IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 8, May 2023

Automatic Banking System Using a Blockchain Technology

P. Immaculate Rexijenifer[1], R.Vasanth[2], P. R. Srinivas[3], T. Vignesh[4]

Assistant Professor, Department of Computer Science Engineering[1]

Students, Department of Computer Science and Engineering[2,3,4]

Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Abstract*: Our current banking system is based on a central server where every branch is connected to each other. If the server made any changes to the data of a branch then other branches get affected. In this system, Corruption can be easily occurred because of unauthorized access which is totally insecure in transaction systems. But, Blockchain is a secure system where the transactional history regarding crypto-currency cannot be modified or destructed. Since 2008, Blockchain has gained immense interest due to exclusion of third-party organization participation in monitoring of the transactions. Ethereum is a protocol which is based on Blockchain technology and has several benefits over other crypto-currency based system and is best suited for creating a secure lending system. Every Ethereum based system runs on 'Smart-Contracts' which are lines of code and makes the system automated. As the system gets automated, proper algorithms can make the system reliable and secure as each and every step of the system is maintained and executed by the algorithm inside the Smart-Contracts. Blockchain systems work with peer-to-peer networks and also uses a consensus algorithm that's why there is no possibility of data modification.*

Keywords: Automatic Banking System, Ethereum, Smart-Contract

I. INTRODUCTION

1.1 Overview

All the executed bitcoin transactions are considered to be a public ledger in the Blockchain technology. The records of transactions made in Bitcoin or other crypto-currency are stored in blocks and maintained across all the computers that are linked in a peer-to-peer network. A Blockchain is the ―current‖ part of a Blockchain which records some or all of the recent transactions, and once completed, goes into the Blockchain as a permanent database. Each time a new block is generated based on the completion of each block. Blocks are linked together in a linear fashion where each block contains a hash value of the previous block. In comparison with the traditional banking systems, Blockchain keeps all the transaction histories. Chronological Bitcoin transactions are entered in a Blockchain which is similar to the regular transaction in the bank. Meanwhile, blocks are similar to individual bank statements. Blockchain keeps records of every Ethereum based transaction ever executed. Thus, it provides a relationship on past transactions that happened and also, generates values belonged to a particular address. Some developers have begun looking at the creation of other different Blockchain that allows for tradeoffs and improved scalability using alternative, completely independent Blockchain, thus, allowing for more innovation It secures the transactions in a way that any record of the transaction that occurred in the past, cannot be modified as the modification changes the hash of several blocks. Changing the hash of the blocks will inevitably result in the breakage of the links among the blocks. Also, all the peers connected to that system do not support that modification excluding the modifier, which is based on the consensus algorithm.

1.2 Background

Current banking systems are based on central server mechanisms where all the personal information of account holders, his/her bank balance, and all other necessary information related to the bank are stored. All other branches are connected to the central server where every branch retrieves personal information, bank balance and history

DOI: 10.48175/IJARSCT-10264

from the server. Failure in the central server causes all other branches to fall down which results in great damage to its users.

1.3 Ethereum

Bitcoin provides a simple stack-based programming language known as Script, which can be used to create features such as multi- signatures and escrow transactions. Although this script can be considered to be a programming language, it is not turning completed and its capabilities are also limited. The main reason behind this is that a Turning complete Blockchain language can be easily taken advantage. A simple infinite loop can create a great complication in detecting which computations are needed to be performed. As an alternative to the Bitcoin system, Ethereum provides turning complete smart contract that run on the EVM.

1.4 Ethereum Details

Ethereum is considered to be a state-transaction system. The objects in the Ethereum system are known as accounts. There are two main types of accounts: –externally owned accounts‖ and ―contracts accounts.‖ Externally owned accounts are controlled by private keys while contract accounts are fully autonomous and governed by their contract code. Both types of accounts have the ability to send messages and create new accounts. A message is essentially a transaction. Message transfer Ethers, which is the currency for Ethereum, from account to account. If a contract account receives a message, its code will be triggered in order to determine what actions to be executed next .

