IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203107 |

Secure Bank Transaction based on Digital Technology using Blockchain, SHA

Prof. Pramod Dhamdhere[1], Nilesh Garkal[2], Gauri Sonawane[3], Santosh Kalshetty[4], Vineet Kumar[5]

Professor, Department Of Computer Engineering Moze College, Wagholi, Pune, India[1]

Students, Department Of Computer Engineering, Moze College, Wagholi, Pune, India.[2,3,4,5]

ABSTRACT: With the evolution of Internet Technology, payment methods have undergone drastic changes from entity exchange to Internet banking. Almost every sector has gone through the transformation from conventional technologies to digital technologies. With the arrival of online payment and digital wallet system, making payments has become easier than ever and with the increasing demand for such services, the number of users using instant money transfer systems are growing rapidly. However, the existing online payment system has issues like a single point of failure, transparency, and insider problem. Also, security in such online payments is crucial to mitigate risks and financial inefficiencies. In this paper, a private and permissioned Blockchain-based Payment System for the financial sector is proposed. The architecture to seamlessly integrate e-wallets of different banks and participating institutions using blockchains that shall act as a foundation of Digital ledger technology (DLT) for financial sector in India. peer-to-peer network is designed for the proposed e-wallet system. The proposed solution shall minimize the load on the Core Banking Solution of the banks thus reducing the load on the servers at the data centers.

KEYWORDS: Blockchain, Ewallet, Digital Ledger, Money Trans- action.

I. INTRODUCTION

A blockchain is a decentralized peer to peer platform which provides security services based on some key concepts, namely authentication, confidentiality, integrity and authorization. It is the process of recording and keeping track of the resources without the intervention of a centralized authority.A blockchain is a distributed data structure which is replicated on various nodes or various computer systems that are not linked based on memory addresses, giving a different notion of linking between nodes and each of these nodes is called a block. We can imagine a blockchain as a series of blocks where each block in the blockchain is connected to its previous block and so it is replicated all over the blocks. The fundamental benefit of this replication is that, on the off chance that one of the imitation blocks becomes corrupted, different reproductions are available to ensure that the honesty of the information contained in the data structure is maintained and furthermore replication gives one some sort of assurance of the trustworthiness of the data, conveyed as a guarantee that the distinctive PCs engaged in the blockchain platform are really running appropriate calculations to ensure the data consistency and fiability. The consistency of the data is maintained by a process called consensus. Consensus is that everybody agrees that the data that goes into the data called structure is what they agree to put there. For linking, we cannot use memory addresses, so we rely on the cryptographic technique called hashing. Blockchains use hash linking and the integrity of the data is thus maintained because of the use of cryptographic techniques and consensus and replication. Therefore, a blockchain is an information structure that is distributed, duplicated and maintains the integrity of data, i.e., the information cannot be altered. Another view is that blockchain is an immutable ledger of events/transactions, a log that cannot be changed by a malicious party or by mistake. Any tampering with the data is made virtually impossible.

Blockchain technology is used in financial systems to secure transactions between two people in a decentralized manner. In a decentralized system we need to preserve the privacy of the customer and we should also maintain security for the transaction data. Utilizing blockchain innovation, an agreement is first sent by the payer to the bank, and afterward this agreement is forwarded to the arranging bank. This arranging bank in turn sends an encouraging letter to the payee requesting affirmation. Presently the payee sends the archive to the arranging bank which is sent to the bank. This archive is delivered to the payer who can utilize it to start a smart agreement with the payee. In this way a protected exchange is done between two individuals utilizing a blockchain

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203107 |

II. LITERATURE SURVEY

1. Blockchain Based Architecture and Solution for Secure Digital Payment System

In this paper, a private and permissioned Blockchain- based Payment System for the financial sector in India is proposed. The proposed architecture is based on Istanbul Byzantine Fault Tolerance (IBFT) consensus and it also discusses the integration of banks with the system.

