2023 International Conference on Advanced Computing Technologies and Applications (ICACTA)

Secure Peer-to-Peer Communication using Private Network Blockchain Technology

Mohammed Raza Syed
Dept. of Computer Engineering
Dwarkadas J. Sanghvi
College of Engineering
Mumbai, India
mohdraza.syed@gmail.com

Mihir Shinde
Dept. of Computer Engineering
Dwarkadas J. Sanghvi
College of Engineering
Mumbai, India
mihirushinde29@gmail.com

Siddharth Unny
Dept. of Computer Engineering
Dwarkadas J. Sanghvi
College of Engineering
Mumbai, India
sidunny64@gmail.com

Sahil Nair
Dept. of Computer Engineering
Dwarkadas J. Sanghvi
College of Engineering
Mumbai, India
sahilnair329@gmail.com

Ashok Patade
Dept. of Computer Engineering
Dwarkadas J. Sanghvi
College of Engineering
Mumbai, India
ashok.patade@djsce.ac.in

***Abstract*—Although centralised chat applications are frequently used in modern communication, it is becoming more obvious that they have limitations. These systems are susceptible to censorship, privacy risks, and other problems that criminals may exploit against them. Decentralised chat apps that support peer-to-peer communication and disperse data among several nodes on a private blockchain network can alleviate these problems. Customers that use these programmes enjoy more reliable, secure, and confidential communication. Using Go-Ethereum (GETH) technology, a private blockchain network is created to build smart contracts and carry out transactions. The clique consensus method is used in this study to carry out the Proof of Authority (POA) and block validation on the blockchain. By using a private network, platform managers may impose stricter rules and regulations to protect users from undesirable behaviors while also enhancing the security and privacy of users. The proposed research provides users with a safe means of communication, enhancing their experience and placing the highest value on privacy.**

Keywords—Communication, Private Network, Secure Transactions, Smart Contracts, Blockchain Technology, Proof of Authority

I. INTRODUCTION

Blockchain technology is a decentralized digital ledger that securely, openly, and impenetrably logs transactions across a network of computers. Without the use of middlemen, it enables the secure and open transfer of **digital assets** like bitcoins. The network nodes verify the transactions, which are then collected into blocks and appended to the previous chain of blocks (hence the name "blockchain"). Blockchain is a very safe and trustworthy means to store and transfer data since once a block is added to the chain, the data it contains cannot be changed.

The market value of blockchain technology [1] is predicted to reach **$60 billion** by the year **2026** because of its rising popularity. as more companies and sectors adopt blockchain technology into their daily operations and recognize its potential. The sector will continue to flourish as blockchain technology becomes more widely used and its applications broaden to cover fields like real estate, energy management, and digital identification, among others.

Data and applications are kept on a single, **central server** in centralized servers. This makes it possible to have a single point of management and control, but it also leaves the system open to a number of issues. For instance, during times of heavy demand, centralized servers may become overloaded and sluggish, making it challenging for customers to access their data. Due to the fact that all of the data is kept in one location and can be accessed by unauthorized users if the central server is compromised, centralized systems are also vulnerable to **security flaws** and hacking. In order to solve this issue, our application uses a decentralized server. Unreliant on a centralized authority, a decentralized server is a network of computers that work together to store and process data. Decentralized servers have better security and are more resistant to failures than centralized servers, which is their main advantage. Decentralized systems are less susceptible to outages and hacking attempts since there is no single point of failure. Additionally, since all transactions are recorded on a **public ledger** that is challenging to falsify, they promote **transparency** and user confidence. Decentralized servers provide a more reliable and secure solution than centralized servers by dispersing data and processing power across a network of machines

The **decentralized chat system**s that are suggested in this work have various security advantages over centralized chat applications. Decentralized chat apps allow consumers more control over their data by dispersing user data among several nodes, removing a single point of failure or attack. These apps frequently employ end-to-end encryption to further secure communication. Decentralized chat applications, therefore offer a safer and more private solution for those wishing to connect online.

In a blockchain, a **private network** is a closed, permissioned network where only authorized nodes are allowed to observe the ledger and participate in consensus. Private blockchains, as opposed to public ones like those used by Bitcoin or

979-8-3503-4834-7/23/$31.00 © 2023 IEEE

Ethereum, are managed by a single organization that controls who can access the network. Businesses and organizations that need a high level of security and privacy frequently use private blockchains because they give them more control over the network and data while still utilizing the advantages of blockchain technology.

