ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

Decentralized Messaging Web Application: A Blockchain-Based Approach for Secure Communication

[1] Venkat Jayaram Vikram, [2] Mittal Abhinav Krishna, [3] Jashwanth Kumar Reddy, [4] Goutham Senthil Kumar, [5] Ashwin Balaji, [6] Mariappan R

[1] [2] [3] [4] [5] [6] School of Computer Science and Engineering Vellore Institute of Technology, Vellore Vellore, Tamil Nadu, India

Corresponding Author Email: [1] venkatjayaram.vikram2020@vitstudent.ac.in, [2] abhinavkrishna.mittal2020@vitstudent.ac.in, [3] middijashwanth.kumar2020@vitstudent.ac.in, [4] gouthamsenthil.kumar2020@vitstudent.ac.in, [5] ashwin.balaji2020@vitstudent.ac.in, [6] mariappan.r@vit.ac.in

Abstract*— Messaging is one of the most popular modes of communication in the modern world. But centralized messaging applications like WhatsApp and WeChat have many flaws. Blockchain as a distributed ledger technology has become widely popular in the past decade. Its ability to maintain integrity, confidentiality and availability of data has caused its rise to popularity. Using these blockchain features to our favor, we have created a decentralized messaging web application which is safe, reliable and secure, to overcome the shortcomings of centralized messaging applications. Decentralized web Applications (DApps) like ours, are a relatively new development in the blockchain sector which make use of the peer-to-peer nature of blockchain and ensure availability of the application in case of partial failures. The immutable nature of blockchain allows us to send, receive and store messages in a decentralized environment. Decentralization also allows us to ensure reliable and secure communication at relatively lower costs.

Index Terms*— Messaging, Centralized, Decentralized, Blockchain, Distributed ledger technology, Integrity, Confidentiality, Availability, Decentralized Applications (DApps), Peer-to-peer, Immutable, Reliability, Security, Lower costs.

I. INTRODUCTION

Lung disease is common throughout Centralized messaging applications have long dominated the digital communication landscape, offering convenience and connectivity to billions of users worldwide. However, beneath the surface lies a plethora of vulnerabilities and shortcomings that compromise the very essence of privacy, security, and user autonomy. When users engage with centralized systems, they

relinquish control to a single central authority, placing implicit trust in its operations and governance. Unlike democratic processes where individuals exercise agency through voting, users of centralized messaging platforms do not influence the entity dictating their digital interactions.

The repercussions of this trust deficit are profound, particu- larly concerning privacy and security in private messaging. Centralized servers present lucrative targets for malicious actors seeking unauthorized access to sensitive user data, perpetuating the constant threat of breaches and intrusions. Furthermore, the centralized nature of these systems renders them susceptible to censorship, with the central authority wielding unchecked power to silence dissenting voices or comply with external pressures.

Moreover, the fragility of centralized infrastructure exposes users to systemic risks, where the failure or compromise of a primary server can cascade into widespread service disruptions. Natural disasters, power outages, or software vul- nerabilities can swiftly incapacitate entire networks, disrupting communication channels and undermining user reliability.

Recent history bears witness to the devastating conse- quences of centralized system failures, from the February 2017 AWS server outage that crippled major platforms like Trello, Quora, and IFTTT, to the September 2019 server collapses that temporarily brought down behemoths like Facebook and Instagram. These incidents underscore the urgent need for a paradigm shift in digital communication, one that embraces decentralization as a fundamental tenet of resilience, security, and user empowerment.

II. RELATED WORK

M. Mohan et al. [1] advocate for decentralized applications (DApps) utilizing blockchain technology to address risks as- sociated with centralized data storage in applications. Their proposed approach emphasizes data security and integrity through a peer-to-peer network, leveraging blockchain's im- mutable ledger for secure and cost-effective communication. Additionally, the paper introduces a novel method to en- hance instant messaging security by integrating blockchain with Elliptic Curve Diffie-Hellman for End-to-End Encryption, showcasing the feasibility and effectiveness of this approach through evaluation. Furthermore, a secure chat application using blockchain is detailed, highlighting

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

enhanced security features such as OTP authentication and secret keys, with a comparative analysis validating the efficacy of the proposed OTP system.