2. A Hybrid Model for Central Bank Digital Currency Based on Blockchain

In this paper, authors propose a hybrid blockchain sys- tem with a modularity network for CBDC. The account scheme is used to record frequently circulated digital currencies, especially for massive small payment trans- actions when the digital assets and smart contracts with large value fluctuations and weak liquidity are recorded using the Unspent Transaction Output (UTXO) scheme. In terms of network architecture, a modular blockchain architecture is proposed, and a sliced data storage so- lution is designed to enhance the concurrency of this structured network. Authors also proposed a CBDC supervision mode for blockchain, and on this basis, the DPOS-BFT algorithm is optimized, which reduces the two rounds of consensus of the original algorithm to one round. Finally, three simulation experiments on scheme, network, and consensus are carried out, which show this system can comprehensively improve the transaction processing and the consensus speed.

3. Digital Payments: Blockchain based Security Concerns and Future

Technological growth has been tremendous in the past few decades and has brought significant changes in the lifestyle of human beings. One such field where the growth of technology brought a radical change is the field of transactions. Introduction of digital payments and digital money brought a whole new dimension in money payments and transactions. Policies of different governments has encouraged and also discouraged the use of various types of digital money. The paper ad- dresses such issues and finally proposes a better en- hancement for the existing digital payment technologies by using secured and privacy sensitive technologies like blockchain.

4. Future of e-Wallets: A Perspective From Under Gradu- ates'

This paper study about e-payments specifically mobile wallets. As we all know that after demonetization, there is a tremendous increase in number of e-payments. This paper specifically targets undergraduate students and portrays their preferred mode of payment. It also suggest some steps that should be taken for betterment of e- payment facilities.An electronic wallet can be defined as a virtual cashless service which can replace hard cash notes. For purchasing anything, the person do not have to rush to ATMs or banks to withdraw cash, rather transaction can be done there and then in a fraction of seconds. It has become an upcoming way of purchasing goods and services without any physical movement of cash.

5. Digital Wallet: A handy Solution in the wake of Demon- etisation

Demonetisation might have targeted black money and fake currency circulation but its biggest impact is being seen in the shift towards the digital economy, which will emerge as India's biggest long-term gain. Prime Minister's surgical strike on black money on November 8, 2016, changed all that. The country woke up to cash denial and cash shortage that inadvertently pushed them to seek out e-Wallet solutions. Increasing in popularity, and for good reason, the need could not have come at a better time for digital money service providers like Paytm, Freecharge, Mobikwik and many others. The revolution has begun and the end game could well see India surpass developed nations to emerge as one of the largest cashless economies. The proposed paper gives an overview of digital wallets, describes its working and reviews the various types of digital wallets available in India. The paper also discusses the merits and challenges of deploying a nationwide digital wallet solution in India.

III. PROPOSED METHODOLOGY

Currently, cash transfer between two different e-wallets is not allowed in India. An architecture to solve this issue along with Blockchain based DLT architecture is proposed in this paper. Figure 1 illustrates an architecture wherein three different banks are arranged as peers over a network. Each of these banks provides an e-wallet to its customers. Each of the banks has one or more miner. This miner is a high end computation server that is granted access to certain attributes of the customer table in the central database of the bank. Each of the banks has definite trust agreements with each other. The idea is to use Proof of Stake (PoS) as consensus mechanism. Since the banks agree to collaborate, each of these shall ensure that any malicious activity shall directly or indirectly harm their own database and transactions.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203107 |

A. SYSTEM ARCHITECTURE

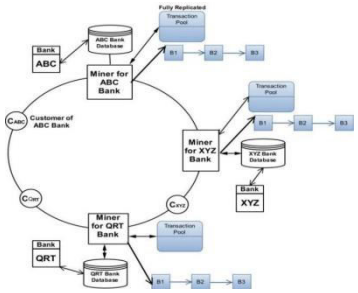


Fig. 1. System Block Diagram

B. METHODOLOGY

The proposed network architecture is swarm based peer to peer network. Each of the participating banks shall have certain number of miners. These miners can be considered as super nodes that shall be persistent (permanent) and fault tolerant. Any customer seeking e-wallet from his bank shall be provided with the network address of all the miners. This customer shall send the join message to the miners. During registration process, a public key and a private key shall get generated. This public key gets updated with the miner. When any offline customer becomes live for performing any transaction, the e-wallet app shall get synchronize the cashbook of the customer with the entries of the Blockchain.

