PEERLINK - A DECENTRALISED SOCIAL MEDIA

A PROJECT REPORT

Submitted by

BINOY BARNABAS (TKM21MCA-2014)

to

The APJ Abdul Kalam Technological University

In partial fulfillment of the requirements for the award of the degree of

MASTER OF COMPUTER APPLICATIONS

Thangal Kunju Musaliar College of Engineering
Kerala

DEPARTMENT OF COMPUTER APPLICATIONS

MAY 2023

DECLARATION

I undersigned hereby declare that the project report on **PEERLINK - A DECENTRALISED SOCIAL MEDIA**, submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of **Prof. Natheera Beevi M**. This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Kollam

16-05-2023

BINOY BARNABAS

DEPARTMENT OF COMPUTER APPLICATIONS

TKM COLLEGE OF ENGINEERING

KOLLAM

2022 - 23

CERTIFICATE

This is to certify that the report entitled **PEERLINK - A DECENTRALISED SOCIAL MEDIA** submitted by **BINOY BARNABAS** (TKM21MCA-2014) to the APJ Abdul Kalam Technological University in partial fulfillment of the Masters degree in Computer Applications is a bonafide record of the project work carried out by him under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor Head of the Department External Examiner

Acknowledgement

First and foremost I thank GOD almighty and my parents and my sister for the success of this project. I owe sincere gratitude and heart full thanks to everyone who shared their precious time and knowledge for the successful completion of my project.

I am extremely grateful to **Dr. Fousia M Shamsudeen**, Head of the Department, Department of Computer Applications, for providing me with best facilities.

I would like to thank my coordinator, project guide and our advisor **Prof. Natheera Beevi M**, Department of Computer Applications, who motivated me throughout the project .

I profusely thank all other faculty members in the department and all other members of TKM College of Engineering, for their guidance and inspirations throughout my course of study.

I owe my thanks to my friends and all others who have directly or indirectly helped me in the successful completion of this project.

BINOY BARNABAS

ABSTRACT

PEERLINK - A DECENTRALISED SOCIAL MEDIA - Decentralised social media is an emerging paradigm that aims to address the issues of censorship, privacy, and control that are inherent in centralised social media platforms. This model of social media is built on distributed networks that allow users to communicate and share content without the need for a central authority. Decentralised social media platforms are designed to be resistant to censorship, ensuring that users can express their opinions and ideas freely. Moreover, these platforms provide greater control over personal data and privacy, empowering users to own their data and control who can access it. By leveraging blockchain technology and other distributed ledger technologies, decentralised social media platforms offer a more secure and transparent way to share information and interact online.

Users can share their pictures to the feed and can get incentives from other users to promote their contents with the help of cryptocurrencies. The contents are free from censorship and the users have complete control over their content by limiting the reusage of contents.

Contents

List of Figures

Chapter 1

Introduction

Social media has become an integral part of our lives in the 21st century, with billions of people worldwide actively engaging on various platforms. Social media provides a way for individuals to connect with friends, family, and strangers from all over the world, share their experiences, and stay informed about current events. With the advancement of technology and the availability of smartphones, social media has become more accessible than ever before, allowing people to engage with their favorite platforms at any time and from anywhere. However, the rise of social media has also led to concerns over privacy, cyberbullying, and the spread of misinformation, highlighting the need for responsible and ethical use of these platforms.

PEERLINK - A DECENTRALISED SOCIAL MEDIA has potential solutions to some of the problems associated with centralized social media platforms. Unlike traditional social media, decentralised social media runs on a blockchain, a distributed ledger technology that provides a secure and transparent way of storing and sharing data. This technology allows users to have full control over their data and eliminates the need for intermediaries such as social media companies to manage and control user information. Decentralised social media also promises to address issues of censorship and content moderation by giving users the power to moderate the content they see on the platform.

Decentralised social media platforms operate on the principle of distributed control, which means that users have equal ownership and control over the network. This is achieved by using a blockchain-based system, where each user has their own private key that allows them to access and manage their data. Since the data is stored on a decentralised network, it is much more difficult for third-party entities to access or manipulate it without the consent of the user.

This results in a higher level of privacy and security for users, as well as greater transparency in how their data is being used.

One of the most significant benefits of decentralised social media is that it eliminates the need for a centralized authority or corporation to manage the platform. This means that users are no longer subject to the terms and conditions set by social media companies, which often include complex legal agreements that give companies broad rights over user data. Instead, decentralised social media is governed by a set of rules that are encoded in the blockchain, and users have the power to enforce these rules by participating in the network.

1.1 Existing System

Traditional social media has become an integral part of modern life, with billions of users around the world relying on these platforms to connect with friends and family, share information, and stay up-to-date on current events. The most popular social media platforms, such as Facebook, Twitter, Instagram, and TikTok, offer a range of features that enable users to share photos and videos, post updates and comments, and interact with others in a variety of ways.

However, traditional social media has also come under scrutiny in recent years due to a range of concerns, including privacy violations, the spread of misinformation and fake news, and the negative effects on mental health and well-being. Social media companies have been accused of collecting vast amounts of user data and using this information to generate profits through targeted advertising. They have also been criticized for their handling of user data, with many users feeling that their privacy is not adequately protected.

In addition, traditional social media platforms have been accused of facilitating the spread of misinformation and fake news, particularly during high-profile events such as elections and political campaigns. Social media algorithms can amplify certain types of content, creating echo chambers and reinforcing biases. This can lead to the spread of false information and divisive content that can have a harmful impact on individuals and society as a whole.

Overall, traditional social media has revolutionized the way we connect with others and share information, but it has also raised a range of concerns related to privacy, the spread of misinformation, and negative effects on mental health. As a result, many people are looking for alternative platforms that offer greater security, transparency, and control over user data and online identity.

1.2 Problem Statement

The drawbacks of currently existing models are:

1. Privacy concerns : Centralized social media platforms often collect and use user data for targeted advertising and data analysis, which can raise privacy concerns for users.

2. Censorship : Centralized social media platforms have a central point of control, which means that they can censor certain types of content or users.

3. Data breaches : Centralized social media platforms store user data in a central location, which can make it vulnerable to hackers and data breaches

4. Lack of control over content : Centralized social media platforms have their own set of rules and guidelines for content, which may not align with the views or values of some users.

5. Algorithm bias : Centralized social media platforms use algorithms to curate content, which can lead to bias and a lack of diversity in the content shown to users.

6. Revenue inequality : Centralized social media platforms often generate revenue through advertising, which can lead to a concentration of wealth among a small group of people or companies.

Inorder to solve the above stated issues, the proposed method can uses decentralised model as the backbone of the social media so as to solve the mentioned problems in the current system.

1.3 Proposed System

Decentralised social media that works on blockchain is an emerging type of social media platform that offers a range of benefits over traditional social media. These platforms are built on blockchain technology, which provides a secure, transparent, and decentralised way of storing and sharing data. Unlike traditional social media, which is often controlled by a small number of corporations, decentralised social media platforms are designed to be owned and controlled by the users themselves.

One of the main benefits of decentralised social media platforms is that they offer greater privacy and security. Since data is stored on a decentralised network of computers rather than a central server, it is much harder for hackers and other malicious actors to gain unauthorized access to user data. Blockchain technology provides an added layer of security by ensuring that data cannot be tampered with or altered without the agreement of the network participants.

Decentralised social media platforms also offer greater control over user data and online identity. Users can own and manage their data in a transparent and secure way, which allows them to decide how their data is used and shared. This gives users greater control over their online presence and enables them to participate in online communities on their own terms.

Another advantage of decentralised social media platforms is that they enable more democratic and transparent governance. Since these platforms are decentralized, users can participate in the decision-making process and help to shape the rules and policies that govern the platform. This means that users have a greater say in how the platform is run, and can work together to create a more equitable and user-centered environment.

Overall, decentralised social media that works on blockchain offers a range of benefits over traditional social media, including greater privacy and security, control over user data and online identity, and more democratic and transparent governance. They represent a promising development in the ongoing effort to create a more secure, transparent, and user-centered online environment.

1.4 Objectives

1.4.1 Resisting censorship

Since there is no single point of control or authority that can be pressured or coerced into removing or suppressing content. In traditional social media platforms, content moderation is typically centralized, with a few large corporations controlling what content is allowed on their platforms. This can lead to issues of bias and censorship, as these companies may have their own agendas and interests that they seek to promote or suppress. In contrast, decentralised social media platforms enable users to resist censorship by giving them greater control over the content they create and consume. By enabling users to control their own data and content, these platforms provide a more democratic and decentralised alternative to traditional social media platforms.

1.4.2 Creating new economic models

Decentralised social media can create new economic models for content creators, by enabling them to directly monetize their content through micropayments or other decentralised mechanisms. One of the key advantages of decentralised social media is that it enables users to directly monetize their content and earn rewards for their contributions to the network. This is made possible through the use of blockchain-based tokens, which can be used to incentivize users to create and share high-quality content. Another advantage of decentralised social media

is that it enables more equitable distribution of rewards and value. In traditional social media platforms, a small number of corporations capture the majority of the value created by user-generated content. In contrast, decentralised social media platforms can distribute rewards more evenly among users, ensuring that everyone who contributes to the network is fairly compensated.

1.4.3 Promoting data ownership

Promote data ownership by giving users more control over their personal data and enabling them to store it in decentralised storage networks thus reduces the power imbalance between users and corporations. Traditional social media platforms are notorious for collecting vast amounts of user data, often without the explicit consent or knowledge of their users. This data is then used to generate profits for social media companies through targeted advertising and other means.