Pansara et al. [2] propose a groundbreaking method to bolster instant messaging security by integrating blockchain technology with Elliptic Curve Diffie-Hellman for End-to-End Encryption. This innovative approach harnesses the decentralized and secure characteristics of blockchain networks, synergising them with the robust key agreement capabilities of Elliptic Curve Diffie-Hellman. The paper likely includes an evaluation of the proposed solution, showcasing its feasibility and effectiveness through a comprehensive assessment of implementation.

Ellewala et al. [3] introduce a secure chat application powered by blockchain technology, meticulously detailing its requirements, architecture, methodologies, and implementation technologies. The registration process, encompassing secret keys, OTP authentication, and passcodes, underscores their commitment to robust security measures. Through rigorous research and minor modifications, they validate the technical feasibility of their approach, while highlighting the application's enhanced security features, including a comparative analysis of the OTP system. This paper stands as a significant contribution, shedding light on the fusion of blockchain and secure communication systems.

Menegay et al. [4] present a pioneering endeavor in crafting a secure communication infrastructure utilizing blockchain technology. Their work encompasses the development of email, chat, and a Multiple Independent Peer Review (MIPR) application, all integrated within the blockchain framework. Leveraging blockchain's inherent security, email messages are routed through established protocols, while web-based and IRC chat applications are built on Steem and BitShares blockchains. Through meticulous integration of web services and robust encryption mechanisms, the study showcases the feasibility of their approach, marking a significant stride in the realm of secure communication systems.

Mirko Franco et al. [5] undertake a crucial endeavor aimed at mitigating the non-consensual sharing of private

self-generated content to promote safer online communities. Their research delves into technological interventions, with a particular emphasis on decentralized architectures, as promising avenues for addressing this issue. The methodology likely entails an exhaustive review of existing technologies, a meticulous analysis of their applicability in combating non-consensual sharing, and potentially the proposition or evaluation of specific decentralized frameworks. This study represents a significant contribution to the ongoing efforts to enhance online safety and privacy.

Sea´n Durban's work [6] encapsulates a comprehensive review of existing literature addressing privacy and security concerns in digital communication. The study conducts an in-depth analysis of the technical specifications of the Whisper protocol, likely supplemented with simulations or hypothetical scenarios to evaluate its functionality and performance. However, the research may be constrained by the absence of empirical validation through real-world user testing or deployment, potentially limiting its applicability to practical scenarios. Nonetheless, this study contributes valuable insights to the discourse on enhancing privacy and security in digital communication systems.

Matthew Weidner et al. [7] embark on a comprehensive research journey comprising several key stages. Initially, they conduct an exhaustive review of existing methodologies in group messaging, encryption, and decentralized networks. Subsequently, they design a novel decentralized group key agreement (DCGKA) protocol tailored for secure group messaging, emphasizing scalability and robustness. Rigorous anal- ysis and formal verification techniques are then employed to ensure the protocol's security properties. Following this, a practical implementation of the DCGKA protocol is devel- oped, leveraging contemporary software engineering practices and blockchain technology where applicable. Finally, the protocol's efficiency and effectiveness are evaluated through rigorous testing protocols, and the findings are meticulously documented and presented in a cohesive paper, providing com- prehensive insights into its design, analysis, implementation, and performance evaluation.

Tian Min et al. [8] embark on a methodical investiga- tion, commencing with the meticulous collection of pub- lic Ethereum blockchain data, spanning user addresses and transaction records. Subsequently, they process this data, converting hexadecimal addresses into readable application names and categorizing users based on their DApp usage patterns. Employing unsupervised clustering techniques, the team then delves into behavioral analysis, discerning distinct user groups and studying their interactions within DApps. Furthermore, the researchers scrutinize the correlation between user behavior and external factors like ETH prices or market trends. Their study culminates in practical demonstrations of their data mining findings, showcasing applications such as anomaly detection or recommendation systems tailored for DApp ecosystems. Ultimately, in their conclusion and recommendations, they underline the importance of continued research into human behaviors within decentralized ecosys-tems to bolster DApp development and foster growth in the broader Metaverse landscape.

