Decentralized Social media Applications Using Blockchain

Tanvir Ahmed Apu,
Department of CSE,
University of Information Technology & Sciences,
Dhaka, Bangladesh
2125051045@uits.edu.bd

Md. Riad Hossain,
Department of CSE,
University of Information Technology & Sciences,
Dhaka, Bangladesh
2125051029@uits.edu.bd

Md. Al Shahriar Labib,
Department of CSE,
University of Information Technology & Sciences,
Dhaka, Bangladesh
2125051028@uits.edu.bd

Md. Abdullah Al Mamun,
Department of CSE,
University of Information Technology & Sciences,
Dhaka, Bangladesh
2125051030@uits.edu.bd

Abstract—This paper investigates the integration of blockchain technology into social media platforms to overcome challenges related to data privacy, user control, and content authenticity. By leveraging Ethereum's smart contracts, the decentralized application ensures the immutability and integrity of user-generated content, enabling peer-to-peer interactions without centralized authorities. The decentralized architecture empowers users by eliminating issues like data censorship, biased moderation, and unauthorized access, while offering full control over their data. Through tokenization, content creators are fairly rewarded, incentivizing active participation and creation. The platform's smart contract system also supports secure, automated transactions for various user activities, including posting content and earning tokens. Rigorous testing with tools like Ganache and Truffle validated the system's security, scalability, and efficiency. The results highlight the feasibility of a decentralized social media platform that fosters user autonomy, reduces censorship, and creates a fair economic model for content creators. This research contributes to blockchain-based social media advancements, setting the foundation for future developments.

Keywords: *Decentralized social media, Data privacy, Censorship resistance*

1. Introduction

The rise of blockchain technology has opened new avenues for decentralization, including its application in social media. Traditional platforms often grapple with issues like data privacy violations, censorship, and centralized control over user content. Blockchain's features of decentralization, transparency, and immutability present a viable solution, enabling a paradigm shift in how social media platforms operate by addressing these persistent challenges.

Current social media platforms centralize control over user data and content, leaving users with limited authority. Administrators dictate content policies and monetize user data, often compromising privacy and security. This centralized model has fueled demand for decentralized systems that empower users with data ownership, control, and equitable participation, fostering greater trust and transparency in online interactions.

Blockchain technology, particularly smart contracts, offers the tools to build decentralized applications (**dApps)** that function on peer-to-peer networks. Ethereum, a leading blockchain platform, provides the infrastructure for secure transactions, automated processes, and data integrity. Integrating blockchain into social media allows for the development of platforms where users own their data, ensuring a transparent and secure environment that enhances user autonomy and participation.

This paper focuses on designing and developing a decentralized social media platform leveraging Ethereum and smart contracts. Key functionalities include decentralized user registration, content posting, and tokenized reward systems. By eliminating intermediaries, this platform fosters direct, secure, and immutable interactions, addressing the limitations of centralized social media and paving the way for a user-centric digital ecosystem.

1.1 Problem Statement

Traditional social media platforms are centralized, leading to various challenges, including data privacy violations, content censorship, and a lack of user control over personal information. These issues have raised concerns about the ethical implications of centralized platforms, highlighting the need for a decentralized alternative that empowers users with control over their data, content, and interactions while ensuring transparency and security.

1.2 Objectives

This project aims to design a decentralized social media application that overcomes the limitations of centralized platforms by utilizing blockchain technology. The focus is on empowering users with data ownership, ensuring content immutability, and fostering a censorship-resistant and transparent environment. The key objectives are:

- **Core Features:** User registration, event creation, and secure rewards for participation using Ethereum smart contracts.
- **Scalability:** Optimized for managing high activity with reliable performance and real-time updates.

- **Monetization:** Token-based incentives to encourage event hosting, participation, and engagement without centralized fees.

1.3 Project significance and Motivation

The significance of this project lies in its potential to reshape the social media landscape by providing a decentralized alternative to traditional platforms. It offers an opportunity to address the growing concerns around data privacy, user autonomy, and content censorship, which have been exacerbated by centralized platforms. The motivation behind this project is driven by the desire to empower users, promote ethical digital interaction, and leverage blockchain technology's transparency and security to build a more equitable and user-controlled social media experience.

2. Literature Review

The integration of blockchain technology with social media systems has gained significant attention due to its potential to resolve key issues such as privacy, security, and data ownership. Several studies have explored the feasibility of decentralized social media platforms by leveraging blockchain technology. This section reviews the key literature in this field, examining various blockchain implementations for improving security, privacy, and transparency in social media.

