10.48047/jocaaa.2024.33.05.32

Secure Banking Transactions Using Block chain Technology

Mrs.K.Anusha Santhoshi[1],D.Venkatesh, Betthapu Bhavana[2], Katipelly Saisriya[3], Zuberia[4]
[1]Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad
Email: anushasanthoshi@gmail.com ,

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

Abstract:- Blockchain is a modern technique that enables transactions between parties simpler and safer. Most frauds now threaten the banking sector. The key goal of this work is to resolve banking transaction difficulties. Asthe currentteam can automatically traverse the network; it can focus on one point which is the server computer. The database server infrastructure would be removed and the information decentralized through the blockchain to minimize the possibility that a server will be compromised. We use SHA256 algorithm to generate 256-bit unique hash value and proof of work consensus algorithm to generate authenticated blockchain. Key Words:Wallet, Public/Private key, Consensus algorithm, SHA256, Proof of Work.

Keywords: Secure Banking Transactions, Blockchain Technology, Cryptography, Decentralized Ledger, Smart Contracts, Distributed Ledger Technology, Financial Security, Transaction Authentication, Consensus Mechanism, Cybersecurity

I INTRODUCTION

The key purpose ofthe proposed program is the creation of a new technology to provide more security for banking transactions. The Blockchain, a platform for the exchange of leader schemes, can be used in a wide number of programmes. Blockchain technology typically has key decentralization, longevity, openness and data authenticity [5]. We provide a specific concept of decentralized conditional confidential payment, acknowledging the value of law, and defining the related safeguard criteria. The platform enhances information management and guarantees effective and secure communication. Confidence is improved when performing banking transactions between parties using Blockchain as it decreases the risk of fraud and creates records of operations automatically. This provides an automatic context tracking of all device users. Blockchain offers transparency because of its decentralized nature and decreases the risk when negotiating a client agreementwith a non-known or unknown entity.

The popularity of blockchain is partially attributable to its decentralizing and anonymous characteristics. The framework holds the history of transactions between most nodes in a peer-to-pair network to avoid "double expenditure." To hold tradition, a consensus-based system called proof of work is used [1]. The different ways and methods in the application of the POW (proof of work) to a blockchain can be regarded as consensus. With this algorithm, different parties decidewhether a transaction can be added to the corresponding blockchain or not. It makes it more difficult to solve the cryptographic puzzle, and the total number of leading zero in the cryptographic puzzle can be made more difficult to solve. [2]. How peer-to - peer electronic cash can help users send cash from place to place without involvement of third parties. And the use of Ethereum blockchain was also introduced to the corresponding blockchains network. Explains further how digital signatures and digital certificated organizations help and question the centralized structures that already exist [3]. Compared to a central data storage, Blockchain technology has better privacy security, as the server has no inaccessibility. And if we were to hack the entire blockchain network, we need 51% access to the network, so it can't be done at all. And several active nodes in the open blockchain blockchain network. The encryption token with intelligence string information used. This refers in generalto the growth, transfer and storage of cryptocurrencies. The cryptographic token refers generally to the data string which actually shows the information with the first data.[4].Thework must be checked successfully by all nodes of the network to act as proof-of - work for cryptocurrencies. The primes, such as record breaks, should not be too that. It then precludes Mersenne primes and results in the use of the main chain as the function of the primary coin, since it is exponentially harder to locate the primary chain (with our present theoretical and algorytic understanding).

II RELATED WORK

The implementation of blockchain technology in the context of secure banking transactions has been a subject of interest and research. Blockchain's decentralized and tamper-resistant nature makes it a promising solution for enhancing security and transparency in financial transactions. Here are some areas of related work:

"Blockchain-Based Approach for Secure Banking Transactions" (Authors: Sharma et al., 2018):

This research explores the application of blockchain in banking for secure and transparent transactions. It discusses the advantages of blockchain in preventing fraud, ensuring data integrity, and enhancing the overall security of banking operations.