Chirag Jani et al. [9] embark on a comprehensive journey aimed at addressing the prevalent issues of misinformation in educational settings and the limitations of centralized digital messaging platforms. Their endeavor begins with a meticulous needs assessment to grasp the nuances of these challenges. Subsequently, they design and implement a decentralized messaging application (DMApp) on a blockchain framework, prioritizing tamper-resistant and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

secure communication chan- nels. Authentication mechanisms are then developed to restrict access to authorized users from educational institutions, en- suring the integrity of information shared within the DMApp. The integration of provenance features enables the tracking of information origin and history, leveraging blockchain's decentralized nature for transparency. Through rigorous testing and validation procedures, the team evaluates the DMApp's security, authenticity, and resilience against various potential threats. Finally, user experience evaluation, conducted through feedback collection and testing scenarios, offers insights into the DMApp's usability and effectiveness within educational environments.

K. Khalkar et al. [10] embark on a systematic exploration to meet the demand for secure and decentralized communication and resource sharing, diverging from the constraints posed by centralized systems. Their endeavor commences with a comprehensive requirement analysis to discern the necessi- ties of decentralized solutions. Subsequently, they undertake the design and development of a decentralized application prototype, ingeniously integrating blockchain technology for messaging and resource sharing functionalities. The explo- ration extends to the implementation of diverse consensus mechanisms to enhance the efficiency of resource sharing and communication within the application. Rigorous security and reliability testing protocols are then employed to assess the application's robustness against conventional centralized messaging systems. Finally, the team meticulously documents their findings and presents the advantages of their decentral- ized application, elucidating its prowess in overcoming the limitations of traditional messaging platforms.

R. A. Sarıtekin et al. [11] introduce Cryptouch, a pioneering communication application engineered to harness the capabil- ities of a distributed system model by seamlessly integrating blockchain and IPFS technologies. Tailored to meet the com- munication needs of enterprises, Cryptouch endeavors to fur- nish a secure and decentralized communication environment. Offering an array of features including private messaging, file sharing, video meetings, and announcements, Cryptouch operates within an organization's private network, ensuring confidentiality and integrity. Leveraging blockchain for times- tamping and transaction recording, and IPFS for storing vast amounts of data such as messages and files, Cryptouch embod- ies a robust infrastructure. The planned development involves employing Hyperledger Fabric and Meteor for the backend, while the frontend will encompass web, Android, and iOS applications, ensuring accessibility across various platforms.

Enhanced security measures, including cryptographic tech- niques like asymmetric encryption, underscore Cryptouch's commitment to safeguarding sensitive communications.

Abdulaziz et al. [12] delve into the development of a decentralized messaging application employing the Ethereum Whisper protocol. The article outlines a methodology focused on harnessing blockchain technology to uphold fundamental principles of data integrity, confidentiality, and availability. Central to the application's design is its deployment on the Ethereum platform, leveraging the innate decentralization and adaptability of the Whisper protocol. Through this approach, the researchers aim to create a messaging platform that ensures secure and reliable communication in decentralized environ- ments.

Gonza´lez et al. [13] undertook a comprehensive examination of security challenges inherent in decentralized, blockchain- based messaging systems. Through their analysis, common risks including DDoS attacks, spam, and phishing were iden- tified, prompting the proposal of mitigation strategies such as proof of work algorithms and reputation systems. The paper underscores the significance of establishing a secure infrastructure and prioritizing user education to foster threat awareness. By addressing these challenges and advocating for robust security measures, the authors aim to enhance the resilience and reliability of decentralized messaging systems in the face of evolving threats.

