank balance, and all necessary information related to banks are stored. All branches of a bank are connected to a central server from which every branch retrieves personal information, bank balance and history of a customer from the server itself. Failure or modification in the central server causes all banks to fall down which results in great loss and causes a large amount of processing time and cost. Considering all the issues of the current centralized banking system, the proposed blockchain based decentralized mechanism will provide a banking system in a cost efficient and a secure way.

VI. PROPOSED APPROACH /METHODOLOGY

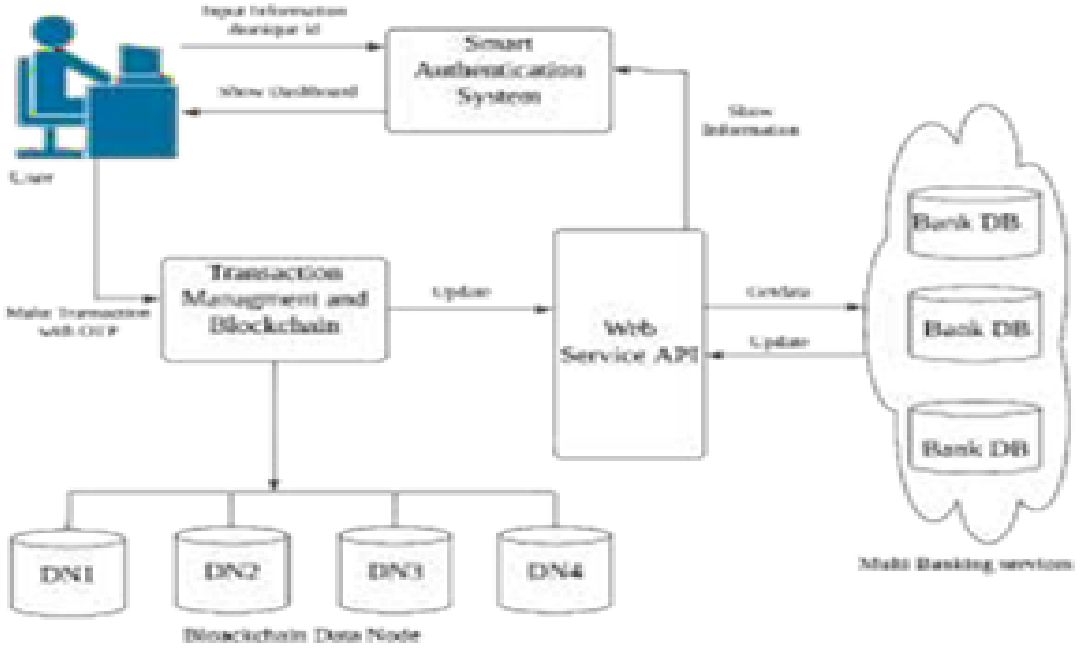


Fig 1. System Architecture

Hardware Requirement

- System : Intel I3 8th Gen 2.9 Ghz
- Hard Disk : 256 GB (Min)
- Monitor : 15 VGA Color
- Mouse : Logitech.
- Ram : 4 GB (Min)

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Software Requirement

- Operating System : Windows 8 onwards.
- Java Version : JDK 1.8 & Above.
- Coding Language : Java/J2EE
- Back-end(DB) : MYSQL 5.5.
- Web Server : Apache Tomcat/XAMPP.
- IDE : Eclipse Oxygen

VII. PROJECT SCHEDULE

Project task set:

Major Tasks in the Project stages are:

Task 1: Correctness

Task 2: Availability

Task 3: Integrity

Task network:

