International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Systematic Review Paper on Decentralized ChatApp using Blockchain

Ashith Rajeev, B Harikeerthana, B Haritheetha, Muahammed Musthafa, Dr Reema Mathew
Department of Computer Science
Vimal Jyothi Engineering College, Chemperi, Kannur

***Abstract*—** Secure communication has become a cornerstone in the digital age, especially for instant messaging where sensitive information is frequently exchanged. But traditional centralized systems often suffer from weaknesses such as data breaches, unauthorized permissions, single points of failure, highlighting the immediate need for innovative solutions They are known to be combative against manipulation, blockchain technology provides a promising basis for enhancing message security, privacy and reliability.This paper systematically reviews the major contributions to blockchain-based secure messaging by examining eleven important studies. The research explores a variety of approaches including advanced cryptography techniques, privacy protection systems, decentralized architecture, and technologies such as smart contracts, decentralized identifiers (DIDs), interplanetary file systems (IPFS), and end-to-end integrating encryption All these technologies user authentication, data They address important issues such as authentication and privacy. Our findings provide insights into existing approaches, existing challenges, and potential opportunities for future improvement. Although blockchain-based systems exhibit strong potential to transform secure messages, issues of scalability, latency, and interoperability remain major hurdles to overcome to achieve adoption large The aim of this research is robust, efficient, scale -And future development of blockchain-enabled communication system It is to guide research efforts.

I. INTRODUCTION

In today's connected world, instant messaging systems play an important role in personal and professional communication. However, the growing reliance on these platforms has also raised data security and privacy concerns. Centralized messaging systems, even the most widely accepted, often have vulnerabilities such as unauthorized access, data breach, single point of failure, etc. To address these issues, researchers and operators have turned to blockchain technology, which provides a decentralized and tamper-proof infrastructure

Blockchain works on a distributed ledger mechanism that ensures data integrity, transparency and robustness against tampering. Additionally, end-to-end encryption and other encryption techniques further strengthen the privacy of user communications. These features have made blockchain an attractive solution for secure messaging systems, and encouraged innovation in the design of decentralized platforms Integrating blockchain into messaging systems presents unique opportunities and challenges. Key technologies such as smart contracts enable automatic and secure enforcement of custom rules, while decentralized identifiers (DIDs) provide robust identity management without relying on centralized authorities including as IPFS provides distributed storage mechanism for, ensuring safe and secure data storage. Finally, endto-end encryption, when combined with a blockchain, ensures that transactions remain private and resist interception. While these technology promise to mitigate issues of centralization and decorate privateness, additionally they pose barriers along with increased latency, aid-intensive operations, and scalability constraints. To navigate these complexities,

researchers have proposed various answers, starting from hybrid architectures to the incorporation of machine mastering techniques for optimization.

II. A SYSTEMATIC LITERATURE REVIEW

A. Research methodology

This systematic literature review follows a systematic approach to identifying, analyzing, and classifying relevant studies. The process included the following steps

1) Research design: Relevant documents were searched using keywords such as ”blockchain-based secure messaging,” ”end-to-end encryption with blockchain,” ”secure communications,” and ”blockchain for instant messaging.” Databases such as IEEE Xplore, Springer, ACM Digital Library, and Google Scholar were used.

2) Attachments: Papers focusing on blockchain-based solutions for secure transactions. A study that proposes or tests cryptographic techniques in message processing. Articles published in peer-reviewed journals, conferences, or workshops

3) Exclusion criteria: Research unrelated to blockchain or messaging systems. Papers without technical or experimental contributions. Contains duplicate figures or incomplete information.