Table I

Ref.	**Problem Area**	**Data Type**	**Data Size**	**Data Sources**	**Availability**
Pandey et al. (2023)	Secure and Transparent Content Sharing	Content data	Large	IPFS, Blockchain	Open access
Michelia et al. (2023)	Blockchain Impact on Security in Social Media	User data	Medium	Literature, Survey	Open access
Chen et al. (2023)	Autonomous Decentralized Social Network	User data	Large	Social networks	Open access
Song et al. (2023)	Blockchain Notarization for Social Media	Content data	Medium	Social media platforms	Open access
A. De Salve et al., 2023	Privacy enforcement in decentralized social networks	Text	Hundreds of research articles and experiments	Social media platforms, user data	Limited access

D. Di Francesco Maesa, P. Mori, 2023	Trust framework for Self-Sovereign Identity	Text	Data from multiple pilot projects, over 150 case studies	Blockchain, identity management systems	Open access
C. Blanco-González-Tejero et al., 2024	Leveraging blockchain for industry funding	Text	Data from over 300 research articles	Social media analysis, industry reports	Limited access

Table II

Ref.	**Methods/Techniques**	**Results/Outcomes**	**Research Gap/Limitations**	**Future Direction/Future Work**	**Opinion/Comments/Feedback**
Pandey et al. (2023)	Blockchain, IPFS	Improved security and transparency; integration issues remain	Difficulty in platform integration	Research on better integration between IPFS and blockchain	Effective for secure sharing, integration challenges
Michelia et al. (2023)	Systematic literature review	Identified significant security benefits; user adoption challenges	Complexity in interfaces and adoption	Research on simplifying user interfaces for wider adoption	Usability is key for real-world implementation
Chen et al. (2023)	Blockchain, Decentralized governance	Decentralized control, scalability issues remain	Scalability and user engagement problems	Research on improving scalability and increasing user engagement	Innovative, but needs better scalability solutions
Song et al. (2023)	Blockchain, Notarization	Enhanced accountability and security for content sharing	Practical deployment in large platforms	Study on large-scale deployment and practical implementation	Strong potential for improving content accountability
A. De Salve et al., 2023	Privacy models, enforcement techniques	Identified limitations in current	Limited scope, need for broader application	Development of new privacy models	Gaps in current privacy models, future focus on multi-layer techniques for

		privacy models			decentralized platforms.
D. Di Francesco Maesa, P. Mori, 2023	Multi-layer trust framework	Effective in enhancing trust in identity management	Implementation challenges, need for standardization	Further research on framework standardization	Requires real-world testing and standardization for decentralized networks
C. Blanco-González-Tejero et al., 2024	Social media analysis, blockchain application	Demonstrated potential of blockchain in industry funding	Need for more empirical data, broader scope	Future work on empirical studies, expanding scope	Potential in funding and social media; more empirical studies needed.

2.1 Key gaps in literature on decentralized social media

Despite growing interest in decentralized social media, significant gaps remain in the literature. Scalability issues in large networks are not well addressed, with few studies focusing on maintaining smooth performance as user bases and data volumes increase. Performance bottlenecks, particularly during peak traffic, and network latency further hinder user experience, but effective solutions remain underexplored.

User adoption and engagement also face challenges due to the complexity of decentralized platforms. Novel interfaces and technologies make these systems less intuitive, impeding mass adoption. Additionally, integrating decentralized platforms with traditional systems is still a major barrier. Practical deployment challenges in ensuring security, performance, and usability at scale also require further research. Closing these gaps is vital for making decentralized social media a viable alternative to centralized platforms.

3. Methodology

The development of a decentralized social media platform will follow a multi-phased approach focused on security, scalability, and user experience. Blockchain technology will serve as the backbone, ensuring transparent and immutable transactions via smart contracts for user registration, content publication, and decentralized governance. Decentralized storage using IPFS will safeguard content, while a hybrid consensus model (**PoS** and **PoW**) ensures energy efficiency and security. User authentication will be secured using public-key cryptography and decentralized identifiers (**DIDs**), with encryption protecting sensitive information.

For communication, **WebRTC** and Socket.io will provide secure, real-time, peer-to-peer messaging. Scalability solutions like sharding and **IPFS** combined with **CDNs** will optimize performance as the platform grows. Security measures, including audits and penetration testing, will protect against threats, and regulatory compliance (e.g., **GDPR**) will ensure data privacy. The user interface will be designed for accessibility and simplicity, incorporating iterative feedback to refine the app, ensuring a secure and user-friendly decentralized experience.

