Towards Trustless Messaging: Blockchain Architectures and Economic Implications

Shubham Deshmukh., Ruchita Deodhar., Ritika Mahajan., Dr. Prof. Swapna Bhavsar

Progressive Education Society's Modern College of Engineering Pune, India

DOI: https://doi.org/10.51244/IJRSI.2026.1303000173

Received: 22 March 2026; Accepted: 27 March 2026; Published: 12 April 2026

ABSTRACT

Blockchain technology provides a platform for developing secure and decentralized communication systems such as chat applications through transparent and trustless interactions across a distributed blockchain network, without the need for centralized servers. In these communication systems, smart contracts manage decentralized identities, control access permissions and validate message transactions. This ensures that the communicated data remains immutable and tamper proof. Authentication and privacy are achieved using cryptographic techniques such as hashing, digital signatures, public-private key, and encryption. Inter Planetary File System (IPFS) is commonly implemented to handle the immense amount of data generated in a chat-based communication system while still maintaining the ability to verify the data through cryptographic hashes. From a design perspective, blockchain-based chat applications offer enhanced data ownership, stronger integrity guarantees, and improved resistance to censorship and single points of failure. However, challenges related to scalability, latency, transaction costs, and usability continue to affect practical deployment. Addressing these issues is essential for enabling real-world adoption and large-scale implementation of decentralized blockchain-based communication systems.

Keywords: Blockchain, decentralized chat application, interplanetary file system (IPFS), secure communication

INTRODUCTION

Instant messaging services are now an essential element in modern digital communication, enabling social, organisational, and personal communication. In order to handle user authentication, message routing, and data storage, popular platforms like WhatsApp, Telegram, and Signal primarily rely on centralized server-based architectures [1], [2]. While these systems offer convenience and scalability, their centralized nature introduces several limitations single points of failure, vulnerability to data breaches and dependence on reliable third parties [2], [6]. Centralized servers often control over message routing and metadata information even when end-to-end encryption is used, which has raised ongoing privacy and trust concerns [6], [7].

By distributing control across peer-to-peer (P2P) networks, decentralized communication has emerged as a practical alternative to centralized messaging models [3], [4]. In such systems, users communicate directly with one another, which improves fault tolerance and strengthens resistance to censorship [4], [7]. Despite these advantages, purely P2P messaging systems face challenges related to trust establishment, identity management, message integrity, and coordination among mutually untrusted participants [2], [7]. Blockchain technology addresses these limitations by providing a distributed and tamper-resistant ledger that enables secure and trustless interactions between communicating parties [1], [5].

Decentralized chat apps can accomplish transparent coordination, secure identity management, and unchangeable message verification without centralized oversight with the help of blockchain [5], [9]. Blockchain based chat systems can ensure data integrity and accountability while ensuring user autonomy by incorporating cryptographic primitives, and smart contracts [6], [10]. The majority of contemporary methods use hybrid architectures, which store message content off-chain using decentralized storage solutions [5], [7], [12].

In recent years, blockchain-based chat applications have been widely explored through research studies and prototype implementations, with proposed solutions built on platforms such as Ethereum and decentralized

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

storage networks [3], [6], [9], [10]. At the same time, industry-led Web3 messaging platforms have begun integrating blockchain components to enhance privacy, interoperability [12], [13]. Despite this growing interest, existing work often focuses on specific implementations or architectural models and lacks a comprehensive comparative analysis of the broader design space [11], [14], [15].

Inspired by this gap, this paper offers a brief introduction of blockchain-based decentralized chat applications. This survey attempts to give researchers and practitioners a clear picture of the present situation and potential future directions of blockchain-based decentralized communication systems by summarising previous research [1]-[15].

Blockchain Enables Trustless And Decentralized Communication

Conventional chat applications rely on centralized servers for user authentication and message exchange, which creates a strong dependency on a single controlling authority. Blockchain technology enables decentralized communication by allowing peer-to-peer interaction across distributed networks. Through a shared ledger maintained by multiple nodes, no single entity can fully control, modify, or censor communication data, thereby improving transparency, fault tolerance, and system resilience [1], [7].

In blockchain-based chat systems, cryptographic techniques such as public–private key pairs, hashing, and digital signatures are used to authenticate users and ensure message integrity. Messages, or their corresponding cryptographic hashes, can be stored on the blockchain, making unauthorized modification or forgery computationally impractical. This design allows participants to independently verify communication events without relying on trusted intermediaries, supporting secure and trustless interaction among untrusted peers [3], [11].

Consensus mechanisms further strengthen decentralized communication by requiring network-wide agreement on message-related transactions. Even in the presence of potentially malicious nodes, consensus protocols ensure that the system maintains a consistent and reliable state [3], [10]. This collective validation process strengthens confidence in message authenticity and ordering across the network.

