IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106035 |

Implementation towards Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain

Yogita D Jadhav[1], Prof. R. N. Devray[2]

P.G. Student, Dept. of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra India[1]

Assistant Professor, Dept. of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra, India[2]

ABSTRACT: Last decade had been worst for humanity as it faced Covid-19. The pandemic invited many things unknown to humans such as lockdown, compulsory mask and no contact with other people or things. The `No Contact' initiated much awaited progress in payment from being entity exchange to being digital. The digitization of payment became biggest transformation, every common citizen realized the use of digital payment. The evolution of cash payment to internet banking and internet banking to e-wallet has made transaction easier for all the services without exhibiting physical form. Payment Gateways, Digital Wallet, Internet Banking use has risen as being fast and instant. Though the recent payments are secure on theft front with the use of digital money by many users at many times online payment system might face problem on digital money transfer with issues such as wrong payment, link failure or single point failure. There might be more problems such as insider problem and transaction being transparent. For such situations more secure and private path towards security is needed as insufficiency will give rise to risk mitigation. The paper proposes a payment system which will be based on privacy and permission laid by blocks to blocks for use in financial sector. The architecture proposed integrates the digital wallet with different banks to give foundation of Blockchain for secure transactions. The peer-to-peer network will share transactions as well share load to minimize load on central banking system keep the load distributed and secure over all data centres.

KEYWORDS: Blockchain, Ewallet, Digital Ledger, Money Transaction.

I. INTRODUCTION

A blockchain is a decentralized peer to see platform which affords protection offerings primarily based totally on a few key concepts, specifically authentication, confidentiality, integrity and authorization. It is the technique of recording and maintaining tune of the assets without the intervention of a centralized authority. A blockchain is a dispensed records shape that is replicated on numerous nodes or numerous laptop structures that aren't related primarily based totally on reminiscence addresses, giving a special belief of linking among nodes and every of those nodes is known as a block. We can believe a blockchain as a chain of blocks in which every block withinside the blockchain is connected to its preceding block and so it's far replicated everywhere in the blocks. The essential advantage of this replication is that, at the off hazard that one of the imitation blocks will become corrupted, special reproductions are to be had to make sure that the honesty of the records contained withinside the records shape is maintained and moreover replication offers one a few type of guarantee of the trustworthiness of the records, conveyed as a assure that the distinctive PCs engaged withinside the blockchain platform are actually jogging suitable calculations to make sure the records consistency and fiability. The consistency of the records is maintained through a technique known as consensus. Consensus is that everyone is of the same opinion that the records that goes into the records known as shape is what they comply with placed there. For linking, we cannot use reminiscence addresses, so we depend at the cryptographic approach known as hashing. Blockchains use hash linking and the integrity of the records is consequently maintained due to the use of cryptographic strategies and consensus and replication. Therefore, a blockchain is an records shape this is dispensed, duplicated and continues the integrity of records, i.e., the records cannot be altered. Another view is that blockchain is an immutable ledger of events/transactions, a log that cannot be modified through a malicious celebration or through mistake. Any tampering with the records is made actually impossible.

Blockchain era is utilized in monetary structures to stable transactions among human beings in a decentralized manner. In a decentralized gadget we want to keep the privateness of the client and we need to additionally keep protection for the transaction records. Utilizing blockchain innovation, an settlement is first despatched through the payer to the financial institution, and later on this settlement is forwarded to the arranging financial institution. This

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106035 |

arranging financial institution in flip sends an encouraging letter to the payee soliciting for affirmation. Presently the payee sends the archive to the arranging financial institution that is despatched to the financial institution. This archive is delivered to the payer who can put it to use to begin a clever settlement with the payee. In this manner a covered trade is completed among people utilising a blockchain.

Paper is organized as follows. Section I gives brief introduction to the topic; Section II describes survey done to understand the problem and detect the underlying problem in system. The diagram represents the step of the process with blockchain. After transaction, how process takes place is given in Section III. Finally, Section V presents conclusion.