1.5 Ethereum Fees and Gas

Ethereum solution to the infinite loop/excessive computation problem" is to charge a small number of fees for the computation. Each message that is to be sent specifies an amount of Gas for the message. Each computational step requires some Gas. If the Gas is completely spent before the code is completely executed, the execution stops and all changes are reverted. Otherwise, if all the statements of a specific code-block are successfully executed, any leftover gas is returned to the sender of the message. This prevents infinite loops in any smart contracts, as the amount of Gas to be supplied for a transaction is finite, forcing all computation to come to an end eventually. This phenomenon also prevents malicious users from attacking the Ethereum network via excessive computation since the amount of computation is proportional to the amount paid. With the introduction of decentralized smart contracts, several protocols for decentralized lending have been proposed .

II. PROBLEMS IN EXISTING SYSTEM

In central server mechanisms, a hacker can easily modify the transaction records and hence personal information. As all the branches are connected to the central server then if the central server falls down, it will affect all the other branches. Corruption can be easily occurred due to unauthorized access. This mechanism is not secure and reliable for users.

III. PROPOSED SYSTEM

The proposed system in banking sector uses the block chaining technique to improve security and to combine multiple existing data storage platforms into one. The details such as transactions that are made among users, withdrawal of money are stored in every block which is then encrypted. Block contains data, hash values, and hash values of previous blocks which are linked to each other. This prevents hacking of data in banks where hackers find it difficult to change hash values of all the blocks that are linked. The blocks are created using doubly Linked List. A linked list is a data structure consisting group of nodes which together represent the sequence. MD5 (message digest) algorithm is used because it‗s a perfect solution for security, so it does not support block break

IV. LITERATURE REVIEW

In 2013, V. Buterin published the paper ―Ethereum: A Next-Generation Smart Contract and Decentralized Bitcoin system, which (Ethereum) provides turning complete smart contracts that run on the EVM [1]. D. Vorick and L. Champine researched on ―Sia: Simple Decentralized explained about Siacoin transaction [2]. In 2013, N. V.

Saberhagen published the paper ―Monero: Crypto V2.0 ‖ in Whitepaper Database which is based on the CryptoNote protocol [9]. In 2017, S. Singh and N. Singh focused on published inIEEE Xplore [6]. S. Nakamoto researched researcher described the electronic cash system transaction and which is published in October 2008 [3]. In 2016, E. Heilman, L. AlShenibr, and F. Baldimtsi published the paper Payment Hub ‖ where the author described TumbleBit [11]. S. Kulechov, R. Morano, and Q. Fang researched ―ETHLend.io White Paper - Democratizing Lending ‖ which is published in February 2018 [7]. In 2018, D. Vujicic, D. Jagodic, and S. Randiz published ―Blockchain technology, bitcoin, and the fundamental overview of Ethereum [10]. E. Schneider G. Fenu, L. Marchesi, M. Marchesi, and R. Tonelli published smart contract environment ‖ where the researchers interpreted the relationship among Ethereum smart contract and ICO phenomenon .

V. SYSTEM MODULES

Blockchain

The block chain is an ethical advanced record of monetary exchanges that can be modified to record money related exchanges as well as essentially everything of esteem. Information hung on a block chain exists as a common ― and persistently accommodated ―database. The block chain database isn't put away in any single area, which means the records it keeps are really open and effectively evident. No incorporated form of this data exists for a programmer to degenerate. Facilitated by a great many PCs all the while, its information is open to anybody on the web.

Identity Management

Identity management (ID management) is a wide authoritative region that bargains with distinguishing people in a framework and controlling their entrance to assets inside that framework. Such data incorporates data that validates the identity of a client, and data that depicts data and activities they are approved to get to and additionally perform. It additionally incorporates the administration of clear data about the client and how and by whom that data can be gotten to and adjusted

Bank Management

This programming will perform and satisfy every one of the undertakings that any client would want. The motto is to build up a product program for dealing with the whole bank process identified with client accounts, worker accounts and to keep each track about their property and their different exchange forms productively. Hereby, our primary target is the consumer loyalty's thinking about the present quicker world. In the ongoing years, PCs are incorporated into practically all sort of maintains and sources of income everybody goes over in the daily practice. The accessibility of the product's for pretty much every procedure or each framework has taken the world in its best apparatus and affixes the everyday life. So, we have attempted our best to build up the product program for the Bank Management System where every one of the undertakings to deal with the bank framework is performed effectively and proficiently. It deals with every one of the exchanges like new record passage, store just as pull back section, and exchange of cash for different procedures, advance passage, overseeing charges money or check, and so on.

