IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

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 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204062 |

Blockchain-Powered Chat Application Enhancing Security Communication

Mrs. C. Gayathri, D. Kirthikraj, G. Manogar, S. Mubarak, N K Suchdev Darshan

Assistant Professor, Department of Computer Science Engineering, Mahendra Institute of Technology, Namakkal District, Tamil Nadu, India

Department of Computer Science Engineering, Mahendra Institute of Technology, Namakkal District, Tamil Nadu, India

Department of Computer Science Engineering, Mahendra Institute of Technology, Namakkal District, Tamil Nadu, India

Department of Computer Science Engineering, Mahendra Institute of Technology, Namakkal District, Tamil Nadu, India

Department of Computer Science Engineering, Mahendra Institute of Technology, Namakkal District, Tamil Nadu, India

ABSTRACT: Enhancing security in real-time communication applications, particularly in blockchain-based chat platforms, is paramount for safeguarding user privacy and data integrity. Traditional chat applications often lack robust security measures, leaving users vulnerable to various threats such as eavesdropping, data breaches, and identity theft. This paper introduces the requirements and challenges involved in developing a secure blockchain-based chat application. It addresses four key research questions pertaining to identifying essential factors for secure communication, examining the current state of research in the field, harnessing the advantages of blockchain and cryptography in bolstering security, and outlining future research avenues. Through an exhaustive review of existing literature and solutions, this paper presents a comprehensive overview of security mechanisms applicable to blockchain chat applications. It delves into cryptographic protocols, decentralized network architectures, and consensus mechanisms crucial for ensuring confidentiality, integrity, and availability of communication data. Furthermore, it proposes an innovative framework comprising five interconnected modules: Data Management, Encryption Module, Decentralized Authentication Module, Trust Management Module, and Real-time Security Monitoring Module. This framework aims to provide a robust foundation for building highly secure and resilient blockchain-based chat applications. Additionally, this work identifies promising directions for future research, offering insights to academics and researchers seeking to advance the field of secure real-time.

I. INTRODUCTION

In today's generation chatting over messaging platforms are a part of an individual's lifestyle. Today's most of the communication happens over social media platforms. All these platforms also provide users the option to share multimedia attachments leveraging their communication protocols over sockets. All these chat or messaging platforms are processed through centralized servers. All the user's message or information (maybe confidential) is being processed by the central server before transmitting the same to intended recipients. The issue with these kinds of system is that all the information are visible at processing servers even if the messages or information transmitted are claimed to be end to end encrypted. The author has created a messaging or rather say a simple chat application and has explained experimentally shown how the transmitted messages are visible at processing servers. Nevertheless, the system of the centralized system has scalability issues when compared to decentralized computing systems. In this work, the author has proposed a blockchain based solution based on ethereum platform using Whisper Protocol to the issues that exist in traditional messaging or chat applications.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204062 |

