iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XI Month of publication: November 2025

DOI: https://doi.org/10.22214/ijraset.2025.74891

BitChat: A Decentralized Messaging App

Anushka Vinod Patil[1], Prof. Pallavi A. Chaudhari[2]
Department of Computer Engineering Met's Institute of Engineering, Adgaon

Abstract: Secure and private communication has become crucial in today's era of data breaches, cyber-attacks, and surveillance. This paper presents the design and implementation of BitChat, a blockchain-based decentralized messaging application that ensures anonymous, tamper-proof, and fully encrypted communication. Unlike conventional messaging systems that depend on centralized servers or internet connectivity, BitChat operates on a peer-to-peer decentralized network, allowing communication even during network outages. A comparative study with mainstream messaging platforms like WhatsApp and Telegram highlights differences in privacy, security protocols, and network dependency. The proposed system emphasizes autonomy, resilience, and censorship resistance, offering a secure and reliable communication platform for sensitive and critical environments.

Index Terms: decentralized messaging, peer-to-peer communication,cybersecurity, encryption, privacy, BitChat.

I. INTRODUCTION

Messaging apps like WhatsApp and Telegram have become vital for communication but depend on centralized servers, internet access, and personal identifiers, raising privacy and security concerns. BitChat is a decentralized messaging solution that enables secure, anonymous, and offline peer-topeer communication using BLE mesh networking. Each device acts as both sender and router, ensuring connectivity even during network failures. The system uses Curve25519 and AES-256 encryption for end-to-end security and employs blockchain smart contracts for identity verification and message integrity.. The platform is designed to be censorshipresistant, transparent, and effective in low-network or highsurveillance environments.

II. MOTIVATION

In a world where communication has become the backbone of everyday life, the need for privacy, security, and freedom of expression is greater than ever. Traditional messaging platforms, though convenient, rely heavily on centralized servers and con tinuous internet connectivity. This structure makes them vulnerable to data breaches, surveillance, and government censorship. BitChat was created to challenge this dependency and to build a platform that allows people to communicate safely even without the internet. It is not just a new technology; it represents a shift in how we think about communication, privacy, and digital independence

III. OBJECTIVES

The main goal of BitChat is to build a secure and private communication system that functions without centralized servers or internet connectivity. It empowers users with full control over their data while maintaining uninterrupted communication in all conditions. The system adopts a peer-topeer mesh structure where every device acts as both sender and relay, ensuring reliable and decentralized messaging. Using Bluetooth Low Energy (BLE) mesh technology, BitChat enables offline connectivity across multiple hops, making it effective in disaster zones or rural areas.Being open-source, BitChat promotes transparency, community collaboration, and trust. It also demonstrates real-world applicability in emergency and censorship-prone environments.

IV. LITERATURE SURVEY

Existing studies emphasize the advancement of blockchainbased decentralized messaging systems for secure and private communication. Example works:

- Ghosh (2025) studied BitChat, an off-grid blockchainintegrated app using Bluetooth mesh for offline encrypted messaging, ensuring anonymity and censorship resistance.
- Philip & Rajeswari (2024) developed an Ethereum-based chat app using smart contracts, MetaMask, and QR-based login for tamper-proof and pseudonymous communication.
- Zheng et al. (2023) reviewed blockchain-based DApps, outlining architectures like smart contract and fully decentralized models, and identified issues such as incentive design and performance limits.

- Bagade &Wankhade (2022) proposed a peer-to-peer messaging model using blockchain and 256-bit encryption, featuring local user profiles, distributed hash tables, and strong authentication.

V. METHODOLOGY

A. Methodology BitChat follows the principle of secure, private, and decentralized communication. Its methodology ensures user control, anonymity, and message integrity through the following steps:

- Establish Peer-to-Peer Network
- Store-and-Forward Messaging
- Encrypt and Authenticate: Curve25519 is used for key exchange and AES-256-GCM for end-to-end encryption.
- Privacy Enforcement
- Verification

B. System Model:

The BitChat model is structured into four layers:

- User Layer: Provides the chat interface for composing and reading messages.
- Application Layer: Handles UI, authentication via blockchain wallets (e.g., MetaMask), and key exchange.
- Blockchain Layer: Executes smart contracts for message integrity, user verification, and ledger security using stored message hashes.
- Security Layer: Ensures confidentiality and integrity through AES-256/RSA encryption, SHA-256 hashing, and digital identity verification.