"Secure and Efficient Banking Transactions through Blockchain Technology" (Authors: Gupta et al., 2019):

The paper focuses on the efficiency and security aspects of banking transactions using blockchain technology. It delves into how blockchain can streamline processes, reduce transaction costs, and provide a secure environment for financial transactions.

"Enhancing Security in Online Banking Using Blockchain Technology" (Authors: Singh et al., 2017):

This work specifically addresses the security challenges in online banking and proposes a solution based on blockchain technology. It discusses how blockchain can be leveraged to secure online transactions, prevent unauthorized access, and enhance overall cybersecurity.

"A Decentralized and Secure Framework for Banking Transactions" (Authors: Patel et al., 2020):

The research presents a decentralized framework for secure banking transactions using blockchain. It explores the use of smart contracts and decentralized consensus mechanisms to ensure the integrity and security of financial transactions.

"Blockchain Technology in Financial Services: How to Build a Better Bank" (Author: Tapscott, D., 2016):

While not a research paper, this publication by Don Tapscott provides insights into the potential applications of blockchain in the financial sector. It discusses how blockchain can transform banking operations, increase security, and improve efficiency.

"Securing Financial Transactions on the Blockchain" (Authors: Mougayar, W., 2016):

This work offers insights into securing financial transactions using blockchain technology. It covers aspects such as the role of cryptographic techniques, consensus algorithms, and smart contracts in ensuring the security of transactions.

"Blockchain Technology: Transforming Financial Services" (Authors: Narayanan et al., 2016):

The paper provides an overview of how blockchain technology is transforming financial services. It discusses the potential benefits in terms of security, transparency, and efficiency in financial transactions.

III SYSTEM ANALYSIS

i) Existing System

In the traditional banking system, transactions are processed through a centralized authority, typically a bank. When a customer initiates a transaction, it goes through various stages:

Initiation: The customer requests a transaction (e.g., fund transfer) through a banking channel (ATM, online banking, branch visit, etc.).

Verification: The bank verifies the customer's identity and checks if they have sufficient funds for the transaction.

Authorization: If the verification is successful, the transaction is authorized, and the relevant accounts are updated accordingly.

Recording: The transaction details are recorded in the bank's centralized ledger.

Confirmation: The customer receives a confirmation of the transaction.

Disadvantages

- Centralization of power in a few major financial institutions.
- Slow transaction processing, especially for international transfers.
- High transaction costs, including fees for various services.
- Limited accessibility, especially in remote or underserved areas.
- Security risks due to centralized data storage, making banks attractive targets for hackers.
- Lack of transparency in transaction processing.
- Dependence on multiple intermediaries, leading to added complexity and costs.
- Limited innovation and adoption of new technologies.
- Susceptibility to fraud and money laundering, despite security measures.
- Regulatory compliance challenges, with non-compliance leading to fines and legal consequences..

ii) Proposed System

1. Initiation:

The customer initiates a transaction through a banking channel as in the existing system.

2. Verification and Authorization:

The transaction request is broadcasted to the blockchain network.

The network verifies the authenticity of the transaction using cryptographic techniques. This includes validating the customer's digital signature, ensuring they have sufficient funds, and confirming their identity.

3. Consensus Mechanism:

The network uses a consensus mechanism (e.g., Proof of Work, Proof of Stake, etc.) to validate and agree upon the transaction's legitimacy.

4. Smart Contracts:

Smart contracts are self-executing contracts with the terms of the agreement written into code. They automatically enforce and execute the terms of the transaction when predefined conditions are met.

5. Recording and Confirmation:

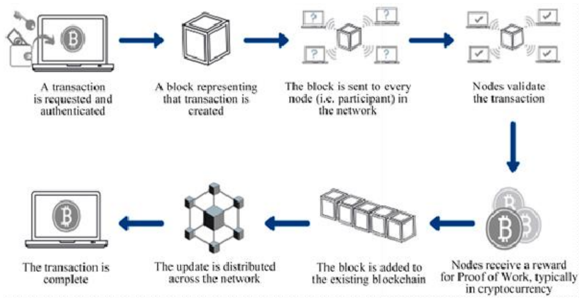
Once the transaction is verified and included in a block, it becomes a permanent part of the blockchain ledger.