II. RELATED WORK

1) The Blockchain Based Architecture and Solution for Secure Digital Payment System

In this paper, a non-public and permissioned Blockchain primarily based totally Payment System for the monetary quarter in India is proposed. The proposed structure is primarily based totally on Istanbul Byzantine Fault Tolerance (IBFT) consensus and it additionally discusses the combination of banks with the system. [1]

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

In this paper, authors advise a hybrid blockchain gadget with a modularity community for CBDC. The account scheme is used to document regularly circulated virtual currencies, particularly for huge small price transactions while the virtual property and clever contracts with large cost fluctuations and susceptible liquidity are recorded the use of the Unspent Transaction Output (UTXO) scheme. In phrases of community structure, a modular blockchain structure is proposed, and a sliced statistics storage answer is designed to decorate the concurrency of this dependent community. Authors additionally proposed a CBDC supervision mode for blockchain, and in this basis, the DPOS-BFT set of rules is optimized,which reduces the 2 rounds of consensus of the unique set of rules to at least one round. Finally, 3 simulation experiments on scheme, community, and consensus are carried out, which display this gadget can comprehensively enhance the transaction processing.[2]

3) Digital Payments: Blockchain based Security Concerns and Future

Technological increase has been great in the beyond few many years and has added sizeable modifications in the way of life of human beings. One such area in which the increase of era added a thorough alternate is the sphere of transactions. Introduction of virtual bills and virtual cash added a complete new size in cash bills and transactions. Policies of various governments has recommended and also discouraged using diverse kinds of virtual cash. The paper addresses such problems and finally proposes a higher enhancement for the present virtual payment technology through the use of secured and privateness sensitive technology like blockchain.[3]

4) Future of e-Wallets: A Perspective From Under Graduates'

This paper examine approximately e-bills in particular cellular wallets. This paper in particular objectives un-dergraduate college students and portrays their desired mode of payment. It additionally advise a few steps that ought to be taken for betterment of e-payment facilities.An digital pockets may be described as a digital cashless carrier that could update difficult coins notes. For buying anything, the individual do now no longer ought to rush to ATMs or banks to withdraw coins, as a substitute transaction may be performed there after which in a fragment of seconds. It has turn out to be an upcoming manner of buying items and offerings without any bodily motion of coins.[4]

5) Digital Wallet: A handy Solution in the wake of Demonetisation

Demonetisation would possibly have focused black cash and pretend foreign money flow however its largest effect is being visible withinside the shift toward the virtual economy, if you want to end up India's largest long-time period gain. Prime Minister's surgical strike on black cash on November 8, 2016, modified all that. The awakened to coins denial and coins scarcity that inadvertently pushed them to are seeking out e-

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106035 |

Wallet solutions. Increasing in popularity, and for exact reason, the want may want to now no longer have come at a higher time for virtual cash provider companies like Paytm, Free charge, Mobi Kwik and plenty of others. The revolution has started and the cease recreation may want to nicely see India surpass evolved international locations to end up certainly considered one among the most important cashless economies. The proposed paper offers an outline of virtual wallets, describes its operating and evaluations the numerous sorts of virtual wallets to be had in India. The paper additionally discusses the deserves and demanding situations of deploying national virtual pockets answer in Indiaalgorithm.

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.

