A Survey Paper On Secured Communication App

Dr. S Satish Kumar
Prof, Dept of ISE
RNSIT,
Bengaluru, India

R Tushar
Dept. of ISE,
RNSIT,
Bengaluru, India

Pranath P
Dept. of ISE,
RNSIT,
Bengaluru, India

Prajwal D
Dept. of ISE,
RNSIT,
Bengaluru, India

Prajwal M
Dept. of ISE,
RNSIT,
Bengaluru, India

Abstract: ***One of the main problems that most firms encounter is defining the lines between personal and commercial communications. The use of risky and insecure applications at work presents significant security threats. Businesses don't know enough about the apps that are installed on the devices of their employees. The protection of messages and shared files becomes problematic when it comes to crucial business communications involving the sharing of trade secrets, company referrals, and important business decisions. There are cross-industry system hazards because the majority of publicly accessible communication platforms do not give enterprises the ability to control, monitor, and scale their communication as well as comply with data protection laws. Because of this, when utilizing instant messaging apps, both individuals and corporations voice serious concerns regarding data security and privacy protection.***

Keywords: *Block chain, Ethereum, Smart Contract, Cryptocurrency.*

I.INTRODUCTION

Blockchain is a shared, unchangeable ledger that makes it easier to track assets and record transactions in a network of businesses. Similar to traditional public, it is a series of blocks that together include a complete list of transaction data.

Blockchain is an effective tool for swiftly and efficiently resolving complicated problems. Its capacity to offer security in an open setting makes it appealing for use in a range of different industries, such as finance, health care, and Internet of Things applications. By regularly updating package positions on the blockchain, consortium blockchain help e-commerce businesses and delivery partners prevent fraud during transit.
This kind of distributed ledger technology (DLT) records transactions using a hash, an unchangeable cryptographic signature.

Because blockchain technology stores information on an immutable ledger that only authorized network users can access, it offers instantaneous, shareable, and fully transparent information. A blockchain network has the ability to monitor accounts, production, payments, orders, and much more. Additionally, you can see every aspect of a transaction from beginning to end because all members have access to the same version of the truth. This gives you increased trust as well as additional opportunities and efficiencies. Blockchains, like Ethereum and Bitcoin, are constantly expanding due to the addition of new blocks, which greatly strengthens the ledger's security.

Conventional chat programmers are centralized, meaning that all of the data is kept on one server. Thus, the main issue with this arrangement is that the entire network collapses if the central server fails. The WhatsApp server, for instance, kept all of its user data on a single central server. Should that server go down, user data may be lost, or the server could potentially leak user data.

II.LITERATURE SURVEY

2.1"Act natural!": Having a Private Chat on a Public Blockchain[1]

Conventional chat programmers are centralised, meaning that all of the data is kept on one server. Thus, the main issue with this arrangement is that the entire network collapses if the central server fails. The WhatsApp server, for instance, kept all of its user data on a single central server. Should that server go down, user data may be lost, or the server could potentially leak user data.

2.2 Take Back your Friends with DCS: A Decentralized Connectivity Service for private social communication apps[2]

The Decentralised Connectivity Service (DCS), a blockchain-based connectivity service for distributed social communication applications that protects privacy, is presented in this study. Through point-to-point connections made possible by DCS, users regain control over their interactions with other users and can do so without the assistance of a centralised party. Another step in assisting individuals in reclaiming their online identities is DCS.

2.3 Brain-Computer Interaction and Silent Speech Recognition on Decentralized Messaging Applications[3]

This research intends to present an alternate approach to human-computer interaction that supports the aforementioned individuals by using surface electrodes for electromyography and an electroencephalography headset for text input and application navigation, respectively. Data security and communication availability can be guaranteed by doing away with the centralised method.

2.4 Applications of Blockchain Technology beyond Cryptocurrency [6]

The technology known as Blockchain (BC), which powers the Bitcoin cryptocurrency system, is noted for being both enticing and essential for guaranteeing improved security and (in certain cases, untraceable) privacy for a wide range of applications in numerous other domains, such as the Internet of Things (IoT) ecosystem.

***2.5 A Decentralized Approach to Messaging Using Blockchain Technology* [4]**

This article aimed to analyze the inefficiencies of the conventional centrally managed messaging apps and use Ethereum smart contracts in a secure and trustless decentralized application to remedy such issues. Some of the future approaches include adding features like uploading photos and videos, creating personalised chat groups, and investigating a brand-new blockchain messaging system called Whisper.

***2.6 A Decentralized Application for Secure Messaging in a Trustless Environment*[5]**

The proof-of-concept for the suggested system, a safe and anonymous decentralised messaging software, was constructed utilising the Ethereum platform and the Whisper protocol. Even when there is an adversary in control of a majority of the network, the application may send end-to-end encrypted messages while guaranteeing the anonymity of both the sender and the recipient. One area where the application might be expanded for future work is the ability to retrieve messages anonymously while offline.