Gebhardt et al. [14] offer a conceptual investigation into decentralized instant messaging systems, highlighting the prominence of peer-to-peer networks for facilitating direct communication among users. Their methodology entails a thorough examination of the benefits, notably privacy and security enhancements, alongside tackling pertinent challenges such as scalability and interoperability. The conclusion drawn from their analysis underscores the imperative for meticulous design considerations to optimize the efficacy and widespread adoption of decentralized messaging systems. By addressing these aspects, the authors aim to contribute to the evolution of messaging infrastructures towards more decentralized and resilient models.

Weidner et al. [15] recognized the necessity for decen- tralized secure group messaging and proceeded to devise a protocol to address this requirement. The implementation likely entailed leveraging elliptic curve cryptography to bolster message security and thwart potential attacks. Subsequent testing and validation procedures were likely conducted to ascertain the protocol's effectiveness in furnishing robust security measures for group communication. Through their endeavors, the authors aim to contribute to the advancement of decentralized messaging systems by providing a secure and reliable protocol for group messaging scenarios.

Aitzhan et al. [16] engineered a solution amalgamating multi-signatures, blockchain technology, and anonymous mes- saging. The development process likely encompassed imple- mentation and rigorous testing to validate the efficacy of the approach. Evaluation metrics were likely defined to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

meticu- lously assess the performance of the solution, ensuring its

viability and effectiveness in real-world scenarios. Through their research efforts, the authors aim to contribute to the advancement of secure and privacy-preserving communication systems by leveraging innovative technologies and robust cryptographic techniques.

III. METHODOLOGY

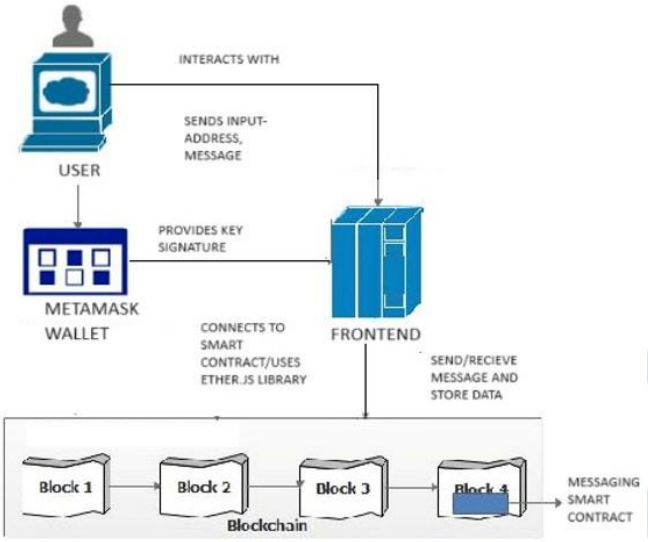

Fig. 1. Architecture Diagram of Decentralized Messaging Web Application

The proposed system delineates a decentralized messaging web application, designed to mitigate the inherent limitations of centralized counterparts while harnessing the transforma- tive potential of blockchain technology. Unlike traditional messaging applications, which rely on centralized backend infrastructure for operation, our system diverges at the core architecture, particularly in the backend implementation.

On the hardware front, traditional applications typically rely on a singular server or a limited set of servers, each tasked with distinct operational functions. In contrast, our system leverages a network of computer nodes, collectively perform- ing similar operational tasks. Whereas popular applications like WhatsApp segregate their backend functions between application and database servers, our system consolidates both application services and data storage onto a unified set of de- vices. The scalability of this infrastructure is contingent upon the blockchain network hosting our decentralized application (DApp), accommodating potentially vast numbers of devices. At the software level, our application is constructed en- tirely from smart contracts, utilizing Solidity's rich feature set including mappings and functions for data storage and retrieval. React components interface with the application smart contract deployed on the blockchain network through the ethers.js library. Leveraging the ethers.contract() function, React components initiate calls to the smart contract, estab- lishing connections through the connect() function using the user's public key address. This process mirrors the familiar paradigm of API calls in traditional applications, where React

interfaces with backend functionality via axios. Through this mechanism, users interact with the application by accessing functions embedded within the smart contract, facilitating seamless communication within a decentralized framework.

