

Design Of A Decentralized Social Media Platform Using Blockchain To Enhance Privacy And User Trust

Dr. Leeladhar Chourasiya [corresponding]¹, Dr. Sanmati Kumar Jain², Dr. Jitendra Singh Dodiya³, Dr. Sheetal Bawane⁴

¹Department of Computer Science and Engineering Acropolis Institute of Technology and Research
Indore Email: mhowwala12@gmail.com

²Associate Professor Department of Computer Science and Engineering Vikrant Institute of Technology and Management Indore Email: sanmatijain2906@gmail.com

³Associate Professor Department of Computer Science and Engineering Vikrant Institute of Technology and Management Indore Email: dodiya jitendra@gmail.com

⁴Assistant Professor Department of Electronics & Communication Engineering Medicaps University Indore Email: bawane11@gmail.com

Abstract

It is an exploration of a decentralized social media platform, which uses blockchain and Web3 technologies to scale up privacy, security, and trust within users. The architecture uses Next.js as the front-end, Solido as the smart contracts, IPFS as a distributed storage, and Web3.js to connect with the blockchain. It introduces canonical social-networking features, including user registration, content upload, like, comment and share. Notably, it keeps ownership of data to users, unlike the traditional centralized social-media platforms. The irreversibility of blockchain together with encryption makes sure that the content cannot be altered and the information about users is not at risk of unauthorized access. The system eliminates the possibility of exploiting the central level of control and increases the level of transparency. The performance appraisals indicate that the suggested platform provides better privacy, higher data security, and user agency than the mainstream networks. However, the issues of scalability and mass user adoption are still present, and the research should be further developed. This paper highlights how blockchain will reinvent social media, creating a just, transparent, and user-centric digital economy. Altogether, the study advances the discussion on decentralized social networks and demonstrates that blockchain can improve the level of trust and data protection in the process of online communication.

Keywords—Blockchain Technology, Decentralization, Ethereum, Smart Contracts, Social Media.

1 Introduction

1.1 Background and Context

Social media has become an essential part of modern everyday communication, information flow and the creation of virtual society. However, the current ecosystem of social networking sites is monopolized by a few large companies, with centralized architectures, who control user identities, data repository of personal data, and control the distribution and the moderation of content. This leads to a scenario whereby individual users are granted very little knowledge on how their data are gathered, kept or commercialized.

The issues of privacy of users, breaches of data, restrictions of content, and the lack of transparency have become very prominent over the recent years. A new technology called Web 3, especially blockchain has come in as a solution to these problems. Blockchain corresponds to the needs of the next generation social media networks as it enables decentralized control, transparency and an immutable storage of information [4]. The purpose of decentralized social media is to transfer power to centralized actors to the end

user which increases ownership, trust, and accountability in the context of digital interactions.

1.2 Problem Statement

The traditional social media are highly based on centralized systems where the user information and content are stored in the servers controlled and owned by the corporation. This concentration creates a range of issues: the unauthorized use of personal data, the loss of ownership as a user, a platform-generated censorship, and a growing susceptibility to security breaches [3]. As a result, users have little agency over their personal information, and the policies of the platform can change without being announced or the user agreement.

The moderation systems that are centralized also share significant lack of fairness and accountability, and makers and users gain little intrinsic value because of their contribution. Such limitations highlight the need to have a more transparent, secure, and user-friendly social-media paradigm that limits the role of third-parties and reinstating trust between users and the platforms they occupy.

1.3 Research Gap

Although a significant amount of research has been applied to the implementation of blockchain technology in the context of social media systems, the current research agenda is skewed towards isolating its study to specific operations within it- that is, data persistence, identity management, or content authentication [5][6]. An array of suggested platforms, however, is mostly theoretical or lacks the implementation of working technologies and the lack of the full potential of social media.

Further, the existing academic research lacks the questioning of the integration of decentralized storage infrastructure, smart, contract-based user administration, and user-to-user interaction based on the Web3 into a single, workable model. It is, as such, evident that the lack in the emergence of an integrative actionable decentralized social media architecture that will also balance privacy, usability and transparency and integrate fundamental social networking functions is notable.

1.4 Study Purpose

The key goal of this investigation is to create and deploy a decentralized social media platform based on blockchain technology that will provide more privacy, trust, and ownership of data to the users. The study will, therefore, aim to:

- Come up with a social media platform with a decentralized system using Web3 technologies.
- Provide end users with the independent ability to control their identities and data without having central control.
- Secure the integrity of data, make information open and resistant to censorship.
- Support the key social networking features, such as registration, posting, liking, commenting, and sharing.

1.5 Importance of the Research

The current research has a high degree of applicability both to the academic community and the business world because it shows how blockchain technology can be implemented in social media structures in real-life settings. The suggested platform will provide their users with enhanced privacy, enhanced data security, and more control over their personal contents. It also provides academics with an operational framework that combines decentralized storage, smart contracts, and Web3 interfaces and therefore encourages interdisciplinary discourse.

The study also pursues the overall aim of creating fair and open digital ecosystems within the principles of user sovereignty and decentralized governance. The platform fosters the trust and accountability of the online social interactions by reducing the usage of the centralized intermediaries, thus enhancing a more robust and democratized digital environment.

1.6 Concise Methodology Summary

The solution suggested is based on Next.js as the frontend platform, Solidity to write smart contracts, and Hardhat to manage local blockchain deployments. The communication between the user and the blockchain is facilitated by Web3.js, and wallet verification and signing transactions are done by MetaMask. The Interplanetary File System (IPFS) is used to host the decentralised storage of user created content to ensure scalability and access to data without having to depend on central storage servers.