Cryptography

Using MD5 algorithm for password security. The MD5 Message-Digest Algorithm is a generally utilized cryptographic hash work that creates a 128-bit (16-byte) hash value. Although MD5 is a broadly spread hashing calculation, is a long way from being secure, MD5 produces genuinely feeble hashes.

Transparency

The implication of transparency is that the majority of an association's activities ought to be sufficiently trustworthy to tolerate open investigation. Progressively, the nature of internet-based life and different interchanges implies that even activities proposed to be mystery might be brought into the general population's mindfulness, regardless of an association's earnest attempts to keep them covered up. In general, transparency is the nature of being effectively

DOI: 10.48175/IJARSCT-10264

observed. The significance of transparency is somewhat extraordinary in a software engineering setting, coming nearer to importance imperceptible or imperceptible. Optional importance alludes to finish consistency, as, in a straightforward PC framework or program, the yield is completely unsurprising from knowing the information.

VI. METHODOLOGY

Implementation Tools

The following programming languages are used to build the proposed lending system:

- Solidity for writing smart contracts
- Javascript for integrating with smart contracts
- HTML for desigining front-end.

The following frameworks and libraries are used:

- React.js for developing front-end
- Node.js JavaScript Runtime Environment
- Mocha JavaScript Framework for testing purposes
- Web3 JavaScript Library Collection
- Truffle as Ethereum Virtual Machine (EVM)

The following browser extension is used:

- MetaMask for accessing Ethereum enabled distributed applications

Implementation details

The proposed protocol is implemented by following the steps mentioned below:

- The Back-end of the proposed system consists of a smart contract. Starting from registration, depositing money, sending money, earning interests and all of these tasks will be managed by the contracts.
- 'Mocha' testing framework is used to test whether smart contracts are functioning properly.
- 'Solc' compiler is conducted to compile the contracts and JSON files are created corresponding to that smart contracts.
- The system is firstly implemented on Ethereum Test Network which is known as Rinkeby. To implement the system in the Rinkeby network, an account is created in Infura.com.
- After signing up, Infura.com provides a URL which is of Rinkeby Test Network. The byte codes and ABIs of the smart contracts located in JSON files are then deployed to the URL of the Rinkeby Test Network by Truffle-HD- Wallet- Provider and web3.
- After deploying the smart contracts to Rinkeby Test Network, the addresses of the smart contracts are returned and saved.
- An interactive front-end (GUI) is developed using React.js.
- The front-end of the proposed system interacts with the smart contracts using the contracts' addresses and byte code
- Web3 works as the interface between the Rinkeby Test Network and Front-End. It creates a bridge between the test network and the implemented DAPP.
- MetaMask Extension is used to access the implemented Ethereum enabled DAPP from the browser. Managing the accounts and all the transactions are done by the MetaMask

Solidity for Writing Back-End Logics

The following steps are used to build the proposed Back-End logics which are mentioned below:

- Three smart contracts are written using the Solidity programming language. Most of the algorithms of the proposed system are included in these contracts.
- The smart contract named _bankingSystem.sol‘ contains four methods for each of the banking tasks.
- _Registration‘ method is used to register Ethereum users into the p2p banking system.

DOI: 10.48175/IJARSCT-10264

- _Deposit Money‘ are responsible for transferring Ethers from Ethereum users to his/her own bank account.
- _Send Money‘ is used to send money from one‘s own bank account to another user‘s bank account

Contracts Compilation using Solc

Before uploading the contracts to the Ethereum network, these contracts need to be compiled. Solc compiler is used to compile a smart contract and generates bytecode and an ABI for each of the contracts. This bytecode and ABI are uploaded to the Rinkeby Test Network and are required by the systems to interact with the smart contracts. All the bytecodes and ABIs of the proposed system's smart contracts are acquired by the compilation using Solc.

