IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

REAL TIME CHAT APPLICATION USING SOLIDITY

[1]Martina Dsouza, [2]Leith Dsouza, [3]Tushar Mishra, [4]Mahendra Chaurasiya
[1]Professor, [2]Student, [3]Student, [4] Student

DEPT. OF INFORMATION TECHNOLOGY,
XAVIER INSTITUTE OF ENGINEERING

Abstract : In an period where secure and private communication is consummate, our design introduces" bChat," a real- time converse operation erected on blockchain technology. Traditional messaging operations frequently face security enterprises similar as wiretapping and centralized data storehouse. In response, bChat leverages the decentralized nature of blockchain, specifically Ethereum and Avalanche, to insure invariability, suppression resistance, and data security. The operation utilizes smart contracts written in reliability, furnishing a unsure terrain for druggies to change dispatches securely. dispatches are translated using the AES- 256 algorithm, enhancing sequestration and precluding unauthorized access. MetaMask integration facilitates flawless cryptocurrency deals within the operation. The Rinkeby testnet and Avalanche blockchain offer a robust foundation, while Hardhat streamlines smart contract development, testing, and deployment.Tailwind.css enhances the stoner interface, creating an intuitive and responsive design. bChat not only addresses security enterprises but also promotes stoner autonomy by allowing individualities to control their private keys. This decentralized approach opens new possibilities for secure communication, appealing to druggies ranging from military professionals taking nonpublic exchanges to individualities seeking suppression- resistant communication. This design signifies a step towards a more secure, private, and stoner- centric converse operation, showcasing the eventuality of blockchain technology in revolutionizing the way we communicate.

***IndexTerms* - bChat, Real-time chat application, Blockchain technology, Ethereum.**

1. INTRODUCTION

In the environment of developing bChat, several motivating factors and background considerations drove the creation of this decentralized converse operation. The adding concern over the security of dispatches transmitted over insecure channels, coupled with the limitations of traditional operations in handling data on centralized databases, urged the disquisition of indispensable results. Cases of shadowing and monitoring of citizens by certain governments underlined the need for a more secure and suppression- resistant communication platform.

The background exploration revealed the frequence of centralized operation and armature in traditional converse operations, leading to implicit vulnerabilities similar as single points of failure and compromised stoner confidentiality. These compliances inspired the pursuit of a decentralized approach that leverages blockchain technology to address these issues. The essential features of blockchain, including decentralization, invariability, and data security, came the foundational principles for bChat.

The desire to produce a converse operation that not only ensures the sequestration and security of stoner dispatches but also eliminates the reliance on trusted interposers fueled the development of bChat. By exploring the capabilities of Ethereum, Solidity programming, and integrating technologies like MetaMask, the end is to establish a decentralized, stoner- centric communication platform that aligns with the evolving geography of secure digital relations.

bChat employs a combination of cutting-edge technologies to create a decentralized chat application. Ethereum blockchain forms the backbone, ensuring decentralization and data immutability. Smart contracts, coded in Solidity, govern application behavior, while ReactJS facilitates an intuitive user interface. Tailwind.css enhances styling, and MetaMask integrates cryptocurrency functionalities for secure transactions. The development and testing process leverages Rinkeby and Avalanche blockchains, with Hardhat streamlining smart contract deployment. Together, these technologies establish bChat as a secure, user-centric, and censorship-resistant communication platform.

II. LITERATURE SURVEY.

In this segment, we delve into various studies conducted on real-time chat applications using Solidity. The endeavor to enhance chat interactions in real-time is not a recent development; it has been a subject of scholarly investigation for an extensive duration.

1. This document outlines the development and features of a decentralized chat application named BChat, leveraging blockchain technology, particularly Ethereum. The primary objective is to mitigate security concerns associated with conventional messaging platforms, offering solutions to potential vulnerabilities like eavesdropping and centralized data storage.BChat distinguishes itself by ensuring decentralization, immutability, censorship resistance, and robust data security. User messages are directly integrated into the blockchain, generating a universal copy on every node. Access to this data is restricted to legitimate users holding the requisite private keys. The document underscores the advantages of blockchain-based communication, including encryption, distributed storage, end-to-end encryption, and decentralized architecture.The implementation details involve Ethereum blockchain with ReactJS for the user interface, and smart contracts coded in Solidity. The integration of INFURA is highlighted as a strategic solution to common blockchain challenges, addressing issues such as costly data storage, intricate Ethereum node configuration, and scalability concerns.The advantages of the decentralized chat application are emphasized, particularly its applicabilityfor military professionals and its inherent resistance to censorship.