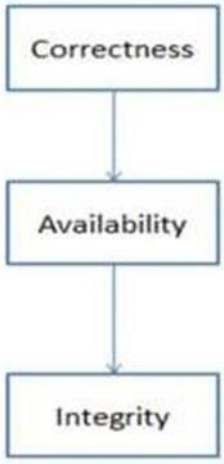


Figure 2: TaskNetwork

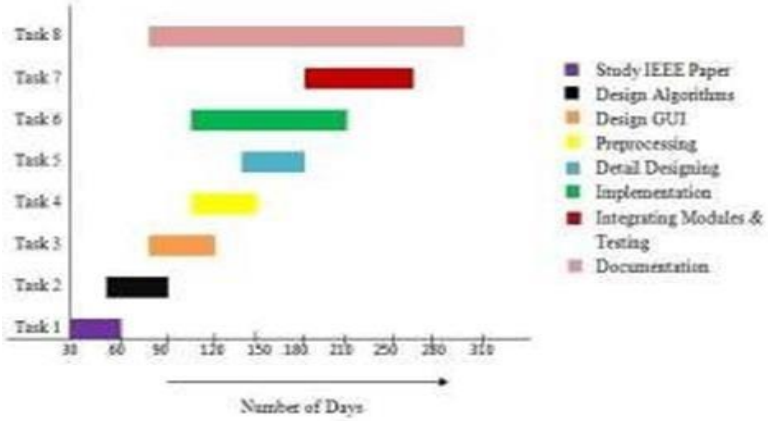


Fig 3. Gantt chart of project

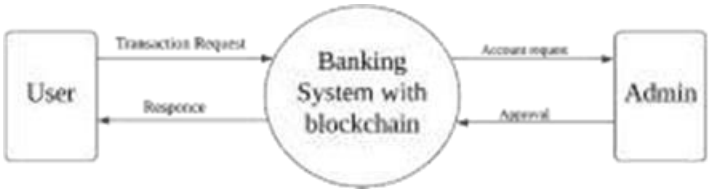
VIII. DATA FLOW DIAGRAMS

- The DFD is also called a bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that

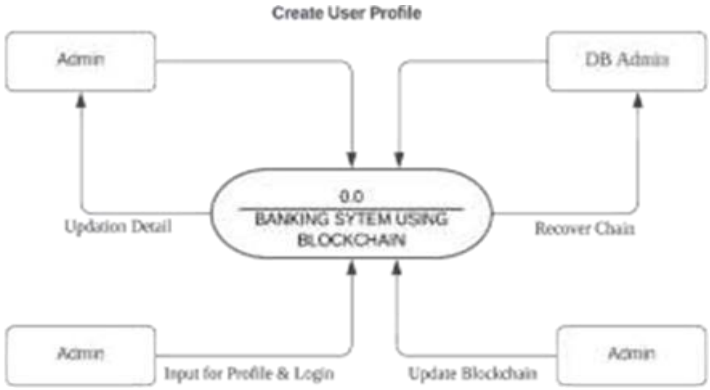
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

interacts with the system and the information flows in the system.

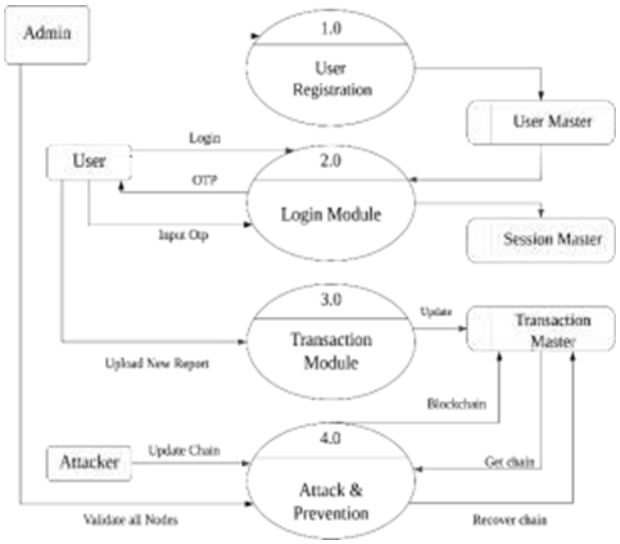
- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



Level 0 Data Flow Diagram



Level 1 Data Flow Diagram



Level 2 Data Flow Diagram

IX. OVERVIEW OF PROJECT MODULES

1. User Registration and Authentication

First users apply for a bank system on a web portal with uploading all details/documents.User input unique user identification using security questions and to enter into the system using secure authentication with OTP.

2. Third Party Verification

Web portal is authenticating trusted third parties which validate all user input details from user etc.Once successful verification has been done from the bank system it will store data into the blockchain and at the same time it generates the unique id returned to the user.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

3. User Identification

User input as unique user identification number.

4. Dashboard Access

Once the system validates the authenticating the current request it will show the dashboard where all the user's account information.

5. Account Login and Verification

Users can select a specific account and login with their own credentials and system send the OTP and two step verification.