4) Reviewed Papers: The following papers were selected for review:

1. Blockchain-Based Trusted Instant Messaging Model

Research by Huiyuan Wang. [10]

2. Blockchain-Enabled End-to-End Encryption for Instant

Messaging Applications by Raman Singh. [7]

3. A Secure Blockchain-Based Communication Approach for

UAV Networks by Elias Ghribi et al. [4]

4. The Existence of Cryptography: A Study on InstantMessaging by Vania Beatrice Liwandouw and Alz Danny

Wowor. [6]

5. Secure Messaging Platform Based on Blockchain by Sina

Turotchi et al. [2]

6. Making P2P Accountable without Losing Privacy by Mira

Belenkiy et al. [1]

7. IBM Blockchain: An Enterprise Deployment of a Distributed Consensus-Based Transaction Log by Ben Smith and Konstantinos Christidi. [8]

8. Secure Instant Messaging Application in Prenatal Care by

Osnat Ezra et al. [3]

9. Securing Instant Messaging Based on Blockchain with

Machine Learning by Haibo Yi. [11]

10. Design and Implementation of Secure E-Mail System

Using Elliptic Curve Cryptosystem by Wongoo Lee and Jaekwang Lee. [5]

11. Symmetric and Asymmetric Encryption Algorithms inCryptography by M.Sowmiya and S.Prabavathi [9]

Refer table 1 shows, summarizing the evaluation criteria used across the reviewed studies, which compares their methodologies, datasets, and evaluation metrics.

B. Conclusions and analysis

1) Improved security in instant messaging: Several studies have investigated hybrid blockchain to improve the security of messaging systems: Huiyuan Wang proposed a blockchainbased trusted instant messaging system, which focuses on decentralization and user privacy.

Raman Singh introduced an end-to-end encryption system using blockchain, which provided privacy and attack resistance.

2) Introduction to Cryptography: Advanced coding techniques were used in the reviewed studies: Vania Beatrice Liwandou highlighted the role of cryptography in advancing secure instant messaging. Wonggu Lee and Jaekwang Lee used elliptical curved cryptography (ECC)

for secure email systems, which can be extended to instant messaging.

3) *Decentralization and trust:* Decentralized channels of communication were key: Elias Ghribi et al., who proposed a blockchain-based network for UAV networks. Sina Turotchi et al., focused on decentralized messaging platforms with blockchain as the backbone.

4) *Integrating Machine Learning:* Haibo Yi explored the intersection of blockchain and machine learning to enhance secure messaging.

5) *Confidentiality and Liability:* Mira Belenky and others. A framework for responsible P2P transactions without compromising privacy was developed.

6) *Enterprise Applications:* Mira Belenky and others. A framework for responsible P2P transactions without compromising privacy was developed.

III. RELATED WORKS

Blockchain technology is used in most cryptocurrencies (Bitcoin, Ethereum), supply chain management (IBM Food Trust), and secure voting systems (Estonia's e-voting). Decentralized Identity (DID) gives the user self-sovereign identity management, removing reliance on central authorities and providing privacy (e.g., Sovrin, Microsoft DID). Data Wallets, such as MetaMask and Trust Wallet, are crucial for interaction with decentralized applications (DeFi), securely storing private keys and digital assets. IPFS decentralized file storage enables fast and safe storing and sharing, used on such platforms as Filecoin for digital content, NFTs in general, in the sense of enabling persistence without requiring centralized servers to maintain a service. In effect, they have been altering different industries to promote more safety, privacy, and user control. [10]

These implementations show the practical use of blockchain for secure messaging, targeting privacy and trust in applications like e-commerce and general instant messaging platforms. [11]

The paper highlights the use of a secure instant messaging system implementation Siilo to solve fundamental problems in medical communication, such as confidentiality, latency, and quality of patient care Siilo ensures secure patient data sharing, stores information in an encrypted vault, and deletes messages after 30 days. During prenatal care, she was treated by technicians, doctors, and HMOs. Siilo reduces patient burden, reduces loss to follow-up, and ensures faster decisions in complex cases while maintaining medical confidentiality and effective communication. [3]

The paper proposes a blockchain-based E2EE system for instant messaging, which ensures true privacy through the use of keys and certificates through the blockchain. Created a real-time messaging application using Android, Firebase, and Ethereum blockchain. Features include secure group messaging, one-to-one messaging, encrypted backup, and decentralized certificate management. This eliminates reliance on service providers for encryption and decryption. [7] The paper explores cryptographic applications (Encrypt, AES-Crypto, EnDe-Crypto, Kryptokaz) for immediate secure messages using AES algorithm. Encrypt ranks first overall, excelling in keyspace complexity, while AES-Crypto performs well in ciphertext randomness and specific avalanche impact tests. EnDe-Crypto shows good results in a few clear texts in avalanche impact analysis, and Kryptokaz performs well but the lowest. While none of them completely follow the Kerkhoff principle, they all exhibit strong cryptographic capabilities, providing secure communication. [4]