In contrast, decentralised social media platforms enable users to take control of their data and determine how it is used and shared. This is made possible through the use of blockchain-based systems that provide a secure and transparent way of storing and sharing data. Each user has their own private key that allows them to access and manage their data, and the decentralized nature of the platform means that no central authority or corporation has access to user data without the user's consent.

1.4.4 Empowering users

Putting users back in control of their data and online interactions, by creating platforms that are governed by decentralised protocols rather than centralized corporations.Unlike traditional social media platforms, which are often controlled by a small number of corporations, decentralised social media platforms enable users to take control of their online presence and engage with others on their own terms.

One way that decentralised social media platforms empower users is by giving them greater control over their data and online identity. By using blockchain-based systems, users can own and manage their data in a secure and transparent way. This gives users more control over how their data is shared and used, and enables them to participate in online communities on their own terms.

1.4.5 Enhancing network resilience

Decentralised social media can enhance network resilience by distributing data and processing across many nodes, which makes it more difficult for a single point of failure to bring down the entire network. Traditional social media platforms are often centralized and rely on a single point of control, which can make them vulnerable to censorship, hacking, and other forms of disruption. In contrast, decentralised social media platforms are designed to be more resilient and resistant to disruption.

Decentralised social media platforms use a distributed network architecture that is designed to be more robust and resilient than traditional social media platforms. Rather than relying on a single point of control, these platforms distribute control and data across a network of nodes, making it much harder for any one point of failure to take down the entire network.

Chapter 2

Literature Survey

A literature survey, also known as a literature review, involves analyzing scholarly sources related to a particular subject. Examining the available literature, it provides a comprehensive overview of the state of the field, allowing you to identify relevant theories, approaches, and gaps in the existing body of knowledge. When conducting a literature review from an audit perspective, the main focus is on evaluating the relevant literature. This process covers information that has been published in a specific field of study and sometimes includes information published within a specific time frame.

2.1 Purpose of the Literature Review

1. It gives readers easy access to research on a particular topic by selecting high quality articles or studies that are relevant, meaningful, important and valid and summarizing them into one complete report.

2. It provides an excellent starting point for researchers beginning to do research in a new area by forcing them to summarize, evaluate, and compare original research in that specific area.

3. It ensures that researchers do not duplicate work that has already been done.

4. It can provide clues as to where future research is heading or recommend areas on which to focus.

5. It highlights the key findings.

6. It identifies inconsistencies, gaps and contradictions in the literature.

7. It provides a constructive analysis of the methodologies and approaches of other researchers.

2.2 Related Works

Decentralised social media platforms, powered by blockchain technology, are emerging as a compelling alternative to traditional social media. These platforms offer a range of benefits that surpass their centralized counterparts. By utilizing the secure and transparent nature of blockchain, decentralised social media platforms prioritize user control and ownership. A key advantage of decentralised social media platforms is the heightened privacy and security they provide. Unlike centralized platforms, where data is susceptible to breaches, decentralised platforms distribute data across a network of computers, making unauthorized access significantly more challenging. Additionally, the immutability of blockchain ensures data integrity, preventing any tampering without consensus from the network participants.

Ting Cai et al. [1] have discussed The use of blockchain technology in social media has garnered considerable attention due to its potential to address data ownership and security concerns. This literature review examines the implications and effectiveness of applying blockchain in social media platforms, with a focus on data storage and sharing systems.

In recent years, social media incidents involving illegal surveillance and data breaches have raised questions about the centralized data ownership model adopted by popular applications. To address these concerns, researchers have proposed decentralised alternatives such as SocialChain, a blockchain-based social data storage and sharing system that aims to return data ownership to users. SocialChain adopts a Personal Data Store approach, leveraging off-chain storage to ensure data separation from social applications. An identity establishment mechanism, based on WebID and certificateless cryptography, enables secure authentication functions for users. The design of SocialChain incorporates smart contracts to automate the secure storage and sharing of social data. By utilizing blockchain's immutability and traceability, it provides an auditable ledger of all operations on shared data, enhancing accountability and enabling the detection of malicious attempts. Experimental evaluations conducted on an Ethereum-based software prototype demonstrate that SocialChain offers user-friendly interfaces with relatively low latency, cost, and overhead. These findings support the

feasibility and real-world applicability of decentralised social media systems.

However, the literature also highlights certain limitations of applying blockchain in social media. Storing large volumes of data on the blockchain incurs significantly higher costs compared to conventional web servers. This cost disparity raises concerns about future performance implications, particularly in terms of request and response handling within the blockchain network. In conclusion, the integration of blockchain technology into social media platforms presents promising solutions to data ownership and security challenges. Projects like SocialChain demonstrate the potential of decentralized systems in returning control of user data to individuals. While blockchain offers benefits such as enhanced authentication, traceability, and accountability, the cost of storing extensive data on the blockchain remains a concern that needs to be addressed. Further research and development are required to optimize performance and scalability in blockchain-based social media applications.

2.2.1 Digital identity and Data storage on block chain

Yifan Yang et al. [2] aims to provide users with a tool for verifying the provenance of online digital identities. The service is designed to assist non-expert users in making informed decisions about whom to trust online. TAPESTRY leverages the concept of digital personhood (DP), which encompasses the longitudinal and multi-modal signals generated by users' lifelong digital interactions, as a foundation for establishing the authenticity of identity.

The paper presents a secure infrastructure that combines hybrid on- and off-chain storage, along with deep learning techniques for DP analytics and visualization. This infrastructure enables users to exchange trust evidence derived from their DP with others, while maintaining granular privacy and preserving the coherence and longevity of their online behavior. The authors emphasize that TAPESTRY does not make trust decisions on behalf of users; rather, it serves as a decision support service that facilitates the exchange and visualization of trust evidence, empowering users to make more effective trust-related judgments. The challenges addressed by TAPESTRY are addressed through three key technical contributions. Firstly, a secure data architecture is proposed, incorporating off-chain storage of encrypted trust evidence derived from the DP. The integrity and provenance of this evidence are ensured through an unpermissioned proof-of-work (PoW) blockchain. Secondly, a machine learning algorithm is introduced to transform DP activity into compact descriptors, serving as the fundamental unit of trust evidence for sharing within the platform. A deep neural network (DNN) is proposed,

employing semantic embedding and temporal modeling techniques to extract this evidence and detect behavioral deviations over time. Lastly, a data visualization technique is developed to represent the regularity and coherence of trust evidence within a single static image.

Mohd Sameen Chishti et al. [3] focuses on the utilization of smart contracts within the Ethereum blockchain network and addresses the limitations associated with their current implementation. Smart contracts are self-executable scripts that facilitate the management of tokenized assets and access rights among entities on the blockchain. They offer transparency and reliability for maintaining digital relationships. However, certain challenges, such as immutability and code secrecy, hinder their full potential.

The paper under review specifically addresses the issue of smart contracts' inability to directly access on-chain data. Presently, smart contracts rely on external oracles to fetch this data, creating a potential vulnerability that could compromise the integrity of transactions. To overcome this limitation, the authors propose a decentralized mechanism that enables smart contracts to access blockchain data directly. This is achieved by indexing various transaction parameters within each block using the Merkle-Patricia Trie (MPT) data structure. The objective is to enhance the transparency of blockchain applications. The proposed approach introduces a sequential search methodology capable of retrieving transactions satisfying specific conditions from a given number of blocks with a complexity of O(N). To further optimize efficiency, the paper suggests partitioning the blockchain data into k disjoint subsets, enabling parallelism in the search procedure. Consequently, the complexity is reduced to O(N/k). To validate the effectiveness of the proposed methodology, the authors conducted experiments using Ethereum blockchain data and present a case study illustrating its application.

2.2.2 Data storage on IPFS

Ammar Ayman Battah et al. [4] focuses on the challenges associated with multi-party authorization (MPA) systems and the limitations of existing centralized implementations. MPA involves multiple parties collaborating to control and grant access to shared data, aiming to mitigate insider attacks by preventing a single authority from acting independently. However, current MPA solutions lack trusted, secure, immutable, auditable, and decentralized mechanisms for logging and tracing permissions granted. Additionally, centralized proxy re-encryption algorithms employed for secure data sharing raise concerns about trustworthiness.

In this paper, the authors propose a fully decentralized blockchain-based solution to address these limitations. The MPA system is implemented using Ethereum smart contracts, while proxy re-encryption algorithms, known for their computational complexity, are executed using multiple oracles. The encrypted shared data is stored on a public and decentralized storage platform, such as the Interplanetary File System (IPFS). The smart contracts facilitate result validation by leveraging the majority consensus among the oracles. To enhance trust, the proposed system incorporates reputation mechanisms within the smart contracts to evaluate the oracles' behaviors, distinguishing between malicious and non-malicious actions. The paper presents comprehensive algorithms, implementation details, and thorough testing and validation processes. The proposed system's security, cost-effectiveness, and generalizability are evaluated, demonstrating its reliability and practicality. Furthermore, the authors have made the source code of the smart contracts publicly available on Github.