6. Transaction Access

Once OTP is validated by the system it will show a home page where the user can do any transaction like check balance, withdraw etc.

7. Blockchain Storage

When any transaction has completed, the system stores entire information into the blockchain.

8. Blockchain Algorithms Execution

During the storage the transaction information into the blockchain system executes various algorithms like SHA-256 for hash generation, Mining for generating valid hash, smart contract for system policy and consensus for validate current blockchain on all Peer to Peer nodes.

X. PERFORMANCE EVALUATION

The time difference between the completion of a transaction (tx2) and the deployment time (tx1) is measured in seconds. As the number of transactions increases, the execution time also increases. In this context, a transaction refers to the various functions utilized in the smart contract. When a single user interacts with the system functions, such as depositing money, transferring money, accessing money lending services, and obtaining loan details, the execution times for these functions are as follows:18.291 seconds for the deposit money function,1 minute 48.02 seconds for the transfer money function,50.01 seconds for the money lending function,20.02 seconds for the loan details function However, when multiple users simultaneously use the system, the execution time will further increase.

Throughput: Throughput refers to the amount of data transferred within a given time unit and is typically measured in kb/sec. In Figure 6, the system's throughput is depicted. JMeter is employed to simulate user counts ranging from 100 to 500. The experiment reveals that as the number of user requests increases, the system's throughput also increases.

XI. ALGORITHM DETAILS

11.1 Protocol for Peer Verification

Input: User get IP address, User Transaction TID,

Output: Enable IP address or current query if any connection is valid

1. User generate the any transaction DDL, DML or DCL query
2. Get current IP address
3. For each (read IP into IP address)
4. If (connection(IP) equals(true)) Flag true
5. Else-Flag false
6. End for
7. Step if (Flag == true) Peer to Peer Verification valid
8. Else Peer to Peer Verification Invalid
9. End if

11.2 Hash Generation:

Input: Genesis block, Previous hash, data d, Output: Generated hash H according to given data

1. Input data as d
2. Apply SHA 256 from SHA family

3. CurrentHash= SHA256(d)
4. Return CurrentHash

11.3 Mining Algorithm for valid hash creation:

Input: Hash Validation Policy P[], Current Hash Values hash ValOutput: Valid hash

1. System generate the hash Value for ith transaction using Algorithm 1
2. if (hash Val.valid with P[]) Valid hash Flag =1
3. Else Flag=0 Mine again randomly
4. Return valid hash when flag=1

XII. CONCLUSION

This proposed system suggests or summaries a secure and efficient way to store data on the Distributed cloud. Blockchain-based cloud storage with data encryption gives data security in a decentralized zed structure. The proposed framework for the security model is suitable for measures initially used in banking transactions including blockchain technology. The algorithms used to implement the system model are efficient and require less time and give high security for the data which is being stored on the cloud.

XIII. REFERENCE

[1] Sincy Joseph, Smitha Karunan in A Blockchain Based Decentralized Transaction Settlement System in Banking Sector in 2021 Fourth International Conference on Microelectronics, Signals & Systems(ICMSS) |978-1-6654-4885-7/21/$31.00©2021IEEE DOI:10.1109/ICMSS53060.2021.9673610

[2] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[3] Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, and Wenlin Han In the Security Applications and Challenges in Blockchain Published in 2019.

[4] X. Lin, R. Xu, Y. Chen and J. K. Lum, "A Blockchain-Enabled Decentralized Time Banking for a New Social Value System," 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1-5, doi: 10.1109/CNS.2019.8802734.

[5] J. Cheng, N. Lee, C. Chi and Y. Chen"Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp.1046-1051, doi: 10.1109/ICASI.2018.8394455.

[6] Y. Hao, Y. Li, X. Dong, L. Fang and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain," 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, pp. 280-285, doi: 10.1109/IVS.2018.8500557

[7] Suganya T., Vignesh A., Kumar V., "Decentralized secure money transfer using blockchain". IEEE Transactions on Knowledge and Data Engineering (2018), vol 30(6), pp1366–1385

[8] G Zyskind O Nathan A 'Pentland Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security and Privacy Workshops (2015), pp180–184

[9] A Vigil P Pathak S Upadhyay D Singh V Garg Blockchain Over Transaction System," International Conference.