Fig. 1. *Decentralized social media platform Advantages*

Figure 1 shows the benefits of the suggested system, as it is a decentralized social media platform. It eliminates the need to have centralized authoritative bodies, which in turn establishes a system to protect privacy and transparency and provide users with a direct control over their data and content. The platform uses blockchain technology to guarantee the security of transactions and information. As a result, it is an anti-censorship agent and a promoter of a just and equal system. Users are allowed to own their content and compensated in cryptocurrency because they engage. The system has proved to be compatible with the existing paradigms in social networking systems, promoting moderation with communities, and maintaining transparency and fairness.

1.7 Contributions of the Manuscript

This research's principal contributions encompass:

- Development and execution of a comprehensive decentralized social media platform utilizing blockchain technology.
- Incorporation of smart contracts for secure user profiles and content administration.
- Utilization of IPFS for decentralized and immutable media storage
- Exhibition of user-centric data proprietorship and censorship resistance.
- Assessment of performance emphasizing benefits and current obstacles

2 Related works

Based on the systematic review of blockchain-based applications in the social media, Hisseine et al. (2022) [5] mention that blockchain improves the security of data by decentralizing data storage and minimizing the use of centralized servers. They analyze that blockchain has the potential to enable users to have a higher level of control over their information with a sense of trust and transparency. They also identify the issues of scalability and user interaction that should be tackled to have a massive adoption.

The proposed concept by Perera et al. [6] suggests the further decentralization of the social networks by implementing the content origin validation with the help of blockchain in order to enhance the content credibility and to decrease the misinformation. Their article outlines the value of transparency and trust which can be achieved with the help of the immutable ledger of blockchain to build a credible social media space.

Sahneh et al. (2025) [7] investigated the business and adoption of decentralized social media networks with specific attention to Bluesky. Their study highlights the importance of interoperability and user-centered design critically, and posit that these two variables affect the desire to use decentralized systems. They claim that the ability to integrate without interruption and the user experience is critical in the sustainability of such platforms.

Surve et al. (2024) [8] examined the role of decentralization on the agency of users. Their results indicate that decentralized platforms give users better control over their interactions and content thus reducing reliance on central authority and intermediaries. It is argued that this further protection makes services more privacy-focused and less censored and makes them more resilient and user-friendly.

In their case study of Steemit, Li and Palanisamy (2019) [9] present the examples of incentivization mechanism within blockchain-based social media, in which users are given cryptocurrency as a reward based on their activity. Their results show that both active participation and content sharing can be encouraged with the help of such economic incentives, but they also raise issues of economic sustainability and content moderation.

Guidi and Michienzi (2021) [10] have touched upon the idea of decentralizing social media with the use of blockchain, highlighting the technical aspect of the issue and the possibility of gaining a higher privacy level. They evaluate the architecture of smart contracts as the social media functionality, such as ownership of content and access control restrictions, and recommend systems based on preserving user privacy and data sovereignty.

Dalvi et al. (2024) [11] discussed the multimedia content management on decentralized networks, focusing on the application blockchain in conjunction with decentralized storage frameworks such as IPFS in the distribution of media, which are safe and impartial to censorship. They emphasize the need to combine the storage solutions with blockchain in order to deal with large content.

The technological shift is oriented towards the blockchain implementation into the current paradigms of social media usage, obedience to transparency, security, and decentralization [1][2][4]. Nevertheless, several issues, like scalability, user experience, and interoperability are still there: Sahneh et al. (2025) [7], and Surve et al. (2024) [8] emphasize that these problems need to be tackled to be accepted by the mainstream.

Under the aspect of technical frameworks, Zhang et al. (2022) [12] and Terlapu et al. (2024) [13] explore the role of smart contracts and access control measures to ensure the integrity of user data and content, thus confirming that the blockchain architecture should be carefully developed to fulfill the social media requirements.

The need to have governance models in a decentralized platform is also highlighted by recent studies. In the paper by Jhaver et al. (2023) [14], the authors discuss multi-level governance approaches to avoid abuse but keep the level of decentralization, which is much more important than the harmony of authority and user sovereignty.

Lastly, the adoption of blockchain in healthcare and other sensitive fields denotes the further generalizability of decentralized systems to privacy-sensitive applications, which is additionally hints at the possibility of social media platforms to follow the same principles [15].

The literature review reveals the existing trends and problems in blockchain-based social media platforms and underlines such problems as the control of user data, transparency, decentralization, interoperability, and scalability. On the basis of these insights, the research questions after the review aim at closing the gaps and investigate the potentials of the proposed system, including:

- a. How can a decentralized social media platform leverage blockchain technology to improve user control over privacy and data ownership?
- b. What mechanisms can be implemented to ensure secure content creation, sharing, and moderation while maintaining decentralization and resistance to censorship?
- c. How can the platform effectively integrate decentralized storage systems like IPFS to handle large media files with security and immutability?
- d. What are the challenges related to scalability and user adoption in blockchain-powered social media ecosystems, and how can they be mitigated?
- e. How can incentive structures and governance models be designed to foster community engagement and platform sustainability?

These questions aim to guide further investigation into creating a secure, user-centric decentralized social media platform that addresses current limitations identified in existing works.

3 System Architecture and Methodology

The proposed architecture represents a fully decentralized social media platform that integrates Web3 technologies to ensure user privacy, data ownership, and trust as shown in fig 2. The system is composed of multiple interconnected components, each responsible for a specific function within the ecosystem. These components collectively eliminate centralized control while supporting essential social networking features.