Erik Daniel et al. [5] talks about data storage on P2P networks. The proliferation of cloud storage providers has become the norm for data storage and sharing among users. However, these centralized systems give rise to concerns related to data silos, accessibility, availability, and confidentiality. Users relinquish control over their data to a single entity, which can lead to issues such as censorship and security breaches. To address these challenges and reduce trust assumptions, peer-to-peer (P2P) data networks have emerged as a decentralized alternative. The first generation of P2P data networks, exemplified by Napster and Gnutella, focused primarily on file sharing. These networks introduced concepts such as anonymous storage and retrieval (e.g., Freenet) and protocols for maintaining structured overlay network topology (e.g., Chord, CAN, Pastry). BitTorrent, with its incentive mechanism for achieving network efficiency, garnered significant attention from both users and researchers.

In the transition phase, Bitcoin's introduction in 2008 revitalized the idea of joint data replication and incentivization within P2P networks. Distributed ledger technologies, including cryptocurrencies, offered availability, integrity, and fault tolerance in decentralized systems. This phase paved the way for the next generation of P2P data networks. The next generation of P2P data networks, starting with IPFS in 2014, aimed to break free from data silos and enhance decentralized sharing and storage. These systems utilize knowledge from previous networks while incorporating new developments. IPFS, Swarm, Hypercore Protocol, SAFE, Storj, and Arweave are prominent examples of this next generation. IPFS, in particular, gained popularity as a storage layer for blockchains. The surveyed literature highlights the

building blocks, similarities, and trends observed in P2P data networks. While each system has its unique purpose and focus, such as distributed cloud storage (Storj) or large dataset distribution (Hypercore Protocol), they share commonalities in network organization, file lookup, decentralization, redundancy, and privacy. Kademlia is frequently used for network structuring, and incentivization mechanisms play a crucial role in enhancing functionality. Research also explores the integration of P2P data networks with blockchains, examining aspects such as immutability, scalability, and latency. Some networks, however, deliberately avoid blockchain integration due to specific challenges. Therefore, a broader perspective on data networks is necessary, considering design decisions beyond blockchains.

2.2.3 Web3 and Blockchain

Nicholas Paul Imperius et al. [6] emphasizes the importance of testing methods for smart contracts in blockchain applications. In recent years, the integration of smart contracts into mainstream technology, particularly within the development of Web3 and the metaverse, has unveiled the technological future. Smart contracts are poised to play a crucial role in decentralizing and automating various day-to-day tasks. As a result, there has been a growing body of literature focusing on testing methods for smart contracts in blockchain applications. This paper presents the findings of a systematic mapping study conducted to provide a structured overview of the information available in primary sources. Systematic mapping is a well-established method for identifying and categorizing research papers within a field that has seen a substantial increase in literature. In this study, the researchers performed a search for studies published between 2017 and March 2022, resulting in 303 initial results. Through specific inclusion and exclusion criteria, 47 papers were selected as relevant to the study. The selected papers were then analyzed, and a concept map was created to summarize the key attributes identified from the primary sources. These attributes included research type, contribution type, blockchain network, smart contract language, development process, testing methods, and testing environment. Additionally, the researchers categorized the trends and demographics observed in the selected papers, considering factors such as publication year and the country of the authors. The systematic mapping study revealed that the field of smart contract testing is still relatively new but rapidly expanding, with new research being published regularly. The results of this study can provide valuable insights for researchers interested in this field, offering opportunities for future work and exploration.

Ammar Ayman Battah et al. [7] tries the emphasize about account classification on ethereum blockchain networks. Account classification plays a critical role in detecting illegal behavior, tracking transactions, and de-anonymizing the Ethereum transaction system. As Ethereum accounts are increasingly utilized in various services and businesses, the need for effective methods to classify and analyze these accounts becomes paramount. This literature review focuses on addressing the account classification problem in Ethereum through the utilization of Graph Convolutional Networks (GCN). The Ethereum transaction records can be represented as a large-scale transaction network, where accounts are interconnected based on their transaction activities. An important characteristic of this network is its high heterophily, indicating that accounts with different features and labels are interconnected. This heterophily poses a challenge for accurate account classification. To overcome this challenge, the authors propose a novel GCN-based model known as EH-GCN. By leveraging the power of graph convolutional networks, EH-GCN captures the intricate relationships and patterns within the transaction network. It incorporates the graph structure and individual account features to enhance the accuracy of account classification in Ethereum. Experimental results on a realistic Ethereum dataset demonstrate that EH-GCN achieves state-of-the-art performance in account classification, effectively capturing diverse account behaviors and characteristics present in the Ethereum transaction network. This enables accurate classification and detection of illegal activities. Furthermore, benchmarking experiments showcase EH-GCN's competitiveness even under homophily, where interconnected accounts share similar features and labels. This highlights the robustness and generalizability of the proposed method across different network structures and data scenarios.This underscores the significance of account classification in Ethereum and the pressing need for effective methods to address this challenge. By employing GCN-based models like EH-GCN, the potential of graph convolutional networks in analyzing transaction networks and detecting illicit behavior is showcased. The proposed EH-GCN model contributes to the existing body of knowledge by offering an advanced solution for Ethereum account classification. Through its ability to leverage the graph structure and incorporate features, EH-GCN enhances classification accuracy, facilitating transaction tracking and de-anonymization within the Ethereum system. Overall, this research advances the understanding of account classification in Ethereum and provides valuable insights for researchers and practitioners involved in Ethereum account analysis and classification.

Ruiguo Yu et al. [8] the authors propose an efficient privacy-preserving algorithm designed

to safeguard information in social networks. Community detection is a crucial aspect of social network analysis, but the influence of social factors such as user intimacy, influence, and interaction behavior is often overlooked in existing methods. While some approaches focus on single classification algorithms, there remains a gap in the development of multi-classification algorithms that can effectively identify overlapping communities. Previous studies have addressed the calculation of intimacy based on user relationships to divide them into social communities. However, the potential for malicious users to acquire other users' relationships raises concerns about privacy infringement and the manipulation of information. The algorithm addresses the challenges posed by malicious users by implementing identity verification during community expansion based on mining seed. By utilizing the recognition and non-tampering properties of the blockchain, the authors store users' public keys and bind them to block addresses for authentication purposes. This approach enhances security and prevents unauthorized access. To further protect against honest but curious users attempting to gain unauthorized access to other users' information, the authors employ a strategy where plaintext data is not directly transmitted after authentication. Instead, the attributes are hashed using mixed hash encryption, ensuring that users can only compute matching degrees without gaining access to specific information about other users. Through comprehensive analysis, the authors demonstrate that their proposed protocol is effective in defending against various types of attacks. This literature review highlights the significance of community detection in social network analysis. It emphasizes the limitations of existing methods in considering social factors and the lack of comprehensive multi-classification algorithms for identifying overlapping communities. The proposed privacy-preserving algorithm addresses these limitations by incorporating identity verification and secure data transmission techniques. The use of blockchain technology for authentication and the encryption of attributes contribute to the overall security and privacy of the social network.

Chapter 3

Methodology

Decentralised social media refers to social networking platforms that operate on a peer-to-peer (P2P) network, without a centralized authority controlling the data. The methodology behind decentralised social media involves the use of blockchain technology and distributed ledger technology to enable users to have full control over their data and interactions on the platform. The data is encrypted, and transactions are recorded on a public ledger, which ensures transparency and security. Instead of relying on a central authority to store and manage user data, decentralised social media uses a network of nodes, where each node holds a copy of the data. This approach ensures that user data is not owned or controlled by a single entity, and the platform is more resistant to censorship and hacking attempts. Additionally, decentralised social media allows for a more democratic and open system, where users have equal say in the decision-making process, and there is no bias towards any particular group or individual.

3.1 Architecture

3.1.1 System Design

The system has end users who are the active participants on the social media. They can post images on the live feed. The image uploaded by the user is stored on IPFS also known as InterPlanetary File System and every image is associated with a unique hash to identify the image. Here we use Infura IPFS server which uses Base58 encoded hash. The image hash generated is then stored on the block chain network as a smart contract along with the user's unique address that are generated over the block chain network while they create their account

for the web3(ethereum) based ecosystem. The block chain network used for this platform is Ganache which is a local ethereum based block chain network. Every users should login through their web3 account via the metamask wallet so as to become a user. Every users should pay a gas fee for posting their content as per the requirements. Users can tip or give incentives to other users for encouraging them. The incentives are send as ethereum cryptocurrency and the tips are send directly to the users account. Truffle is a compiler used to compile smart contracts written on Solidity programming language. The initial smart contracts are migrated to the ethereum block chain network and then further activities on by user are tracked by new transaction on the block chain and thus the activities are stored on the block chain network.