3.1 Project UML design

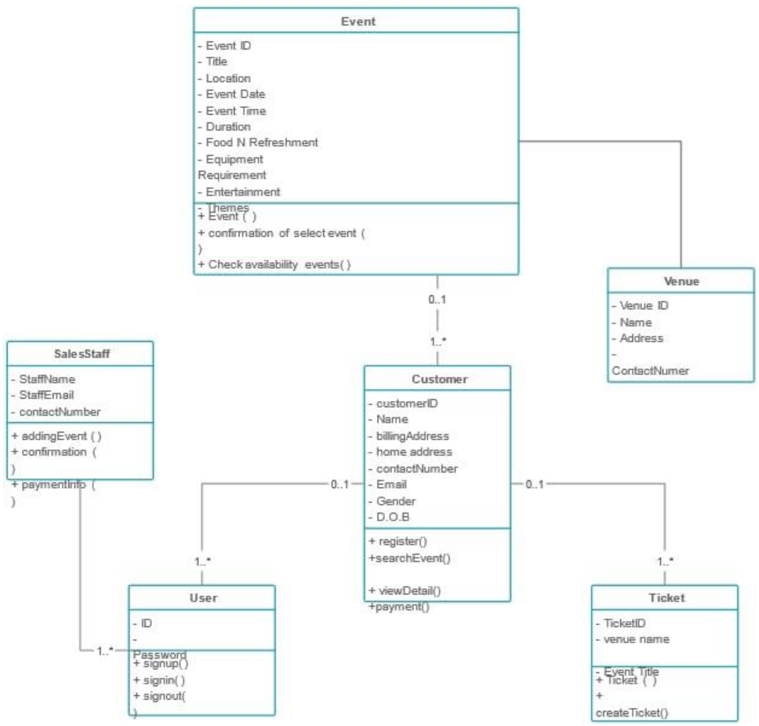


Fig.3.1.1 Entity Relationship Diagram

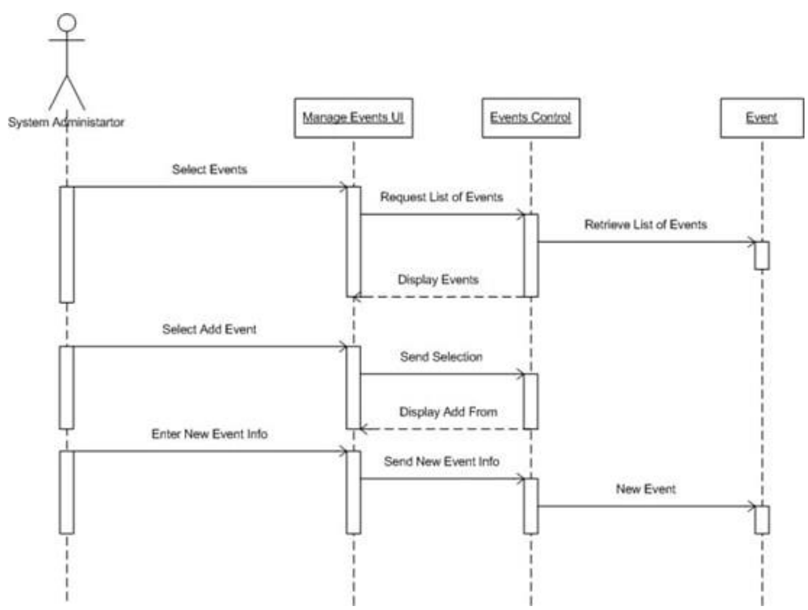


Fig.3.1.2 Sequence Diagram

3.2 Project Architecture

Designing the architecture for a **Decentralized Social Media App** using **Blockchain** requires a comprehensive, modular approach to ensure privacy, security, and seamless functionality. The following sections outline the key components involved in building the architecture of the platform:

1. Blockchain Integration

A permissioned blockchain with Proof-of-Stake (PoS) ensures security, scalability, and efficient transaction validation.

2. User Authentication

Cryptographic authentication secures user identities with private keys, enabling users to control data access and visibility.

3. Decentralized Storage

Content is stored using IPFS for distributed, immutable storage, with end-to-end encryption protecting user data.

4. Smart Contracts

Smart contracts automate platform rules and manage content rights, ensuring transparency and eliminating centralized intermediaries.

5. Content Distribution

IPFS ensures decentralized, reliable content delivery, while algorithms personalize recommendations based on user preferences.

6. Scalability & Performance

Sharding and caching enhance scalability, while load balancing ensures smooth performance during high traffic.

7. Community Governance

Token-based voting ensures decentralized decision-making and transparency in moderation and platform rules.

3.3 Data preparation

To fully comprehend the implications and functionality of blockchain technology within the context of decentralized applications (dApps) and databases, it is essential to first understand the core principles of blockchain and its distinction from traditional databases.

Blockchain is a decentralized digital ledger that records and stores transactional data across a network of nodes. Unlike traditional databases that depend on a centralized structure, blockchain ensures data integrity and security through cryptographically linked blocks. Its immutability, powered by consensus protocols, prevents tampering, making blockchain ideal for secure applications like cryptocurrencies and NFTs. However, this immutability comes with limitations in flexibility, as altering data requires significant computational effort, hindering its suitability for dynamic applications.