The remaining portions of the research paper are structured as follows. In **Section II**, the Literature Survey is covered. The study's **Section III** goes into more depth about the technique employed. Results and discussions are included in **Section IV**. A conclusion and information regarding future research works are included in **Section V** and **Section VI** respectively.

II. LITERATURE SURVEY

The whole blockchain-based mechanism for an electronic cash system was provided by Satoshi Nakamoto [2] in his article, allowing internet payments to be sent directly from one party to another without passing via a banking institution. To perform risk-free and secure transactions, it describes a distributed network system, such as a peer-to-peer network, that provided a fix for double expenditure and the Proof of Work method.

R. Singh et al. [3] in his work suggested an End-to-End Encryption framework based on blockchains that can eliminate many of the current weaknesses. Any user can use a ratchet forward encryption mechanism to securely connect with another user by retrieving their certificate from the application server.

U. P. Ellewala et al. [4] provided a suggestion for a secure messaging system that employs blockchain technology to safeguard user privacy and stop message manipulation. Particularly in circumstances where privacy and security are top priorities, like in the healthcare and financial industries, the system can offer a more secure and private alternative to conventional messaging systems. The authors developed an Ethereum blockchain-based proof-of-concept application and assessed its performance and security features.

A decentralised application for communication and resource sharing is required in today's environment, according to Abhishek Takale et al. [5]. Decentralised applications are immune from network failures that can result from central node failure since they employ peer-to-peer networks. Therefore, the shortcomings of conventional messaging applications are overcome by using blockchain-based decentralised applications.

Sourabh et al. [6] explained security concerns of sending messages over insecure channels. Even encrypted messages can be attacked by methods like Eavesdropping, MITM, EFAIL, etc. They made a decentralized system for users to exchange messages securely using blockchain. Major focus was on people who live in countries like China and South Korea, who are being constantly tracked and monitored by their government for what they are chatting and sharing.

Judmayer, Aljosha et al. [7] discussed the use of blockchain technology as a consensus ledger and cryptographic currency, and the difficulties associated with managing digital assets. They also discussed the usability, privacy, and security of Bitcoin, as well as the idea, traits, and necessity of the blockchain, and how it functions. The article aims to showcase the influence of blockchain on how banks and other financial institutions will operate in the future.

Wang, H. et al. [8] suggested that messages are stored on a distributed ledger, and their confidentiality and integrity are protected using cryptographic methods. The model also includes a reputation system that grades users' trust based on their actions, and this rating is then used to decide how much access they have to the network. A simulation is used to test the concept, and the findings indicate that it offers an effective and secure instant messaging solution.

The above-discussed articles offer an understanding of the prospect of blockchain technology for producing secure and decentralized messaging systems. Nonetheless, there is an absence of information on how to execute and enlarge such systems. Many authors have constructed proof-of-concept applications while others have concentrated on the need for decentralized messaging and the security issues of current systems. Moreover, there is no agreement on the most reliable cryptographic techniques to guard user privacy and stop message alteration.

III. PROPOSED METHODOLOGY

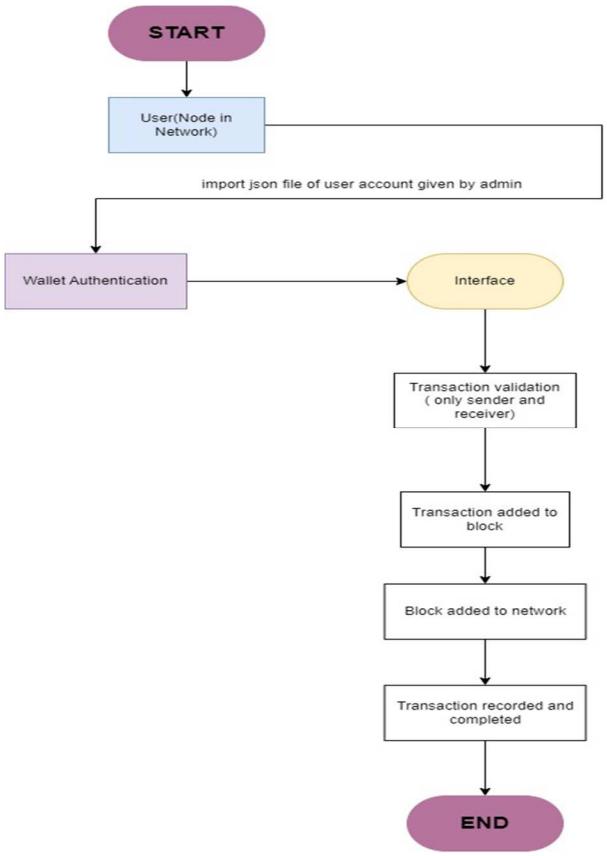

Fig. 1. Workflow of Proposed Methodology

For messaging and communication, a user must import the JSON file for their account that was issued by the administrator of the private network to use the messaging platform for the first time. This user will now be able to carry out transactions and send messages to the receiver following

the authentication of the user's account wallet using the metamask wallet in the browser.