III. EXISTING RECOGNITION SYSTEMS

3.1Status (Status.im):

Status is a mobile browser and open-source messaging platform made specifically for interacting with Ethereum blockchain decentralised apps, or DApps. Users can access decentralised services, send and receive cryptocurrency, and communicate. An open-source mobile application called Status acts as a decentralised browser and messaging service for Ethereum DApps.Users can engage with decentralised apps, send and receive cryptocurrency, and communicate. constructed on the Ethereum network.

3.2 Raiden Network (Raiden):

Although Raiden's main focus is on Ethereum off-chain scaling solutions, it also includes decentralized communication components. It makes quick and inexpensive transactions possible, making micropayments in chat applications one possible usage for it. Raiden Network features components for decentralized communication, but its main goal is to provide Ethereum with off-chain scaling options. allows for quick and inexpensive transactions, making it suitable for small-scale transactions inside chat apps. Built with an emphasis on off-chain scaling on Ethereum.

3.3 BeeChat (BeeChat): A decentralised messenger based on the Ethereum blockchain is called BeeChat uses blockchain technology to decentralise messaging in order to offer private and secure communication. Constructed using the Ethereum network.

3.4 Tox(Tox.chat): Tox is a decentralised, safe messaging app that is worth mentioning even if it isn't specifically based on blockchain technology. Without the need for a central server, it allows users to communicate directly over a peer-to-peer network. Tox is a safe and decentralised *texting app. makes use of a peer-to*-peer network, enabling direct user communication independent of a central server. peer-to-peer online; notdependent on blockchain technology specifically. Although Raiden's main focus is on Ethereum off-chain scaling solutions, it also includes decentralised communication components. It makes quick and inexpensive transactions possible, making micropayments in chat applications one possible usage for it. Raiden Network features components for decentralised communication, but its main goal is to provide Ethereum with off-chain scaling options. allows for quick and inexpensive transactions, making microtransactions possible.

IV.PROPOSED SYSTEM

In order to create a decentralized chat application with blockchain technology, specifically on Ethereum and the Avalanche network, smart contracts for user identification, message storage, and transactions must be created on Ethereum. Decentralized identity solutions are used for user authentication, allowing users to keep ownership of their private keys for safe access. For effective and safe communication, an off-chain messaging protocol with end-to-end encryption is put into place. User interaction with smart contracts and decentralized storage options, such as IPFS for message storage, are all part of the integration with the Ethereum blockchain. Bridges are created to interface with the Avalanche network and take use of its quicker consensus mechanism in order to improve transaction speed.

V.RESULTS & DISCUSSIONS

Figure 1.0 shows hardhat setting up the environment for the chat application. It is initializing different account with their private key to identify unique users.

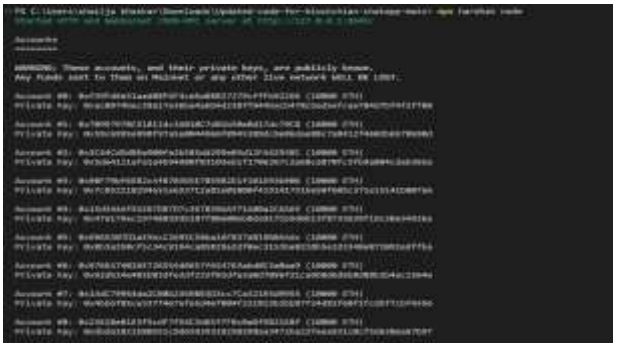

Figure1.0 - hardhat setup

Figure 1.1 shows the smart contract that is written in solidity language is running on the terminal in order to verify the message that is supposed to be sent or received.

Figure 1.1 – Smart contract

Figure 1.2 – Metamask Wallet

Figure 1.2 displays the metamask wallet. A complete transaction history of all the messages sent and received on the test network is shown in the wallet interface. Users may effortlessly monitor the message flow, guaranteeing accountability and openness in their communication endeavours. By offering a concise summary of message exchanges, this feature improves user experience and encourages more structured and knowledgeable communication within the decentralised chat programme.

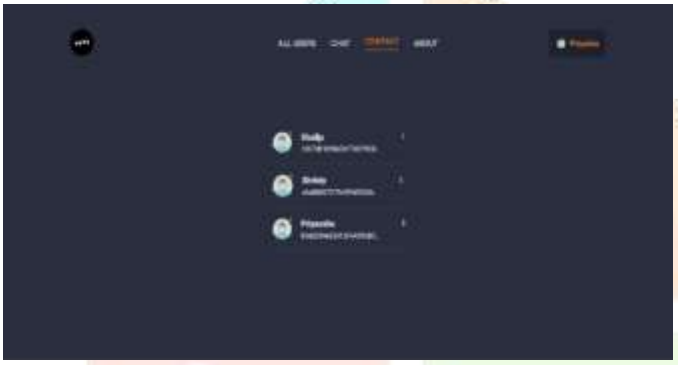

Figure 1.3 – Display of friends to user

Figure 1.3 shows the different friend for a user. Within the decentralized chat application, users can send and receive buddy invitations. Accepting a friend request creates a link between the two users that is necessary to start a conversation.

Figure 1.4 – Friend Request

Figure 1.4 shows the different friend for a user. Users have the option to send and receive friend invitations within the chat application. The first step in starting a conversation with another user is to become friends by accepting each other's friend requests. By putting privacy and consent first and limiting communication to approved connections, this strategy gives consumers a safe and customised talking experience.