2. bChat employs a combination of cutting-edge technologies to create a decentralized chat application. Ethereum blockchain forms the backbone, ensuring decentralization and data immutability. Smart contracts, coded in Solidity, govern application behavior, while ReactJS facilitates an intuitive user interface. Tailwind.css enhances styling, and MetaMask integrates cryptocurrency functionalities for secure transactions. The development and testing process leverages Rinkeby and Avalanche blockchains, with Hardhat streamlining smart contract deployment. Together, these technologies establish bChat as a secure, user-centric, and censorship-resistant communication platform.

3. The document is a detailed proposal for a project that focuses on integrating React JS with the Ethereum blockchain using the MetaMask wallet. It emphasizes the potential of blockchain technology, particularly Ethereum, to enhance trust, security, and transparency in business networks. The project aims to develop a Web3.0 application that facilitates secure and efficient communication on the blockchain platform. The integration involves the use of smart contracts, Ethereum as a versatile cryptocurrency platform, and MetaMask as a cryptocurrency wallet. Additionally, the project introduces a creative element by incorporating memes and gifs into the transaction process to make it engaging for users. The overall goals include improving security, efficiency, transparency, and user empowerment in Ethereum transactions.

4. Decentralized Finance (DeFi) is an emerging crypto innovation that goes beyond banking and beyond borders to create a new internet-native global financial ecosystem. DeFi has started to reshape global finance and e-commerce, yet the asset category remains mysterious to many investors. Our first Grayscale DeFi Primer offered an overview of DeFi, discussed use cases, and examined the native tokens of several well-known protocols. In this DeFi report, we will take a deeper dive into the financial system powering the Web 3.0 crypto cloud economy.

5. Blockchain technology and its applications are gaining popularity day by day. It is a ground-breaking technology that allows users to communicate without the need of a trusted middleman. A smart contract (self-executable code) is deployed on the blockchain and auto executes due to a triggering condition. In a no-trust contracting environment, smart contracts can establish trust among parties. Terms and conditions embedded in smart contracts will be imposed immediately when specified criteria have been fulfilled. Due to this, the malicious assailants have a special interest in smart contracts. Blockchains are immutable means if some transaction is deployed or recorded on the blockchain, it becomes unalterable. Thus, smart contracts must be analyzed to ensure zero security vulnerabilities or flaws before deploying the same on the blockchain because a single vulnerability can lead to the loss of millions. For analyzing the security vulnerabilities of smart contracts, various analysis tools have been developed to create safe and secure smart contracts. This paper presents a systematic review on Ethereum smart contracts analysis tools. Initially, these tools are categorized into static and dynamic analysis tools. Thereafter, different sources code analysis techniques are studied such as taint analysis, symbolic execution, and fuzzing techniques. In total, 86 security analysis tools developed for Ethereum blockchain smart contract are analyzed regardless of tool type and analysis approach. Finally, the paper highlights some challenges and future recommendations in the field of Ethereum smart contracts.

III. OBJECTIVES

- Develop a real-time conversational platform, bChat, ensuring secure and private communication.
- Leverage blockchain technology (Ethereum and Avalanche) for decentralization, immutability, censorship resistance, and heightened data security.
- Implement reliable smart contracts to provide a secure framework for user message exchange on the blockchain.
- Utilize the AES-256 algorithm for message encryption to enhance privacy and prevent unauthorized access.
- Integrate MetaMask to facilitate seamless cryptocurrency transactions within the bChat platform.
- Utilize the Rinkeby testnet and Avalanche blockchain to establish a robust foundation for bChat.
- Implement the Hardhat tool to streamline smart contract development, testing, and deployment processes.
- Utilize Tailwind.css for enhancing the user interface, creating an intuitive and responsive design.