A. The transaction flow of the private network is as follows:

- Only the sender and recipient will validate the transaction when a user sends a message to the requested account address, as opposed to all nodes (users) doing so as in the case of a public blockchain.
- Following validation, the transaction is hashed to the block, which is then connected to all preceding blocks in the chain.
- As a result, the transaction process is finished, and the transaction data are safely recorded and saved in the block.

B. Tech Stack Utilized:

In this study, the tech stack listed below has been used to implement and assess our proposed approach.

- **ReactJS:** ReactJS offers Web3 packages to integrate the smart contracts deployed on a private network into the proposed solution and make it usable for end users as shown in Fig. 2.
- **Go-Ethereum (GETH):** An Ethereum client created in Go is called Geth or Go-Ethereum [9]. Go-Ethereum is used to construct and maintain private blockchain networks.
- **Solidity:** Solidity is used as the programming language for creating smart contracts in Ethereum and integrating it into the blockchain network.
- **Remix:** Remix is used as a tool for effective deployment smart contracts and testing their functionality.

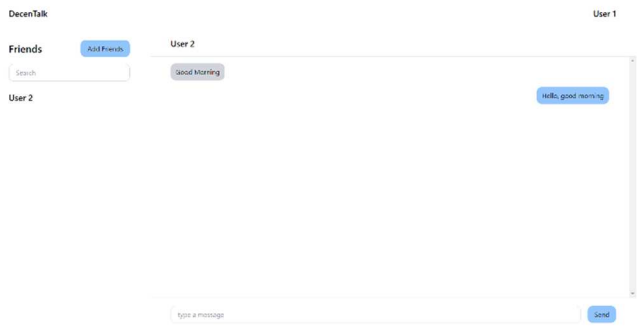

Fig. 2. User Interface

C. The Private Network creation in Blockchain:

This study uses the **Go-Ethereum** (GETH) technology to build a private network. Go-Ethereum is an Ethereum execution client that is used to build and administer private networks. To communicate with the Ethereum network, it uses the command-line interface. It also manages transactions, the deployment and execution of smart contracts, and it has an essential element called the **Ethereum Virtual Machine** (EVM), which oversees carrying out smart contract execution and keeping track of the network's state.

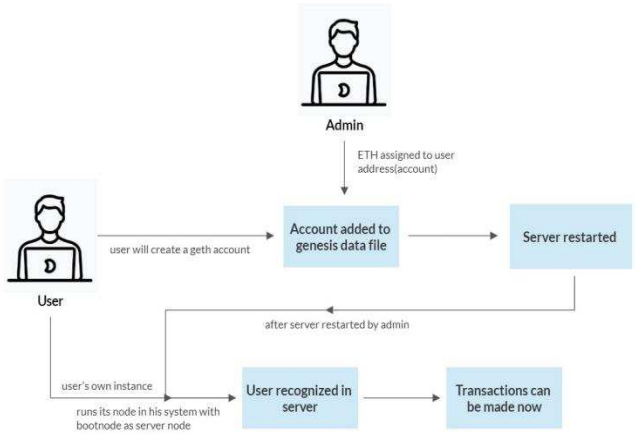

Fig. 3. Architecture of the Private Network

This work then employs the clique consensus technique given by the GETH client to increase the security of the network where the administrator may control the status of the accounts on the network. **Clique** consensus [10] is a Proof of Authority (PoA) mechanism in which only authorized 'signers' can produce new blocks. In EIP-225, the clique consensus protocol is described. The genesis block configures the first list of authorised signers in our study, just one signer, administrator.