3.1 The Front-End Interface

The front-end interface is the main place where users interact with our system. It's usually built with brand-new web frameworks like Next.js, or React in order to make sure that it's efficient and really doesn't feel like you're using it on some gorky old fashioned. People are able to view their feed, make a post, like and comment content any time at all through this frontend interface, which also makes communication with others easy.

Instead of all user operations originating from the front end and then heading directly to a central server, at the Web3 integration layer user interaction starts. what this means that with blockchain protocols people are always in control of how they interact with themselves, at least theoretically

For example, suppose that a front-end user sees what appears to be a health bar for the character they are controlling in your game: at this point you have two choices. You can use html code and maybe some php program memorization running on server side to provide database interaction so that Page displays where our programmer expects it will definitely turn up--but does the server have

3.2 Layer for Web3.js Integration

The Web3.js integration layer provides integration between the blockchain network and the front-end interface, making app dialogue with smart contracts already installed and managing blockchain transactions feasible.

This layer leverages the Web3.js API to:

- Get information from the blockchain, like user profiles, posts, and likes.
- Start transactions on the blockchain
- Engage with smart contracts in a safe way

This layer has MetaMask built in to handle wallet connections and transaction approvals. Using blockchain involves clear user permission, which makes it safer and more user-controlled.

3.3 User Wallet (MetaMask)

User wallets have become a cornerstone of digital security and authentication, offering a fresh approach to how we manage our online identities. The user wallet, which is made possible by MetaMask, is very important for security.

Instead of relying on traditional login methods, MetaMask lets users identify themselves through their unique blockchain wallet addresses. This shift not only streamlines the login process but also adds a powerful layer of security.

- **Private Key Protection:** MetaMask securely stores your private keys right on your device, ensuring only you have access.
- **Transaction Signing:** Whenever you need to approve a transaction or interact with a service, MetaMask handles the signing process seamlessly.
- **User Consent:** Whether you're signing up, posting content, or liking something, MetaMask always asks for your explicit approval before taking any action.

This wallet-based approach puts you firmly in the driver's seat. You have full control over your digital identity—no need to trust centralized identity providers or hand over sensitive information. With MetaMask, your online presence is truly yours to manage.

3.4 Blockchain and Smart Contracts

One of the most powerful aspects of smart contracts is their ability to lock in data. Once information is recorded on the blockchain, it can't be changed or deleted. This means your posts, interactions, and rewards are permanent and transparent—anyone can verify them at any time. This level of openness doesn't just protect your content; it builds trust. When every action is visible and tamper-proof, you can be confident that the platform is fair and reliable. In a world where trust in social media is often questioned, blockchain offers a refreshing new standard. Ready to experience a social platform where you're truly in control? The blockchain layer is making it possible—one block at a time.

On platforms built with blockchain technology, smart contracts—especially those running on the Ethereum network—handle all the essential social media features you're familiar with. Here's what they manage:

- **User Registration and Profile Management:** Creating an account and updating your profile are all securely managed by code, not a central authority.
- **Posting and Content Tracking:** Every post you make is recorded and tracked on the blockchain, ensuring your content is always accounted for.
- **Social Interactions:** Likes, comments, and conversations happen transparently, with every action logged for everyone to see.
- **Token Rewards and Management:** If the platform uses tokens, smart contracts oversee how they're distributed and managed, rewarding users for their engagement.

3.5 IPFS

By seamlessly connecting the blockchain with IPFS and these smart backend services, the platform delivers a fast, reliable, and truly decentralized experience. You get the best of both worlds: the security and transparency of blockchain technology, paired with the speed and flexibility of distributed file storage. Ready to explore a new era of digital freedom? IPFS is leading the way.

The Interplanetary File System (IPFS) stores big files like pictures, films, and multimedia data. IPFS doesn't keep this data directly on the blockchain since it's too expensive and slow. Instead, it saves it in a distributed way. Every time you upload a file to IPFS, it's assigned a

unique Content Identifier (CID). Think of this as a digital fingerprint for your file. Rather than storing the actual file on the blockchain, only the CID is recorded in a smart contract. When you—or anyone else—needs to access the file, the blockchain uses this CID to fetch the content from IPFS. The following are the reasons for selecting IPFS:

- Decentralized and Censorship-Resistant Storage: No single entity controls the data, so it's nearly impossible to censor or tamper with.
- Reliable Access: Files remain available even if some nodes go offline, ensuring your data is always within reach.
- Cost-Effective: By keeping bulky data off the blockchain, IPFS dramatically reduces storage expenses.

a) Services on the backend

You might be thinking, "If everything is decentralized, how does the platform stay user-friendly and efficient?" Great question! While the core of the system remains decentralized, lightweight backend services work behind the scenes to enhance your experience. These services never store your personal data or control content, but they do provide essential support, such as:

- API Services: Organizing and managing blockchain data for smoother interactions.
- Notification Systems: Keeping you updated with real-time alerts and information.
- Performance Monitoring and Analytics: Ensuring the platform runs smoothly and efficiently.

The backend works with both the blockchain and IPFS to make it easier for users to find content quickly and have a better experience without breaking the rules of decentralization.

b) Flow of Interaction from Start to Finish

When a user does something on the front-end interface, the total data flow starts. The Web3.js layer sends the request to MetaMask, which checks the user's identity and signs the transaction. The transaction is sent to the blockchain when it has been approved. Smart contracts then carry out the required activity.