Smart contracts play a crucial role in automating identity management, access control, and message verification within blockchain based chat platforms. These programmable contracts enforce predefined rules in a transparent and immutable manner, significantly reducing the need for centralized authentication servers. Existing studies indicate that decentralized identity models implemented using smart contracts enhance system security, decentralization, and fault tolerance while also offering greater flexibility in managing user identities and permissions [4], [6].

Apart from the security and trust advantages, the encrypted communication systems using the blockchain technology allow users more autonomy to control their own identity and communication data. This is different from the central systems that allow users to access services using their identity and metadata stored by the providers of such services. With the decentralized systems, users are given the autonomy to control their identities using cryptographic keys. This makes users depend less on any third-party platform and minimizes risks associated with the misuse of their data and/or unauthorized surveillance.

Moreover, the integration of blockchain with off-chain and hybrid architectures makes it feasible to implement decentralized messaging applications. As blockchain provides security, integrity, and coordination, the other system is responsible for managing messages in an appropriate and efficient way. It has been observed that blockchain-based communication systems are well suitable for messaging applications because it helps in balancing decentralization with performance. Existing literature reveals that improvements in architecture are being pursued for better user experience and efficiency.

Although the advantages are clear, the adoption of blockchain messaging systems is set to experience new challenges, especially with regard to usability and complexity. This is due to the fact that users would need to manage crypt keys, meaning that the loss of private keys would result in the loss of identities for communication.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

Furthermore, the use of wallets and smart contacts is likely to lead to system complexity in the use of blockchain messaging systems, especially by ordinary users. This poses significant challenges in terms of developing key management and recovery systems that will improve the usability of blockchain messaging systems.

Architectural Models Of Blockchain-Based Chat Systems

Chat systems on blockchain can be classified into fully on-chain solutions and hybrid models, depending upon where the messages and metadata are stored. The architecture matters a lot when it comes to latency, cost, scalability, and integrity.

Fully On-Chain Architecture:

In a completely on-chain solution (Fig. 1), all message contents, metadata, and interactions performed by the users are stored on the blockchain itself [5], [6]. Users can send messages that are verified by nodes in the network, and all transactions are stored permanently in the blockchain. This makes the solution completely transparent and immutable as any user can verify message authenticity independent of others.

This system has high latency requirements, as every message has to undergo the consensus process before being considered finalized. Also, the high gas cost associated with storing the content of the messages directly onto the chain makes communication inefficient [5], [6], [10]. This latency overhead significantly impacts real-time communication scenarios where low delay is a critical requirement. As the number of participating nodes increases, the time to reach consensus can further degrade system responsiveness.

The system design has scalability issues due to the continuous expansion of the blockchain for every message sent. Nonetheless, the design ensures completely trustless functionality without the involvement of any central server for all transactions to be verifiable by anyone [1], [5].

This trade-off highlights the inherent tension between decentralization and performance in blockchain-based communication systems. Increased storage requirements impose additional burden on node operators, potentially limiting network participation. These challenges motivate the exploration of hybrid and off-chain approaches to improve efficiency while preserving trustless guarantees.

Fig. 1. illustrates how users interact with smart contracts, which handle message submission and verification. All message data is stored directly on the blockchain as transactions, and each message requires payment of gas fees. Every message sent by users is processed through smart contracts and permanently recorded on the blockchain.

Fig. 1 also highlights the economic and performance implications of this approach. Each message transaction requires the payment of gas fees, which increases the cost of communication, particularly in high-frequency messaging scenarios. Moreover, because messages must pass through the consensus process before being finalized, the system experiences higher latency. As indicated in the figure, these factors collectively result in high operational costs and delayed message delivery, making fully on-chain architectures unsuitable for real-time chat applications inspite of their strong trustless and security guarantees.

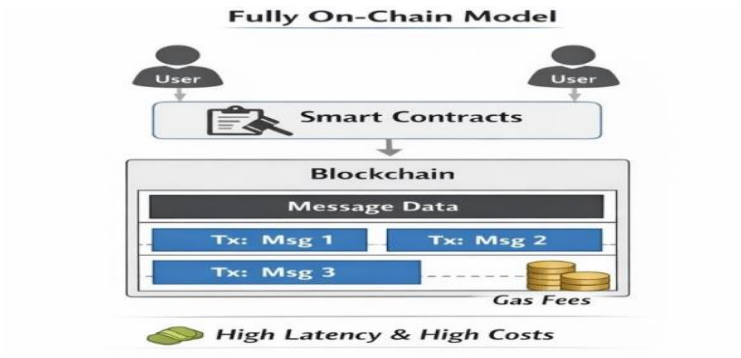

Fig. 1. Fully On-Chain Architecture of Blockchain-Based Chat System

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

Hybrid Architecture:

The hybrid model (Fig. 2) is commonly seen in the current state-of-the-art blockchain-supported chat systems due to its efficiency and scalability [5], [7], [12]. In this model, the actual message contents are maintained outside the blockchain in decentralized storage solutions like IPFS and metadata, message hashes, and transaction information are stored in the blockchain. This reduces the transaction costs as well as storage costs without sacrificing the safety and integrity of the blockchain [5], [7].