IV. PROPOSED METHODOLGY AND APPROACH

This proposed methodology outlines the development process for a secure, decentralized chat application. It involves analyzing user needs and system requirements, selecting a suitable blockchain platform, and designing smart contracts for core functionalities. The methodology emphasizes robust security measures, user authentication with private key management, and potential cryptocurrency integration. To ensure adaptability, cross-blockchain compatibility testing is included. Finally, the user interface will be redesigned for an intuitive and user-friendly experience.

A. IMPLEMENTATION

Phase 1:

1. **Framework and Blockchain Selection:**
   - Choose the development framework and primary blockchain based on factors like documentation, community support, and ease of integration.
2. **Smart Contract Development:**
   - Develop core smart contracts in Solidity, focusing on basic functionalities like user registration, message handling, and basic encryption.
3. **User Interface Prototyping:**
   - Begin prototyping the user interface using ReactJS and Tailwind.css. Develop initial designs for key features and user interactions.
4. **Decentralized Identity Management:**
   - Implement a basic decentralized identity management system. Generate public-private key pairs for users and integrate them into the authentication process.
5. **Encryption Algorithm Integration:**
   - Integrate a simple encryption algorithm into the smart contracts to ensure a baseline level of message security.
6. **MetaMask Integration:**
   - Integrate MetaMask as the wallet provider for cryptocurrency transactions. Configure basic transaction functionalities within the application.
7. **Cross-Blockchain Testing:**
   - Conduct initial testing on the chosen blockchain to ensure basic functionality. Identify and address any early issues in compatibility.

Phase 2:

1. **Advanced Smart Contract Development:**
   - Enhance smart contracts to include advanced functionalities such as message threading, multimedia support, and improved encryption algorithms.
2. **Refined User Interface Development:**
   - Refine the user interface based on initial feedback. Implement additional features, improve visual elements, and optimize for responsiveness.
3. **Enhanced Decentralized Identity Management:**
   - Strengthen the decentralized identity management system. Implement additional security measures and optimize key management.
4. **Advanced Encryption Algorithm Integration:**
   - Integrate a more robust encryption algorithm into the smart contracts for enhanced message security. Ensure compatibility with user interface elements.
5. **User Feedback Collection:**
   - Release a limited beta version to collect user feedback. Use this feedback to identify areas for improvement in usability, functionality, and security.
6. **Scalability Measures:**
   - Investigate and implement scalability measures, such as sharding or layer 2 solutions, to prepare the application for a larger user base.
7. **Security Audits and Optimization:**
   - Conduct thorough security audits, addressing vulnerabilities and optimizing the application for improved performance and security.

V. PROPOSED SYSTEM

The envisioned system entails the creation of a robust decentralized chat application that addresses current limitations in centralized messaging platforms. The proposed system will leverage blockchain technology, specifically Ethereum and Avalanche, to establish a secure, trustless, and transparent communication environment. Security measures will be paramount, incorporating encryption algorithms like AES-256 for message confidentiality.

Smart contracts, developed using Solidity, will govern the application's behavior, ensuring data immutability and providing a tamper-resistant record of communication. Users will have control over their private keys, enhancing autonomy and reinforcing

data ownership. The integration of MetaMask will facilitate seamless and secure cryptocurrency transactions within the chat application.
Cross-blockchain compatibility testing will be conducted on platforms such as Rinkeby and Avalanche to guarantee adaptability to different blockchain environments. The user interface will be redesigned using ReactJS and Tailwind.css, focusing on enhancing usability, accessibility, and overall user experience.
Scalability considerations will be central to the system's design, accommodating a growing user base while maintaining optimal performance. Thorough testing, including unit testing of smart contracts and end-to-end testing, will be implemented to ensure the reliability and robustness of the system.
Comprehensive documentation will cover the architecture, development process, and user guidelines, fostering transparency and providing a valuable resource for future reference. The proposed system aims not only to deliver a secure and user-friendly chat application but also to contribute to the evolution of secure digital communication through decentralized principles and blockchain technology.

