Blockcrypt cryptography based communication

Pratiksha Madhukar Kamble[1]; Rushikesh Prakash Ichake[2]; Pratiksha Vishnu Jawale[3]; Sunil Krishna Dokfode[4]; Guide- Prof. Poonam Tiware [5]

[1,2,3,4,5]Department of Computer Engineering, University of Mumbai, Maharashtra, India

Corresponding Author Email: pratikshak3659@gmail.com

Abstract─Blockchain is a new technology that overcomes threats and allows decentralization of sensitive tasks while maintaining high performance. security. It eliminates the need for trusted intermediaries. Blockchain is a new technology that provides a decentralized platform that ensures data integrity, transparency, traceability, anonymity, non-repudiation, accountability and non-tampering. Blockchain accesses all network nodes and tracks all transactions taking place. The aim of our work is to propose secure communication based on blockchain technology. In this project, we explain why blockchain will make communication more secure and present a design for blockchain-based messaging to protect the efficiency and security of data stored on the blockchain. The system is a combination of blockchain and cryptographic methods of communication.

Keywords: - decentralization, security, blockchain, cryptography.

I. INTRODUCTION

In today's digital environment, centralized systems where information is stored on a server have long been the standard for sharing and communication. However, this approach comes with significant risks, such as data loss due to server failure, vulnerability to hacking attacks, and lack of transparency in the information sharing process. These challenges have become even more pronounced with the growth of digital commerce and communications, especially in India, where initiatives such as Unified Payments Interface (UPI) and Aadhaabased payments are rapidly gaining traction on the technology. To solve these important problems, the idea of inter

system distribution using blockchain technology has emerged as a promising solution. Blockchain provides a distributed system where information is distributed and stored over a computer network, providing transparency, security, and the ability to prevent tampering or data loss. The motivation behind leveraging blockchain and encryption technologies such as BLOKKCRYPT is to create a secure, tamper-

proof platform for digital transactions while building trust between parties and reducing the risk of fraud. and privacy has become a top concern, especially with the implementation of Personal Data Protection (PDPB); BLOKKCRYPT aims to provide a connectivity language that manages user privacy and allows people to control their personal information. By integrating blockchain technology into communication, BLOKKCRYPT aims to create a transparent exchange where participants can verify and verify communication history, thus increasing users' trust and responsibility.

 Especially in India, where data protection and privacy have become a major concern with the passage of the Personal Data Protection Act (PDPB), BLOKKCRYPT aims to provide a communication system that protects user privacy and gives individuals control over their personal information. By integrating blockchain technology into communication, BLOKKCRYPT aims to create a transparent exchange where participants can verify and verify communication history, thus increasing users' trust and responsibility.

II. LITERATURE SURVEY

Teacher Shivaji Vasekar, Akash Adhav, Anirudha Adekar, Kshitij Kanake, Shubham Gondhali Decentralized applications leverage decentralized networks to ensure that the organization does not fail due to failure of its focal point. [1]

Dr. R.K. Gupta helped clarify the nature of cryptography by making connections between different cryptographic methods and different hashes. It performs different mixed power attacks. More attacks can be created by analyzing current security levels and creating a strong system. [2]

Obamehinti Adeolu Seun1, Touraj Khodadadi2, Sellappan Palaniappan3 Blockchain is a technology that offers a way to solve many challenges in various fields. Documents, contract language have attracted the attention of researchers over the years as they are considered transparent, secure, third-party-free and tamper-proof public data storage for products and assets. [3].

Abdalbasit Mohammed Cryptography is a machine used to process secret messages. This word has a special meaning in Greek: "secret writing." However, today, the confidentiality of individuals and organizations is ensured by advanced encryption technology, ensuring that the transmitted information is secure and accessible to authorized persons. [4].

Thomas Kitsantas, Evangelos Chytis Blockchain is a technology that can bring significant changes to our business environment and will have a major impact for many years to come. It can change the way we look at business processes and change the way we do business. Blockchain is a decentralized ledger technology designed to ensure transparency, data security and integrity because it cannot be altered or counterfeited. Most of the current research on blockchain technology focuses on its application in cryptocurrencies such as Bitcoin; Only limited research focuses on exploring the use of blockchain technology in another context or domain. Blockchain technology is much more than cryptocurrency; It can have many applications in areas such as government, finance and banking, finance and business management. Therefore, this study attempts to explore and explore the opportunities and problems of current or future use of blockchain technology. [5].