Smart contracts form the centrepiece of hybrid architectures in managing identity, access control, and message indexing by storing pointers to the content of messages running off-chain, permissions verification for users, and maintaining an auditable log of message hashes. This reduces on-chain storage overhead while retaining verifiability of communication events. By limiting blockchain interactions to metadata and control logic, the system achieves improved efficiency without compromising security guarantees.

With this design, the system ensures that only authorized users can access messages, while at the same time preserving immutability and accountability [6], [9], [12]. In fact, hybrid architectures effectively integrate decentralization and trustless verification of blockchain with high performance and scalability of off-chain storage solutions that make them very proper for real-time chat applications [5], [7]. Such architectures enable low-latency message delivery suitable for interactive communication.

Fig. 2. illustrates the hybrid architecture, whereby users send messages, each of which is stored on IPFS, with metadata and cryptographic hashes stored on-chain. Smart contracts manage access, identity, and indexing for secure and verifiable communication. It emphasizes some of the efficiency gains, a resultant reduction in gas costs, and reduced network congestion compared to a fully on-chain model.

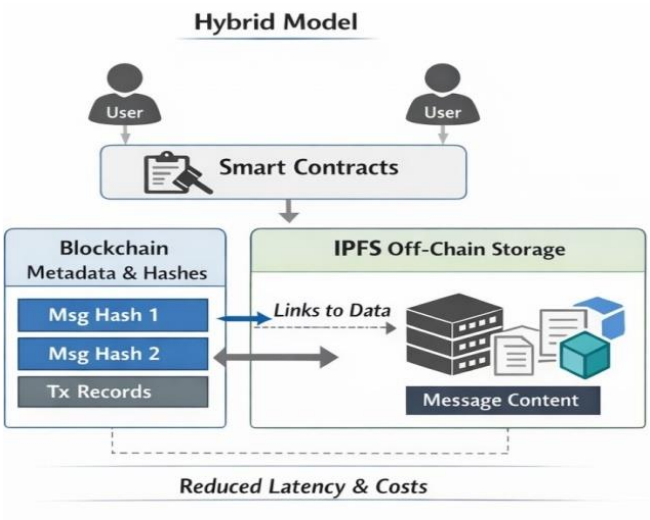

Fig. 2. Hybrid Architecture of Blockchain-Based Chat System

Off-Chain Architecture:

This off-chain model is an architecture that includes all of the communication logic and message content completely outside of the blockchain [1], [2]. In this case, user interaction will be directly with off chain messaging and storage services, i.e., distributed file systems and/or standard cloud-based databases to store and retrieve message data [3]. The use of off chain message payloads will reduce communication latency and operational costs by removing the overhead of on chain data storage and transaction execution [4].

Unlike the other two architectures described above, in this model, blockchain acts as an optional support tool instead of being the primary communication medium [1], [5]. Blockchain's primary function is to act as a reference point to store or validate metadata related to the off chain messages (e.g., transaction records, hash values, etc.) or to prove the integrity of a message via lightweight metadata (e.g., cryptographic checksums) [6], [7].

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

By separating off chain messaging from optional on chain anchoring, this architecture provides better scalability than the fully on chain and hybrid models [1], [8]. Since each message exchanged requires no blockchain consensus nor does it incur transaction fees per message, this architecture allows for higher frequency messaging and thus supports more efficient messaging scenarios when there is a need for high frequency messaging (i.e., real time messaging) [3], [9].

Fig. 3 illustrates how blockchain can be selectively added to decentralized communication systems to add integrity and keep the efficiency of the existing messaging infrastructure as a whole [2], [6]. Overall, this architecture shows the benefit of reducing the dependency on blockchain execution and storage, thus providing a realistic tradeoff between decentralization and system performance, and makes it an attractive alternative for scalable and cost sensitive decentralized chat applications [1], [4], [8].