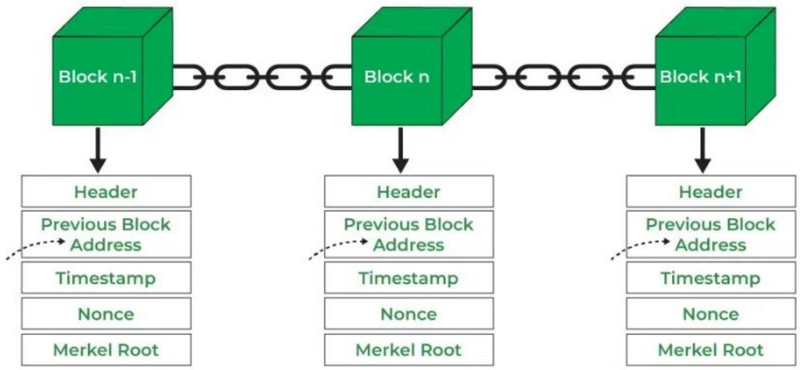


Fig.3.3.1 Blockchain Structure

Traditional databases, in contrast, support CRUD (Create, Read, Update, Delete) operations, allowing flexible data management. Blockchain, however, focuses on securely storing and verifying transactional data, prioritizing transparency and security over performance. While blockchain ensures immutable records, it suffers from slower data retrieval and modification processes, making it less suitable for applications requiring high-speed queries. For dynamic, high-performance environments, traditional databases remain more effective.

To address blockchain's performance challenges, a hybrid architecture combining blockchain with traditional databases has been proposed. In this model, the blockchain layer manages critical data such as transactions and audit trails, ensuring decentralization and security. The traditional database layer, on the other hand, supports fast querying and CRUD operations for non-sensitive data like user profiles or media. A bridging mechanism connects these layers, ensuring data integrity while optimizing performance and flexibility.

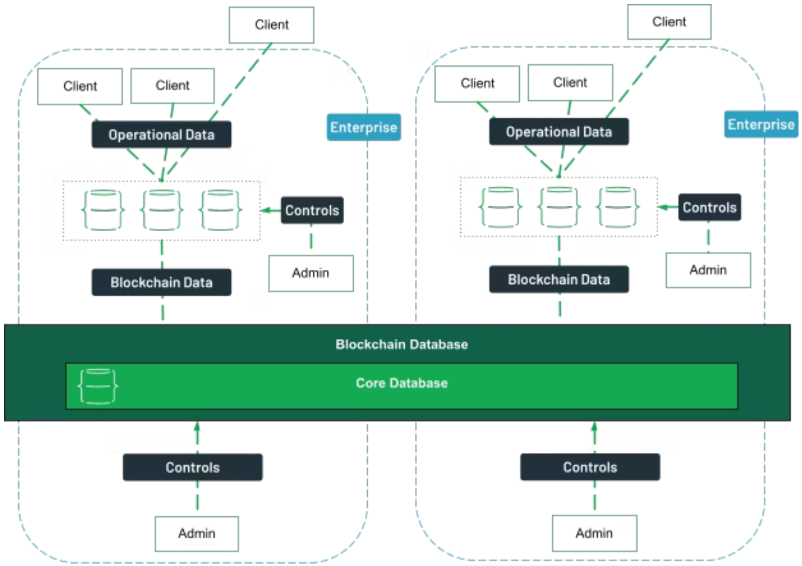
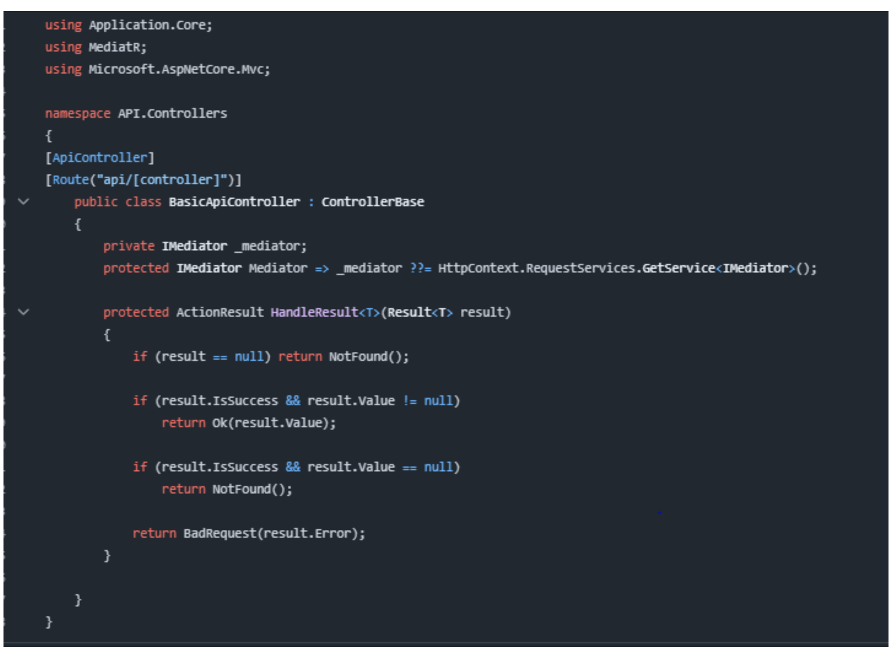


Fig.3.3.2 Non-operational data in a decentralized system

In decentralized systems, operational data is directly accessed by clients, as seen in cryptocurrencies where users query the blockchain. Non-operational data, however, often requires intermediaries for access. Decentralized social media platforms, leveraging blockchain, secure non-operational data while ensuring privacy and control for users. With blockchain scalability remaining a challenge, solutions like off-chain storage, layered architectures, and permissioned blockchains blend decentralization with control, enabling broader blockchain application across diverse fields.