When a message is sent, BitChat encrypts it using AES-256GCM, establishes a Curve25519 session, and routes it through the mesh. If the recipient is offline, the message is stored and later delivered. Privacy features like disappearing messages and cover traffic are applied, ensuring confidentiality, authenticity, and reliability in all conditions.

VI. ALGORITHM AND DATA FLOW

1) Initialize system: Generate cryptographic identities and form a BLE mesh network among nearby devices.
2) Message input: User sends a message which is split, encrypted, and assigned unique IDs with TTL.
3) Broadcast and relay: Encrypted chunks are shared across the mesh; relay nodes store and forward them for offline delivery.
4) Reception and decryption: Receiver verifies signatures, decrypts with Curve25519-derived keys, and reconstructs the message.
5) Blockchain logging: Smart contracts record identity verification and proof-of-delivery timestamps immutably.
6) Privacy features: Cover traffic, disappearing messages, and panic wipe ensure confidentiality.

This flow ensures secure, private, and censorship-resistant communication without internet dependency.

VII.APPLICATIONS

1) Used during disasters and emergencies (e.g., earthquakes, floods) to help rescue teams and civilians communicate offline.
2) Works in protests or censorship zones where the internet is blocked or monitored, enabling anonymous communication for activists and journalists.
3) Useful in remote and rural areas lacking telecom access, allowing farmers, teachers, and NGOs to stay connected.
4) Effective in large events or gatherings (concerts, sports, festivals) where mobile networks are jammed, enabling updates and emergency alerts via the mesh network.

VIII. ADVANTAGES AND DISADVANTAGES

A. Advantages:

- Enables decentralized, serverless communication via peer-to-peer BLE mesh.
- Works offline using store-and-forward for reliable message delivery.
- Ensures strong privacy through end-to-end encryption and secure key exchange.
- Integrates blockchain and smart contracts for identity verification and data integrity.

B. Limitations:

- Limited connectivity range **-** works only within short BLE range.
- Difficult user discovery **-** requires manual key exchange or scanning.
- Reliability depends on intermediary devices staying active; offline nodes may disrupt delivery.

IX. FUTURE WORK

- Add Wi-Fi Direct support to extend range while maintaining offline functionality.
- Encourage community adoption by NGOs, disaster teams, and rural institutions.
- Enhance identity verification to prevent impersonation or fake devices.
- Improve user interface for easier use by non-technical users.
- Promote open-source development for community-driven updates and features.

X. CONCLUSION

We presented BitChat, a decentralized, privacy-focused messaging application that enables secure communication without internet using Bluetooth mesh and store-and-forward mechanisms. It ensures anonymity, security, and censorship resistance through strong encryption, decentralized identity management, and privacy features like disappearing messages and panic wipe. While still evolving, BitChat demonstrates how smartphones can form resilient offline networks for emergencies, protests, and remote areas—marking a step toward self-sovereign, secure communication in the digital era.

XI. ACKNOWLEDGMENT

The author expresses sincere gratitude to Prof. Pallavi A.Chaudhari for guidance, and to Dr. P. M. Yawalkar (HOD), Prof. Manjusha F. Gaikwad (Seminar Coordinator), family and friends for support during this seminar project.

REFERENCES

[1] BitChat: A Decentralized Blockchain-Integrated Messaging Platform; Pronabesh Ghosh, In Adamas University, July 2025.

[2] A Blockchain-Enabled Chat Application System for Secure Communi cation; Bhaskar S. V., Harshith C. M., Ashok K., and Santhosh Krishna B. V., Vol.: 2025, Issue: ICEARS, pp: 944–947, (2025).

[3] Decentralized Messaging Web Application: A Blockchain-Based Ap proach for Secure Communication; Venkat Jayaram Vikram, Mittal Abhinav Krishna, Jashwanth Kumar Reddy, and Goutham Senthil Kumar, Vol. 11, Issue: 06, pp. 112–117, (June 2024).

[4] Decentralized Chatting Application Using Blockchain Technology; Jim Mathew Philip and Rajeswari R., In International Research Journal of Engineering and Technology (IRJET), Vol.12, Issue:V, pp:184-190, (May 2024).

[5] Decentralized Secure Messaging Application Using BlockchainTechnology; Shweta Dnyaneshwar Bagade and Prof. (Dr.) N. R. Wankhade, In International Journal for Research in Applied Science and Engineering Technology (IJRASET), Vol.04, Issue:09, pp:1548–1553, (September 2022)