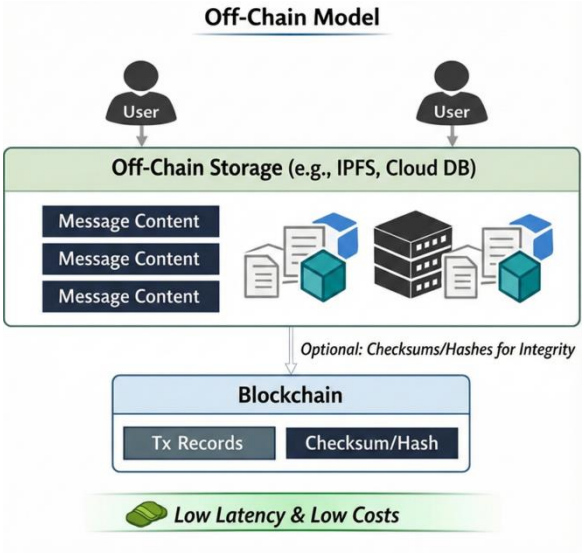

Fig. 3. Off-Chain Architecture of Blockchain-Based Chat System

Decentralized Identity And Key Management

Decentralized messaging apps have made use of decentralized identity systems constructed through wallets instead of a central inputting server for identity authentication. Instead of logging in with a username and password, users rely on blockchain addresses generated from cryptographic key pairs. This approach removes the need for any central authority to manage identities [1], [7].

Public key cryptography is the basis for secure peer-to-peer authentication in blockchain messaging systems. When someone wants to send a message, they sign it with their private key, and others verify it using the public key. This way, authentication stays secure with no personal details leak, and users can't deny their actions later. [6], [12].

Smart contracts take identity and access management a step further. They automate authentication rules and restrictions, making the process clear and unchangeable. They can control operations like registering a user, accessing a message, or joining a group, providing for a decentralized system to manage identities automatically. Research shows that identity management through smart contracts really does boost both security, identity management and decentralization. [4], [9].

Even with these benefits, wallet-based identity systems aren't always easy to use. If you lose your private key or it gets stolen, your identity is gone for good. The absence of the recovery option in the decentralized identity infrastructure platforms makes identity technologies using wallet architecture difficult to use by novice users [2], [11].

The key management and recovery phase has to be addressed for the large-scale adoption of decentralized chat solutions. Researchers are working on things like letting trusted contacts help you recover your keys, using

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

multi-signature wallets, and blending different identity systems together. But balancing security with a smooth user experience is still a big challenge for decentralized identity management. [8], [15].

Message Integrity And Privacy

Message integrity in a decentralized chat means no one can secretly change, remove, or forge messages without detection. In most traditional messaging apps such as WhatsApp when you edit or delete message and replace or delete the earlier versions. There's no way to see what was originally sent. Lack of history traceability can be easily used for spreading misinformation, manipulating disputes, or malicious activities . In some cases previous states of messages cannot be independently verified [2], [6]. Blockchain-based systems solve this issue by maintaining unalterable message logs, saving cryptographic hashes and timestamps of those messages are permanently recorded on the ledger, which makes any attempt to make modifications detectable and auditable [1], [5].

This immutability in the blockchain makes sure that any message reference marked in the blockchain cannot be modified without the consensus of the whole network. This is regardless of whether the message added to the blockchain is done offline; the hash of the message in the blockchain is used to verify that indeed the message is as presented. This is because if the message is modified or altered in any way, the hash value will no longer be valid for the message, thereby creating authenticity of evidence [7], [10]. Immutability is more significant for message communication security, specifically in scenarios in which accountability is required [10].

While immutability protects the data, privacy has been established through the systems employing encryption-based practices. Data in the blockchain is transparent by nature; therefore, messages that are sent through distributed platforms have to employ end-to-end encryption methods before being retained or before being sent out. The sender and receiver alone have to decrypt these messages to remove nodes and third parties access to the messages on the distributed platform. A combination of immutable data and rigorous encryption practices for off-chain data storage allows distributed platforms to possess the perfect amalgamation of data traceability and data privacy regarding the misuse of distributed platforms for the quick communications blockchain [6], [9], [12].

Wallet – Based Authentication And Smart Contract Integration

Wallet-based authentication has taken the stage, sending traditional centralized authentication servers to the backburner, when we talk about blockchain-enabled messaging systems. Gone are the days when usernames and passwords were stored remotely. Users now authenticate themselves using blockchain wallets that manage cryptographic key pairs.[1], [7]. Well-known, a user's public key becomes a decentralized identifier, whereas the private key serves as the authentication credential and gives the owner complete control over their digital identity. The dependence on centralized infrastructure for storing and verifying these credentials has been cut down, and, since private keys don't leave the user's wallet, mass-scale data breaches are nearly impossible to occur.

This approach brings people closer to the principles of decentralization and self-soignty by enabling them to shield their identity information and interact with decentralized chat platforms without handing out their personal data to third parties.