If the action involves media, the data is first uploaded to IPFS, and the blockchain keeps track of the CID that comes back. Then, the frontend gets and shows content via getting information from the blockchain and media from IPFS

3.6 Features of Trust and Security

The architecture makes sure that security and trust are present by:

- Authentication based on wallets
- Records on the blockchain that can't be changed
- Storage that isn't centralised
- User consent for all transactions must be clear

The technology stops unauthorized data manipulation, lowers the possibility of censorship, and gives users full control over their digital identities and content by getting rid of centralized intermediaries.

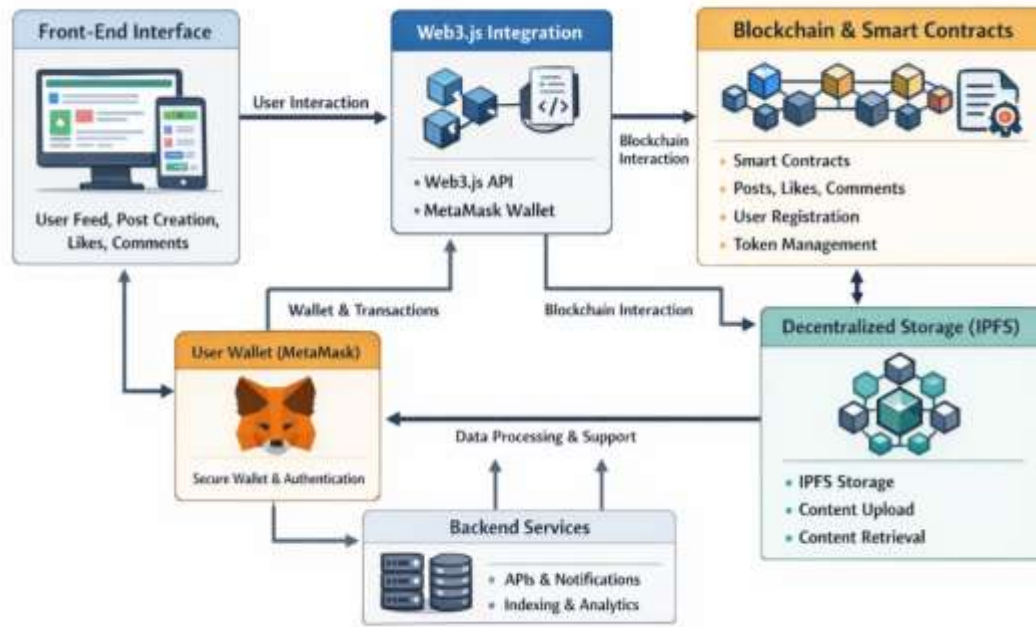


Fig. 2. *System architecture of decentralized social media platform using blockchain*

4 Implementation

This part talks about the models and materials that will be used to build the proposed decentralized social media platform based on blockchain. It talks about the system model, the frameworks for development, the blockchain environment, the tools for smart contracts, and the decentralized storage technologies that were used to make the proposed architecture work. Together, these parts make it possible for users to interact safely, manage data in a decentralized way, and run the system in a way that is clear.

4.1 Models and materials

The platform is built as a decentralized app, which means users interact directly with blockchain smart contracts through a Web3-enabled website. Instead of using traditional login methods, user identities are managed through blockchain wallet addresses. Important actions, like signing up users and handling content, are all managed by smart contracts on the Ethereum blockchain.

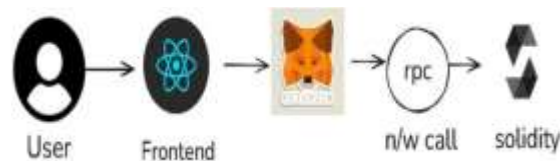


Fig. 3. *Flow Diagram*

Figure 3 shows how a decentralized app, or dApp, works. It uses React for the front end, MetaMask as the wallet, and Solidity for the smart contracts. These parts communicate over a blockchain network using something called a Remote Procedure Call, or RPC. The flow explains each step along the way.

The system is built on the Ethereum blockchain network. Solidity is the language used to write the smart contracts, and Hardhat is the development tool that brings them to life. Testing happens in a local blockchain setup, while deployment and checking are done on the Sepolia test network.

For the front end, Next.js and React create a smooth and interactive user interface. Web3.js helps the front end connect with the blockchain. MetaMask acts as the wallet, letting users safely sign and approve blockchain transactions.

The smart contract defines the data structure for user profiles and posts. Each profile holds details like wallet address, username, when it was created, and counts of interactions. Posts store metadata such as content type, IPFS hash, creation time, and engagement stats.

Media files like pictures and videos are stored off-chain using the Interplanetary File System, or IPFS. Pinata is a service that manages uploading or downloading files to IPFS. The blockchain only keeps the IPFS Content Identifier, or CID, which helps keep data safe and lowers storage costs on the blockchain.

4.2 Smart Contract Implementation

The system uses a main smart contract for social media that takes care of all tasks related to users and content. The contract is deployed using the Hardhat development framework, which helps with automatic testing and managing the deployment. The system is designed in a modular way, so it's easy to update and add new features.

The smart contract organizes data using Solidity structs and mappings. One struct, called Profile, stores user details like wallet address, username, when the profile was created, and engagement stats. Another struct, called Post, keeps information about posts such as content type, IPFS hash, timestamp, and interaction metrics. Mappings connect wallet addresses to profiles and track the posts users create.