A transaction in this work represents a cash or amount or payment that is digitally signed with the private key of the initiator who is making payment or vice versa with the use of its public key specified in the transaction [6]. Miners record these transactions in a Blockchain and carry out the task for the following three major scenarios: a) Transferring cash from home bank account into the ewallet, b) Transfer of cash between two different e-wallets and c) Transfer of cash from e-wallet to bank account.

C. ALGORITHM

1. *SHA256:* SHA-256 (256 bit) is part of SHA-2 set of cryptographic hash functions, designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). A hash function is an algorithm that transforms (hashes) an arbitrary set of data elements, such as a text file, into a single fixed length value (the hash). The computed hash value may then be used to verify the integrity of copies of the original data without providing any means to derive said original data. Irreversible, a hash value may be freely distributed, stored and used for comparative purposes. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor.

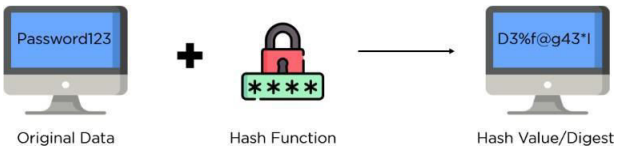


Fig. 2. SHA256

2. *AES :* AES algorithm helps to encrypt the template. The algorithm uses 10 or 14rounds for encryption with given key depending on 128 bytes or 256bytes respectively . Each Round consist of 4 steps which includes SubByte where one each byte is substituted with another byte. The next is row shifting were whole row is shifted. next is mixcolumn where columns are mixed and the last one is adding round key. One round is shown in Fig

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203107 |

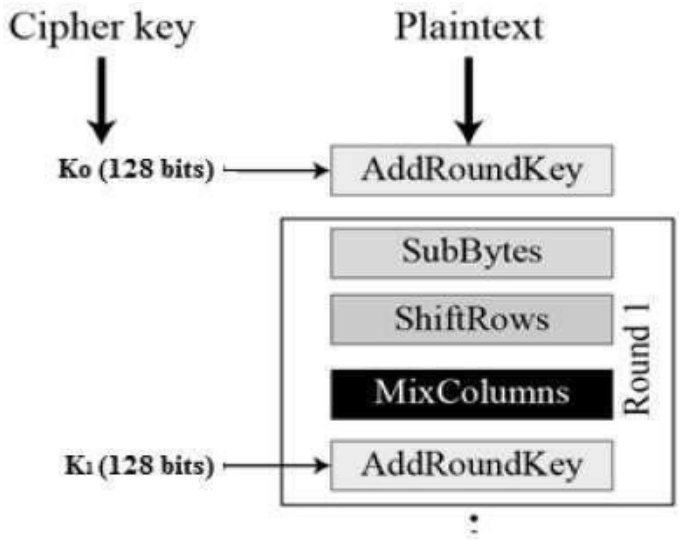


Fig. 3. AES

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 = Id
I3 = cast transaction I4 = submission

Process (P) represented as: P = P0, P1, P3, P4 P0 = Login by user-side
P1 = Approval of login P3 = block chain
P4 = transaction process

Output (O) represented as: O = O0, O1, O2, O3 O0 = show details
O1 = receiver id
O2 = user transaction successful O3 = view receiver transact details