MetaMask is probably one of the most popular wallet interfaces that link users with blockchain applications. Coming as both a browser extension and a mobile wallet, MetaMask securely manages the user's private keys and empowers the cryptographic signing of transactions all the while never revealing the key materials to the applications themselves. This provides users with strong guarantees of security as they sign up, log in and engage in conversations with blockchain-based chat systems[7],[9].

Many decentralized messaging platforms integrate MetaMask to provide a seamless wallet-based login experience and facilitate interaction with messaging-related smart contracts. Through this integration, users can authorize actions such as sending messages, registering identities, or managing access permissions using

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

cryptographic signatures, eliminating the need for traditional login credentials. This improves security while preserving ease of use for users already familiar with blockchain wallets.

Smart contracts play a crucial role in supporting wallet-based authentication within decentralized chat platforms. These contracts define and enforce rules related to user registration, access control, and message validation in a transparent and tamper-resistant manner. Because smart contracts operate on the blockchain, all authentication and authorization logic remains publicly verifiable and resistant to unilateral modification.

The marriage of wallet-based authentication and automated smart-contract-driven logic takes identity management and coordination to a brand new level by completely eliminating the reliance on intermediaries. In spite of the numerous merits, usability problems and complications with wallet interfaces and private key administration mean there is more to be done to popularize these systems [4], [11], [15].

Off-Chain Support For Multimedia Messaging

Blockchain technology is highly effective in maintaining data integrity and supporting decentralized coordination across distributed systems. Its cryptographic foundations and consensus mechanisms make it well suited for secure record keeping and trustless interaction. But, these strengths do not translate into efficiency when handling large-scale multimedia communication.

Multimedia data such as images, audio clips, and video files are inherently large in size and require substantial storage capacity and bandwidth. Blockchain networks, by design, have limited throughput and constrained block sizes, which makes the direct storage of such data impractical. Attempting to store multimedia content on-chain results in excessive resource consumption.

Storing large files directly on a blockchain significantly increases transaction costs due to higher gas fees. In addition, each large transaction contributes to rapid blockchain growth, increasing the storage burden on participating nodes. This expansion negatively affects network performance by slowing down block propagation and increasing overall latency [5].

These limitations are particularly problematic for communication systems that demand real-time or near real-time data exchange. Increased latency caused by consensus delays and data replication can disrupt the user experience, making fully on-chain multimedia messaging unsuitable for chat applications.

To overcome these challenges, blockchain-based communication platforms increasingly rely on off-chain storage solutions implemented through decentralized storage systems. These systems are designed to store large volumes of data outside the blockchain while preserving redundancy, availability, and resistance to single points of failure.

In hybrid architectures, multimedia content is uploaded to decentralized storage networks, while only essential references such as cryptographic hash values, content identifiers, or access pointers are recorded on the blockchain. This reduces on-chain storage requirements while still allowing message authenticity and integrity to be verified [5], [12].

Therefore, hybrid architectures have emerged as a practical solution for scalable multimedia messaging. In these systems, blockchain technology is primarily used for coordination, identity management, access control, and verification, while decentralized storage handles content delivery. This division of responsibilities enables efficient transmission of audio, image, and video messages without compromising immutability or trustlessness. Its effectiveness can be seen in prior studies, such as the work by Dalvi et al., which combines blockchain with decentralized storage to achieve secure and scalable multimedia communication [5].

Economic Impact Of Digital Currency Usage

Digital currencies in blockchain-based chat applications introduce a different economic layer that affects usability, scalability, and mass adoption directly. Unlike the centralized ones where message transmission is free from end users, blockchain-based systems usually ask their users to pay a transaction fee to record messages like

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

operation indexing, identity registration, or access control on the ledger. These fees change when transactions surge heavily and also depend on demand. This makes communication costs unpredictable and often times too expensive for routine messaging [1], [2]. This is an economic overhead which traditional models do not have.

Transaction fees form a double-edged incentive as well as a constraint. In a network context, transaction fees serve as a motivator for miners/users to maintain a consensus method that is free from attacks and spam. But when considering chat applications that have recurrent interactions among users, even a small fee for a transaction can be prohibitive. In a congested Ethereum network, for instance, research has demonstrated the inefficiency of keeping every message recorded on a blockchain by charging a few dollars for a single transaction [3]. Users in developing countries are the worst affected by such high fees that can make blockchain-based chat applications seem unrealistic for social interactions [4].

Most blockchain messaging systems follow the cost-performance trade-offs achieved using architectural optimizations to overcome these challenges. Hybrid approaches reduce the number of operations performed on-chain by recording only the required metadata, which can be message hashes or timestamps, on the blockchain and storing the actual message contents on decentralized storage systems such as IPFS and Filecoin. These systems greatly reduce gas expenses without impacting integrity. Experiments have shown that the security and audibility of messaging can be maintained while the cost of operations is reduced to below 90 percent compared to the cost of operating messaging on the blockchain [5], [6].