II.I. PROPOSED SYSTEM

The Blockcrypt system concept is proposed as a secure communication platform using blockchain technology and cryptographic techniques. The system will run on blockchain infrastructure, providing a decentralized and transparent place for users to exchange encrypted messages. Users will register on the platform using cryptographic keys and ensure their identities are managed securely on the blockchain. Secret messages sent by users will be protected using the recipient's public key, ensuring that only the intended recipient can decrypt and access the content. Smart contracts will play an important role in defining messaging policies such as access control and message policy. These agreements can also resolve conflicts and ensure effective communication. Offchain storage solutions such as IPFS (Interplanetary File System) will be used to efficiently store data, while blockchain data will store metadata and cryptographic hashes for verification and integrity. Native tokens can be introduced to support network participation and used for transaction fees, storage payments, and system administration. This is despite having great potential in terms of security and transparency. The platform is powerful and reliable.

The Blockcrypt system can provide users with enhanced privacy, tracking and communication control through the use of smart contracts and business infrastructure; The ability to convey the exchange of secure communication methods has been done many times. However, the success of such a system must ensure a good relationship with the legal and regulatory system to overcome economic barriers and ensure understanding and trust among users.

III. METHODOLOGY AND IMPLEMENTATIONS

After the trial is over, the first phase begins. An important phase of the development life cycle is the implementation of new designs. Implementation simply means turning innovation into action. That is the moment of truth, and the first question that comes to everyone's mind is: Is the system capable of providing all the desired results it accepts?
The project evaluation process includes needs analysis and structural analysis. The implementation phase of software design consists of various tasks that must be completed in a single session to achieve the desired results. Ensuring deliveries at the end of each stage. The following eight principles are set out as guidelines for creating effective practices. The framework provides flexibility to react and adapt to the characteristics of each project and includes the following:
1. Project Management and Planning
2. Scope and Requirements Specification
3. Risk and Problem Management 4
4. Quality Management
5. Post-Study Evaluation
6. File
7. Knowledge
Project Management and Planning
Project Management is the art and science of communicating between individuals with different responsibilities, perspectives, and expectations to aid teamwork and support the organization. value and end product Theoptimization process should be driven by the management process and the opinion of the people working together. Project managers facilitate collaboration so partners can work together to achieve agreed-upon goals.

Scope and Requirements
Specifications The method used should be based on results. This means that the process demonstrates the identification of business needs specific to the organization's particular goals. This is achieved through a method that develops a solution that translates goals and objectives into operational requirements (key success factors, headlines).

Risk Management
Risk is associated with almost everything we do, and certainly with software projects. A risk is something that "will" happen, meaning the probability is less than 100% and if it happens it will have a negative impact on the project. If it is 100%, then it will be a

problem. Such problems are solved differently than dangerous ones. Effective risk management can be divided into four levels for
 risk management: Level

1: Analysis level

2: Quantity level

3: Response level

4: Control

Problem Management

Problems are real problems. To solve this problem, an action needs to be sent to "someone" who must do "so

mething" by the "deadline". Issues should be tracked by type, status, and priority. The method in managing the problem should inc
lude the following steps:

1. Keep an issue log that is easily accessible to everyone on the project.

Data flow diagram
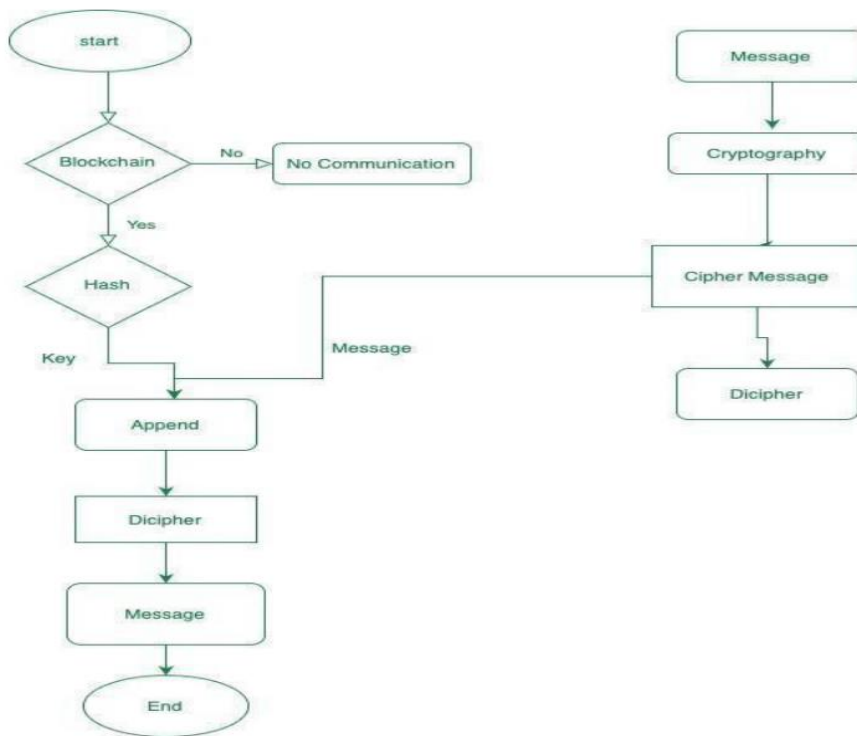
System Architecture
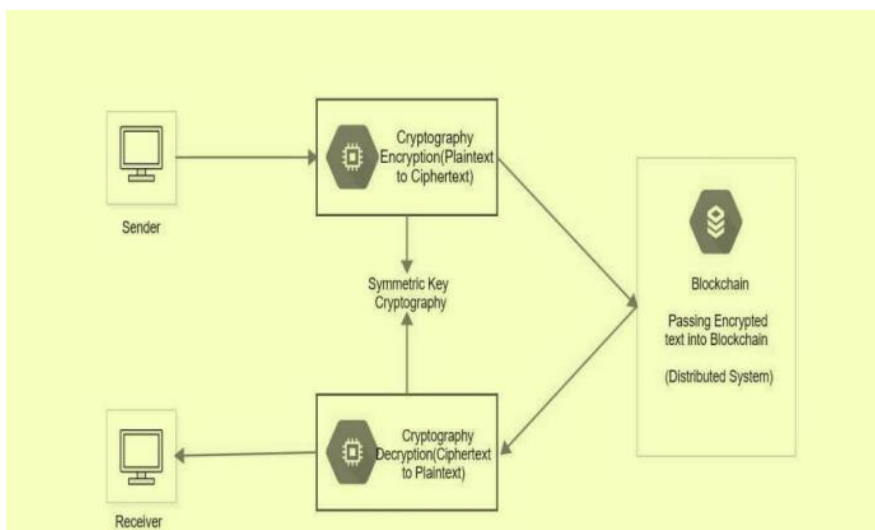
IV. RESULT