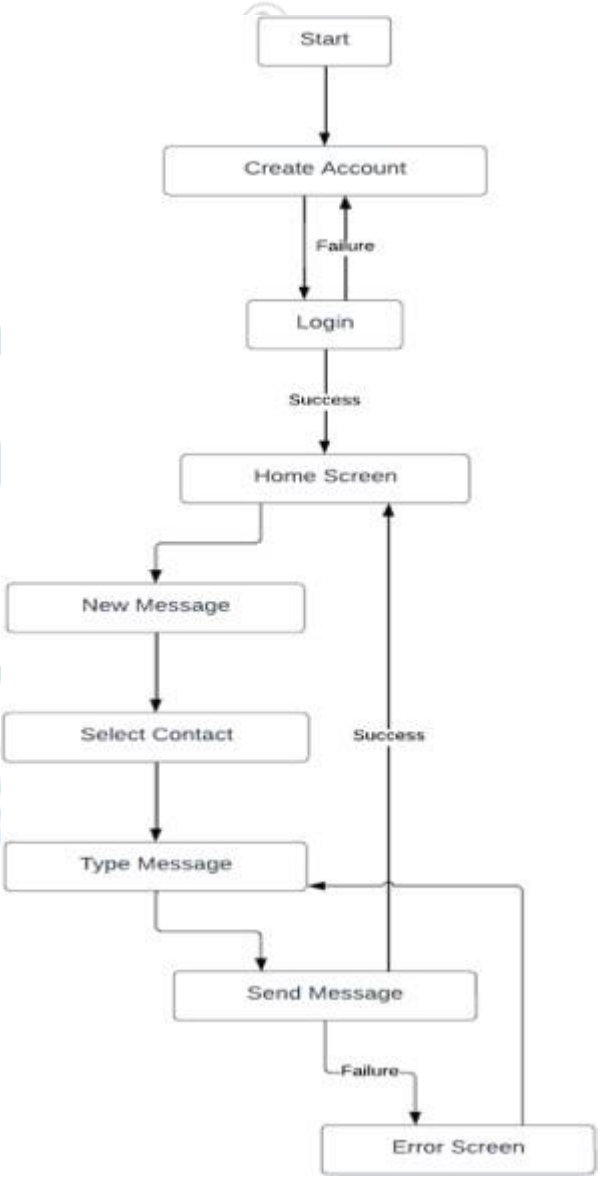

Fig. 2. Flowchart of the functionality

IV. SYSTEM MODULES

A. User Interface

The user interface is constructed using fundamental web technologies including HTML, CSS, and the React framework. It features event-driven triggers and handlers that invoke functions responsible for interfacing with smart contracts to execute the application's business logic.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

B. Login/User Registration

Initiating the login process triggers specific functions within the smart contract, namely RegisterUser and checkUserRegis-

tration. The checkUserRegistration function validates whether the user's public key address is stored in the smart contract. Upon verification, the RegisterUser function adds the user's public key to the smart contract's storage data, utilizing a mapping data structure to store user key addresses.

C. Inbox/View

Following successful registration or login, users are presented with their inbox messages. Utilizing a mapping data structure and user-defined struct, the smart contract maps all messages to the recipient's address. The Inbox View function within the smart contract iterates through the inbox mapping variable, retrieving relevant messages to be dynamically displayed on the frontend using the Document Object Model (DOM).

D. Message Send

This module comprises the sendMessage function within the smart contract, the Inbox Mapping variable, and the sendMessage event function in the React frontend. Users are provided with fields to input the recipient's address and message content. Upon sending, the message is associated with the recipient's address in the inbox mapping variable, facilitating message delivery.

E. User Wallet

An online wallet, such as MetaMask, serves as the repository for the user's key pair and facilitates the digital signing of transactions related to the user's actions on the messaging ap- plication. This enables the authentication and recording of user activities on the Ethereum blockchain, ensuring transparency and security.