VI. DATA FLOW DIAGRAM

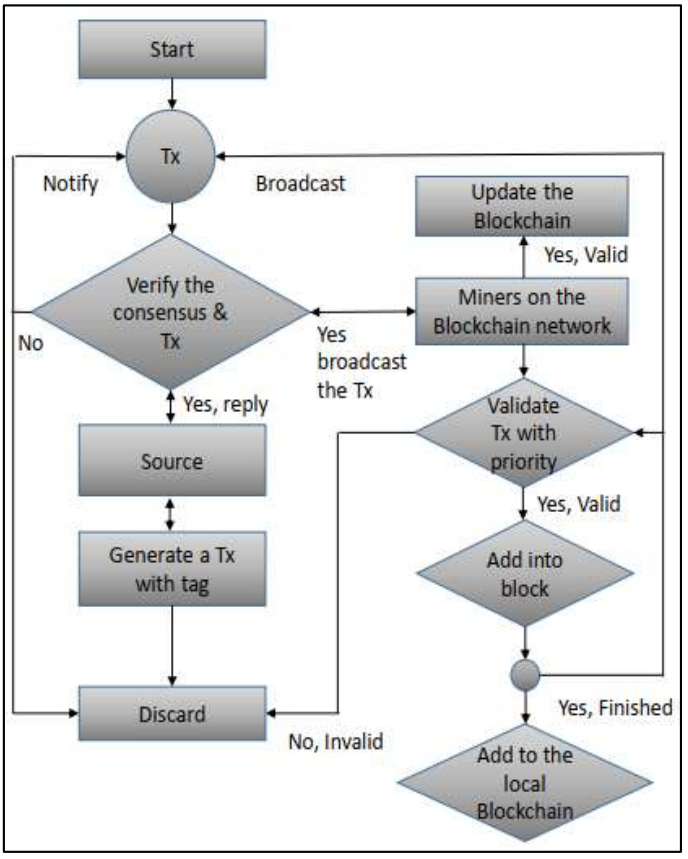

Figure 1.5 Data flow diagram

A data-flow diagram shows how data moves through a system or process (typically an information system). Information regarding each entity's inputs and outputs as well as the process itself are also provided by the DFD. There is no control flow, no decision rules, and no loops in a data-flow diagram. A flowchart, as seen in figure, can represent particular operations based on the data.

VII. CONCLUSION

This project introduces the Decentralized Connectivity Service, a blockchain-based, privacy-preserving connectivity solution for dispersed social apps like chat and VoIP. With DCS, users can communicate with each other point-to-point without relying on a centralized third party. By severing a user's contacts list from their use of social media, DCS reclaims control over their connections with other people—a vital aspect of their identity—from outside parties and returns it to them. DCS is seen as an additional measure to assist users in regaining their online identities.

An application that efficiently utilizes blockchain technology is currently under development. Blockchain has demonstrated its ability to change established industries.

VIII. FUTURE ENHANCEMENT

Block chains can be used to offer cryptographic authentication, which makes sure that only authorized users are sending and receiving messages.

• Encrypted Messaging: To guarantee that communications are sent safely and remain private, a blockchain-based chat program may also employ cutting-edge encryption techniques.

• Micropayments: To encourage users to engage with the network, give back to the community, and preserve the messaging platform's integrity, a blockchain-based may employ micropayments.

Since block chains save more storage, implementing other apps may be an opportunity to experiment with various scalabilities in terms of the chat application's performance and flexibility.
• This could reveal a few obstacles in creating and maintaining security-based chat applications.
Task automation can be used, and teamwork features can be improved.
• By implementing interoperability, chat apps can enable users to communicate with each other without requiring a wallet connection.

IX. REFERENCES

[1]"Act natural!": Having a Private Chat on a Public Blockchain, Thore Tiemann, Sebastian Berndt, Thomas Eisenbarth, Maciej Li´skiewicz, Cryptology ePrint Archive, 2021
[2] Take Back your Friends with DCS: A Decentralized Connectivity Service for private social communication apps, Christos Aslanoglou, Michalis Konstantopoulos, Nikos Chondros, Mema Roussopoulos, In 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (pp. 133-138), IEEE, 2020
[3] Brain-Computer Interaction and Silent Speech Recognition on Decentralized Messaging Applications, Luís Arteiro, Fábio Lourenço, Paula Escudeiro & Carlos Ferreira, In International Conference on Human-Computer Interaction (pp. 3-11). Springer, Cham, 2020
[4] Decentralized Chat Application using Blockchain Technology, Abhishek P. Takale, Chaitanya V. Vaidya, Suresh S. Kolekar, 3rd National Conference on "Changing Technology and Rural Development", 2018
[5] A Decentralized Application for Secure Messaging in a Trustless Environment, Mohamed Abdulaziz, Davut Culha, Ali Yazici, In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 1-5), IEEE, 2018
[6] Applications of Blockchain Technology beyond Cryptocurrency, Mahdi H. Miraz, Maaruf Ali, arXiv preprint arXiv:1801.03528, 2018