JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain-Based Secure Communication for Smartphones

[1] Mr. Onkar Kulkarni, [2] Prof. Yogesh Dongare, [3] Ms. Trupti Ubale, [4] Ms. Gayatri Nikam, , [5] Ms. Rushali Khalkar

[1] B.E Student, [2] Professor of MMIT college, [3] B.E Student, [4] B.E Student, [5] B.E Student
Department Of Computer Engineering,
Marathwada Mitra Mandal's Institute of Technology, Lohegaon, Pune, City

Abstract: In today's time, Blockchain has being necessary for us as nowadays we are completely dependent on updated technology and device. Decentralizing is a way of data storing which is very difficult or can be said as nearly impossible to alter or hack. with the passing of time, blockchain technology is becoming popular and it already provides a completely secure method of exchanging crypto-currencies which can be extended to the communication field. if the central server fails in the centralized system then it has a higher possibility of data losing as it is stored in a centralized database. the data stored at the central server can be altered or hacked. to have good sharing of information and to do communication the use of system with a centralized approach is helpful. blockchain technology has been seeing wide spread interest means to ensure the integrity, confidentiality and availability of data in trustless environment. authentication technology provides access control for system by checking to see if user's credentials match the credentials in database authentication server. they are designed to protect data from both internal and external cyber attacks. the proposed system remove its total dependency from centralized players and able to send encrypted messages securely which overcomes the drawbacks of traditional messaging applications and ensures that no network failure can occurs due to central node failure and provides essential security, unchanging nature, quicker settlement, and decentralized framework. the system is implemented with a peer-to-peer network, xmtp libraries, and mobile app development language, and supports crypto wallet, Ethereum platform that enables smart contracts which provide security and traceability to shared content.

Index Terms **- Blockchain, XMTP, Flutter, Crypto Wallet, and Decentralized networking**

I. INTRODUCTION

The messaging system is one of the most popular mobile applications; therefore, user authentication is essential. Various messaging systems are using encryption-based security protocols, but they are facing many security threat issues, therefore this system required a trustful security procedure. So, to solve this problem, a blockchain-based messaging system could be an alternative. This communication system uses blockchain technology to provide a decentralization messaging service, which is one of the core parts of the mission. Decentralization communication that runs over the decentralization network which completely supports the Peer-to-Peer (P2P) Network refers to the concept that in a network of nodes, each node can communicate with every other node individually. P2P technology has become an important part of communication technology as they avoid any single-point failure.

As a result, both individuals and organizations express deep concern about data security and protection while using instant messages. Non- repudiation in communication not only conveys to the user, but it is also a curial way to establish a relationship of trust and to overcome trust disputes. The purpose of the decentralized index based on P2P communication has the robustness to handle multiple users simultaneously without depending on a central server for communication.

The majority of management decisions or business decisions related to exchanging trade secrets, making business referrals, and strategic business decisions, protecting messages and shared files becomes a challenge. Most publicly available communication platform does not provide compliance with data protection framework, which can result in cross-industry system risks. So, our primary objective through this system is to develop a communication system with more secure channels of enterprise-level communication. We can cover the drawback of traditional communication systems, thereby ensuring confidentiality, integrity, and availability of official data, along with that are some additional features used to implement a communication system.

This system introduces, a private communication platform developed mainly by using XMTP and Blockchain. The application is based on XMTP for distributed data storage and Blockchain's Ethereum platform to securely store the messages and hashes generated by XMTP to protect those data from manipulation. The system would allow authorized users/nodes to connect into the network and communicate and share data/information among the other connected nodes. The frontend for the mobile application development would always interact with the Smart Contact of this system which is deployed on the Ethereum Virtual Machine by using Flutter language. The main objective of developing this system is to emphasize the importance of using XMTP and Blockchain technology. XMTP (Extensible Message Transport Protocol) is an open protocol and network for secure, private messaging between blockchain accounts (also known as crypto accounts). A user can send and receive encrypted XMTP messages using a system with an embedded XMTP client, authenticating using a wallet signature. XMTP network nodes persist the user's messages. It uses AES-

256-GCM and a modified Diffie-Hellman key agreement. Messages are encrypted individually by default and are readable by message participants only.