IV. RESULT:

A. What are the Problems targeted? (RQ1)

In this section, we will provide an answer to Research Question 1 (RQ1). For this question, it was necessary to consider a number of factors that hinder both instant messaging systems and UAV communication systems. From this analysis, we were able to outline five key problems:

1) Privacy and Security Concerns:

- Weaknesses in Encryption Mechanisms Messaging applications such as WhatsApp and Signal have different usages for the Signal interface. The centralized encryption

Paper Title	Methods/Approaches	Datasets	Evaluation Metrics
Blockchain-based Trusted Instant Messaging	Blockchaintechnology, data encryption, DID	IPFS, Distributed identity (DID)	Privacy, security, decentralized communication
Blockchain-enabled Endto-End Encryption	Blockchain for E2EE, Ratchet forward encryption	Androidapplication data, Ethereum blockchain	Encryption strength, decryption efficiency
A Secure Blockchainbased Communication for UAVs	Blockchain, UAV protocols, elliptic curve DH	UAV network simulations, cryptographic methods	Security, throughput, data integrity
The Existence of Cryptography: A Study on IM	Cryptographic algorithms in IM, Signal protocol	IM applications, Signal protocol analysis	Security, encryption algorithm efficiency
Making P2P Accountable without Losing Privacy	Privacy-preserving accountability models	Not specified	Privacy protection, accountability
Secure Instant Messaging Application in Prenatal Care	Secure messaging techniques, healthcare data	Prenatal care data	Security, usability, adaptability

TABLE I EVALUATION MATRIX

key server that WhatsApp uses poses great risk. This configuration poses a risk of man-in-the-middle (MITM) attack, session snatching, and modification of data exchange [7].

- Data Breach by Backups WhatsApp, for instance, keeps its users' information on the cloud through Google Drive and iCloud. Since the decryption keys are solely stored on WhatsApp servers, there is great potential that attackers may use the servers in an attempt to and gain access to the messages [7].
- Cybersecurity in UAVs Once the mission of UAV (Unmanned aerial vehicle) communication systems is set i.e. search and rescue, the risk to the UAV increases. Therefore there is need for appropriate measures to robust encryption and consensus protocols to protect data sent over the air [4].
- Encryption Claims that Mislead: One encryption feature that is marketed by many instant messaging apps is end to end messaging but hardly any of these have the ability to offer quality assurance. This unfortunately leads to users being overly confident in the security features implemented [6].
- Reliance on Centralized Managed Servers: Legacy messaging services and PKI systems employ central servers to manage certificate authorities and certificate-based key pairs. This dependency creates numerous single points of failure making it costly to deploy widely [7] [4]
- UAV Networks Control: Lastly, noise such as communication from a master UAV to a ground control unit (GCS) creates a centralized control in UAV networks and make them disabled. Both the GCS and master UAV may lose connection to the rest of the network and lose integrity as a result [4]

- Barriers to the Practical Application of Blockchain Technology: Most basic characteristic of a blockchain network is decentralization, however, it is faced with many barriers which affect usage in the real world such as delay, capacity and block size. This problem is particularly more worrying when looking at real time systems, such as UAV communication systems or IM services, etc. [4]

- Server's Custodianship of the Encryption Keys: User encryption keys are stored on the servers of applications such as WhatsApp, a fact that alters the trust users have in service that they are using because it allows the service to decrypt their messages [7].
- Lack of Independent Verification: Some messaging tools do not allow third party assessments of the proprietary encryption techniques that they have employed, such as what is the case with WhatsApp. Such a lack of openness makes it Increasingly daunting to trust the encryption process used to secure the messages in these applications [7]
- Widespread Dependency on Trust in Centralized PKI: Trying to manage a global system is extremely expensive and difficult to install, as it requires centralized PKI supliers to trust certain people or businesses to give out and maintain certificates [7].