3.4 Source code:



```
using Application.Core;
using MediatR;
using Microsoft.AspNetCore.Mvc;

namespace API.Controllers
{
[ApiController]
[Route("api/[controller]")]
    public class BasicApiController : ControllerBase
    {
        private IMediator _mediator;
        protected IMediator Mediator => _mediator ??= HttpContext.RequestServices.GetService<IMediator>();

        protected ActionResult HandleResult<T>(Result<T> result)
        {
            if (result == null) return NotFound();

            if (result.IsSuccess && result.Value != null)
                return Ok(result.Value);

            if (result.IsSuccess && result.Value == null)
                return NotFound();

            return BadRequest(result.Error);
        }

    }
}
```

Fig.3.4.1 Basic Api Controller

```csharp
namespace API.Extensions
{
    public static class ApplicationServiceExtensions
    {
        public static IServiceCollection AddConnetions(this IServiceCollection services,
        IConfiguration config)
        {
            services.AddEndpointsApiExplorer();
            // Learn more about configuring OpenAPI at https://aka.ms/aspnet/openapi
            services.AddOpenApi();
            services.AddDbContext<DataContext>(opt => {
                opt.UseSqlite(config.GetConnectionString("DefaultConnection"));
            });

            services.AddCors(opt => {
                opt.AddPolicy("CorsPolicy",policy => {
                    policy.AllowAnyHeader().AllowAnyMethod().WithOrigins("http://localhost:3000");
                });
            });
            services.AddMediatR(cfg => cfg.RegisterServicesFromAssembly(typeof(List.Handler).Assembly));
            services.AddAutoMapper(typeof(MappingProfiles).Assembly);
            services.AddFluentValidationAutoValidation();
            services.AddValidatorsFromAssemblyContaining<Operation>();
            return services;
        }
    }
}
```

Fig.3.4.2 Application Services Extensions Controller

```csharp
        public async Task InvokeAsync(HttpContext context)
        {
            try
            {
                await _next(context);
            }
            catch (Exception ex)
            {
                _logger.LogError(ex, ex.Message);
                context.Response.ContentType = "application/json";
                context.Response.StatusCode = (int)HttpStatusCode.InternalServerError;

                var response = _env.IsDevelopment()
                    ? new AppException(context.Response.StatusCode, ex.Message, ex.StackTrace?.ToString())
                    : new AppException(context.Response.StatusCode, "Internal Server Error");

                var options = new JsonSerializerOptions{PropertyNamingPolicy = JsonNamingPolicy.CamelCase};

                var json = JsonSerializer.Serialize(response, options);

                await context.Response.WriteAsync(json);
            }
        }
    }
}
```

Fig.3.4.3 Middleware Connection

```
using Application.Core;
using Domain;
using MediatR;
using Persistence;

namespace Application.Activities
{
    public class Details
    {
        public class Query : IRequest<Result<Activity>>
        {
            public Guid Id { get; set; }
        }

        public class Handler : IRequestHandler<Query, Result<Activity>>
        {
            private readonly DataContext _context;

            public Handler(DataContext context)
            {
                _context = context;
            }

            public async Task<Result<Activity>> Handle(Query request, CancellationToken cancellationToken)
            {
                var activity = await _context.Activities.FindAsync(request.Id);

                return Result<Activity>.Success(activity);
            }
        }
    }
}
```

Fig.3.4.4 (CRUD) Details

```
import { Button, Container, Menu } from 'semantic-ui-react'
import { NavLink } from 'react-router-dom';

export default function NavBar() {

  return (
    <Menu inverted fixed='top'>
    <Container>
        <Menu.Item as={NavLink} to='/' header>
            <img src="/assets/logo.png" alt="logo" style={{marginRight:'10px'}}/>
            Reactivities
        </Menu.Item>
        <Menu.Item as={NavLink} to='/activities' name="Activites" />
        <Menu.Item>
            <Button as={NavLink} to='/addActivity' positive content='Add Activity' />
        </Menu.Item>
    </Container>
</Menu>
  )
}
```

Fig.3.4.5 Navbar

```
import React from 'react'
import { Dimmer, Loader } from 'semantic-ui-react'

interface Props{
    inverted?: boolean,
    context?: string
}

export default function LoadingComponent({inverted = true,context = 'Loading....'}:Props) {
  return (
   <Dimmer active={true} inverted={inverted}>
    <Loader context={context} />
   </Dimmer>
  )
}
```

Fig.3.4.6 Loading Component

4. Results

Blockchain integration in decentralized social media platforms offers substantial advantages, particularly in enhancing data ownership and control. By leveraging blockchain's immutability, users gain full autonomy over their personal data, reducing risks associated with unauthorized access and manipulation. This shift improves privacy and transparency compared to centralized systems, while also fostering greater accountability.