II. PROBLEM STATEMENT

a) Many other systems use a centralized approach in communication systems whereas the data is stored on a centralized server and this data storing process can cause collapse problems in the server.

b) Also, the centralized server data might get hacked looking over this problem we are implementing a secure communication system.

c) This system will take the support of the blockchain which works with nodes and each node is dependent on one other. So, blockchain can overcome the drawback.

d) The world deserves secure communication that gives free control, ownership, and security by anyone entity; where users also have free about their identity and message

III. MOTIVATION

a) This system supports communication features with blockchain security and also this communication system supports IOS and android devices with all similar features.

b) As, it does not have a central server so, It will completely work on the decentralization server which supports the peer-to-peer network.

c) Decentralization is the key motivation behind the technology & future system.

IV. LIMITATION

a) The limitation is that the system requires a stable network connection for connecting to the API server.

b) The limitation of this chat application is it does not support audio conversations. To overcome this limitation, we are concurrently working on developing better technologies.

V. LITERATURE REVIEW

a) DECENTRALIZED APPLICATION FOR SECURE MESSAGING IN A TRUSTLESS ENVIRONMENT

Mohamed Abdulaziz et al || 2018

The client uses Geth, an Ethereum client, to run a node and to serve as an interface to interact with the Whisper network. The front end consists of a web application built on Node.js and was chosen due to the abundant support for web3.js, the Ethereum JavaScript API.

b) SECURE MESSAGING PLATFORM BASED ON BLOCKCHAIN

U.P Ellewala et al || 2020

Hashing and Timestamping. HMAC-SHA-256 algorithm is used as per RFC 2014

VI. SYSTEM DIAGRAM

Step 1: Create a User Interface for the application for which the flutter framework can be used.

Step 2: The live messaging process of saved and the update is going to be implemented in Xmtp.

Step 3: For security setup, the system required the blockchain algorithm and methods.

Step 4: To check the functionality working of the system we are going to use two device with different OS so that the reference to diagram 1.

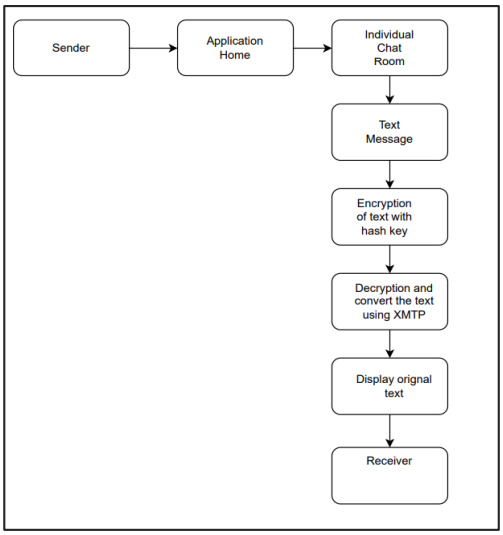

Fig 1. System Diagram

VII. DEVELOPMENT DIAGRAM

Deployment diagrams are used to visualize the topology of the physical components of a system where the software components are deployed. So deployment diagrams are used to describe the static deployment view of a system. Deployment diagrams consist of nodes and their relationships.

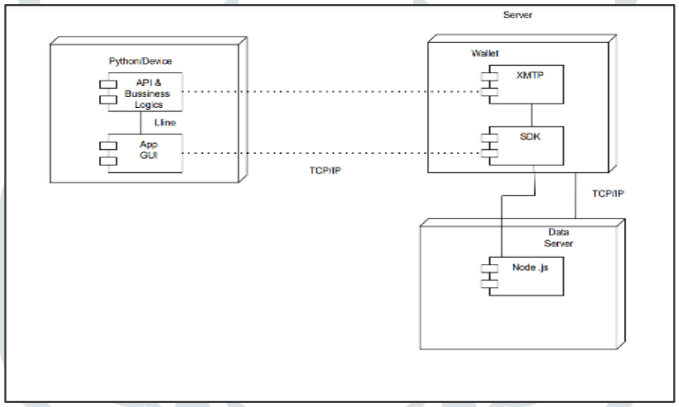

Fig 2. Development Diagram

VIII. WORKING OF SYSTEM

let me tell you the main reason to create the paper is that today we are very much updated on social media and always connect with each other on the chatting system but in any way, we don't feel free to share personal details on the system as they support the security of the centralized server ever all the data has been a store. which has a bit less security to prevent this issue. So, we are implementing blockchain technology for the chatting system, which keeps data secure and safe and gives a user-friendly environment also we don't need to add all our personal details to access the application as the wallet id is enough to use it.

To login into the system we need a crypto wallet id as we enter our crypto wallet id we directly go into the dashboard of the system. This crypto wallet id is easy and safe for processing and this wallet does support the peer-to-peer network.

looking forward to the chatting and live updating we used XMTP which supports the chatting features in blockchain as this is newly introduced so using it is a bit difficult but, we can handle it if we give good attention to the process as this is very much secure which can be used in many other ways in future and also this helps the system to add more interesting details.