Table I: Cia Model for the Web App

Security Component	Objective Met
Confidentiality	The Web App uses SHA-256 to hash the messages in order to provide confidentiality. The user registration only uses an address on the blockchain to enhance privacy.
Integrity	Integrity is assured through cryptographic verification mechanisms for message authenticity and tamper resistance.
Availability	The web app is reliable and available due to utilizing the blockchain and routing the messages to random set of nodes

collect data from a conversation, the attacker would have to hack and gain access to most nodes on the network as the routing of data changes periodically and is much more difficult than just hacking into a central server.

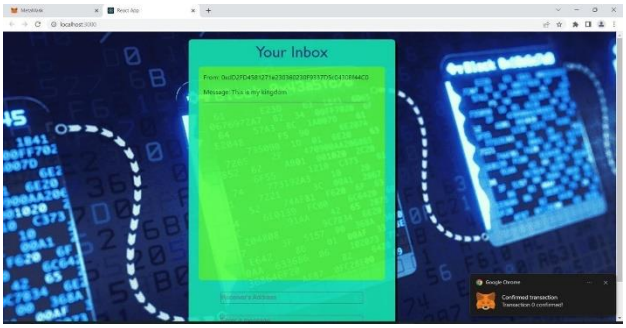

Fig. 3. Demo of the Web Application.

V. RESULTS AND DISCUSSION

A. System Impementation

In the implementation of our research project, the Hardhat environment played a pivotal role in both the development and testing phases of our application. Hardhat stands out as a comprehensive development toolkit tailored specifically for Ethereum software. Within this environment, various components are dedicated to essential tasks such as editing, compiling, debugging, and deploying smart contracts and decentralized applications (dApps). Table 1. details how the web app ensures security using the CIA model. Through seamless integration, Hardhat provides a cohesive and unified development ecosystem, streamlining the process of crafting Ethereum-based solutions. Fig. 3 shows the User Interface and a working demo of the Web Application.

B. Discussion

The Peer-to-Peer Messaging DApp send messages by routing them through a random set of nodes. These set of nodes changes periodically, so a malicious node can only listen to a tiny fraction of the entire conversation. DApps are trust less because the blockchain guarantees anonymity and security without needing to trust other nodes or a central authority. To

The application makes it impossible for third parties to pry user information, because in a fully decentralized system, the entity which created the network does not have the capability to collect that information without the appropriate key signature. This application is highly available as compared to popular chat applications. This is because the application logic in our solution is served by thousands of computers nodes instead of a single server where a single point failure could occur.Moreover,the application is censorship-resistant by design. There is no central authority that makes decisions on which users can access the application – so there is no chance of an individual, group of users or entire countries being blocked or banned from accessing data or censorship of the data. Centralized applications can never be trusted to be fully safe from censorship, secure or private, since code is not tamper proof and the logic of the code is never transparent.

VI. FUTURE WORK

In future iterations of the project, the focus will be on

augmenting the exception handling mechanisms within the application to effectively manage anomalies in user behavior. This enhancement aims to fortify the application's resilience against unexpected scenarios, thereby bolstering its robustness and reliability in real-world usage scenarios.

Furthermore, efforts will be directed towards expanding the maximum message size allowable within the application. Currently capped at 32 bytes, this limitation imposes constraints on the richness and complexity of communication that users can engage in. By exploring methods to increase this limit, the objective is to enable users to transmit more comprehensive and detailed messages, thus enhancing the overall user experience and utility of the application.

VII. CONCLUSION

In conclusion, this research paper has presented the development and implementation of a decentralized messaging web application leveraging blockchain technology. By addressing the limitations inherent in centralized messaging systems, such as privacy vulnerabilities and susceptibility to censorship, our decentralized application offers a promising alternative char- acterized by enhanced security, reliability, and user autonomy. Through the utilization of the Hardhat development envi- ronment, we have successfully built and tested the application, laying the groundwork for future enhancements and scalability. Our ongoing efforts to bolster exception handling mechanisms and expand message size capabilities underscore our com- mitment to continuous improvement and optimization of the application's functionality.