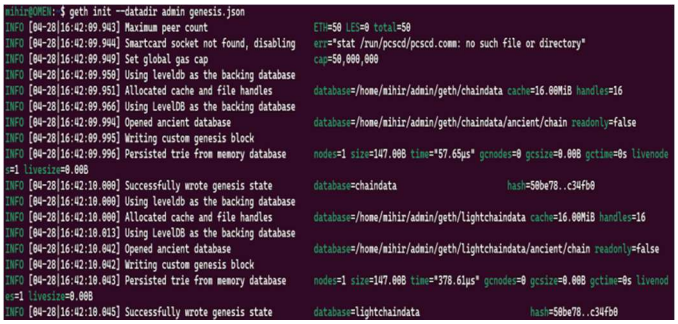

Fig. 4. Geth Initialization

A genesis file, the first block in the private network, is created after the consensus method, and it contains the network's initial configuration and parameters, including the network ID, the chain's configuration, the consensus algorithm, the initial account balances, and, in the case of a PoA consensus mechanism, a list of authorized signers.

D. Connecting Smart Contracts with the Private Network:

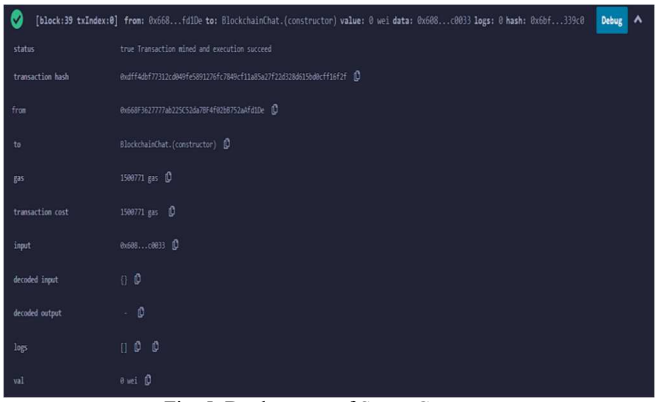

Fig. 5. Deployment of Smart Contract

After the genesis file creation in the first block, Remix, an Integrated Development Environment (IDE), is used to connect and deploy the smart contracts written in the Solidity programming language to the private network as shown in Fig. 5. This smart contract includes features like user creation, user address addition, and message sending and receiving in Fig. 6. For maintaining the security and integrity of the data, it also includes cryptographic functions.

Fig. 6. Smart Contract

IV. RESULTS

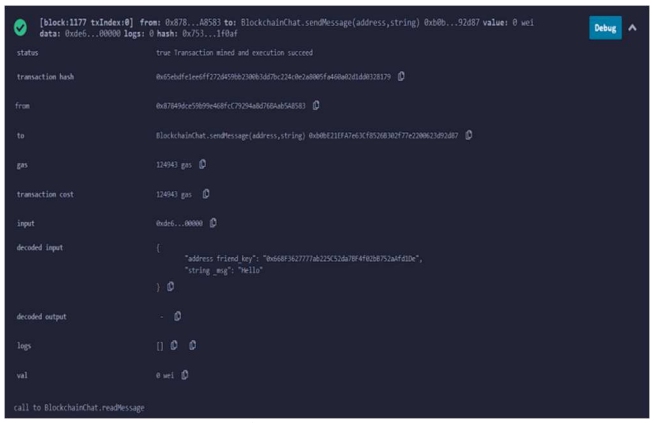

Fig. 7. Message Sent

The message transaction is completed successfully. Using the recipient's public address, the message is encoded and delivered to that address using Clique Consensus Algorithm for integrity and authorization. A transaction hash is also generated, and a small gas price is charged for the message transaction as shown in Fig. 7.

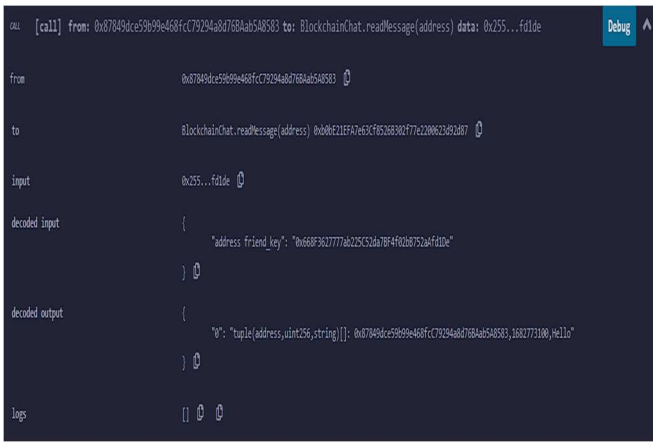

Fig 8. Message Received

The message is obtained on the receiving end by activating the read message feature. The decoded message, along with additional metadata, is contained in the received data. The message can be successfully viewed by the user as shown in Fig. 8. So, using a private network, the sender and receiver can communicate securely and safely.