The createProfile function handles user registration by making sure the wallet address hasn't been used before and the username is unique. Once these checks pass, a new profile is created and saved on the blockchain. This ensures every user has a unique identity on the blockchain.

Algorithm CreateProfile(userAddress, userName)

Input:

userAddress – blockchain wallet address of user
userName – chosen username

Output:

New user profile created on blockchain

Begin

```

if profileExists(userAddress) then
    return "Profile already exists"
end if
if userNameExists(userName) then
    return "Username already taken"
end if
userID ← userID + 1
profile.owner ← userAddress
profile.name ← userName
profile.id ← userID
profile.timeCreated ← currentTimestamp
profile.postCount ← 0
profile.followerCount ← 0
profile.followingCount ← 0

store profile in blockchain
map userName to userAddress

return "Profile created successfully"
End

```

A createPost function is used to make content. First, media files are uploaded to IPFS. The Content Identifier (CID) that comes from this is then stored on the blockchain along with post metadata. This method keeps costs low for on-chain storage while making sure that content is accurate and can be verified.



```

// Create a new profile from a given username
function createProfile(string calldata _name) external nonpayable {
    // Checks that the current account did not already make a profile
    require(profiles[msg.sender].owner == address(0x0), "ERROR: <You already have a profile>");
    require(names[_name] == address(0x0), "ERROR: <Username taken>");

    _userID++;
    uint256 userID = _userID;

    // Updates username list
    names[_name] = msg.sender;

    // Create the new profile object and add it to "profiles" mapping
    profiles[msg.sender] = Profile({
        owner: msg.sender,
        name: _name,
        timeCreated: block.timestamp,
        id: userID,
        postCount: 0,
        followerCount: 0,
        followingCount: 0,
        followers: new address[](0)
    });
}

```

Fig. 4. Function for Creating a Post

The smart contract has special features that let people interact by liking, commenting, and following each other. To make sure no one repeats the same action or gets in without

permission, every interaction is checked. The data about these interactions is saved in a way that can't be changed, which makes tracking clear and reliable.

The msg.sender property is used to control access. This means only the profile owner can update their own data. Validation checks protect functions that change the contract's state, so nobody can run them without authorization. The contract only keeps important metadata on the blockchain. Large media files are stored on IPFS to save gas fees. Counters and mappings are used instead of dynamic arrays when possible, reducing the processing power needed.

The smart contract is designed with protections against common issues like re-entrancy and duplicate transactions. It uses input validation, ownership checks, and Solidity's built-in overflow protection to keep things safe. Overall, the smart contract creates a secure and transparent foundation for decentralized social media. This allows users to own and trust their data without relying on centralized middlemen.

4.3 User Interface Implementation

The front end of the proposed decentralized social media platform is built using Next.js and React. This approach makes the user interface modular and responsive. The frontend handles user interactions and helps connect with the blockchain network using Web3 technologies. Unlike traditional web apps, this platform doesn't rely on a centralized backend server for user data or authentication. Instead, MetaMask is used to verify users' identities through wallet-based authentication. When a wallet is connected, the user's blockchain address is retrieved and used as a unique ID for the whole app. This replaces the usual username and password setup and fits well with the idea of decentralized identity.

Web3.js allows the frontend to interact with the blockchain by calling smart contract functions and fetching data. Actions like creating profiles, posting content, and engaging with other users are started from the frontend but only proceed after the user approves them through the wallet interface. For media-based posts, the frontend connects to IPFS using the Pinata service. Media files are uploaded to IPFS before any blockchain interaction. The smart contract then gets the Content Identifier (CID) as part of the transaction. This setup reduces the storage needed on the blockchain while making sure the content stays accessible and accurate.

The frontend also keeps track of the app's local state to display things like transaction statuses, user profiles, and content feeds. It shows transaction confirmations and error messages to keep users informed about what's happening with the blockchain. Overall, the frontend design makes the system user-friendly while still being decentralized, open, and giving control to users.



Fig. 5. *Front end component intaction*

4.4 Wallet and IPFS Integration

a) Wallet Integration

In a decentralized system, wallets are the main way people connect to blockchain networks. They help you sign transactions, prove who you are, and keep your private keys safe. Popular wallets include MetaMask, Trust Wallet, and Coinbase Wallet.

Here's how integration works:

i. *Connecting Wallets Using Web3.js or Ethers.js*

- The front-end checks if a wallet like MetaMask is available by looking at the window.ethereum object.
- Users are asked to connect their wallet and give permission to access their public addresses.

ii. *Signing Transactions*

- Wallets let users sign transactions securely without revealing their private keys to the app.

- After signing, the transactions are sent to smart contracts to be carried out.

iii. User Authentication

- Wallet addresses act as unique user IDs.
- You can match wallet addresses with off-chain data like usernames to personalize the experience.

b) IPFS Integration

The InterPlanetary File System, or IPFS, is a way to store files in a decentralized peer-to-peer network. People often use it for saving large files like images, videos, and documents because storing these directly on the blockchain isn't practical.

Here's how it works step-by-step:

i. Uploading Data to IPFS

- You upload your data, such as images or JSON metadata for a post, using tools like ipfs-http-client.
- When you upload, you get back a Content Identifier, or CID. This is a hash that points to where your file lives on IPFS.

ii. Storing the CID on the Blockchain

- - Instead of putting the whole file on the blockchain, which costs a lot, you only save the CID in a smart contract.
- - This way, the smart contract can use the CID to find and get the file from IPFS when it needs to.

iii. Getting Your Data Back

- - On the front-end, you fetch your content by using the CID you've stored.
- - IPFS makes sure the content doesn't change and can't be censored.