A. SYSTEM ARCHITECTURE

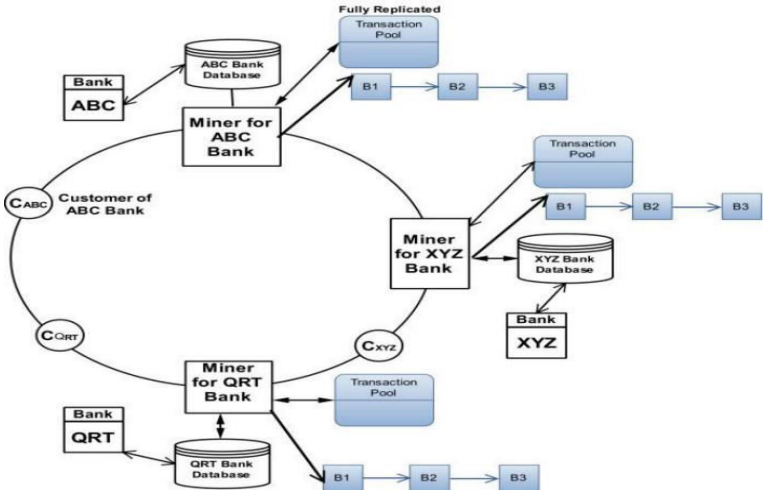
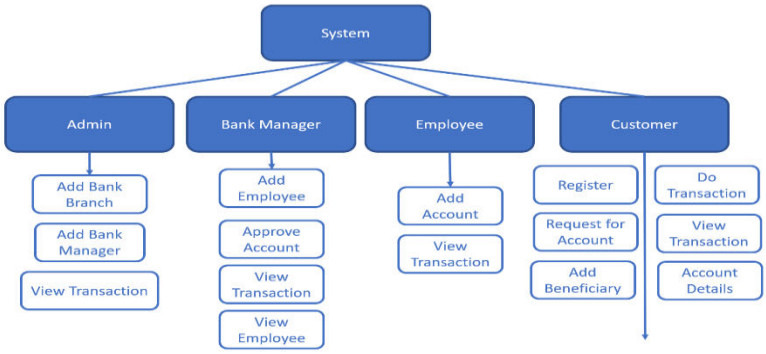


Fig. 1. System Block Diagram



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106035 |

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-2includes a significant number of changes from its predecessor.

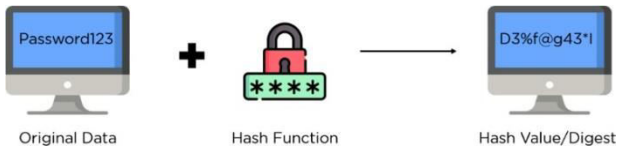


Fig. 2. SHA256

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

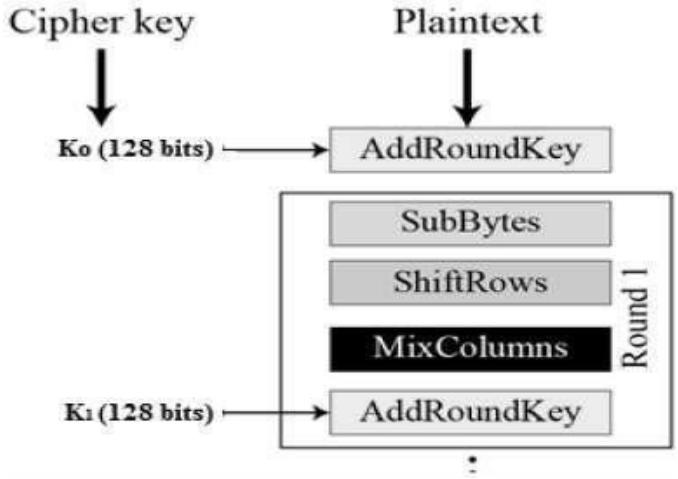


Fig. 3. AES

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106035 |

IV. MATHEMATICAL MODEL

Let S be the whole System,
Set S = I, P, O Where,
Input (I) represented as: I = I0, I1, I2, I3, I4I0 = User Registration Details
I1 = User LoginI2 = Id
I3 = cast transactionI4 = submission

Process (P) represented as: P = P0, P1, P3, P4P0 = Login by user-side
P1 = Approval of loginP3 = block chain
P4 = transaction process

Output (O) represented as: O = O0, O1, O2, O3O0 = show details
O1 = receiver id
O2 = user transaction successful O3 = view receiver transact details