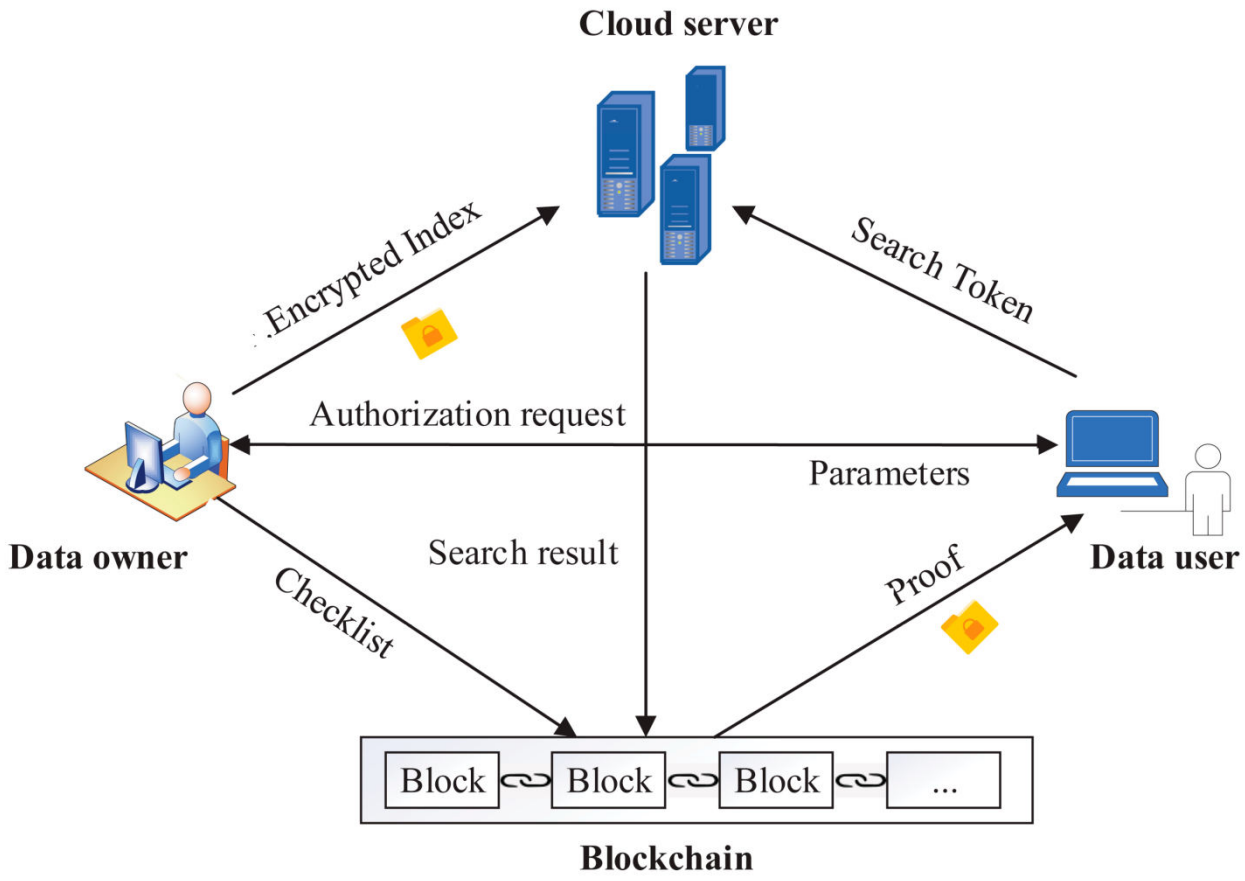

Fig 1: Block diagram

As we all know, traditional chat applications are centralized i.e., all the data is stored on a centralized server. Therefore major problem of this structure is, if the central server fails then whole network collapses. For example, WhatsApp server stored all the data on a central server, if in case that server is destroyed then there can be a loss of user data, or they can even leak the user information stored on the server.

To overcome this, our project makes the use of decentralized Application approach (dApps). In our application all the user data is stored on a block which is connected to other blocks forming a chain. As the name suggests, a decentralized application does not have a centralized server. It is basically a peer-to-peer network. Also the data that is stored in block is almost impossible to view as a very secure encryption and hashing functions (256 bits) are used. Also is a hacker tries to make changes to the information in block then, he/she will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible. Though block are on all nodes, they cannot access the information in it, only the person for whom the information if can access it.

II. LITERATURE SURVEY

Nakamoto, Satoshi [2]. In this paper, the complete mechanism of blockchain technology for a electronic cash system that basically allows online payments to be sent directly from one party to another without going through a financial institution is presented. It explains a network system which is distributed i.e. peer to peer network which resulted to be a solution for double spending and the Proof of Work algorithm for carrying out safe and secure transactions.
Judmayer, Aljosha et.al [3] presented an overview of blockchain technology in technical point of view also introduced the concepts of cryptographic currencies and the consensus ledgers. This paper mainly focused on the Bitcoin cryptographic currencies saying that the current scientific community is relatively slowly to this emerging and fast-moving field of blockchain technology reason as not sufficient resources available other than bitcoin. It explained deeply about bitcoin and why it has gained a huge market and interest in today's technology and also highlights the challenges in the area of digital assets management and presents a discussion of Bitcoin usability, privacy, and security

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204062 |

challenges from the user's perspective, the concept, characteristics, need of Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking, financial institutions.