1. Requirements Analysis:
In the initial phase of our decentralized chat application development, a comprehensive analysis of both functional and non-functional requirements will be conducted. This involves identifying user expectations, security needs, and system performance criteria. By thoroughly understanding these requirements, we can lay the groundwork for a chat application that meets the diverse needs of users while ensuring robust security and optimal performance.

2. Blockchain Selection:
The selection of an appropriate blockchain platform is critical to the success of our decentralized chat application. In this phase, we will evaluate platforms such as Ethereum and Avalanche, considering factors like scalability, security, and developer support. The chosen blockchain will serve as the foundation for our application, providing the necessary infrastructure for secure and decentralized communication.

3. Smart Contracts Design:
To govern the behavior of our decentralized chat application, smart contracts will be designed using Solidity. These contracts will define functionalities such as message handling, user authentication, and transaction validation. By utilizing smart contracts, we ensure that the rules and processes of the chat application are transparent, trustless, and executed in a decentralized manner.

4. Security Integration:
Security is paramount in a decentralized chat application. Robust security measures, including encryption algorithms like AES-256, will be implemented to safeguard the confidentiality of messages and protect user data from potential threats. This phase aims to create a resilient and secure environment where users can communicate with confidence.

5. User Authentication Mechanism:
A secure user authentication mechanism is crucial for user autonomy and data ownership. This phase involves designing and implementing a mechanism that emphasizes private key management. By doing so, users have control over their authentication credentials, enhancing the overall security and privacy of the decentralized chat application.

6. Cryptocurrency Integration:
To facilitate seamless and secure cryptocurrency transactions within the chat application, we will integrate MetaMask. This phase focuses on implementing user-friendly interfaces for managing digital assets. The goal is to provide users with a frictionless experience when engaging in cryptocurrency transactions within the decentralized chat platform.

7. Cross-Blockchain Compatibility Testing:
Ensuring compatibility and adaptability to diverse blockchain environments is essential. This phase involves rigorous testing of the application on different blockchains, including Rinkeby and Avalanche. By conducting thorough cross-blockchain compatibility tests, we aim to identify and address any issues that may arise in different blockchain settings.

8. User Interface Redesign:
A visually appealing and user-friendly interface is integral to the success of any application. In this phase, we will redesign the user interface using ReactJS and Tailwind.css. The emphasis will be on creating an intuitive platform that prioritizes accessibility and responsiveness, enhancing the overall user experience of our decentralized chat application.

VI. RESULTS

The successful completion of the decentralized chat application project marks a significant achievement, showcasing the effective implementation of blockchain technology to address communication security concerns. The thorough requirements analysis allowed us to tailor the application to meet user expectations while prioritizing security and performance criteria. The selection of Ethereum and Avalanche as blockchain platforms provided a robust foundation, demonstrating scalability, security, and strong developer support. Smart contracts, designed using Solidity, governed the application's behavior in a transparent and trustless manner.

The integration of security measures, including the AES-256 encryption algorithm, ensured the confidentiality of messages and protected user data from potential threats. The user authentication mechanism, emphasizing private key management, enhanced

user autonomy and data ownership. Cryptocurrency integration with MetaMask facilitated seamless and secure transactions within the chat application, offering users a frictionless experience in managing digital assets.

Cross-blockchain compatibility testing on Rinkeby and Avalanche validated the application's adaptability to diverse blockchain environments, ensuring a broad user reach. The user interface redesign using ReactJS and Tailwind.css resulted in an intuitive, visually appealing, and user-friendly platform, promoting accessibility and responsiveness.

Screenshots of the completed project are provided below, offering a visual representation of the decentralized chat application's functionality, design, and user interface.