Blockcrypt cryptography-based communication aims to use blockchain technology and cryptographic methods to secure and enhance communication systems. Users are authenticated using cryptographic keys, and messages are encrypted with the recipient's public key, ensuring only authorized parties can access the content. Blockchain provides a transparent and immutable ledger for storing transaction records and metadata, enhancing integrity and transparency. Smart contracts enforce messaging rules, and off-chain storage solutions like IPFS store message payloads efficiently. Tokenization can incentivize network participation
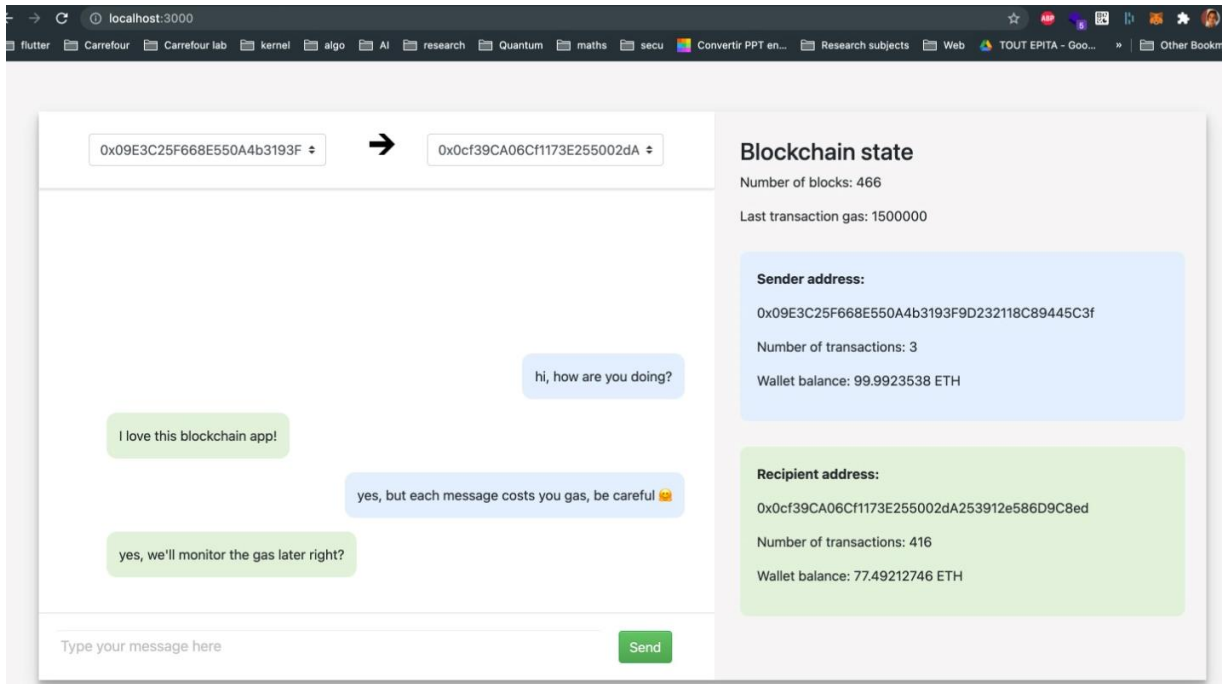
V. CONCLUSION

In conclusion, BLOKKCRYPT, a blockchain and cryptography-based communication system, offers a secure and decentralized platform for exchanging messages and ensuring data confidentiality, integrity, and authentication. By leveraging the power of blockchain technology and robust cryptographic algorithms, BLOKKCRYPT provides users with a high level of privacy and security

VI. FUTURE SCOPE

Although BLOKKCRYPT has made significant progress in secure communications, there are many areas that need future research and development:

• Usability:

Continuous improvements to BLOKCRYPT's user interface and user experience (UI/UX) will increase adoption and make it easier for users with greater levels of expertise.

• Interoperability:

Exploring interoperability with other blockchain platforms and communications will lead to seamless communication between different networks and improve the overall ecosystem.

• Integration with external services:

BLOKCRYPT's integration with external services and applications (such as email clients or messaging services) will maintain its work and provide better communication.

• Additional Security Enhancements:

Continuous security testing, encryption algorithm updates, and compliance with emerging security standards are critical to BLOKKCRYPT's security against threats.

™Mobile Application:

Developing a mobile application for BLOKCRYPT will expand its reach and enable users to communicate securely on the go. Overall, BLOKKCRYPT has the potential to revolutionize secure communications through the use of blockchain and cryptography. Continuous research, development and improvement will help its growth and adoption, ensuring the privacy and security of digital communications for users worldwide.

REFERENCE

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

2. Buterin, V. (2014). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. https://ethereum.org/whitepaper/

3. Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

4. Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. In Proceedings of the Annual International Cryptology Conference (CRYPTO) (pp. 139- 147).

5. Boneh, D., & Shacham, H. (2008). Group Signatures with Verifier-Local Revocation. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) (pp. 255-274).

6. Wood, G. (2014). Ethereum: A Secure Decentralized Generalized Transaction Ledger. https://ethereum.org/ethereum.html

7. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382-401.

8. Bonneau, J., et al. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy (S&P) (pp. 104-121).

9. Rege, A., & Bansal, S. (2020). Blockchain Applications: A Systematic Literature Review. Journal of Enterprise Information Management, 33(2), 405-432. 36

10. Kumar, N., et al. (2019). Blockchain Security: A Survey. IEEE Communications Surveys & Tutorials, 21(1), 858-880.

11. Szabo, N. (1997). The Idea of Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LO Twinterschool2006/szabo.best.vwh.net/idea.html