Zibin Zheng et al. [4] provided an overview of blockchain architecture firstly and compared some typical consensus algorithms used in different blockchains. Also discussed various blockchain based applications that are covering numerous fields like financial services, reputation system, IOT so on. Furthermore, technical challenges of blockchain technology such as scalability of security problems waiting to be overcome and recent advances are briefly listed and possible future trends for blockchain.

Software has evolved from a technology tool for solving specific problems to an industry that is omnipresent in most of today's corporate activities over the previous 60 years. Software engineering is defined as "the use of a systematic, disciplined, quantifiable methodology to the development, operation, and maintenance of software; that is, the application of engineering to software," according to IEEE Standard 610.12 [10]. The Software Engineering Body of Knowledge (SWEBOK) provides a complete description of the core SE Knowledge Areas (KAs) , which are also taken into account in this research. Software requirements, software process, software testing, software quality, software maintenance, software configuration management, and engineering management are examples of knowledge areas.

A few (optional) studies have audited the utilization of blockchain, e.g., applications and shrewd agreement improvement. One of the latest orderly planning concentrates on blockchain innovations was performed.. In this review the creators mean to distinguish and plan different spaces of exploration connected with blockchain and perceive potential headings for future examination. Additionally,it led a methodical writing audit of blockchain and savvy contract advancement. Specifically, the creators identi?ed strategies, methods, apparatuses and challenges looked during the creation and testing of blockchain-arranged programming. Their examination recommends future exploration on the best way to adjust standard testing procedures to blockchain-arranged programming and how to gauge code measurements for code improvement. Both past investigations answer questions connected with the more extensive utilization of blockchain innovation, yet they don't analyze speci?cally its use in further developing SE exercises. To be sure, they didn't investigate the commitments that blockchain angles can bring to SE.Speci?cally, comparable to the use of blockchain to SE, to the best of our information, there give off an impression of being extremely restricted optional investigations. The more intently related study is a methodical planning study directed by Tariq and Colomo-Palacios]. This concentrate on wrote about the purposes of blockchain in programming and illustrated the bene?ts that this new innovation can bring to the SE ?eld. The consequences of this study demonstrate that savvy contacts can computerize the veri?cation of undertakings that normally require human-in-the circle. Shrewd agreements execute tests, produce results and naturally reward programming engineers. Also, blockchain can improve the trust between parties in rethinking programming improvement.

III. METHODS

he inherent properties of blockchain, such as decentralization, immutability, and transparency, to provide secure and private communication between users. Here's a brief description of how such a chat application might work: Decentralized Network: The chat application operates on a decentralized network, where multiple nodes (computers) participate in maintaining the network. This decentralization ensures that there's no central authority or single point of failure, making the chat application resilient and resistant to censorship or data manipulation. User Identity and Authentication: Each user has a unique digital identity, represented by a cryptographic key pair. The public key is visible to other users, allowing them to verify the identity of the message sender. Users can authenticate themselves using their private keys, ensuring that only authorized individuals can access and send messages.

Message Encryption: To ensure privacy, messages sent through the chat application are encrypted using cryptographic algorithms. Only the intended recipient possessing the corresponding private key can decrypt and read the message. This encryption protects the content of the communication from unauthorized access. Blockchain Storage: Instead of storing chat messages on a centralized server, the chat application utilizes a blockchain as a distributed ledger. Each message is treated as a transaction and added to a block. The blocks are cryptographically linked, creating an immutable chain of messages. This ensures that messages cannot be altered or tampered with once they are added to the blockchain. Message Validation: Before a message is added to the blockchain, it goes through a validation process performed by the network nodes. Consensus algorithms, such as proof-ofwork or proof-of-stake, are used to validate and agree on the order of messages, ensuring the integrity and consistency of the chat history.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204062 |

Transparency and Auditability: The blockchain's transparent nature allows users to independently verify the integrity of the chat history. Any user can access the blockchain and view the entire transaction history, ensuring trust and accountability in the communication process. Incentive Mechanism: To incentivize network participants to maintain the blockchain, a reward mechanism can be implemented. For example, in a proof-of-work system, participants who validate and add blocks to the blockchain can earn cryptocurrency as a reward, motivating them to contribute their computing power and resources.