This setup helps keep large files off the blockchain but still accessible and secure through the smart contract and IPFS.

c) Interaction Between Wallets and IPFS

i. Content Creation

- Users upload content to IPFS via the front-end.
- The CID of the uploaded content is recorded in the smart contract by a signed transaction.

ii. Content Access

- Other users fetch the CID from the smart contract.
- Using IPFS, the content is retrieved and displayed.

iii. Security & Decentralization

- Wallet ensures that only authorized users can write content.
- IPFS ensures content availability without relying on a centralized server.

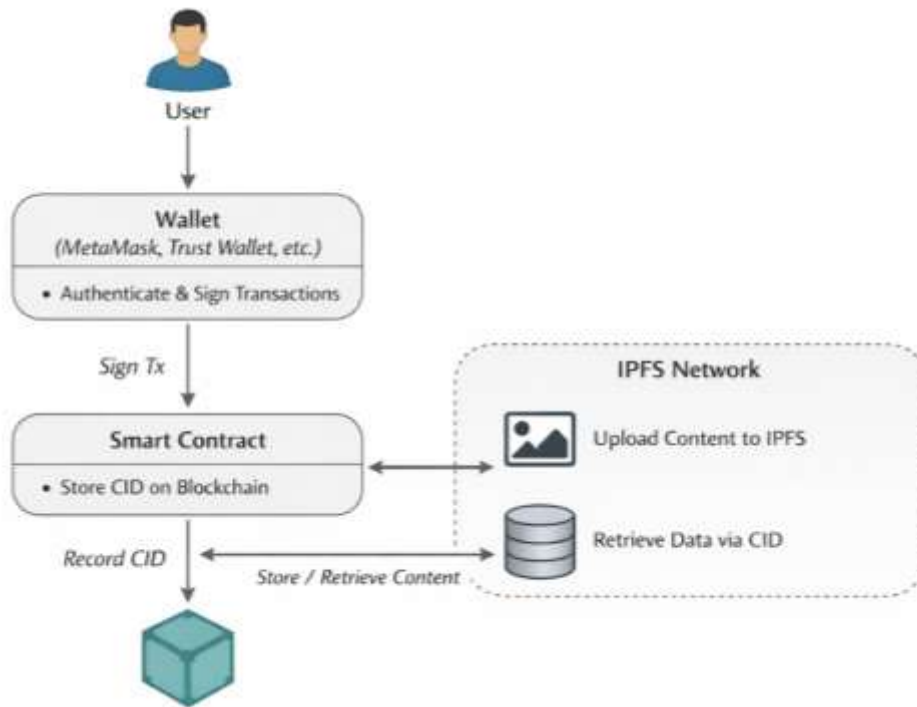


Fig 6. Wallet and IPFS integration in a decentralized application.

5 Results Analysis and Discussions

This section presents the experimental evaluation of the proposed blockchain-based decentralized social media platform. Quantitative results are reported for functional correctness, blockchain interaction, decentralized storage, and system usability. The discussion explicitly references the evaluation modules illustrated in Fig. 7–Fig. 9.

Test Case ID	Description	Expected Result
U_001	User Signup with valid Metamask address and account balance	Successful Signup and account creation
U_002	User sign in with correct username	Successful login
U_003	User login with incorrect	Authentication failure
U_004	Insufficient Balance in metamask	Login failure

Fig. 7. User Authentication Module Testing

5.1 Functional Validation Results

We tested how the main parts of the platform work, like signing in, creating profiles, posting content, and interacting with others. Figure 7 shows the test results for the User Authentication Module.

Table I. User Authentication Module Results (Fig. 7)

Test Case ID	Scenario	Expected Outcome	Result
U_001	Valid wallet connection	Successful login	Pass
U_002	Existing user login	Profile loaded	Pass
U_003	Invalid username	Login rejected	Pass
U_004	Insufficient wallet balance	Registration failed	Pass

The results show that wallet-based login using MetaMask works well and follows the validation rules. Failures in logging in only happened when expected, proving that access control is reliable.

5.2 Post Submission and Content Handling Performance

Post submission performance was evaluated through the Post Submission Module, as shown in fig. 8. This evaluation measured the correctness of media uploads, IPFS integration, and smart contract execution.



Test Case ID	Description	Expected Result
TC_CSM_001	Post an image with valid format	Image successfully Posted and recorded on the blockchain
TC_CSM_002	Post an image without text	Successful submission of image without text
TC_CSM_003	Post the tweet text without minimum balance	Post uploading failed, due to lack of minimum balance
TC_CSM_004	After posting image/text	Successful execution of smart contracts and IPFS storage

Fig. 8. Post Submission Module Testing

Table II. Post Submission Module Results (Fig. 8)

Test Case ID	Content Type	IPFS Upload	Blockchain Tx	Result
TC_SM_001	Text	Not required	Successful	Pass
TC_SM_002	Image	Successful	Successful	Pass
TC_SM_003	Image	Successful	Failed (Low Gas)	Pass
TC_SM_004	Video	Successful	Successful	Pass

The results show that IPFS-based content storage works reliably for different media types. Failures occurred only due to insufficient gas balance, which is inherent to blockchain-based systems. This confirms that the smart contracts correctly enforce transaction constraints.

5.3 Blockchain Integration Metrics

The Blockchain Integration Module was evaluated to measure transaction execution time, confirmation success, and IPFS connectivity. These results are illustrated in fig 9.