Another economic factor at play is the use of layer-2 (L2) scaling solutions and other blockchains. By layer-2, one means a layer of technology built upon the top of a blockchain (layer-1) to improve the rate of transactions and the associated fees, without having to use the original blockchain. These kinds of scaled-down transaction fees and rates are offered by scaled-down versions of Ethereum, such as Polygon, Arbitrum, and Optimism. Various messaging apps have successfully implemented message indexing and identification in such a setup to the point of having near real-time functionality with essentially no charges for each interaction [7]. There are naturally some trade-offs involved in decentralization and trust models in such L2 networks.

This usage of digital currency also enables new models of motivation within decentralized communication environments. These tokens can be used to punish spammers, reward good behavioural practice, or support communication network upkeep via micropayments. For example, certain models involve participants staking a small amount of tokens to begin communication, with these tokens refunded if communication is successful, thus preventing spammers while still allowing communication [8]. Economically very innovative, these models add complexity to communication systems that may work to exclude legitimate participants if not careful.

The economic impact of digital currency usage is a crucial factor that defines the viability of blockchain-based chat applications. Although transaction fees and cost variability are clearer barriers to adoption, advances in hybrid architecture, off-chain storage, and scalable blockchain networks have steadily reduced these limitations. Long-term feasibility is ensured only if the balance between decentralization benefits and predictable, low-cost interaction models can compete with centralized messaging platforms in terms of user experience and affordability [2], [9].

CHALLENGES

Performance Challenges:

Performance is one of the major weaknesses of blockchain-based decentralized chatting applications, especially if compared to common real-time messaging systems. This is because, in public blockchain systems, there is a consensus process that verifies transactions. This leads to unavoidable latency because of the need to create a block and reach consensus. This is not suitable for instant messaging, which requires low latency to instantly send messages [1], [7].

In decentralized messaging systems, even the simplest operations like message verification, authentication of identities, and establishing connections often entail blockchain transactions. Whenever these transactions happen with high frequency, the speed of communication is affected adversely, especially when the network is

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

congested. This directly impacts the efficiency of blockchain mechanisms when used directly for messaging purposes.

Other performance constraints come from the transaction capacity and synchronization over the network. A public Ledger can only process a few transactions in the time span of one second. This makes such Ledgers limited to the extent to which multiple conversations can be performed. This makes the current possibility of doing conversations fully online inefficient [3], [10].

In view of these challenges, several systems have resorted to minimizing on-chain interactions by using the blockchain only for "critical verification" tasks while performing "message exchange" off-chain [17]. The trade-off between decentralization and real-time performance is still a research focus [6], [15].

Scalability Challenges:

Scalability emerges as another problem with decentralized messaging applications as the number of users as well as the number of messages being exchanged goes up [3]. In the case of public blockchains, each transaction has to be verified and recorded by all the nodes, thus leading to increased storage as data about messages gets stored [1].This continuous expansion of the blockchain places a heavy burden on participating nodes.

The large number of transactions associated with the messages causes the size of the blockchain to increase, resulting in scalability issues as it becomes difficult to participate in the network, especially when one considers the light clients whose resources are minimal [9], [14].

Additionally, the fee charged in cases where scalability is hindered. Consequently, the more the network is utilized, the more the users pay, which is a disadvantage that affects the scalability of the network [11], [12].

In order to scale, most systems include hybrid or permissioned blockchain architectures, in which participation or on-chain data storage is limited or restricted [5], [10]. Even though hybrid blockchain architecture assists with scalability, a trade-off might occur between openness and scalability [5], [10].

Sustainability Concerns:

Blockchain technology faces serious sustainability issues, mainly due to certain consensus algorithms that consume massive amounts of energy. Proof-of-Work is a prime example, it requires so much computing power that it puts pressure on both the economy and the environment [8].

Consider decentralized messaging apps. Each time messages are sent and verified, they generate a surge of transactions. This nonstop activity further increases energy consumption. As a result, people are questioning whether blockchain can truly handle communication needs in the long term [1], [9].

Sustainability here goes beyond environmental concerns, Developers and the broader ecosystem encounter their own hurdles.. The maintenance of the smart contracts, the upgrading of the protocols, the security, among others, are continuous processes that require the expertise of the developers. The studies examining the discussions of the developers pointed out that the issues on sustainability affect the designs [8].

Consequently, various energy-efficient consensus protocols, permissions blockchains, as well as hybrid models have been researched with growing interest to make them more sustainable while still retaining their decentralization attributes [5], [15].