In content management, blockchain enables censorship-resistant environments, allowing users to freely express themselves without fear of arbitrary suppression. Decentralized governance structures also empower users to actively participate in decision-making processes, promoting community ownership and engagement.

Despite these benefits, scalability and complexity remain challenges. However, continuous improvements in consensus algorithms, storage solutions, and user interfaces promise to resolve these issues, positioning decentralized social media as a secure, transparent, and user-centric alternative to traditional models.

4.1 Output

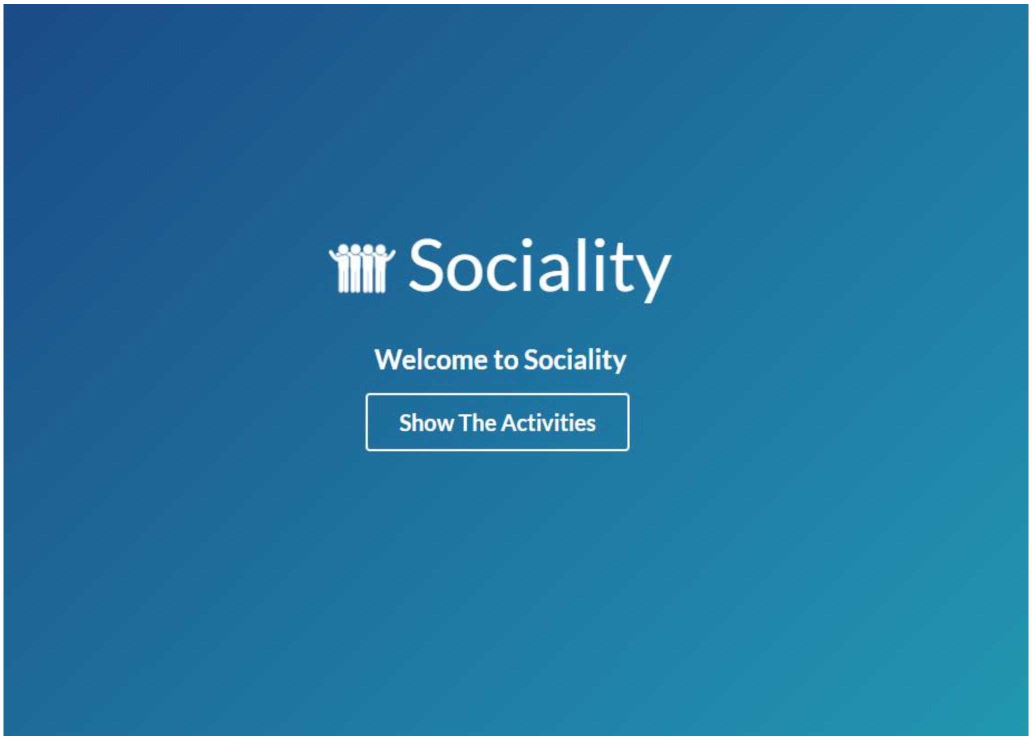


Fig 4.1.1 Home Page – Sociality

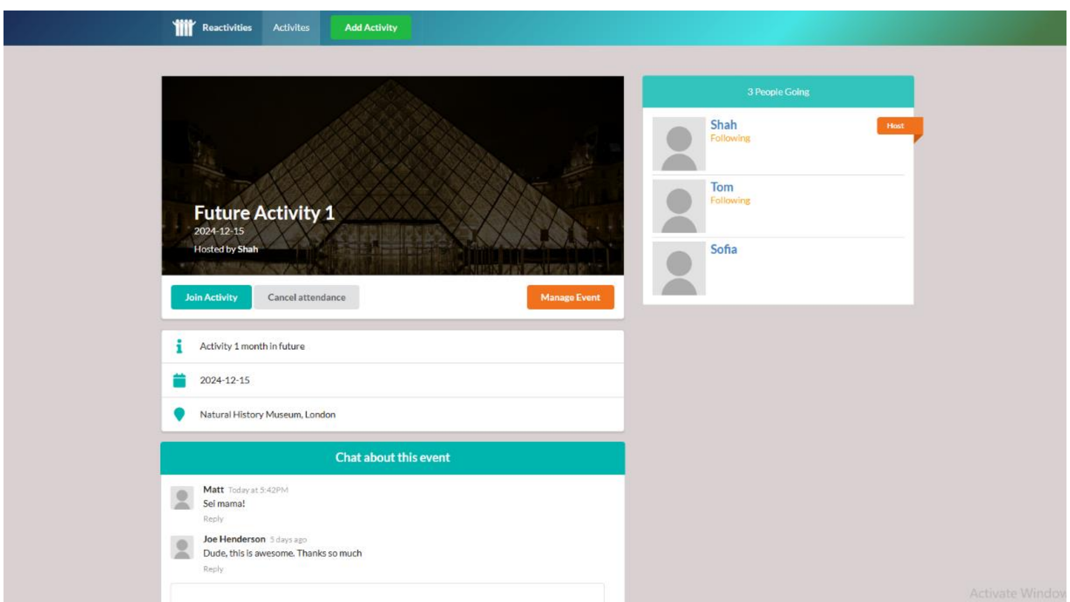


Figure 4.1.2 Activity Details Page

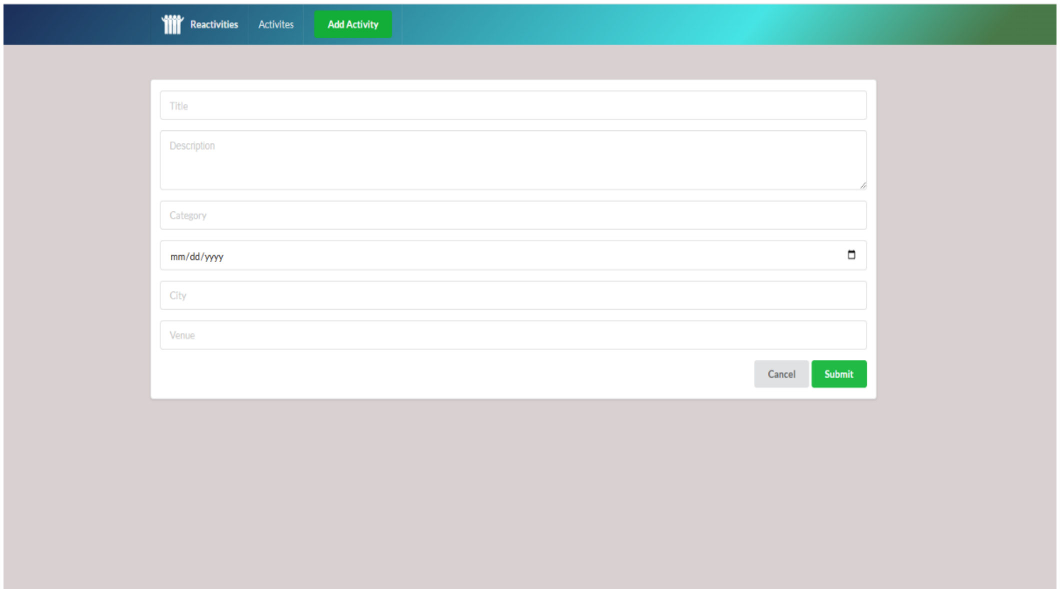


Figure 4.1.3 Add Activity Form

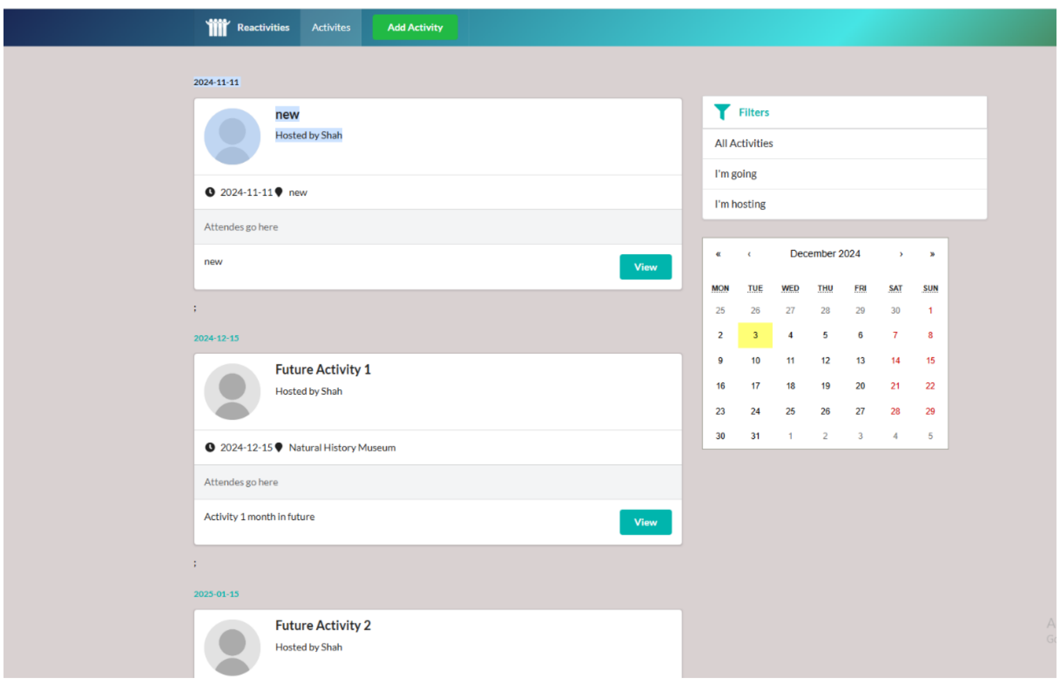


Figure 4.1.4 Activities Page

5. Discussion

Integrating blockchain technology into a decentralized social media platform enhances security and privacy by giving users full control over their data. Blockchain's transparency, immutability, and decentralization ensure that user interactions are cryptographically secured and recorded in blocks, preventing unauthorized modifications. Data is distributed across a decentralized network, eliminating single points of failure and increasing platform integrity, as altering a block requires consensus from multiple nodes.

Blockchain also offers enhanced privacy by allowing users to retain ownership of their content. Decentralized storage solutions like IPFS ensure secure distribution without relying on central servers. Smart contracts automate content moderation, while encryption protects user communication. With decentralized governance, users can engage in decision-making, fostering community ownership. This combination of features provides a secure, transparent, and privacy-focused platform that promotes freedom of expression and addresses data misuse concerns seen in centralized platforms.