V. RESULT AND DISCUSSIONS

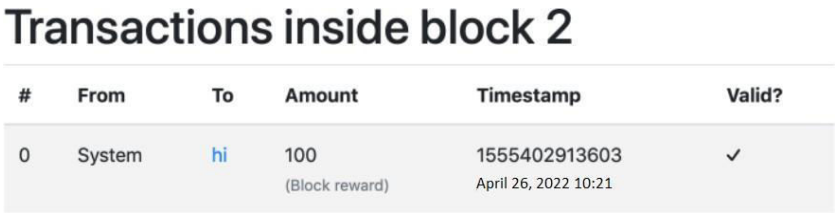
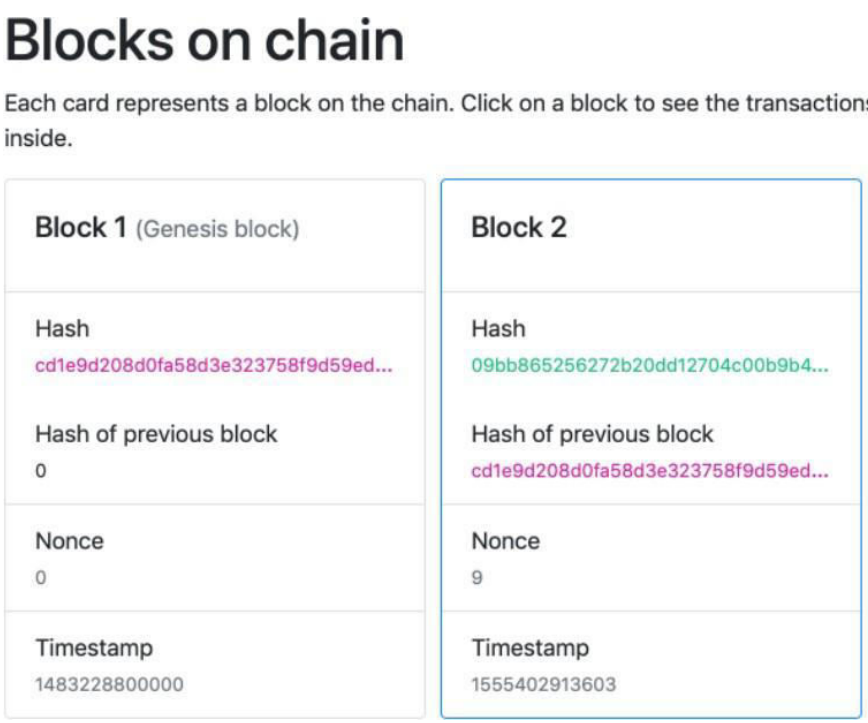


Fig. 4. Transaction

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203107 |



Seeing blocks on the chain & exploring transactions in each block. Each card represents block on chain.

VI. CONCLUSION

A Common Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain has been proposed in this work. The proposed architecture is first of its kind for implementing blockchain architecture for ewallets. It also introduces the architecture for interoperability between e- wallets from different banks or entities. The proposed solution shall minimize the load on the CBS of the banks, reduce the load on the servers and decentralize the processing activities thus harnessing the idle capacities at other centers.

REFERENCES

1. rabab alayham abbas helmi, chua shang ren," securing digital payment by using blockchain technology", 2022 ieee 10th conference on systems, process & control (icspc), doi: 10.1109/icspc55597.2022.10001813
2. Pramod Dhamdhere "semantic patent extended based on conceptual comparability of text with utilizing histogram arithmetic for illustrations to minimize trade mark", journal of data acquisition and processing , ISSN: 1004-9037 ,vol. 37 (5) 2022.
3. M. R. Ahmed, K. Meenakshi, M. S. Obaidat, R. Amin and P. Vijayakumar, "Blockchain Based Architecture and Solution for Secure Digital Payment System," ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500526.
4. Pramod Dhamdhere "semantic trademark retrieval system based on conceptual similarity of text with leveraging histogram computation for images to reduce trademark infringement", Webology (ISSN: 1735-188X), Volume 18, Number 5, 2021.
5. J. Zhang et al., "A Hybrid Model for Central Bank Digital Currency Based on Blockchain," in IEEE Access, vol. 9, pp. 53589-53601, 2021, doi: 10.1109/ACCESS.2021.3071033.
6. M. J. Pillai, "Digital Payments: Blockchain based Security Con- cerns and Future," 2020 International Conference on Smart Elec- tronics and Communication (ICOSEC), 2020, pp. 429-435, doi: 10.1109/ICOSEC49089.2020.9215431.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203107 |

7. K. Singh, N. Singh and D. Singh Kushwaha, ”An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology us- ing Blockchain,” 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 165-169, doi: 10.1109/GUCON.2018.8674919.
8. Chauhan, Madhu, Isha Shingari, and I. Shingari. ”Future of e-wallets: a perspective from under graduates’.” International Journal of Advanced Research in Computer Science and Software Engineering 7, no. 8 (2017): 146.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details