# Chapter 21
# Blockchain-Based Messaging System for Secure and Private Communication:
## Using Blockchain and Double AES Encryption

**Shiva Chaithanya Goud Bollipelly**
*Vellore Institute of Technology, India*

**Prabu Sevugan**
*Pondicherry University, India*

**R. Venkatesan**
*SASTRA University, India*

**L. Sharmila**
*Agni College of Technology, India*

## ABSTRACT

*In recent years, concerns about privacy and security in online communication have become increasingly prominent. To address these concerns, the authors propose a blockchain-based messaging system that provides secure and private communication using double AES encryption. The system utilizes the decentralized and tamper-resistant nature of the blockchain to ensure that messages are not modified or deleted by unauthorized parties. Additionally, they employ double AES encryption to ensure that the content of messages remains confidential even if the blockchain itself is compromised. They evaluate the performance of the system and show that it is scalable and efficient. The system provides a secure and private messaging solution that can be used by individuals and organizations alike.*

DOI: 10.4018/978-1-6684-8098-4.ch021

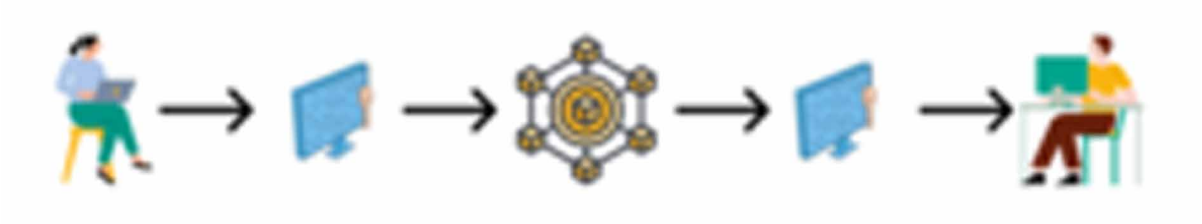
## INTRODUCTION

In today's digital age, the need for secure and private communication has become more important than ever. With increasing concerns over data breaches and privacy violations, individuals and organizations are searching for new ways to protect their sensitive information.

Blockchain technology has emerged as a potential solution for secure and private communication. Its decentralized nature makes it resistant to attacks and manipulation, and its transparency allows for easy verification of transactions. Additionally, the use of advanced encryption algorithms, such as AES, further enhances the security and privacy of blockchain-based communication systems.

In this project, we propose a blockchain-based messaging system with double AES encryption to provide secure and private communication. The messaging system will allow users to send and receive messages without the need for a third-party intermediary, thereby minimizing the risk of data breaches and privacy violations. The double encryption using AES will add an extra layer of security to the messages, ensuring that they can only be decrypted by the intended recipient.

*Figure 1. Blockchain-based messaging system with double AES encryption*



This project aims to provide a practical solution for secure and private communication using blockchain technology and AES encryption. By implementing and evaluating the proposed messaging system, we hope to demonstrate the feasibility and effectiveness of this approach, as well as identify areas for improvement. Ultimately, this project aims to contribute to the development of more secure and private communication systems in the digital age.

## BLOCKCHAIN

In today's digital age, secure and private communication is of paramount importance. The increasing concerns over data breaches, privacy violations, and unauthorized access have prompted the exploration of new technologies to safeguard sensitive information. One such technology that holds great promise is blockchain.

Blockchain technology has emerged as a revolutionary concept that has the potential to transform various industries, including communication and data security. At its core, blockchain is a decentralized and distributed ledger system that ensures secure and transparent recording of transactions. It provides a tamper-proof and verifiable record of events, making it an ideal candidate for enhancing the security and privacy of communication systems.