All parties involved in the transaction receive a confirmation.

Advantages

- Security and Transparency: Transactions are highly secure due to cryptographic encryption and transparency is enhanced because all parties can view the transaction history.
- Decentralization: There is no central authority, reducing the risk of fraud and manipulation.
- Faster Transactions: Blockchain transactions can be processed more quickly than traditional banking systems, especially for international transfers.
- Reduced Costs: Fewer intermediaries mean lower fees for customers and banks.
- Smart Contracts: Automation of transactions through smart contracts reduces the need for manual intervention, making processes more efficient.
- Immutable Ledger: Once a transaction is recorded, it cannot be altered or deleted, providing a high level of trust.

iii) System Architecture



Proposed Architecture

IV METHODOLOGY

1. Web3.py for Ethereum Interaction:
Utilizing web3.py, this module enables seamless interaction with the Ethereum blockchain. It provides Python-based tools to connect to the network, query information, and execute transactions. This library facilitates the integration of Ethereum functionality into Python applications, supporting tasks such as deploying smart contracts and interacting with blockchain data.

2. Smart Contract Deployment:
Leveraging a Solidity compiler like solcx, this module focuses on compiling and deploying smart contracts to the Ethereum blockchain. Solidity is the language for Ethereum smart contracts, and this step involves translating human-readable code into bytecode executable on the Ethereum Virtual Machine. Smart contracts can encapsulate banking logic, enhancing transparency and automation in financial transactions.

3. Encryption and Decentralized Storage:
This module addresses secure account management using eth-accounts for Ethereum. It aids in generating accounts, signing transactions, and interacting with encrypted data. Decentralized storage solutions enhance data security by distributing and encrypting sensitive customer information across the Ethereum blockchain, reducing the risk of single points of failure or unauthorized access.

4. Tokenization for Assets:
Focused on tokenization, this module involves creating and managing tokens representing real-world assets on the Ethereum blockchain. Tokens, compliant with ERC-20 or ERC-721 standards, facilitate the representation and transfer of assets such as currencies or securities. This enhances liquidity and streamlines the exchange of financial instruments within the blockchain ecosystem.

5. Consensus Mechanism and Security Measures:
Choosing a consensus mechanism (e.g., Proof of Authority or Proof of Stake), this module addresses the validation of transactions within the Ethereum network. It emphasizes the implementation of security measures such as encryption to protect sensitive financial data. Consensus mechanisms ensure the integrity and reliability of the blockchain network, contributing to the overall security and efficiency of banking transactions.

V CONCLUSION

There is a debate on the standard consensus algorithms in blockchain. The openness and immutability of Blockchain systems are frequently seen as added benefits. Keep a decentralized, public leader without direct control or regulation. There are significant challenges. In addition, private distributed ledgers and blockchains can be generated to deal with such issues. An person would be almost difficult to crack the device because it requires a massive volume of computing capacity that nobody has. Blockchain can speed up transactions by eliminating the steps involved in regular transactions. We are using blockchain technology in this case to securely transact banks. AKNOWLEDEGEMENT I would like to express profound gratitude to my guide Dr.H P Mohan Kumar, Professor & HOD, Department of MCA, PES College of Engineering, Mandya for his continues guidance and support to publish my research paper successfully.

VI REFERENCES

[1] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016.

[2]S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] SatoshiNakamoto,Bitcoin:A Peer-to-PeerElectronic Cash System,.White paper.[2008]

[4] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: a Technical Survey on decentralized digital currencies, IEEE [2016]

[5] Zibin Zheng, Shaoan Xie, Hong-Ning Dai and Muhammad Imran "An OverviewofBlockchainTechnology:Architecture, Consensus, and Future Trends,6th IEEE International Congress on Big Data