Long Term Feasibility:

The outlook for decentralized chat apps on the blockchain hinges on several important factors. The complexity of blockchain technology is a significant obstacle for most users, as highlighted in [2], [11].

Managing wallet identities introduces further challenges; users must safeguard their private keys, and losing those keys means permanent loss of access. There is still no reliable method for recovering lost keys, which is a major concern for anyone considering long-term use of these platforms [7], [12].

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

Feasibility in economic terms is also an issue, as the cost of transactions is volatile and may rise with time. This could make continuous use of the decentralized messaging systems expensive, such as on public blockchains, thus making them less attractive than the free centralized systems [9], [14].

The studies in the long run also depend on the adaptability of decentralized chat applications to technology changes.

Case Studies

bChat(Sourabh et al., 2020) [9]:

bChat is considered one of the earlier implementations to provide a decentralized messaging system based on Ethereum blockchain. bChat allow users to create unique decentralized identifiers via smart contracts these cryptographic pseudonyms don't depend on any central authority. Every message receives a timestamp and a hash, making it straightforward to verify that the message hasn't been altered since it was posted. Though this method ensures maximum message integrity and facilitates trusted communication between users, it involves high latency because it requires a message to be included in a block. It is also quite costly due to high transaction costs that do not allow users to send numerous messages. The system requires scalable blockchain design techniques, which should be implemented via Layer-2 technology or off-chain storage. bChat also focuses on the need for access control mechanisms where smart contracts check the sender and receiver addresses before storing messages. While there are significant challenges, this prototype is able to demonstrates that that blockchain-based messaging is achievable. To be viable in real-world scenarios, these systems need a thoughtful combination of blockchain security and more adaptable storage solutions.

BitChat (Patil & Chaudhari, 2025) [12]:

BitChat enhances the fully on-chain approach by using a hybrid model of blockchain and off-chain solutions to decrease the associated costs and latency. The system allows message metadata, which includes cryptographic hashes, timestamps, and access controls, to be maintained on the Ethereum blockchain. In contrast, messages that contain text, images, and audio files are maintained using decentralized storage solutions such as IPFS. The system ensures the immutability and auditing capabilities of messages without the need for high gas prices to store the large amount of data on the blockchain. The smart contracts enable identity validation, friendships, and message indexing. These contracts offer a way to authenticate and manage access using a decentralized system. The system ensures message integrity through the hash value stored on the blockchain. The use of the hybrid model helps to decrease the cost of transactions by over 90 percent compared to the fully on-chain model. The trade-offs involved in real-time communication where additional latency is brought forth by retrieving content off-chain are also highlighted. BitChat strikes an accurate balance between performance, security, and economic feasibility by integrating blockchain's security guarantees with scalable storage solutions. It sets a practical benchmark for building decentralized chat applications whose capacity could handle multimedia and large user bases. It also shows how cryptography, blockchain consensus, and user experience interact, thus forming an essential reference to future designs.

Aatmanirbhar Sanchar (Dalvi et al., 2024) [5]:

Aatmanirbhar Sanchar is a blockchain solution that is suitable to multimedia communication and tackles challenges present in audio, video, and image transmission in a decentralized setting. The system uses a hybrid approach that involves storing files on a decentralized storage system and storing only hash and metadata on a blockchain. Decentralized storage is used to address scalability and commercial viability associated with storing large files on a blockchain. All files on this system are encrypted before storage, and this provides users with perfect end-to-end privacy and protects files against any form of unauthorized access. Smart contracts handle identities and friend lists. Each file is verified through computationally efficient methods.

Aatmanirbhar Sanchar showcases enhanced scalability. A problem associated with early on-chain chat models has been addressed through an innovative approach and technology that integrates a blockchain solution and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

decentralized storage. Additionally, data control is provided to users on this system. The system has been tested to handle high-volume multimedia transmissions while maintaining low latency for critical operations.

Aatmanirbhar Sanchar thus serves as an epitome of how the purposes of security, privacy, and usability can all be reconciled in a single, hybrid blockchain architecture and represent state-of-the-art developments for decentralized multimedia chat applications.

CONCLUSION

This paper presented a comprehensive survey of blockchain-based decentralized chat applications, focusing on how blockchain technology addresses the limitations of traditional centralized communication platforms. By leveraging decentralized ledgers and smart contracts, these systems enable trustless communication, improved transparency, and strong data immutability. The analysis of different architectural approaches shows that while fully on-chain designs offer high integrity and security, they introduce significant challenges related to latency, scalability, and transaction costs. Hybrid architectures, which combine on-chain verification with off-chain storage, emerge as a more flexible and practical solution for real-world messaging applications.