REFERENCES

[1] Mohan, M., Agarwal, K., Gupta, K., Arsalan, M. (2023, April). Chat Web App using Blockchain. In 2023 International Conference on Com- putational Intelligence, Communication Technology and Networking (CICTN) (pp. 260-264). IEEE.

[2] Pansara, P., Patel, R., Shah, K., Jhaveri, R., Parmar, V. (2023, March). Chat Application Security: Implementing Blockchain-based End-to-End Encryption. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 496-500). IEEE.

[3] Ellewala, U. P., Amarasena, W. D. H. U., Lakmali, H. S., Senanayaka, L. M. K., Senarathne, A. N. (2020, December). Secure messaging platform based on blockchain. In 2020 2nd International Conference on Advancements in Computing (ICAC) (Vol. 1, pp. 317-322). IEEE.

[4] Menegay, P., Salyers, J., College, G. (2018, October). Secure commu- nications using blockchain technology. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 599-604). IEEE.

[5] Mirko Franco, Ombretta Gaggi, Barbara Guidi, Andrea Michienzi, Claudio E. Palazzi, A decentralised messaging system robust against the unauthorised forwarding of private content,Future Gener- ation Computer Systems,Volume 145,2023,Pages 211-222,ISSN 0167- 739X,https://doi.org/10.1016/j.future.2023.03.025.

[6] Se´an Durban, An Anonymous Decentralised Messaging Application Utilising the Whisper Protocol, School of Computer Science and Statis- tics O'Reilly Institute, Trinity College, Dublin 2, Ireland (2018, May)

[7] Matthew Weidner, Martin Kleppmann, Daniel Hugenroth, and Alastair R. Beresford. 2021. Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 2024–2045. https://doi.org/10.1145/3460120.3484542

[8] Min, T., Cai, W. Portrait of decentralized application users: an overview based on large-scale Ethereum data. CCF Trans. Pervasive Comp. Interact. 4, 124–141 (2022). https://doi.org/10.1007/s42486-022-00094- 6

[9] Chirag Jani, Raaj Anand Mishra, Anshuman Kalla,Secure blockchainized Decentralized Messaging Application (DMApp) for Educational Institute, Software Impacts, Volume 16,2023,100494,ISSN 2665-9638,https://doi.org/10.1016/j.simpa.2023.100494.

[10] K. Khalkar, N. Dhake, S. Kelzarkar, and T. Shinde, "Decentralized Chat Application using Blockchain Technology," International Journal for Research in Applied Science Engineering Technology (IJRASET), vol. 11, no. 1, pp. 1-4, Jan. 2023. [Online]. Available: www.ijraset.com. ISSN: 2321-9653. IC Value: 45.98. SJ Impact Factor: 7.538.

[11] R. A. Sarıtekin, E. Karabacak, Z. Durgay and E. Karaarslan, "Blockchain based secure communication application proposal: Cryptouch," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-4, doi: 10.1109/ISDFS.2018.8355380.

[12] Abdulaziz, M., C¸ ulha, D., Yazici, A. (2018, December). A decentralized application for secure messaging in a trustless environment. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 1-5). IEEE.

[13] Gonza´lez, C. E. C., Romero, F. J. C. (2021, September). Security Issues of a Decentralized Blockchain-Based Messaging System. In 2021 Congreso Internacional de Innovacio´n y Tendencias en Ingenier´ıa (CONIITI) (pp. 1-4). IEEE.

[14] Gebhardt, L., Leinweber, M., Jacob, F., Hartenstein, H. (2022, October). Grasping the Concept of Decentralized Systems for Instant Messaging. In Proceedings of the 17th Workshop in Primary and Secondary Com- puting Education (pp. 1-6).

[15] Weidner, M., Kleppmann, M., Hugenroth, D., Beresford, A. R. (2021, November). Key agreement for decentralized secure group messaging with strong security guarantees. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 2024-2045).

[16] Aitzhan, N. Z., Svetinovic, D. (2016). Security and privacy in de- centralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840-852.