VII. RELATED WORKS

Here are some notable works and projects related to automatic banking systems using blockchain:

- Ripple (XRP): Ripple is a blockchain-based payment protocol designed for seamless and quick cross-border transactions. It aims to enable real-time gross settlement systems, currency exchange, and remittance services. Ripple's technology has been adopted by various banks and financial institutions worldwide.
- IBM Blockchain World Wire: IBM has developed a blockchain-based payment network called IBM Blockchain World Wire. It enables financial institutions to optimize and accelerate cross-border payments by reducing intermediaries and increasing transparency.
- JPMorgan Chase's JPM Coin: JPM Coin is a digital currency developed by JPMorgan Chase, one of the largest banks globally. It is built on a private blockchain and aims to facilitate instant payments and transfers between institutional clients.
- Project Ubin: Led by the Monetary Authority of Singapore (MAS) and in collaboration with several financial institutions, Project Ubin explores the use of blockchain for interbank payments and securities settlement. It aims to improve efficiency, reduce costs, and enhance security in Singapore's financial ecosystem.
- Corda: Corda is an open-source blockchain platform developed by R3, a consortium of financial institutions. It is designed specifically for the banking and finance industry, focusing on privacy, scalability, and interoperability. Corda aims to streamline various banking processes, such as trade finance, asset tokenization, and identity management.
- Stellar (XLM): Stellar is a decentralized blockchain platform designed to facilitate fast and low-cost cross-border transactions. It aims to connect financial institutions, payment systems, and individuals globally to create a more inclusive and accessible financial network.
- Digital Asset Holdings: Digital Asset Holdings provides blockchain-based solutions for financial institutions, focusing on areas such as post-trade settlement, collateral management, and derivatives processing. Their goal is to improve efficiency, reduce risk, and enhance transparency in financial markets.

These projects and initiatives represent advancements in leveraging blockchain technology to enhance automatic banking systems. They showcase real-world applications and collaborations between banks, financial institutions, and technology providers to explore the potential benefits of blockchain in the banking sector.

VIII. SYSTEM ARCHITECTURE

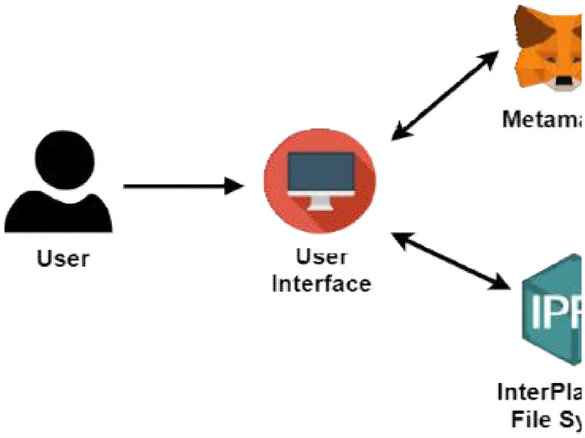
The system architecture of an automatic banking system using blockchain can vary depending on specific requirements and design choices. However, here's a generalized overview of the architecture components:

- Blockchain Network: The foundation of the system is a blockchain network, which can be either a public blockchain (like Bitcoin or Ethereum) or a permissioned blockchain (restricted to a consortium of trusted participants). The blockchain network consists of multiple nodes that maintain a distributed ledger and participate in transaction validation and consensus mechanisms.
- User Interface: The user interface provides a front-end application or platform for users to interact with the banking system. It can be a web-based interface, a mobile application, or other user-friendly interfaces. The

interface allows users to access their accounts, perform transactions, view balances, and manage their financial activities.