- User Data Monetization: Many messaging apps, for example WhatsApp, sometimes disclose user account information, account details, connections, and payment methods to its parent Facebook in order to sell them potential ads. This behavior is intrusive to user privacy as it can lead to the manipulation of personal information [7]
- Shortage of Resources in UAV Systems: The application of blockchain technology into UAV networks can add tremendous resource consumption in terms of processing and storage. This also limits the growth of Blockchain use in a practical setting [4].
- Cryptographic Efficiency Trade-offs: AES is prevalent as a robust cryptographic algorithm, but some inefficiencies can be observed in its use in light weight systems, UAVs, and other devices with constrained resources [6].

- Infiltration of Group Chats: Group attachments to platforms like WhatsApp can easily infiltrated by attackers taking advantage of poor use of authentication mechanisms between group members and malicious users. This subtle but powerful flaw can allow unauthorized changes to group metadata and facilitate dropping of messages without any warning [7]
- Weak Delivery Guarantees: Depending on their chat application of choice, such as Signal, they may not have strong guarantees of delivery integrity for group messages. Such incompleteness lets adversaries to remove, reorder or create duplicate messages and as a result, disrupt the reliability of the communication [6]. This not only serves our purpose to improve secure reliable communication of the messaging applications and UAV's but also emphasizes on the need for more such research in this area.

B. What are the techniques used in the studies? (RQ2)

Year	Technology Used	Study
2021	Instant Messaging	[10]
2022	Instant Message Encryption	[7]
2020	UAV Communication	[4]
2017	Cryptography in Instant Messaging	[6]
2007	P2P Accountability	[1]
2020	Prenatal Care Messaging	[3]
2004	Secure Email with ECC	[5]

TABLE II
TECHNOLOGICAL TRENDS OVER TIME

- End-to-End Encryption (E2EE) End-to-end encryption (E2EE) guarantees that only the sender and the intended recipient can read the contents of a message, adding a vital layer of security to communications. Raman Singh et al. discuss how E2EE can be integrated with blockchain technology to create secure messaging systems. By using cryptographic methods such as public-private key pairs, messages are encrypted by the sender and can only be

decrypted by the recipient. This ensures that no third party, including service providers or potential attackers, can intercept the communication. The combination of E2EE and blockchain also allows for the secure distribution and management of encryption keys without the need for centralized authorities. Furthermore, the decentralized and immutable characteristics of blockchain offer a trustworthy way to verify keys, significantly reducing the risks associated with traditional key exchange methods [7].

- Decentralized Identity (DID) Decentralized Identity (DID) refers to a system where users create and manage their own digital identities independently of central authorities. Huiyuan Wang et al. explain how blockchain can be utilized to establish a DID-based framework for secure and private messaging. In this setup, a user's DID is recorded on the blockchain and associated with their public key, ensuring that their identity remains secure from falsification or tampering. Unlike conventional systems that depend on a central database for user credentials, DIDs mitigate the risks of data breaches and centralized control. Users can create multiple DIDs for various applications, which helps to prevent the linking of their identities and enhances privacy. During communication, DIDs are exchanged and verified through blockchain, enabling users to authenticate one another without disclosing personal information. This method safeguards against identity theft and unauthorized access while ensuring that users retain full control over their identity data [10]
- The Interplanetary File System (IPFS) The Interplanetary File System (IPFS) is a distributed storage protocol that shifts from location-based file retrieval to content-based addressing, which enhances data management in terms of efficiency and security. Huiyuan Wang and colleagues incorporate IPFS into their blockchain-enabled instant messaging system to facilitate secure file storage and sharing. In this setup, files are broken down into smaller pieces, each with a unique cryptographic hash, and spread across the IPFS network. Users can access content by its hash, which guarantees that the data remains tamper-proof and verifiable. Unlike conventional server-based storage, IPFS removes single points of failure and provides redundancy, ensuring that files remain accessible even during network disruptions. This distributed model also lessens reliance on centralized servers, which aligns with the decentralized principles of blockchain technology. By integrating IPFS into messaging systems, both the speed of data transfer and the security of shared content are improved, allowing for scalable and dependable communication. [10]
- Smart contracts Smart contracts are agreements that execute themselves and are stored on the blockchain, aimed at automating specific actions based on set conditions. In messaging systems, Huiyuan Wang and his team use smart contracts to send automated notifications when a message is received. These contracts operate transparently and cannot be modified once they are deployed, which helps maintain the integrity of the automated processes. For example, in a decentralized messaging environment, when a user sends an encrypted file, a smart contract ensures that the recipient receives a notification along with the necessary decryption instructions. This approach removes the need for intermediaries to oversee and manage message delivery. Similarly, Mira Belenkiy and her team investigate the application of smart contracts in resource-sharing systems to facilitate fair exchanges. These contracts promote accountability and automate transactions, ensuring that users meet their obligations without the need for manual intervention. [10] [1]
- Privacy-preserving cryptographic techniques Privacypreserving cryptographic techniques, including Elliptic Curve Diffie-Hellman (ECDH) and Merkle Trees, play a vital role in securing communication and ensuring data integrity in decentralized systems. Huiyuan Wang and colleagues emphasize the importance of ECDH for secure key exchange, which allows encryption keys to be shared safely without the risk of interception. Moreover, Merkle Trees are utilized to efficiently verify data integrity by representing large datasets with a single cryptographic hash. This approach enables users to confirm the authenticity of data without needing to access the entire dataset. For instance, in a decentralized messaging system, Merkle Trees can help verify that file fragments retrieved through IPFS remain unaltered. These cryptographic methods facilitate secure and efficient communication while