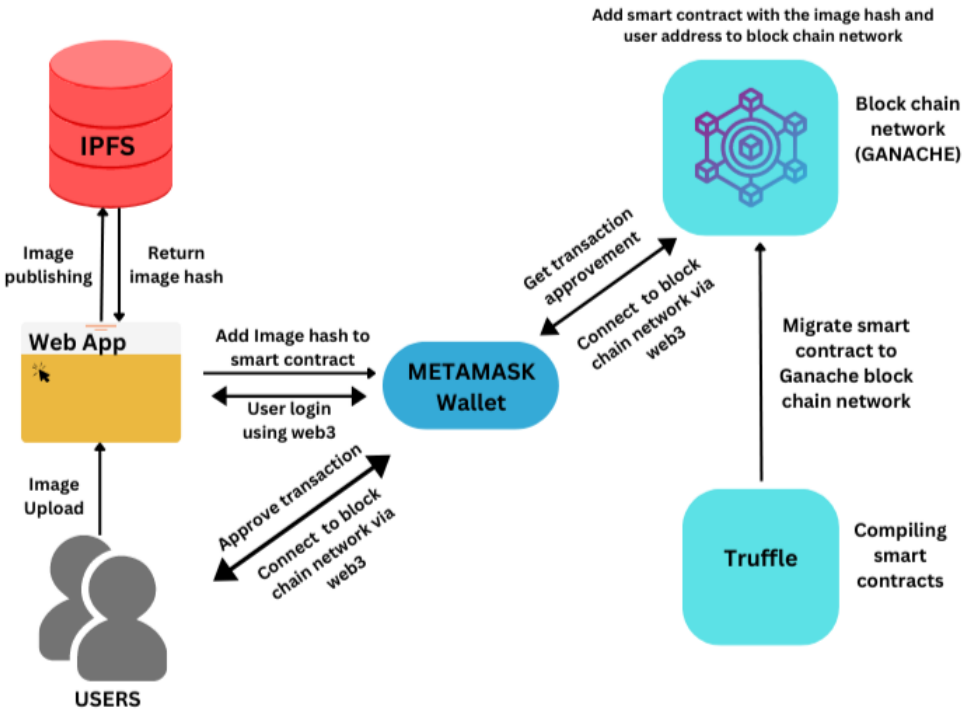

Figure 3.1: System design

3.2 Ganache - Ethereum based block chain network

Ganache is a personal Ethereum blockchain network that allows developers to test and deploy smart contracts and decentralized applications (dApps) in a local, private environment. It is a popular tool in the Ethereum development community and is often used for testing and debugging smart contracts before they are deployed to the live Ethereum network.

Ganache provides a simple and easy-to-use interface for creating a local blockchain network that runs on a developer's machine. The network can be customized to simulate different network conditions and can be used to test a variety of scenarios, such as network congestion, contract failures, and more.

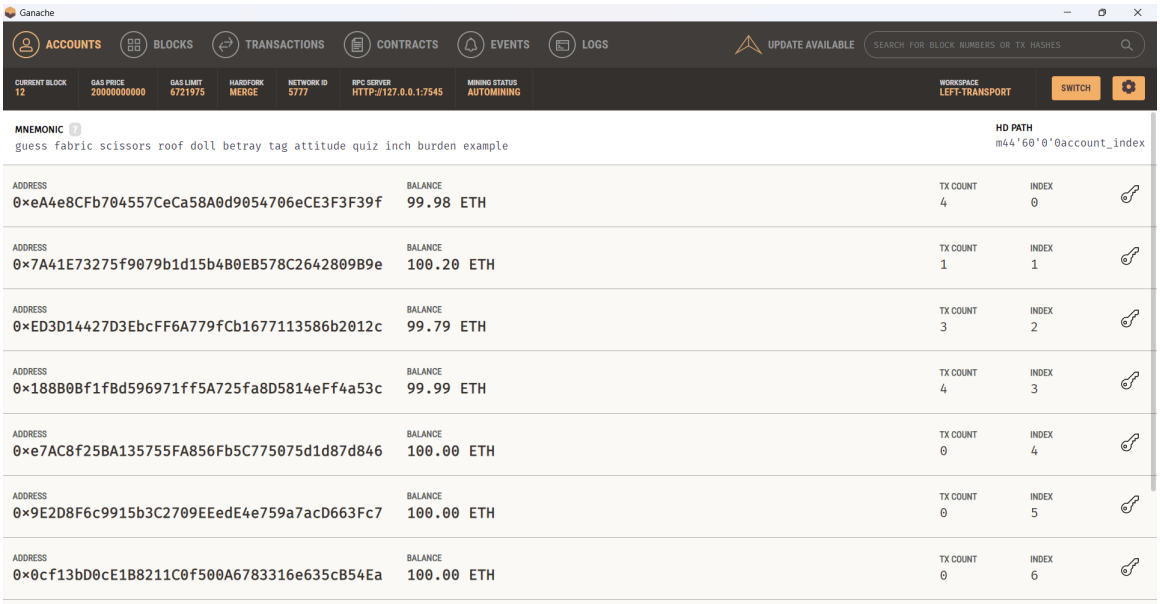

Figure 3.2: Ganache - ethereum based local block chain network

3.2.1 Ganache Ethereum Architecture

Ganache is built on top of Ethereum, which is a decentralized blockchain platform that allows for the creation of smart contracts and dApps. It uses the Ethereum Virtual Machine (EVM) to execute smart contracts and transactions on the blockchain. Ganache consists of three main components: the blockchain network, the accounts, and the user interface.

1. **Blockchain Network** - Ganache creates a virtual blockchain network that runs on a developer's local machine. It simulates a real Ethereum network by creating a series of blocks that contain transaction data. Each block is linked to the previous block, creating

a chain of blocks (hence the name blockchain). Transactions are validated by nodes in the network and added to the blockchain if they are deemed valid.

2. **Accounts** - Ganache also creates a set of accounts that can be used to send and receive Ether (the cryptocurrency used on the Ethereum network) and interact with smart contracts. Each account has a private key associated with it, which is used to sign transactions and authenticate the account. The accounts can be customized to have different balances and permissions, which enables developers to simulate a variety of scenarios.

3. **User Interface** - Finally, Ganache provides a user interface that allows developers to interact with the blockchain network and the accounts. The user interface includes a console that can be used to send commands to the blockchain and monitor transactions, as well as a block explorer that displays information about the blocks in the blockchain.

3.2.2 Internal Components of Ganache

Ganache uses a variety of algorithms and technologies to simulate the Ethereum network and execute smart contracts. Here are some of the key internal components of Ganache:

1. **EthereumJS** - Ganache is built using EthereumJS, which is a collection of JavaScript libraries that implement the Ethereum protocol. These libraries include the Ethereum Virtual Machine (EVM), the Web3.js library for interacting with the blockchain, and the Solidity compiler for compiling smart contracts.

2. **Proof of Authority (PoA) Consensus Algorithm** - Ganache uses a consensus algorithm called Proof of Authority (PoA) to validate transactions and add blocks to the blockchain. In PoA, a set of pre-approved nodes (known as validators) are responsible for creating and validating blocks. This results in a faster and more efficient consensus process than other algorithms like Proof of Work (PoW) or Proof of Stake (PoS).

3. **Gas Limit and Gas Price** - Ganache also uses the concept of gas to regulate the execution of smart contracts and transactions on the blockchain. Gas is a measure of the computational effort required to execute a transaction or smart contract. The gas limit determines the maximum amount of gas that can be used in a block, while the gas

price determines the cost of each unit of gas. This helps prevent spamming of the network and ensures that transactions are executed efficiently.

4. **JSON-RPC API** - Ganache provides a JSON-RPC API that enables developers to interact with the blockchain network and accounts programmatically. This allows developers to automate tasks and integrate Ganache with other tools and platforms.

3.3 Infura IPFS

Infura is a cloud-based infrastructure provider for decentralized applications (dApps) that provides access to various Ethereum and IPFS (InterPlanetary File System) nodes. IPFS, on the other hand, is a peer-to-peer protocol for storing and sharing files in a distributed network. In this answer, I will explain how Infura works with IPFS and how developers can use it to build decentralized applications.

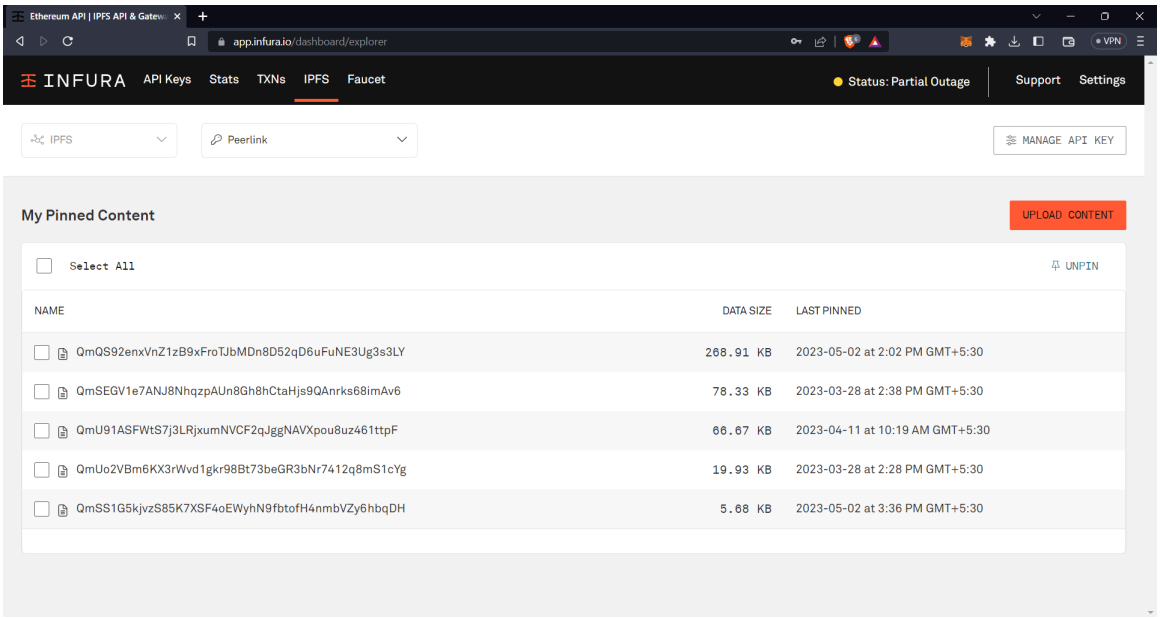

Figure 3.3: Infura IPFS

3.3.1 Infura IPFS architecture

Infura's IPFS architecture is based on a distributed network of nodes that are designed to provide high availability and scalability for storing and sharing files in a decentralized manner. The architecture consists of the following components:

1. **Infura IPFS API** - This is the interface that developers use to interact with Infura's IPFS nodes. It provides a set of APIs that developers can use to upload, retrieve and manage files in the IPFS network.