- Identity Verification and User Management: This component handles user registration, identity verification, and user management. It may involve KYC (Know Your Customer) processes, verification of identity documents, and other authentication mechanisms. Once verified, users are provided with digital wallets or accounts on the blockchain network.
- Wallet Management: The wallet management component handles the creation, storage, and management of digital wallets for users. It securely stores cryptographic keys that enable users to access and control their digital assets, such as cryptocurrencies or digital representations of traditional currencies.
- Smart Contracts: Smart contracts play a crucial role in automating and enforcing predefined rules and conditions. They are self- executing contracts stored on the blockchain that automatically trigger actions based on specific events or conditions. Smart contracts are used for various functions such as fund transfers, payment processing, loan agreements, and more.
- Transaction Processing and Validation: When a user initiates a transaction, it is broadcasted to the blockchain network. The transaction processing and validation component handles the verification of transactions using consensus algorithms specific to the chosen blockchain network. Validated transactions are added to blocks and appended to the blockchain, ensuring immutability and transparency.
- Security and Encryption: Security is a critical aspect of the system architecture. It includes cryptographic techniques to secure user data, transaction details, and digital assets stored in wallets. Encryption, hashing algorithms, and digital signatures are utilized to ensure data integrity, confidentiality, and authentication.
- Integration with External Systems: The automatic banking system may need to integrate with external systems such as traditional banking networks, payment gateways, regulatory compliance systems, or identity verification services. These integrations enable seamless interoperability with existing financial infrastructures and regulatory frameworks.
- Reporting and Analytics: This component handles generating reports, analyzing transaction data, and providing insights for users and administrators. It enables monitoring of system performance, transaction trends, and compliance with regulatory requirements. Scalability and Performance Optimization: As the system grows, scalability becomes important. The architecture should consider techniques such as sharding, off-chain transactions, or layer-2 solutions to enhance scalability and optimize performance, ensuring the system can handle a growing number of users and transactions.

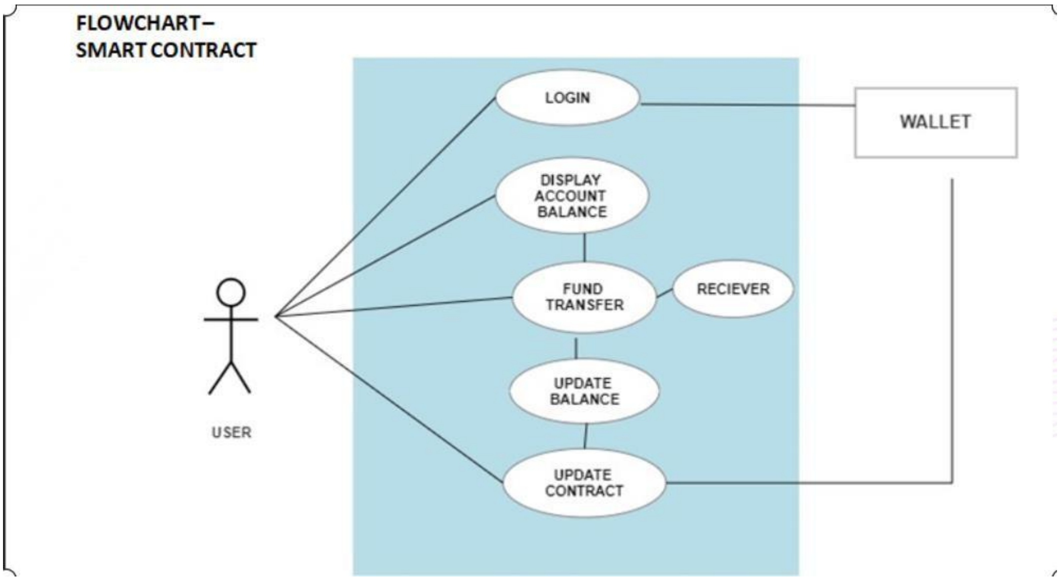
It's important to note that the system architecture may vary based on specific implementation choices, regulatory requirements, and the integration of additional features or services. The outlined components provide a general framework for understanding the key elements of an automatic banking system using blockchain technology.