IV. RESULT ANALYSIS

We have developed a chat application which is based on Blockchain Technology. This application runs on a local server which provide great sense of security and privacy to the users. This type of applications can be used in defence as well as by different security agency as they are always under threat of breach of internal security

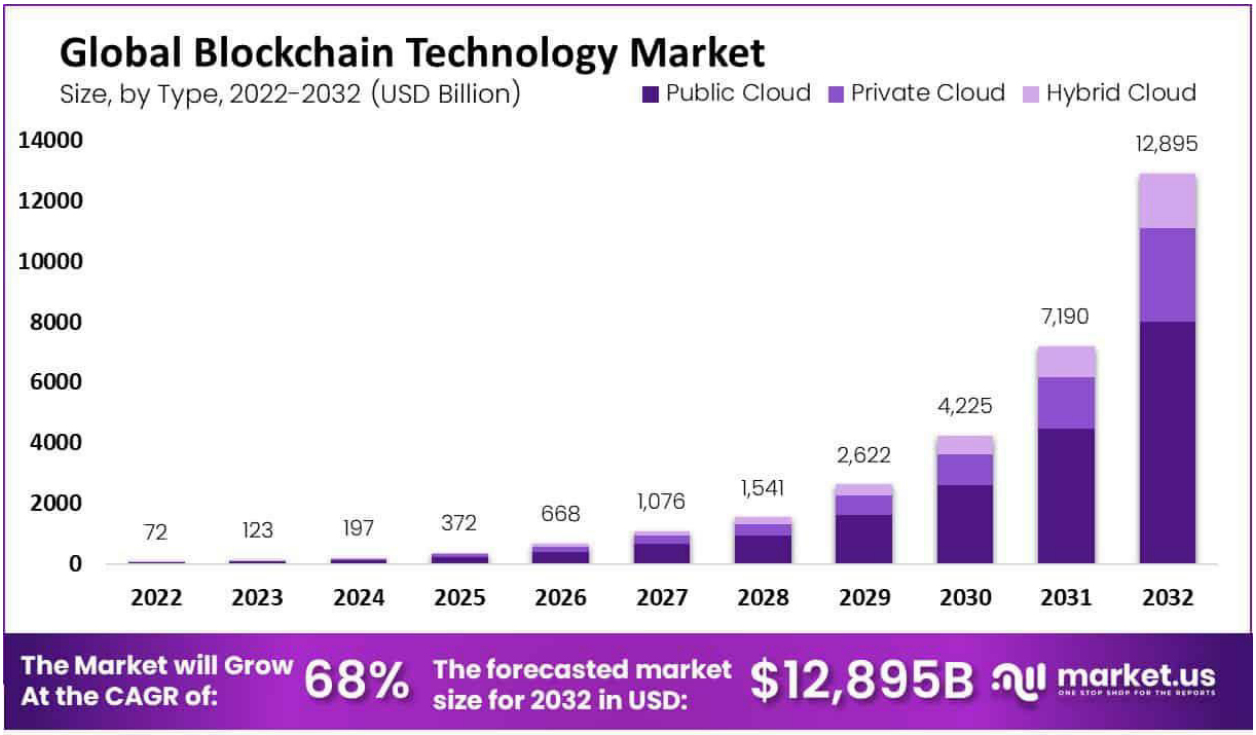

Fig 2: Result analysis

Decentralized Operation make use of peer-to-peer networks, this ensures that no network failure can do due to central node failure. Block chain serves as an unalterable ledger which allows messaging to take place in a decentralized manner. A decentralized operation for communication and resource sharing is need in present's world, where keeping data on a centralized server can be unsafe and expensive experience. With the help of various consensus, we can apply different ways to share resources and communicate. Together with Block chain and Decentralized Applications, we can produce a secure and dependable messaging application that overcomes the draw backs of traditional messaging applications. In decentralized systems, the objects at the different situations frequently differ. Each position controls only a subset of the decision variables but is affected by the opinions made at the other levels.