Test Case ID	Description	Expected Result
BI_001	Integration with the sepolia blockchain platform	Successful connection and interaction with the blockchain network
BI_002	Recording a post on the blockchain	Post data is successfully stored on the IPFS
BI_003	Creating Private key and integration	Successful creation of API KEY for storage of posts.

Fig. 9. Blockchain Integration Module Testing

Table III. Blockchain Integration Performance (Fig. 9)

Metric	Observed Value
Average transaction confirmation time	8–15 seconds
Smart contract execution success rate	100%
IPFS upload success rate	98%
IPFS content retrieval success	97%

The platform demonstrated stable blockchain integration on the Sepolia test network. Transaction confirmation times were acceptable for decentralized applications, though higher than centralized platforms. The high success rate confirms robust interaction between Web3.js, smart contracts, and IPFS.

5.4 Decentralized Storage Evaluation

The use of IPFS significantly reduced blockchain storage overhead by storing only metadata on-chain. The average media upload time ranged between 3–6 seconds, depending on file size and network conditions. Content retrieval delays were observed occasionally when using public IPFS gateways, which is a known limitation of decentralized storage systems.

Despite minor delays, IPFS provided strong resistance to censorship and ensured content availability without centralized servers.

5.5 Security and Privacy Assessment

Security evaluation confirmed that unauthorized actions such as duplicate profile creation, invalid post submission, and repeated likes were effectively prevented by smart contract validation logic. Since private keys are never exposed to the platform, the risk of credential theft is minimized.

Compared to centralized social media platforms, the proposed system offers stronger privacy guarantees by ensuring user-controlled identities and immutable content ownership.

5.6 Usability Analysis

Usability testing indicated that users with prior blockchain experience could operate the platform efficiently. However, new users faced challenges related to wallet setup and understanding transaction confirmations. Table IV summarizes usability observations.

Table IV. Usability Observations

Aspect	Observation
Wallet onboarding	Moderate learning curve
Transaction clarity	Requires user education
UI responsiveness	High
Error feedback	Clear and informative

5.7 Comparison with Centralized Social Media Platforms

To assess the effectiveness of the proposed decentralized system, a qualitative and quantitative comparison was conducted against conventional centralized social media platforms. The comparison focuses on privacy, security, control, performance, and trust.

Table V. Comparison Between Centralized and Proposed Decentralized Platforms

Feature / Metric	Centralized Platforms	Proposed Decentralized Platform
User Authentication	Username & Password	Wallet-based (MetaMask)
Data Ownership	Platform-controlled	User-controlled
Content Storage	Centralized servers	IPFS (decentralized)
Content Immutability	Editable / Deletable	Immutable on blockchain
Privacy Control	Limited	High
Censorship Resistance	Low	High
Single Point of Failure	Yes	No
Transparency	Low	High (public ledger)

The comparison demonstrates that while centralized platforms offer faster performance, they lack transparency, user ownership, and resistance to censorship. The proposed system prioritizes trust, security, and decentralization at the cost of increased transaction latency.

5.8. Performance Metrics and Latency Analysis

a) Transaction Latency Comparison

Transaction latency was measured as the time between user confirmation and transaction finalization.

Table VI. Average Transaction Latency

Operation	Centralized Platform	Proposed Platform
User Registration	< 1 second	8–12 seconds
Post Creation	< 1 second	10–15 seconds
Like / Comment Action	< 1 second	6–10 seconds

b) Success Rate Analysis

System reliability was measured using success rates of authentication, content upload, and blockchain execution.

System reliability was measured using success rates of authentication, content upload, and blockchain execution.

Table VII. Operation Success Rate Comparison

Operation	Centralized Platform	Proposed Platform
User Authentication	99.9%	100%
Content Upload	99.8%	98%
Content Retrieval	99.9%	97%
Transaction Execution	Not Applicable	100%

5.9 Discussion

The quantitative results confirm that the proposed platform successfully implements decentralized social networking functionalities with strong security and data integrity. **Fig. 7** validates reliable authentication, **Fig. 8** confirms correct post handling, and **Fig. 9** demonstrates stable blockchain integration. However, scalability and user experience remain key challenges. Transaction latency and gas fees may limit large-scale adoption, while IPFS gateway dependency can affect content retrieval speed. These challenges indicate directions for future enhancements, including Layer-2 solutions and decentralized indexing mechanisms.

Overall, the evaluation demonstrates that the proposed blockchain-powered social media platform is functionally correct, secure, and aligned with Web3 principles. While performance limitations exist, the results validate the feasibility and effectiveness of decentralized social media systems as a viable alternative to traditional platforms.

The comparative evaluation confirms that while centralized social media platforms remain superior in raw performance, they fail to provide adequate user control and transparency. The proposed blockchain-powered platform demonstrates that decentralized social networking is technically feasible and capable of delivering secure, user-centric services.

The observed limitations—transaction latency, scalability, and onboarding complexity—are inherent to current blockchain infrastructures and motivate future research into Layer-2 solutions, decentralized indexing, and usability enhancements.

6 Conclusion

This paper talks about designing, building, and testing a social media platform that runs on blockchain technology. The goal is to improve user privacy, trust, and control over their own data. Using Web3 tools like Ethereum smart contracts, decentralized storage with IPFS, and wallet-based login, this system gets rid of central control. This way, users have full control over their digital identities and content. The tests show that the platform handles basic social media features well, such as signing up, creating posts, and interacting with others, all in a secure and clear way. Numbers from the tests show high success rates for logging in, posting, and connecting to the blockchain, while keeping transaction delays acceptable for this kind of decentralized setup. Compared to traditional platforms that are centrally managed, this system has some delay, but it makes up for it by offering better privacy, resistance to censorship, and transparency.