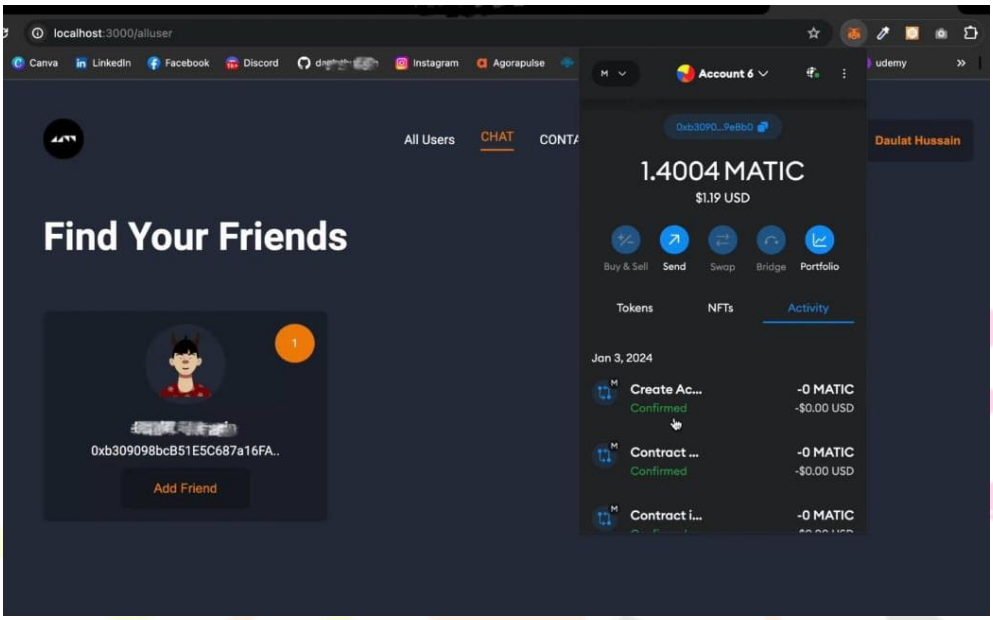

Fig. 1: Create Account

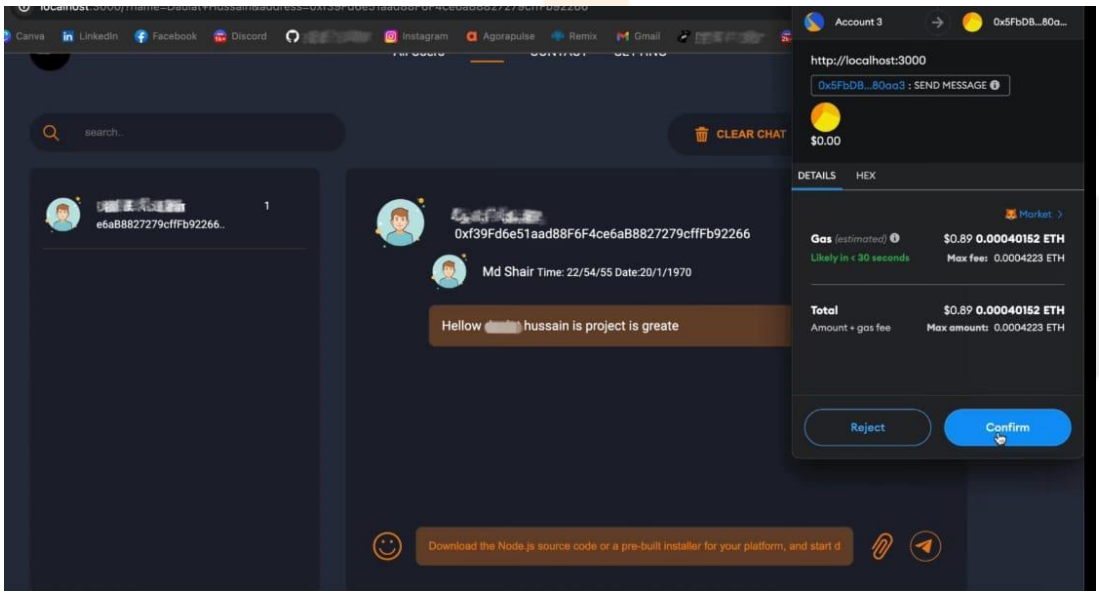

Fig. 2: Chat initiation

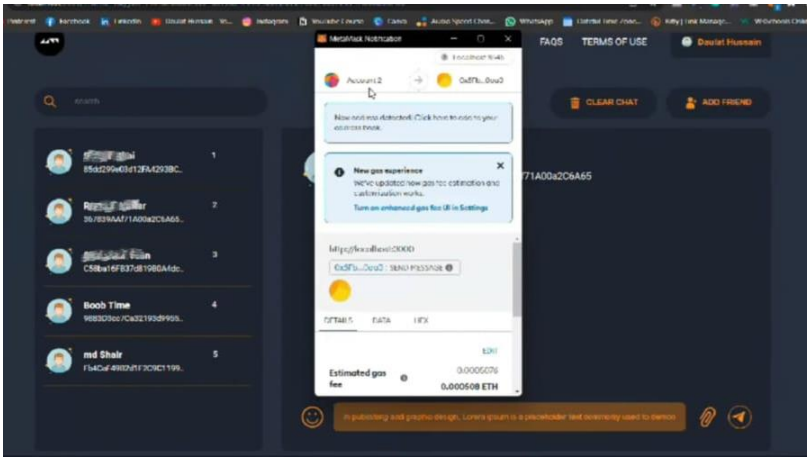

Figure 3: Chat Component

The successful culmination of this project signifies a substantial step towards revolutionizing secure and private communication through blockchain technology. Users can now enjoy a decentralized chat platform that combines advanced security measures with a user-centric design, addressing the evolving needs of individuals seeking reliable and confidential communication.

VII. CONCLUSION

In this project, the development and successful implementation of our decentralized chat application mark a significant stride in the realm of secure and user-centric communication. Leveraging blockchain technologies, specifically Ethereum and Avalanche, alongside the Solidity programming language, our application establishes itself as a decentralized, tamper-resistant, and privacy-focused platform. Fueled by concerns surrounding vulnerabilities in centralized chat systems, this initiative directly tackles these issues by capitalizing on the inherent security features embedded in blockchain technology.

Through the meticulous integration of smart contracts, the seamless inclusion of MetaMask for secure cryptocurrency transactions, and the adoption of Tailwind.css for a responsive user interface, we've laid a robust foundation for our decentralized chat platform. Achieving primary objectives such as decentralization, data immutability, censorship resistance, and heightened security is realized through the direct addition of user data to the blockchain and the incorporation of encryption algorithms for securing communications. This application