A. Comparative Analysis of Gas Fee:

TABLE I. COMPARISON OF GAS FEES

Function	Private Network (In Wei)	Public Network (In Wei)
Creation of an Account	45923	52826
Adding an Account	123146	187618
Sending Message	92937	129890

Table I compares the gas costs for three crucial operations—creating an account, adding an account, and sending messages—between a Private Network and a Public Network. The Private Network consistently costs less for gas than the Public Network. The Private Network charges a gas fee for the creation of an account of 45,923 Wei, whereas the Public Network charges a fee of 52826 Wei. Similar to this, the Private Network records a gas fee for Adding an Account of 123146 Wei whereas the Public Network records a higher fee of 187618 Wei. The Private Network excels once more in terms of Sending Messages with a fee of 92937 Wei, while the Public Network charges a higher fee of 129890 Wei. These results obtained demonstrate the efficiency and cost-effectiveness of using a Private Network for secure peer-to-peer communication, as it utilizes lower gas fees for several crucial tasks.

The results achieved have some limitations, such as the network's maintenance becoming difficult as it expands and its user base rises, its reliance on an internet connection, and its current lack of features, which can be improved as stated in **Section VI** of future scope.

V. CONCLUSION

Data privacy is one of the most crucial issues in the modern technology sector because there are millions of user data breaches or hacks that happen each year while people are communicating. This study proposes a safe, secure mode of communication that makes use of blockchain's features. Through this platform, users' private information is securely stored in the nodes of the blockchain's private network, helping to increase users' privacy and anonymity and allowing only the administrator of the private network to manage them. Additionally, it employed cryptographic hashing algorithms to encrypt data, rendering it impossible for other users to access or modify users' private information.

VI. FUTURE SCOPE

Future research work will concentrate on the creation of channels for group messaging where users can communicate while maintaining their anonymity. Additionally, sharing of multimedia data, including photographs, videos, and audios, will be a focus. Additionally, it will be centred on user-to-

user payments, doing away with the need for third-party payment providers.

ACKNOWLEDGEMENT

Authors would like to extend their gratitude to our mentor at Dwarkadas J. Sanghvi College of Engineering for their constant guidance and an opportunity to showcase our work.

REFERENCES

[1] IDC, “The Blockchain Market at a Glance,” IDC Blogs, 14 October 2020. [Online]. Available: https://blogs.idc.com/2020/10/14/the-blockchain-market-at-a-glance/. [Accessed 1 March 2023].

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, *Decentralized business review*, 2008.

[3] R. Singh, Ark Nandan Singh Chauhan and H. Tewari, "Blockchain-enabled end-to-end encryption for instant messaging applications," *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM),* pp. 501-506, 2022, doi: 10.48550/arXiv.2104.08494.

[4] U. P. Ellewala, W. D. H. U. Amarasena, H. S. Lakmali, L. M. K. Senanayaka and A. N. Senarathne, "Secure messaging platform based on blockchain," *2020 2nd International Conference on Advancements in Computing (ICAC),* vol. I, pp. 317-322, 2020, doi: 10.1109/ICAC51239.2020.9357306

[5] A. P. Takale, C. V. Vaidya and S. S. Kolekar, "Decentralized Chat Application using Blockchain Technology," *International Journal for Research in Engineering Application & Management (IJREAM),* vol. IV, pp. 92-94, 2018.

[6] S. D. Rawat, K. Kapkoti, S. Aggarwal and A. Khanna, "bChat: A Decentralized Chat Application," *International Research Journal of Engineering and Technology (IJRET),* vol. VII, no. 5, pp. 2775-2780, May 2020.

[7] X. F. Liu, X.-J. Jiang, S.-H. Liu and C. K. Tse, "Knowledge discovery in cryptocurrency transactions: A survey," *IEEE Access,* vol. IX, pp. 37229-37254, 2021, doi: 10.1109/ACCESS.2021.3062652

[8] H. Wang, Y. Yu, J. Zhao and J. Wang, "Blockchain-Based Trusted Instant Messaging Model Research," *2021 4th International Conference on Hot Information-Centric Networking (HotICN),* pp. 32-37, 2021, doi: 10.1109/HotICN53262.2021.9680848

[9] Ethereum, "Welcome to go-ethereum," Go-Ethereum, [Online]. Available: https://geth.ethereum.org/docs. [Accessed 31 March 2023].

[10] P. Szilágyi, "EIP-225: Clique proof-of-authority consensus protocol," Ethereum Improvement Proposals, 6 March 2017. [Online]. Available: https://eips.ethereum.org/EIPS/eip-225. [Accessed 20 April 2023].