2. **Infura IPFS Gateway** - This is the endpoint that users can use to access files stored on the IPFS network through Infura. The gateway is designed to provide fast and reliable access to files, regardless of where they are located in the network.

3. **IPFS Nodes** - Infura's IPFS nodes are hosted on a distributed network of servers that are designed to provide high availability and uptime. These nodes are responsible for storing and retrieving files in the IPFS network.

4. **Load Balancer** - Infura's IPFS load balancer distributes incoming requests across multiple IPFS nodes in the network. This ensures that requests are handled quickly and efficiently, and that no single node becomes overloaded.

5. **Monitoring and Management Tools** - Infura provides a set of monitoring and management tools that allow developers to monitor the performance and health of their IPFS nodes, as well as to manage and scale their infrastructure as needed.

   The architecture of Infura's IPFS infrastructure is designed to provide a reliable and scalable platform for developers who want to build decentralized applications that require decentralized storage and content delivery. By hosting IPFS nodes on a distributed network of servers and providing an easy-to-use API, Infura makes it easy for developers to leverage the power of IPFS without having to worry about infrastructure management or maintenance.

3.4 Back-end Architecture and Algorithms of Ethereum Blockchain

3.4.1 Back-end Architecture

1. **Consensus Algorithm**: Ethereum currently uses a consensus algorithm called Proof of Stake (PoS) for block validation and consensus. This algorithm, known as Ethereum 2.0 or Eth2, replaces the previous Proof of Work (PoW) algorithm used in Ethereum 1.0.

PoS relies on validators who lock up a certain amount of Ether (ETH) as a stake in the network. Validators are randomly selected to propose and validate blocks based on their stake, and the probability of selection is proportional to the amount of ETH they have staked.

2. **Merkle** : Ethereum utilizes Merkle trees to efficiently store and verify the integrity of transactions within blocks. A Merkle tree is a binary tree structure where each leaf node represents a transaction, and each non-leaf node is a hash of its child nodes. This allows for efficient verification of transaction data, as any change in a transaction would result in a different Merkle root, indicating tampering or invalidity.

3. **Smart Contracts**: Smart contracts are self-executing contracts with the terms of the agreement directly written into code on the Ethereum blockchain. Ethereum utilizes the Solidity programming language for writing smart contracts. These contracts can define rules and conditions for transactions, automate processes, and facilitate the exchange of assets. The Ethereum Virtual Machine (EVM) executes the bytecode of the smart contracts and ensures their deterministic execution across all network nodes.

4. **Peer-to-Peer Network**: Ethereum employs a peer-to-peer network architecture to distribute and synchronize the blockchain across participating nodes. The network follows the Gossip protocol, where nodes continuously communicate with their peers to exchange block and transaction information. This ensures that all nodes have a consistent view of the blockchain and facilitates the propagation of transactions and blocks throughout the network.

5. **Block Structure**: Each block in the Ethereum blockchain consists of a header and a body. The block header contains metadata such as the block number, timestamp, difficulty, nonce, and the Merkle root of the transactions. The block body includes the transactions and any associated smart contract code. Blocks are linked together using cryptographic hashes, with each block containing the hash of the previous block, forming a chain of blocks.

6. **Gas and Transaction Fees**: Ethereum introduces the concept of ”gas” to regulate the execution of transactions and smart contracts. Gas represents the computational effort required to execute an operation on the Ethereum network. Each operation has a specific

gas cost, and users must pay transaction fees in the form of gas to execute transactions and interact with smart contracts. The gas price is determined by the market and influences the priority and speed of transaction processing.

7. **Blockchain State**: Ethereum maintains a global state, which is a representation of the current state of accounts and smart contracts on the blockchain. The state includes account balances, contract code, contract storage, and other relevant information. The state is updated with each block and is stored in a database known as the ”state trie” to enable efficient querying and retrieval of account and contract data.

These algorithms and the underlying back-end architecture of Ethereum work together to enable the decentralized execution of smart contracts and the secure storage and verification of transactions. They provide the foundation for the functionalities and capabilities of the Ethereum blockchain.

3.4.2 Algorithms used in ethereum Blockchain

Ethereum uses several hashing algorithms for various purposes within its blockchain. Here are the main hashing algorithms employed in Ethereum:

1. **Keccak-256** : Ethereum utilizes the Keccak-256 hashing algorithm, which is a variant of the Keccak cryptographic hash function. Keccak-256 is used in Ethereum’s Proof of Work (PoW) algorithm to mine new blocks. Miners compete to find a nonce value that, when combined with other block data and hashed using Keccak-256, produces a hash value below a certain target difficulty.

2. **SHA-3 (Secure Hash Algorithm 3)** : Ethereum’s Keccak-256 is actually a specific instance of SHA-3. SHA-3 is a family of cryptographic hash functions, and Keccak is the chosen member of this family for Ethereum’s hashing needs. SHA-3 is used for hashing purposes throughout the Ethereum network, including in the creation of block hashes, transaction hashes, and account addresses.

3. **Ethereum’s Patricia Tree (Modified Merkle Patricia Tree)** : Ethereum employs a modified version of the Merkle Patricia Tree data structure to organize and store account and contract information. The Merkle Patricia Tree uses hash functions for efficient and secure data retrieval and verification. Ethereum’s modified version combines the

Patricia Tree structure with the RLP (Recursive Length Prefix) encoding scheme for more compact representation of data.

4. **RIPEMD-160** : Ethereum uses the RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) hashing algorithm for address generation. The algorithm takes the result of a Keccak-256 hash and further processes it to produce a 160-bit hash value. This truncated hash value is used to generate Ethereum account addresses from public keys.

These hashing algorithms are integral to the security, integrity, and functionality of the Ethereum blockchain. They ensure the immutability of data, provide secure message digests for verification, and enable efficient storage and retrieval of information within the network.

3.5 Software Requirements and Specifications

The software requirements for the project include:

1. Solidity
2. JavaScript
3. React
4. Web3.js
5. Ganache
6. Infura IPFS
7. VS code
8. Google chrome

3.5.1 Solidity

Solidity is a programming language that is specifically designed for writing smart contracts on the Ethereum blockchain. Smart contracts are self-executing programs that automatically execute the terms of a contract when certain conditions are met. Solidity is an object-oriented language that is influenced by C++, Python, and JavaScript, and is designed to be easy to learn and use for developers who are familiar with other programming languages. One of the key features of Solidity is its support for inheritance and polymorphism, which makes it easy to reuse code and write more modular and maintainable smart contracts. Solidity also includes a range of built-in data types and operators, as well as support for events, which can be used to track and log changes to the blockchain. Solidity also includes a number of security features that are designed to prevent common vulnerabilities, such as integer overflows and reentrancy attacks. The language includes a range of safety checks and constraints that help to ensure that smart contracts are secure and cannot be exploited by malicious actors. Current version of solidity is v0.8.20.

3.5.2 Javascript

JavaScript is a popular programming language that is used to create interactive and dynamic web pages. It was initially developed in the mid-1990s as a scripting language for web browsers, but has since grown to become one of the most widely used programming languages in the world. JavaScript is often used in conjunction with HTML and CSS to create dynamic user interfaces, as well as with server-side technologies like Node.js to create full-stack web applications. One of the key features of JavaScript is its ability to run code on the client side, which allows web pages to be updated dynamically without the need to reload the entire page. JavaScript is also used to create animations, handle user input, and manipulate the Document Object Model (DOM), which represents the structure of an HTML document. JavaScript is an interpreted language, which means that it is executed by the web browser rather than compiled to machine code. This allows for a more flexible development process, as developers can quickly test and iterate on their code without the need to compile and deploy their application after each change. JavaScript is also an extremely versatile language, and can be used for a wide range of applications beyond web development. It is used to build mobile applications, desktop applications, and even games. In recent years, JavaScript has also been used to build server-side applications using Node.js, which allows developers to use JavaScript on both the front-end and back-end of their applications.

3.5.3 React

React is an open-source JavaScript library that is used for building user interfaces. It was developed by Facebook and is now maintained by a large community of developers. React is often used in conjunction with other front-end technologies like HTML, CSS, and JavaScript, and is designed to be used in large and complex applications. One of the key features of React is its ability to create reusable UI components. Developers can use React to create a library of components, which can then be reused across multiple applications. This makes it easier to build and maintain large applications, as developers can focus on building small, reusable components rather than writing code from scratch for each new application. React also uses a virtual DOM (Document Object Model) to manage updates to the user interface. When a change is made to a component, React updates the virtual DOM rather than updating the actual DOM. This allows React to quickly and efficiently update the user interface without the need to

reload the entire page. React is also known for its declarative programming model. Developers describe what they want the user interface to look like, and React takes care of the underlying implementation details. This makes it easier to write and maintain complex applications, as developers can focus on the high-level logic of their application rather than getting bogged down in implementation details. Overall, React is a powerful and versatile front-end library that is widely used in the development of modern web applications. Its focus on reusable components, virtual DOM, and declarative programming model make it an ideal choice for building large and complex applications, while its open-source nature and large community of developers ensure that it will continue to be a key technology in the world of web development.