The survey also examined key aspects such as decentralized identity management, wallet-based authentication mechanisms, privacy protection techniques, and the economic implications of digital currency usage. Although blockchain technology provides notable improvements in security and censorship resistance, several usability challenges remain, including private key management, fluctuating transaction fees, and system complexity. These factors currently limit widespread adoption among non-technical users. Future research should focus on enhancing usability, reducing economic barriers, and improving scalability through optimized architectures, layer-2 solutions, and user-centric design approaches. Addressing these challenges is essential for decentralized chat applications to compete effectively with centralized messaging platforms in terms of affordability, performance, and user experience.

REFERENCES

1. P. Zheng, Z. Jiang, J. Wu, and Z. Zheng, “Blockchain-Based Decentralized Application: A Survey,” IEEE Open Journal of the Computer Society, vol. 4, pp. 121–133, 2023, doi: 10.1109/OJCS.2023.3251854.
2. H. Jang, S. H. Han and J. H. Kim, “User Perspectives on Blockchain Technology: User-Centered Evaluation and Design Strategies for DApps,” IEEE Access, vol. 8, pp. 226213–226223, 2020, doi: 10.1109/ACCESS.2020.3042822.
3. M. S. Farooq, Z. Kalim, J. N. Qureshi, S. Rasheed, and A. Abid, “A Blockchain-Based Framework for Distributed Agile Software Development,” IEEE Access, vol. 10, pp. 17977–17995, 2022, doi: 10.1109/ACCESS.2022.3146953.
4. J. Zhou, T. Jiang, H. Wang, M. Wu and T. Chen, “DAppHunter: Identifying Inconsistent Behaviors of Blockchain-based Decentralized Applications,” Proc. IEEE/ACM ICSE-SEIP, Melbourne, Australia, 2023, pp. 24–35, doi: 10.1109/ICSE-SEIP58684.2023.00008.
5. S. Dalvi et al., “Aatmanirbhar Sanchar – Blockchain Based Approach for Multimedia Communication,” Proc. IEEE ICBDS, Pune, India, 2024, pp. 1–6, doi: 10.1109/ICBDS61829.2024.10837422.
6. M. R. Syed, M. Shinde, S. Unny, S. Nair and A. Patade, “Secure Peer-to-Peer Communication using Private Network Blockchain Technology,” Proc. IEEE ICACTA, Mumbai, India, 2023, pp. 1–5, doi: 10.1109/ICACTA58201.2023.10393506.
7. Lokhande, N. Deotale, B. Mali, S. Chauhan and J. Dhuri, “BlockChain Based Chat Application,” Proc. IEEE INCET, Belgaum, India, 2023, pp. 1–6, doi: 10.1109/INCET57972.2023.10170739.
8. M. Vaccargiu, R. Neykova, S. Aufiero, R. Tonelli, S. Bartolucci, and G. Destefanis, “Sustainability in Blockchain Development: A BERT-Based Analysis of Ethereum Developers’ Discussions,” Proc. ACM/IEEE ICSE, 2023.
9. S. Sourabh, D. Rawat, K. Kapkoti, S. Aggarwal and A. Khanna, “bChat: A Decentralized Chat Application,” Int. Res. J. Eng. Technol. (IRJET), vol. 7, no. 5, pp. 2775–2780, May 2020.

10. K. Khalkar, N. Dhake, S. Kelzarkar and T. Shinde, “Decentralized Chat Application using Blockchain Technology,” Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET), vol. 11, no. 1, pp. 813–816, Jan. 2023, doi: 10.22214/ijraset.2023.48650.
11. J. M. Philip and R. Rajeswari, “Decentralized Chatting Application Using Blockchain Technology,” Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET), 2024, doi: 10.22214/ijraset.2024.61466.
12. V. Patil and P. A. Chaudhari, “BitChat: A Decentralized Messaging App,” Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET), 2025, doi: 10.22214/ijraset.2025.74891.
13. S. V, H. C. M, S. K. B. V, A. K and H. H. K, “A Blockchain-Enabled Chat Application System for Secure Communication: Design and Implementation,” Proc. IEEE ICEARS, Tuticorin, India, 2025, pp. 944–947, doi: 10.1109/ICEARS64219.2025.10940720.
14. Pandey, R. R. Gupta and A. Choudhary, “A Novel Development of Blockchain based Messaging Application,” Proc. IEEE ICAECIS, Bangalore, India, 2023, pp. 38–43, doi: 10.1109/ICAECIS58353.2023.10170701.
15. P. B. Nair, V.A.G. B., V. K. V., and U. S., “Blockchain-Based Communicator with Multicast Transmission,” Proc. IEEE CSITSS, Bengaluru, India, 2024, pp. 1–5, doi: 10.1109/CSITSS64042.2024.1081673