V. CONCLUSION

Blockchain is a powerful tool for resolving complex issues quickly. Its ability to provide security in an open environment makes it attractive for usage in a variety of other fields, including health care, IoT applications, and finance. E-commerce retailers and delivery partners can use consortium blockchains to avoid fraud during transit by continuously updating package positions on the blockchain. One of the most innovative potential uses of blockchain could be to avoid fraud in chit funds, which are used to save money in Indian society. It can also serve as a ledger for

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204062 |

disadvantaged farmers to share resources. We give a state-of-the-art survey of blockchain technology in this study. We began by discussing the background, classification, architecture, and several sorts of consensus.

REFERENCES

[1] Satoshi Nakamoto \"Bitcoin: A Peer-to-Peer Electronic Cash System.\" March 2009.
[2] Ridhanshi Bhatia, Praveen Kumar, Shilpi Bansal and Seema Rawat. \"BLOCKCHAIN –THE TECHNOLOGY OF CRYPTO CURRENCIES.\" In ICACCE-2018.
[3] XIAO FAN LIU, XIN-JIAN JIANG2, SI-HAO LIU AND CHI KONG TSE. \"Knowledge Discovery in Cryptocurrency Transactions: A Survey\". In Digital Object Identifier 10.1109/ACCESS.2021.3062652.
[4] Vaibhav Shakya, PVGN Pavan Kumar, Lakshay Tewari and Pronika. \"Blockchain based Cryptocurrency Scope in India.\" IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2. (ICICCS 2021)
[5] FAIJAN AKHTAR, JIAN PING LI, MD BELAL BIN HEYAT, SYED LUQMAN QUADRI, SHAIK SOHAIL AHMED, XIAO YUN, AMIN UL HAQ. \"POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN DIGITAL CURRENCY: A REVIEW.\" 978-1-7281-4242-5/19/$31.00 ©2019 IEEE.
[6] Suman Ghimire and Dr. Henry Selvaraj. \"A Survey on Bitcoin Cryptocurrency and its Mining.\" 978-1-5386-7834-3/18/$31.00 ©2018 IEEE
[7] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks. \"A Brief Survey of Cryptocurrency Systems.\" white paper 2016.
[8] Jae Min Kim, Jae Won Lee, Kyungsoo Lee and Junho Huh. \"Proof of Phone:A Low-cost Blockchain Platform\" Self-published.
[9] Yong Yuan and Fei-Yue Wang. \"Blockchain and Cryptocurrencies: Model, Techniques, and Applications\" 2168-2216-2018 IEEE.
[10] Wenzheng Li and Mingsheng He. \"Comparative Analysis of Bitcoin, Ethereum, and Libra\" 978-1-7281-6579-0/20/$31.00©2020 IEEE.
[11] Antea Knezevic, Zvonimir Musa and Tihana Babic. \"Cryptocurrency as the currency of the future: a case study among ALgebra University College students.\" MIPRO 2020, September 28 - October 02, 2020, Opatija, Croatia.
[12] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. \"SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies\" 2015 IEEE Symposium on Security and Privacy. DOI 10.1109/SP.2015.14.
[13] Dr. R. Raju, M. SaiVignesh and K. Infant Arun Prasad. \"A Study of Current Cryptocurrency Systems\" In 2018 INTERNATIONAL CONFERENCE ON COMPUTATION OF POWER, ENERGY, INFORMATION AND COMMUNICATION (ICCPEIC). 978-1-5386-2447-0/18/$31.00 ©2018 IEEE.
[14] CHANDRAMOULI SUBRAMANIAN,ASHA A GEORGE,ABHILASH K A AND MEENA KARTHIKEYAN.”BLOCKCHAIN TECHNOLOGY BOOK”. [15] ”ONLINE PAYMENT USING BLOCKCHAIN” RESEARCH PAPER.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

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