3.5.4 Web3.js

Web3.js is a popular JavaScript library that serves as a crucial tool for developers working with decentralized applications (dApps) on the Ethereum blockchain. It provides a comprehensive set of APIs, allowing developers to interact with the Ethereum network, smart contracts, and decentralized technologies. One of the primary functionalities of Web3.js is its ability to establish a connection between the user's web browser and the Ethereum blockchain. Through this connection, developers can access the Ethereum network, read and write data, and execute transactions. Web3.js simplifies the process of interacting with smart contracts deployed on Ethereum. It abstracts the complexities of working with low-level blockchain protocols, enabling developers to interact with smart contracts using simple JavaScript function calls. With Web3.js, developers can deploy and instantiate smart contracts, call their functions, and handle events emitted by the contracts.

3.5.5 Ganache

Ganache is a personal blockchain for Ethereum development, which is used to test and develop smart contracts and decentralized applications (DApps). It is developed by Truffle Suite, an organization that provides a suite of tools for Ethereum development.Ganache provides a local blockchain environment that mimics the Ethereum mainnet, but with a few key differences. Ganache allows developers to quickly and easily mine new blocks, which can help speed up the development process. It also provides a graphical user interface that allows developers to view and interact with the blockchain, as well as tools for debugging and testing smart contracts. One

of the key benefits of using Ganache is that it allows developers to test and debug their smart contracts in a safe and controlled environment. Since Ganache is a local blockchain, there is no risk of losing real Ether or other tokens during development. This can help developers catch bugs and other issues early in the development process, which can save time and money in the long run.

Ganache is also highly configurable, allowing developers to customize various aspects of the blockchain environment to suit their specific needs. For example, developers can adjust the block time, gas limit, and other parameters to simulate different network conditions and test their applications under different scenarios.Ganache is a personal blockchain for Ethereum development, which is used to test and develop smart contracts and decentralized applications (DApps). It is developed by Truffle Suite, an organization that provides a suite of tools for Ethereum development. Ganache provides a local blockchain environment that mimics the Ethereum mainnet, but with a few key differences. For example, Ganache allows developers to quickly and easily mine new blocks, which can help speed up the development process. It also provides a graphical user interface that allows developers to view and interact with the blockchain, as well as tools for debugging and testing smart contracts.

One of the key benefits of using Ganache is that it allows developers to test and debug their smart contracts in a safe and controlled environment. Since Ganache is a local blockchain, there is no risk of losing real Ether or other tokens during development. This can help developers catch bugs and other issues early in the development process, which can save time and money in the long run.Ganache is also highly configurable, allowing developers to customize various aspects of the blockchain environment to suit their specific needs. For example, developers can adjust the block time, gas limit, and other parameters to simulate different network conditions and test their applications under different scenarios.

3.5.6 Infura IPFS

Infura IPFS is a service provided by Infura, a company that provides infrastructure and tools for building decentralized applications (DApps) on the Ethereum blockchain and the InterPlanetary File System (IPFS). IPFS is a protocol and network designed to create a distributed and decentralized system for storing and sharing files and data.

Infura IPFS allows developers to easily integrate IPFS into their applications without having to run their own IPFS nodes. By using Infura IPFS, developers can take advantage of the

benefits of IPFS, such as increased security, redundancy, and censorship resistance, without having to worry about managing and maintaining their own nodes.

Infura IPFS provides a simple API that developers can use to interact with IPFS, including features such as adding and retrieving files, managing content addresses, and accessing the IPFS pubsub system. Infura IPFS also provides tools for monitoring and analyzing IPFS usage and performance, allowing developers to optimize their applications for the best possible user experience.One of the key benefits of using Infura IPFS is its ease of use and accessibility. By providing a simple and reliable way to access the IPFS network, Infura IPFS makes it easier for developers to build DApps that take advantage of the benefits of decentralized storage and sharing. This can help to promote the adoption and use of IPFS, and ultimately contribute to the development of a more decentralized and resilient internet.

3.5.7 VS code

VSCode, or Visual Studio Code, is a free and open-source code editor developed by Microsoft. It is designed for use in a wide range of programming languages, and includes a number of features that make it a popular choice for developers. One of the key features of VSCode is its built-in support for Git, a version control system commonly used in software development. This allows developers to easily track changes to their code and collaborate with others on a project. VSCode also includes a number of debugging tools, which can help developers identify and fix issues in their code.

Another popular feature of VSCode is its extensions marketplace, which includes a wide range of plugins and add-ons that can be used to customize the editor for specific development tasks. This includes support for a range of programming languages and frameworks, as well as tools for testing, debugging, and code formatting. VSCode also includes a number of productivity features, such as code completion and suggestions, a built-in terminal, and support for multiple windows and tabs. These features help developers to work more efficiently and stay focused on their coding tasks.

3.5.8 Google Chrome

Google Chrome is a popular web browser developed by Google. It was first released in 2008, and has since become one of the most widely used web browsers, with a market share of over

60% as of 2021. One of the key features of Google Chrome is its speed and performance. It is designed to load web pages quickly, and includes a number of optimizations that help to reduce load times and improve overall browsing speed. Chrome also includes a built-in task manager, which allows users to see which tabs and extensions are using the most resources, and to close them if necessary.

Another popular feature of Google Chrome is its support for extensions. Chrome's extension marketplace includes a wide range of plugins and add-ons that can be used to customize the browser and add new functionality. This includes tools for ad blocking, password management, and productivity enhancements. Chrome also includes a number of security features, such as built-in phishing and malware protection, sandboxing of web pages to prevent malicious code from affecting the system, and automatic updates to ensure that users are always running the latest version of the browser.

3.5.9 Hardware and experimental environment

The hardware used for this experiment includes Windows 11 Home 64-bit OS, x64-based processor, AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx 2.10 GHz, 1,200 Mhz, 4 Core(s), 8 Logical Processor(s), 8 GB RAM.

The experimental environment was prepared by using Solidity and Javascript programming languages on VS Code. The local block chain network used is Ganache that runs on Ethereum block chain infrastructure.

Chapter 4

RESULT AND DISCUSSION

A decentralized social media application where users can post images is created. The users can sent incentives to other users in order to promote user activities on the social media. This is done by using ethereum cryptocurrency. The cryptocurrency is send from cryptowallet of one user to the wallet of another user through the ethereum network. The users can only be a participant if and only if they have a web3 based wallet. This helps the user to login to the system and engage in social media activities like posting their content in the form of images along with texts and can also send ethereum cryptocurrency to support users contents.

Decentralized social media has emerged as an exciting new area of research and development in the field of distributed systems and blockchain technology. As traditional social media platforms continue to face criticism over issues such as data privacy, censorship, and the concentration of power in the hands of a few large companies, decentralized social media networks offer a promising alternative that could provide greater control and ownership over user data, enhanced privacy and security, and improved resilience against censorship and interference. However, there are still significant challenges to be addressed in the development of decentralized social media, such as the scalability and efficiency of blockchain and P2P networks, the usability and accessibility of decentralized applications, and the need to establish trust and reputation systems that can ensure the quality and reliability of user-generated content. In this project report, we will explore these challenges in more detail, discuss the results of our research and experimentation with decentralized social media networks, and propose strategies and recommendations for further development and adoption of these innovative technologies.

4.1 Testing and it's types used

The main task following software development is to determine whether the experimental results and the actual results agree. Testing is the process in question. It is employed to ensure that the created system is free from errors.Testing's primary purpose is to find errors and missing operations by running the software. Additionally, it makes sure that the developer satisfies all of the project's goals. Testing's objective is to determine is to identify defects in the developed software as well as ways to increase its correctness, usability, and efficiency. It seeks to gauge a software program's performance, functionality, and specification. The developed programme is put through tests, and the outcomes are compared to the required documentation. Debugging is carried out when there are too many faults that have happened. After debugging, the software is once more tested to make sure there are no errors. Unit testing, integration testing, and system testing are the main testing methodologies used in this project.

- In unit testing, tested to each distinct piece of software. It ensures that the software's many components all function as intended.
- In integration testing, the integrated distinct components are examined to see whether or not the intended purpose was accomplished. It helps us find any problems that might appear after the units are combined.
- The entire piece of software is evaluated during system testing to make sure it meets all the requirements.

4.1.1 Unit testing using chai.js

In this project, unit testing is an important aspect of validation testing, aimed at identifying defects in individual sections of the project. Unit testing is used to evaluate the functionality and performance of each system unit or component in isolation. This testing helps developers to identify and resolve issues early on, thereby minimizing the risk of encountering problems during deployment or integration.

Chai testing is primarily used for unit testing and integration testing of JavaScript applications. It is a testing framework that provides a set of assertion styles and utility functions for writing tests. Chai can be used in conjunction with a test runner such as Mocha, Jasmine,

or Jest to test the behavior of individual functions or modules in an application, as well as to test the integration between different components of the application.

Chai provides a range of assertion styles, including assert, expect, and should, which can be used to verify the behavior of a function or module under different conditions. Chai also provides utility functions for working with common data types such as arrays, objects, and strings, as well as for mocking and stubbing functions. Areas of testing includes :

1. Checking image hash and image description based on an event or activity.
2. Tracking the author balance before purchase.
3. Checking whether the author received funds.
4. Tipping images that does not exist so as to verify the edge case or unusual activity.

4.2 Output Screens and Results

1. Login on web3

   Login page on web3 using Metamask wallet. Users can use their credentials associated with their metamask wallet to login to the system.