DOI: 10.48175/IJARSCT-10264

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, May 2023

IX. FLOWCHART



X. CONCLUSION

Block chain Technology is a standout amongst the most predictable advances when it requires monitoring money related properties. Block chain innovation has pulled in numerous organizations that need to include the particular highlights of it to their security structures. Numerous investigations have been done for computerized monetary forms and block chain innovation, which speaks to that both of these advances will be proceeding to upset the world. Subsequent to perceiving the advantages of Block chain Technology, a few money-related establishments have begun spending extensively in this specific field. Block chain can likewise help in shortening the stream of dark cash and managing the broad cash cleaning in the economy in light of the fact that each location utilized for exchanges is put away perpetually on the databases, making every one of the exchanges provable and dependable. The legislature is watching Block chain as an approach to investigate a scope of alternatives which may apply a fitter control on the country's economy

XI. ACKNOWLEDGMENT

I'd want to use this chance to offer my sincere gratitude to everyone who helped me with the research project report. Throughout the course of my project work, I sincerely appreciate their unwavering direction, priceless constructive feedback, and helpful advise. Their frank and perceptive opinions on numerous project-related issues have been quite beneficial. Additionally, I want to express my gratitude to Principal Dr. S. N. Ramaswamy and the AAMEC management for their unwavering encouragement and support. I owe a great debt of gratitude to my department head, Dr. K. Velmurugan, and my mentor, assistant professor Mrs.P.Immuculate rexi jenifer, for their persistent supervision, steadfast oversight, and providing of the necessary information throughout the project.

REFERENCES

[1] Nir Kshetri "Can Block chain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017,

[2] Dr.Mahdi H. Miraz, "Block chain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017.

[3] Don Tap Scott and Alex Tap Scott, Block chain Revolution: How the Technology behind Bit coin Is Changing Money, Business, and the World, 1st Ed. New York, USA: Penguin Publishing Group, 2016 Mulliner C., Borgaonkar R., Stewin P., Seifert J.P. SMS-Based One- Time Passwords: Attacks and Defense. In: Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2013.

[4] Xu H.Y. China‘s Internet Financial Risks and Countermeasures. Inter- national Conference on Financial Management, Education and Social Science (FMESS 2017), 2017.

[5] Akinyede R.O., Esese O.A. Development of a Secure Mobile E-Banking System. International Journal of Computer (IJC), Vol 26, No 1, 2017.

[6] Gatali I.F., Lee K.Y., et.al a qualitative study on adoption of biometrics technologies: Canadian banking industry. In: Proceedings of the 18th Annual International Conference on Electronic Commerce: e-Commerce in Smart connected World, 2016.

[7] Tray nor P., McDaniel P., La Porta T. Security for Telecommunications Networks. Springer, 2008.

[8] Reaves B., Scaife N., Bates A., et.al Mo (bile) money, Mo (bile) problems: analysis of branchless banking applications in the developing world. In: Proceedings of the 24th USENIX Security Symposium (USENIX Security 2015), USENIX Association, 2015

[9] Haupert V., Müller T. On App-based Matrix Code Authentication in Online Banking. Technical Report Freidrich-Alexander-Universität Erlangen Nurnberg, 2016.

[10] Schueffel P. Taming the Beast: A Scientific Definition of Fintech. Journal of Innovation Management, 4(4) 32- 54, 2017.

[11] Haupert V., Maier D., Müller T. Paying the Price for Disruption: How a FinTech Allowed Account Takeover. In: Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium, 2017.

[12] Rajput Q., Khan N. S., Larik A., Haider S. Ontology Based Expert- System for Suspicious Transactions Detection, Canadian Center of Science and Education, Computer and Information Science; Vol. 7, No. 1, 2014.

[13] Leonard, K. J. Detecting Credit Card Fraud Using Expert Systems. Computers and Industrial Engineering 25(1- 4), 103-1, 1993.

[14] Quah J. T. S., Sriganesh M. Real-time credit card fraud detection using computational intelligence, Expert Systems with Applications 35 (4), 1721– 1732, 2008.

[15] Abdel Hamid D., Soltani K., Ouassaf an Automatic Bank Fraud De-tection Using Support Vector Machines. The International Conference on Computing Technology and Information Management (ICCTIM). Society of Digital Information and Wireless Communication, 2014.

DOI: 10.48175/IJARSCT-10264