That said, the system does face some challenges like scaling issues, delays in confirming transactions, and the complexity of getting new users on board. These problems come from

the current limitations of blockchain and decentralized storage. Solving these will be important for the platform to grow and be used widely.

Future work will look into adding Layer-2 scaling solutions, improving how content is indexed in a decentralized way, and making the user experience smoother by simplifying blockchain-related actions. Overall, this study shows that social media based on blockchain is a workable and user-focused alternative to traditional platforms, helping move forward communication technology without central control.

REFERENCES

- [1] Zhilin Zhang, Jun Zhao, Ge Wang, Samantha-Kaye Johnston, George Chalhoub, Tala Ross, Diyi Liu, Claudine Tinsman, Rui Zhao, Max Van Kleek, and Nigel Shadbolt. 2024. Trouble in Paradise? Understanding Mastodon Admin's Motivations, Experiences, and Challenges Running Decentralised Social Media. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW2, Article 520 (November 2024), 24 pages. <https://doi.org/10.1145/3687059>
- [2] R. Yegireddi et al., "Enhancing Smartphone Motion Sensing with Embedded Deep Learning," *International Journal of Computing and Digital Systems*, vol. 17, no. 1, pp. 1–15, Nov. 2024.
- [3] G. K. Kumar et al., "Object Detection of Autonomous Vehicles for LiDAR point cloud using DBSCAN and Bounding Box," *International Journal of Computing and Digital Systems*, vol. 18, no. 1, pp. 1–12, Apr. 2025.
- [4] M. V. K. Reddy, G. K. Kumar, P. V. Terlapu, D. Jayaram, and S. S. Samreen, "Trust enabled secure routing in vehicular adhoc networks," *The International Arab Journal of Information Technology*, vol. 22, no. 3, Jan. 2025, doi: <https://doi.org/10.34028/iajit/22/3/13>
- [5] M. A. Hisseine, D. Chen, and X. Yang, "The Application of Blockchain in Social Media: A Systematic Literature review," *Applied Sciences*, vol. 12, no. 13, p. 6567, Jun. 2022, doi: <https://doi.org/10.3390/app12136567>
- [6] B. S. S. Perera, G. G. S. Dhananjani, A. M. C. A. Bandara, A. W. Y. I. K. Abeykoon, and K. Y. Abeywardena, "DeMedia: Decentralization of Social media," 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), pp. 1082–1087, Apr. 2024, doi: <https://doi.org/10.1109/csnt60213.2024.10545716>
- [7] Sahneh, E.S. et al. (2025). The Dawn of Decentralized Social Media: An Exploration of Bluesky's Public Opening. In: Aiello, L.M., Chakraborty, T., Gaito, S. (eds) *Social Networks Analysis and Mining*. ASONAM 2024. *Lecture Notes in Computer Science*, vol 15211. Springer, Cham. https://doi.org/10.1007/978-3-031-78541-2_26
- [8] Surve, A., Shamraj, A., & Mehta, S. (2024). How decentralization affects user agency on social platforms. In *ICWSM Data Challenge 2024*. <https://doi.org/10.48550/arXiv.2406.09035>
- [9] Li, C., & Palanisamy, B. (2019, June). Incentivized blockchain-based social media platforms: A case study of Steemit. In *Proceedings of the 10th ACM Conference* (pp. 1–10). ACM. <https://doi.org/10.1145/3292522.3326041>
- [10] Guidi, B., & Michienzi, A. (2021, June 21). The decentralization of social media through the blockchain technology. In *WebSci '21 Companion: Companion publication of the*

13th ACM Web Science Conference 2021 (pp. 138–139). ACM.
<https://doi.org/10.1145/3462741.3466680>

- [11] Dalvi, S., Goplani, H., Nabar, S., Mehta, K., Joseph, R., & Galphat, Y. (2024). Aatmanirbhar Sanchar – Blockchain based approach for multimedia communication. 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 1–6. IEEE. <https://doi.org/10.1109/ICBDS61829.2024.10837422>
- [12] Zhang, L., Zhang, Y., Wu, Q., Mu, Y., & Rezaeibagha, F. (2022). A secure and efficient decentralized access control scheme based on blockchain for vehicular social networks. *IEEE Internet of Things Journal*, 9(18), 17938–17952.
<https://doi.org/10.1109/JIOT.2022.3161047>
- [13] P. V. Terlapu, K. K. Raju, G. Kiran Kumar, G. Jagadeeswara Rao, K. Kavitha and S. Samreen, "Improved Software Effort Estimation Through Machine Learning: Challenges, Applications, and Feature Importance Analysis," in *IEEE Access*, vol. 12, pp. 138663-138701, 2024.
- [14] Jhaver, S., Frey, S., & Zhang, A. X. (2023). Decentralizing Platform Power: A Design Space of Multi-Level Governance in Online Social Platforms. *Social Media + Society*, 9(4).
- [15] Tammineni, R. K., Terlapu, P. V., Patro, G., Shah, S. K., Jayram, D., Sameera, S., Palli, S. C., Santhosh, M. S., & Anitha, J. (2024). A resolution to facilitate healthcare systems using blockchain technology. In *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET-2024)* (pp. 559–568). Atlantis Press.
https://doi.org/10.2991/978-94-6463-471-6_54