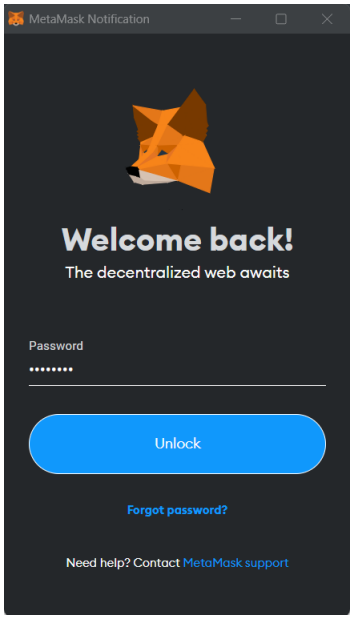

Figure 4.1: Login

2. User account selection

   Selecting a particular user's account for posting content.

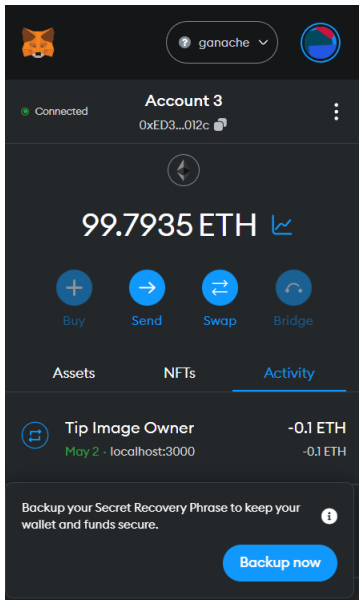

Figure 4.2: Users account

3. Live feed

   The Live feed where all the posted contents are showed to the user. This is the place where the user interactions takes place.

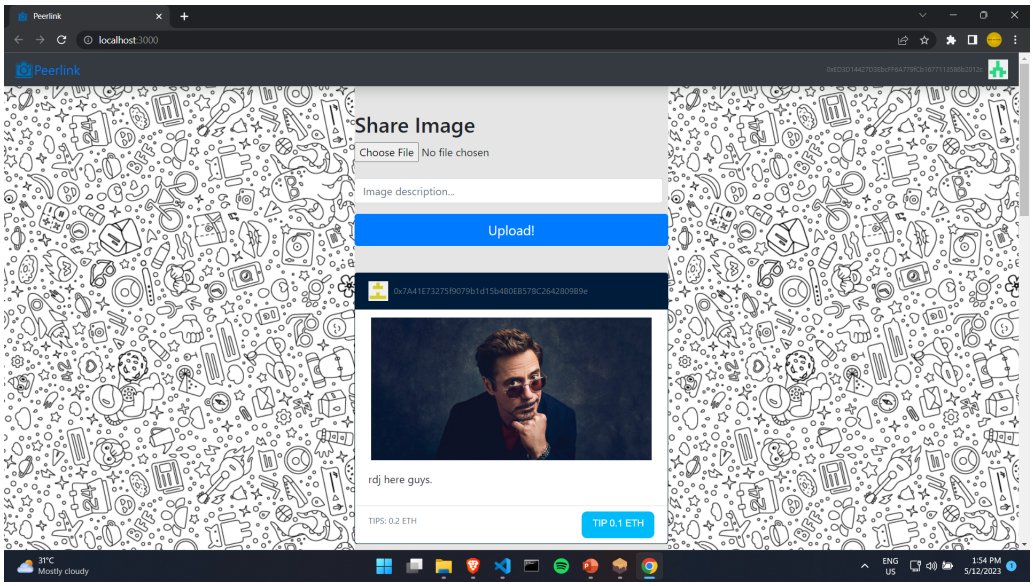

Figure 4.3: Live feed

4. Tipping the post

   The users sending tip to a particular post to support the content. The tips are send via wallet from one user to the other in the form of ethereum cryptocurrency.

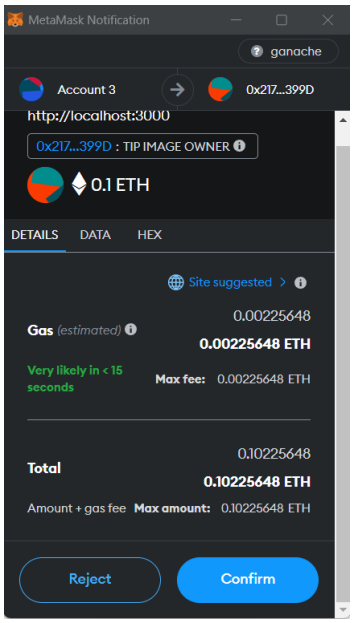

Figure 4.4: Tipping the post

5. Ganache network

   The ethereum based local network used to provide the block chain infrastructure for the social media platform.

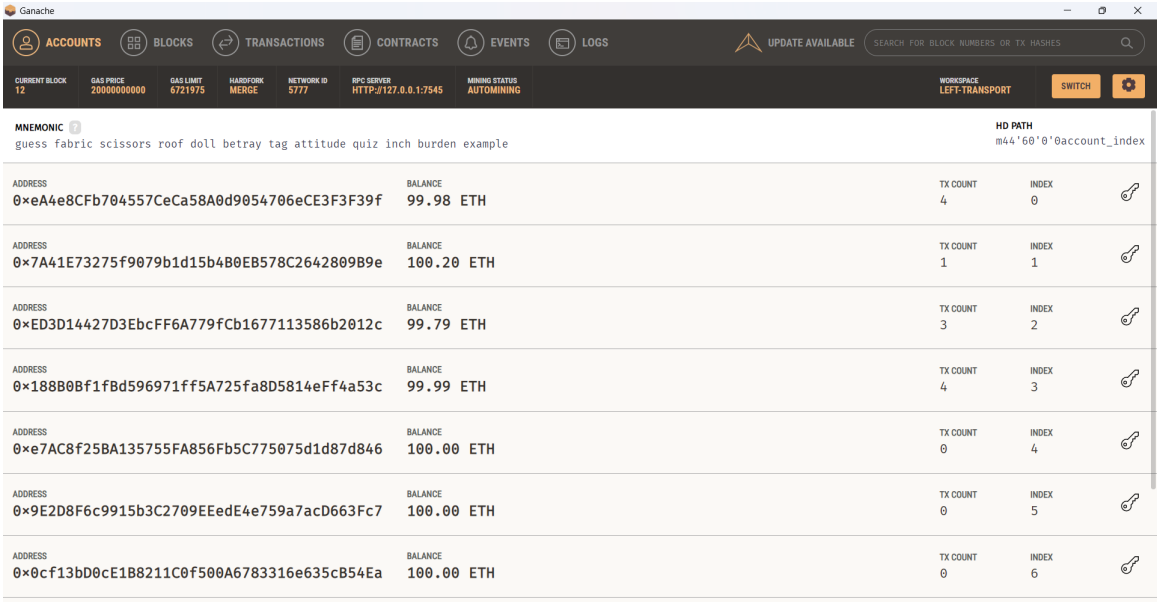

Figure 4.5: block chain network

6. Infura IPFS

   Infura IPFS is the InterPlanetary File System used to store the images over a distributed network.

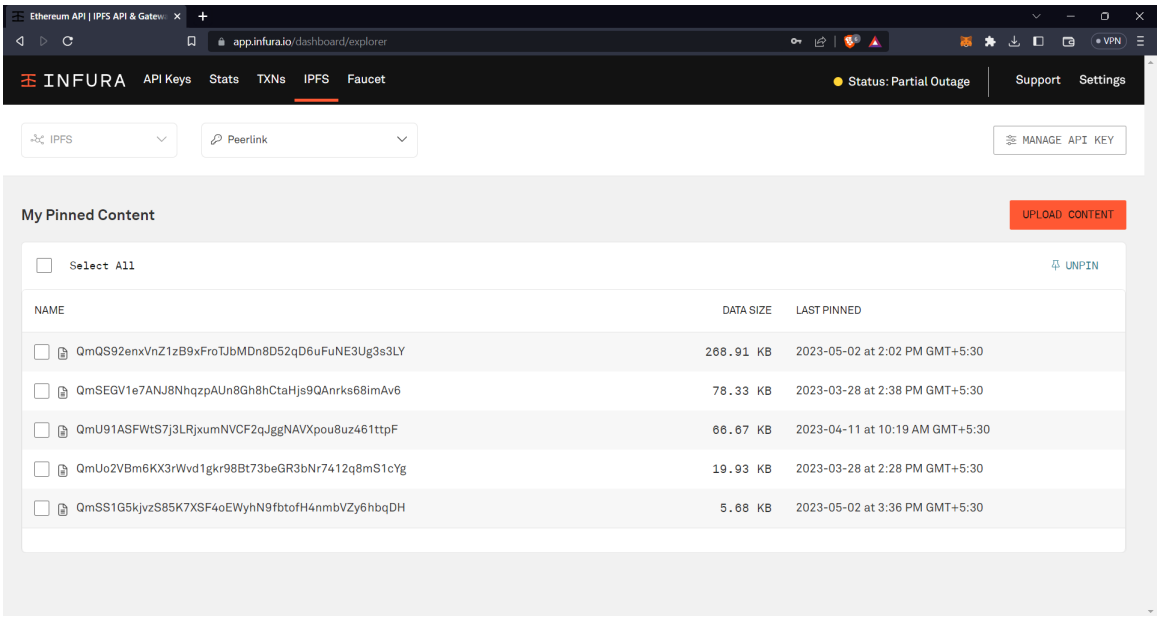

Figure 4.6: Infura IPFS

Chapter 5

CONCLUSION

Decentralized social media refers to social networking platforms that operate on a peer-to-peer (P2P) network, without a centralized authority controlling the data. The methodology behind decentralized social media involves the use of blockchain technology and distributed ledger technology to enable users to have full control over their data and interactions on the platform. The data is encrypted, and transactions are recorded on a public ledger, which ensures transparency and security. Instead of relying on a central authority to store and manage user data, decentralized social media uses a network of nodes, where each node holds a copy of the data. This approach ensures that user data is not owned or controlled by a single entity, and the platform is more resistant to censorship and hacking attempts. Additionally, decentralized social media allows for a more democratic and open system, where users have equal say in the decision-making process, and there is no bias towards any particular group or individual.