Here, is fig- 3 of the XMTP architecture which we have used in our system.

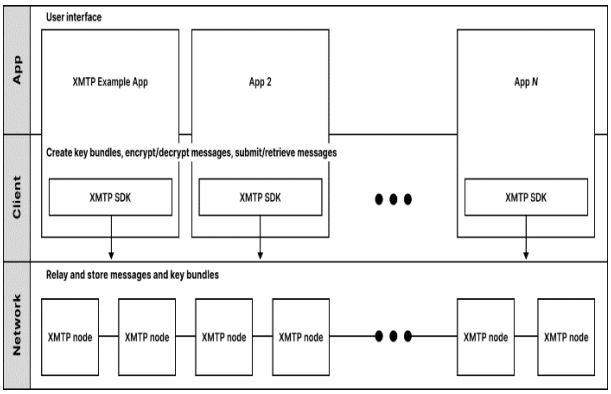

Fig 3. Xmtp architecture

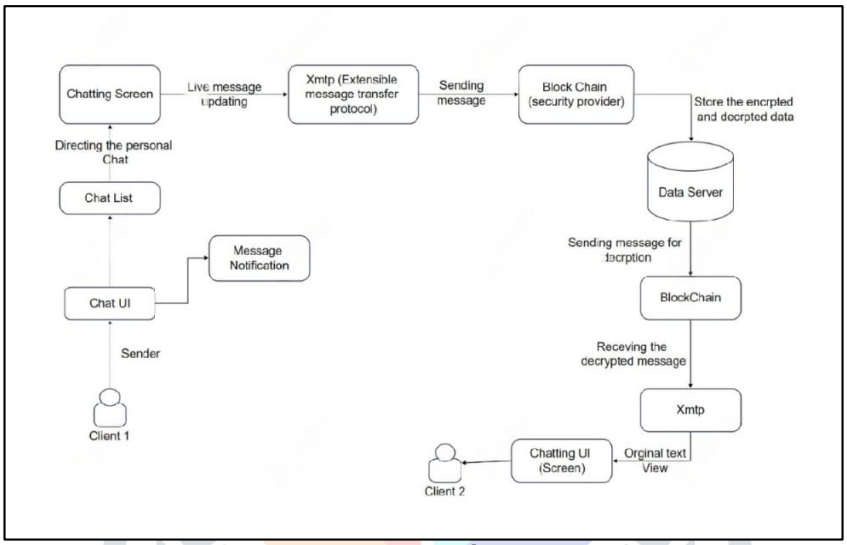

Fig 4. System Architecture

IX. Conclusion

This paper has provided a chatting system solution that enables the maintenance of privacy of personal information while giving access to actionable data and the system architecture is designed to use blockchain for sending messages securely and anonymously as a system component. We described the basic requirements, architecture, and implementation experience in deploying such a work. This research furthermore summarizes and put forward the concept of a chat system using blockchain that can be more useful for co-operate users as most chat systems are not able to give a high – level of security at present. Blockchain has shown its potential to give security to chat systems in a safe manner and by eliminating the centralized approach, users can assure the safety, confidentiality, and availability of data and communication.

References

1) B. Gipp, N. Meuschke, and A. Gernandt, “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin,” no. February, 2015.
2) Zibin Zheng, Shaoan Xie, Hongning Dai, Xiang ping Chen, and Huaimin Wang, —An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends‖, 2017 IEEE 6th International Congress on Big Data.
3) G. Foroglou and A.-L. Tsilidou, —Further applications of the blockchain, || 2015
4) Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, —Hawk: The blockchain model of cryptography and priva-cypreserving smart contracts,‖ in Proceedings of IEEE Sym- posium on security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
5) G. Foroglou and A.-L. Tsilidou, —Further applications of the blockchain,‖ 2015.
6) B. W. Akins, J. L. Chapman, and J. M. Gordon, —A whole new world: Income tax considerations of the bitcoin econo-my,‖
7) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394738
8) https://www.computer.org/csdl/journal/tk/2018/07/08246573/13rRUxD9gYf
9) https://techcommunity.microsoft.com/t5/microsoft-teams/end-to-end-encryption-with-microsoft-teams/m-p/804842
10) https://www.semanticscholar.org/paper/Designing-a-Secure-Architecture-for-Private-Instant-Yusof-Usop/cff1708b3e770f760f0eb0146bd539dd2a1ae76f
11) https://bitcoin.org/bitcoin.pdf