reducing computational overhead, making them ideal for large-scale decentralized applications [10]

V. CONCLUSION

This review highlights the transformational potential of blockchain in secure messaging, addressing critical challenges such as data privacy, decentralization, and security The analyzed studies identify various approaches, including cryptographic development, decentralized frameworks, and including machine learning integration The most important barriers are the same. Future research will focus on optimizing blockchain networks to support real-time transactions and seamlessly integrate with existing systems. By addressing these challenges, blockchain technology can lay a solid foundation for secure and reliable networks across applications.

REFERENCES

[1] Mira Belenkiy, Melissa Chase, C. Erway, John Jannotti, Alptekin Kupc¸¨ u, Anna Lysyanskaya, and Eric Rachlin. Making p2p accountable¨ without losing privacy. pages 31–40, 10 2007.

[2] U. Ellewala, W.D.H.U Amarasena, H.V Lakmali, L.M.K Senanayaka, and Amila Senarathne. Secure messaging platform based on blockchain. pages 317–322, 12 2020.

[3] Osnat Ezra, Arik Toren, and Eldad Katorza. Secure instant messaging application in prenatal care. *Journal of Medical Systems*, 44, 04 2020.

[4] Elias Ghribi, Tala Talaei Khoei, Hamed Taheri Gorji, Ranganathan Prakash, and Naima Kaabouch. A secure blockchain-based communication approach for uav networks. pages 411–415, 07 2020.

[5] Wongoo Lee and Jaekwang Lee. Design and implementation of secure e-mail system using elliptic curve cryptosystem. *Future Generation Computer Systems*, 20(2):315–326, 2004. Modeling and simulation in supercomputing and telecommunications.

[6] Vania Liwandouw and Alz Wowor. The existence of cryptography: A study on instant messaging. *Procedia Computer Science*, 124:721–727, 01 2017.

[7] Raman Singh, Ark Nandan, and Hitesh Tewari. Blockchain-enabled end-to-end encryption for instant messaging applications. 06 2022.

[8] Ben Smith and Konstantinos Christidis. Ibm blockchain: An enterprise deployment of a distributed consensus-based transaction log. In *Proc. Fourth International IBM Cloud Academy Conference*, volume 210, 2016.

[9] M Sowmiya and S Prabavathi. Symmetric and asymmetric encryption algorithms in cryptography. *Int J Recent Technol Eng*, 8(1S2):355–7, 2019.

[10] Huiyuan Wang, Yimin Yu, Jinyi Zhao, and Jingyi Wang.
Blockchain-based trusted instant messaging model research. In *2021 4th International Conference on Hot Information-Centric Networking (HotICN)*, pages 32–37, 2021.

[11] Haibo Yi. Securing instant messaging based on blockchain with machine learning. *Safety Science*, 120:6–13, 12 2019.