V. RESULT AND DISCUSSIONS

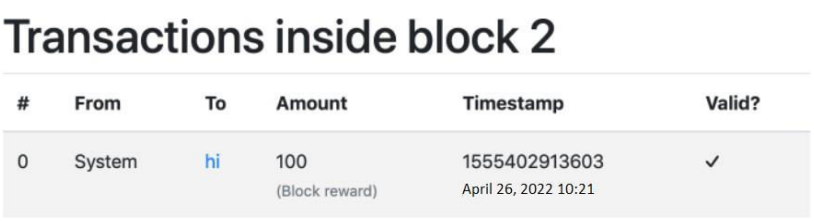


Fig. 4. Transaction

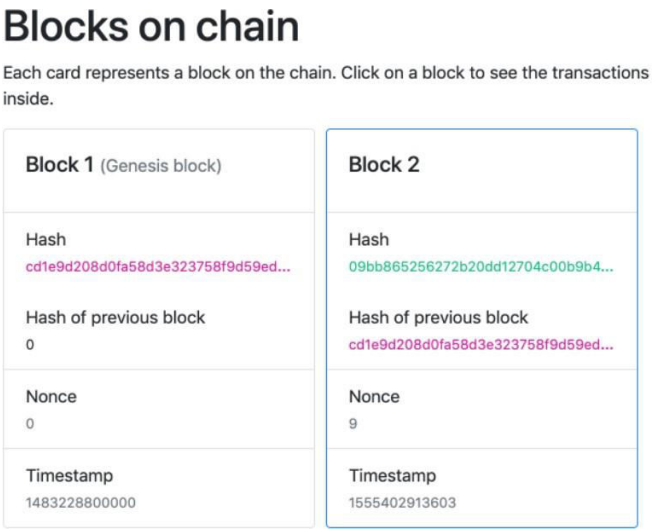


Fig. 5. Block on Chain

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106035 |

VI. CONCLUSION

A Common Secure E-Wallet Architecture primarily based totally on Digital Ledger Technology the usage of Blockchain has been proposed on this work. The system is first of its type for imposing blockchain structure for e-wallets. It additionally introduces the structure for interoperability among e-wallets from specific banks or entities. The proposed answer shall limit the weight on the CBS of the banks, lessen the weight at the servers and decentralize the processing sports accordingly harnessing the idle capacities at different centres.

REFERENCES

[1] Ahmed, Mohammad Rasheed, Kandala Meenakshi, Mohammad S. Obaidat, Ruhul Amin, and Pandi Vijayakumar. "Blockchain Based Architecture and Solution for Secure Digital Payment System." In ICC 2021-IEEE International Conference on Communications, pp. 1-6. IEEE, 2021.
[2] Zhang, Jinnan, Rui Tian, Yanghua Cao, Xueguang Yuan, Zefeng Yu, Xin Yan, and Xia Zhang. "A hybrid model for central bank digital currency based on blockchain." IEEE Access 9 (2021): 53589-53601.
[3] Vijayan, Akash, Akeel Mohammed Ashique, Mathew Koshy Karunattu,Ansamma John, and Manu J. Pillai. "Digital Payments: Blockchain based Security Concerns and Future." In 2020 International Conference on Smart Electronics and Communication (ICOSEC), pp. 429-435. IEEE, 2020.
[4] Singh, Karan, Nikita Singh, and Dharmender Singh Kushwaha. "An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain." In 2018 international conference on computing power and communication technologies (GUCON), pp. 165-169. IEEE, 2018.
[5] 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.
[6] Jain, Mehak, and Ravi Singla. "Digital wallet: a handy solution in the wake of Demonetisation." Biz and Bytes 8, no. 1 (2017): 188-197.
[7] Singla, Ravi. "Digital Wallet: A handy Solution in the wake of Demonetisation." Economic times (2016).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details