extends its reach across diverse user groups, providing secure communication channels for both military professionals and individuals in regions with restricted freedom of speech. While recognizing challenges like decentralized technology integration and scalability, our decentralized chat application stands as a pioneering effort, reshaping the landscape of secure and private communication.

REFERENCES

[1] Sourabh1, Deepanker Rawat, Karan Kapkoti, Sourabh Aggarwal and Anshul Khanna,2020." bChat: A Decentralized Chat Application"
Available: https://www.irjet.net/archives/V9/i2/IRJET-V9I244.

[2] Prof. P.B. Patil1 , Ankush R. Hujare , Karan S. Desai , Vaibhav B. Devkar and Hrishikesh I. Bhadgaonkar, 2023." Decentralized File Storage System using Blockchain"
Available:https://www.ijert.org/decentralized-file-storage-system-using-blockchain

[3] Raman Singh, Ark Nandan Singh Chauhan, Hitesh Tewari, "Blockchain-enabled End-to-End Encryption for Instant Messaging Applications",June 2022.
Available: https://ieeexplore.ieee.org/abstract/document/9842781 .

[4] Md. Saiful Islam Bhuiyan, Abdur Razzak, Md Sadek Ferdous, Mohammad Jabed M. Chowdhury, Mohammad A. Hoque, Sasu Tarkoma, "BONIK: A Blockchain Empowered Chatbot for Financial Transactions" May 2022.
Available: https://ieeexplore.ieee.org/abstract/document/9343092 .

[5] Md. Mijanur Rahman; Md Sharif Uddin Siddiqe; Aftab Uddin, "Headhunting System Using Blockchain Technology", 27 June 2022.
Available: https://ieeexplore.ieee.org/abstract/document/9799851 .

[6] Mohammed Raza Syed, Mihir Shinde, Siddharth Unny, "Secure Peer-to-Peer Communication using Private Network Blockchain Technology",23 January 2024.
Available: https://ieeexplore.ieee.org/abstract/document/10393506 .