6. Conclusion

The development of a decentralized social media platform using blockchain technology revolutionizes digital interaction by giving users full control over their data and content, enhancing privacy and reducing data exploitation. Blockchain's transparent and immutable ledger enables users to track content moderation and interactions, promoting accountability.

This decentralized model improves security by distributing data across nodes, preventing single points of failure. Cryptographic techniques ensure user data is protected from unauthorized access, addressing concerns like censorship and data breaches.

Despite challenges in scalability and adoption, ongoing advancements in consensus mechanisms and user interfaces will enable a more user-centric, secure, and transparent platform for the future.

7. References

[1] A. De Salve, P. Mori, L. Ricci, and R. Di Pietro, “Content privacy enforcement models in decentralized online social networks: State of play, solutions, limitations, and future directions,” *Computer Communications*, vol. 203, pp. 199–225, Mar. 2023, doi: 10.1016/j.comcom.2023.02.023.

[2] A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci, and A. Puccia, “A multi-layer trust framework for Self-Sovereign Identity on blockchain,” *Online Social Networks and Media*, vol. 37–38, p. 100265, Aug. 2023, doi: 10.1016/j.osnem.2023.100265.

[3] C. Blanco-González-Tejero, E. Cano-Marin, K. Ulrich, and S. Giralt-Escobar, “Leveraging blockchain for industry funding: A social media analysis,” *Sustainable Technology and Entrepreneurship*, vol. 3, no. 3, p. 100071, Jan. 2024, doi: 10.1016/j.stae.2024.100071.

[4] Pandey, S., Sinha, M., & G, R. (2023). Exploring the potential of interplanetary file system for secure and transparent social media. *IEEE Transactions on Cloud Computing*, 1–5. https://doi.org/10.1109/vitecon58111.2023.10157092

[5] Michelia, S. M., Kurniawan, F., Antonius, V. H., Moniaga, J. V., & Jabar, B. A. (2022). Systematic literature review and Qualitative survey of blockchain impact on social media security. *2022 5th International Conference on Information and Communications Technology (ICOIACT)*, 54–59. https://doi.org/10.1109/icoiact55506.2022.9972200

[6] Chen, N., & Cho, D. S. (2021). A blockchain based autonomous decentralized online social network. *IEEE Access*, 186–190. https://doi.org/10.1109/iccece51280.2021.9342564

[7] Michelia, S. M., Kurniawan, F., Antonius, V. H., Moniaga, J. V., & Jabar, B. A. (2022b). Systematic literature review and Qualitative survey of blockchain impact on social media security. *2022 5th International Conference on Information and Communications Technology (ICOIACT)*, 54–59. https://doi.org/10.1109/icoiact55506.2022.9972200

[8] Fan, K., Pan, Q., Zhang, K., Bai, Y., Sun, S., Li, H., & Yang, Y. (2020). A secure and verifiable data sharing scheme based on blockchain in vehicular social networks. *IEEE Transactions on Vehicular Technology*, *69*(6), 5826–5835. https://doi.org/10.1109/tvt.2020.2968094

[9] Song, G., Kim, S., Hwang, H., & Lee, K. (2019). Blockchain-based notarization for social media. *2023 IEEE International Conference on Consumer Electronics (ICCE)*. https://doi.org/10.1109/icce.2019.8661978.

[10] GeeksforGeeks. (2024, August 29). *Blockchain structure*. GeeksforGeeks. https://www.geeksforgeeks.org/blockchain-structure