In conclusion, decentralized social media represents a promising new direction for the future of social media and online communication. By leveraging the power of decentralized technology, such as blockchain and P2P networks, decentralized social media networks offer a range of benefits over traditional centralized social media platforms, including enhanced privacy and security, increased control and ownership over user data, and improved resilience against censorship and interference. However, there are still significant challenges to be addressed in the development and adoption of decentralized social media. These challenges include the scalability and efficiency of blockchain and P2P networks, the usability and accessibility of decentralized applications, and the need to establish trust and reputation systems that can ensure the quality and reliability of user-generated content.

5.1 Future Enhancement

The system is designed in such a way that addition of new modules can be done without much difficulty. In order to make the system as versatile and user-friendly as possible, the advanced characteristics of this technology were taken into consideration. Some of the features that can be added in future are:

1. User searching: Searching users on the platform so as to connect with them and share posts to the users that we are connected with.

2. Peer requests: User connections can be established with the help of peer requests to improve groups and clusters of like minded people.

3. Chat app or messenger: To add a messenger service for the users to make better communication with other users and connections.

4. Live broadcast : Users can go live video sharing and can get support for their live video by ethereum transactions from the live viewers.

REFERENCES

[1] SocialChain: Decoupling Social Data and Applications to Return Your Data Ownership. Ting Cai; Zicong Hong; Shuo Liu; Wuhui Chen; Zibin Zheng; Yang Yu; IEEE Transactions on Services Computing. Year: 2023 — Volume: 16, Issue: 1 — Journal Article — Publisher: IEEE DOI: 10.1109/TSC.2021.3128959

[2] TAPESTRY: A De-Centralized Service for Trusted Interaction Online. Yifan Yang; Daniel Cooper; John Collomosse; Constantin Cătălin Drăgan; Mark Manulis; Jamie Steane; Arthi Manohar; Jo Briggs; Helen Jones; Wendy Moncur; IEEE Transactions on Services Computing. Year: 2022 — Volume: 15, Issue: 3 — Journal Article — Publisher: IEEE — DOI: 10.1109/TSC.2020.2993081

[3] Decentralized On-Chain Data Access via Smart Contracts in Ethereum Blockchain. Mohd Sameen Chishti; Farhan Sufyan; Amit Banerjee; IEEE Transactions on Network and Service Management. Year: 2022 — Volume: 19, Issue: 1 — Journal Article — Publisher: IEEE — — DOI: 10.1109/TNSM.2021.3120912

[4] Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data. Ammar Ayman Battah; Mohammad Moussa Madine; Hamad Alzaabi; Ibrar Yaqoob; Khaled Salah; Raja Jayaraman; IEEE Access. Year: 2020 — Volume: 8 — Journal Article — Publisher: IEEE — DOI: 10.1109/ACCESS.2020.3034260

[5] IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks. Erik Daniel; Florian Tschorsch; IEEE Communications Surveys Tutorials. Year: 2022 — Volume: 24, Issue: 1 — Journal Article — Publisher: IEEE — DOI: 10.1109/COMST.2022.3143147

[6] Systematic Mapping of Testing Smart Contracts for Blockchain Applications. Nicholas Paul Imperius; Ayman Diyab Alahmar: IEEE Access. Year: 2022 — Volume: 10 — Journal Article — Publisher: IEEE — DOI: 10.1109/ACCESS.2022.3216874

[7] Ethereum Account Classification Based on Graph Convolutional Network. Tao Huang; Dan Lin; Jiajing Wu; IEEE Transactions on Circuits and Systems II: Express Briefs. Year: 2022 — Volume: 69, Issue: 5 — Journal Article — Publisher: IEEE — DOI: 10.1109/TCSII.2022.3161112

[8] Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network. Ruiguo Yu; Jianrong Wang; Tianyi Xu; Jie Gao; Yongli An; Gong Zhang; Mei Yu IEEE Access. Year: 2017 — Volume: 5 — Journal Article — Publisher: IEEE — DOI: 10.1109/ACCESS.2017.2767285

APPENDIX

Screenshots

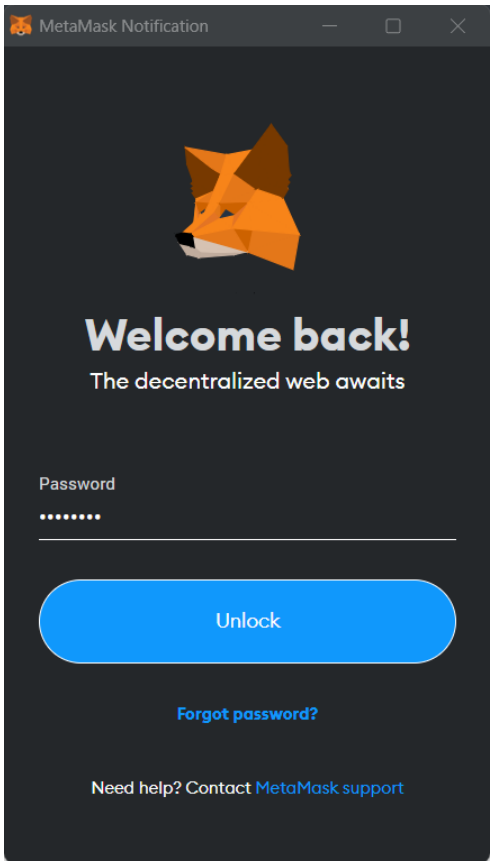

Figure A.1: Login using web3

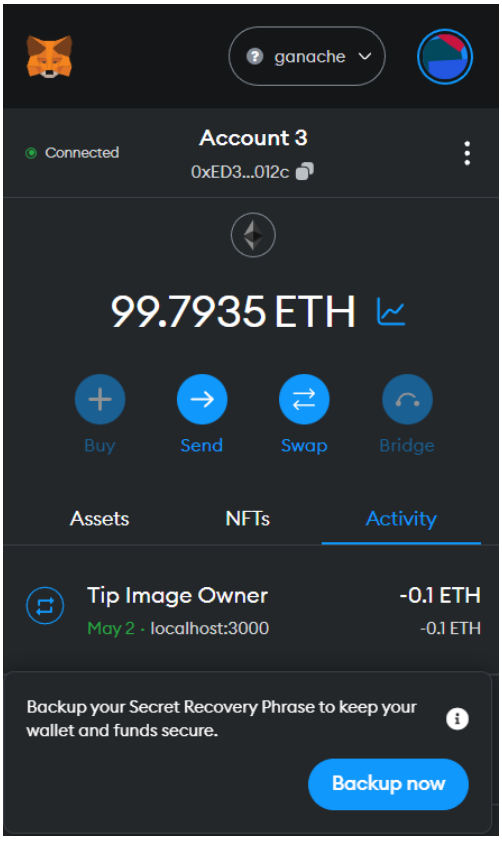

Figure A.2: User's account selection

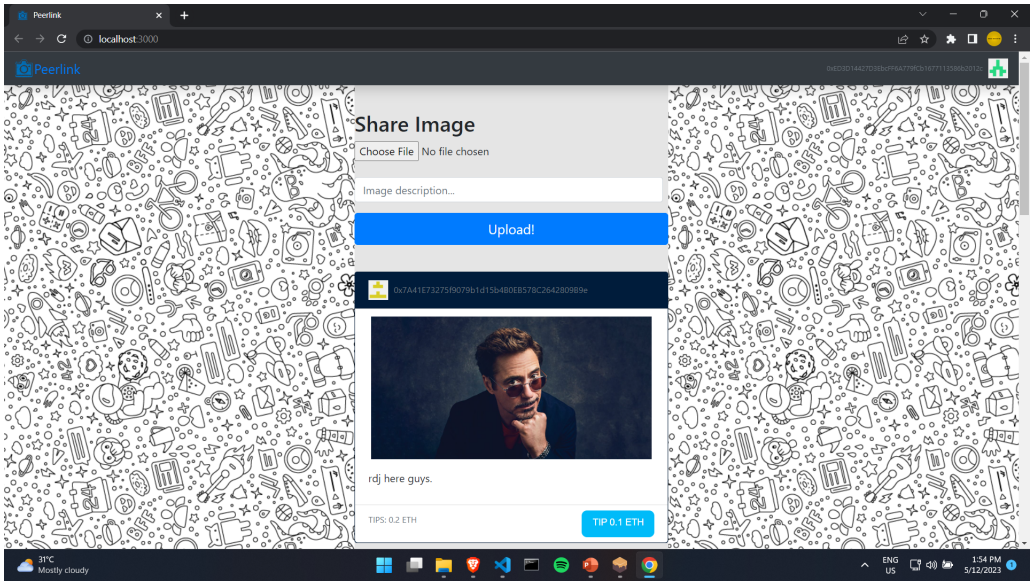

Figure A.3: Live feed

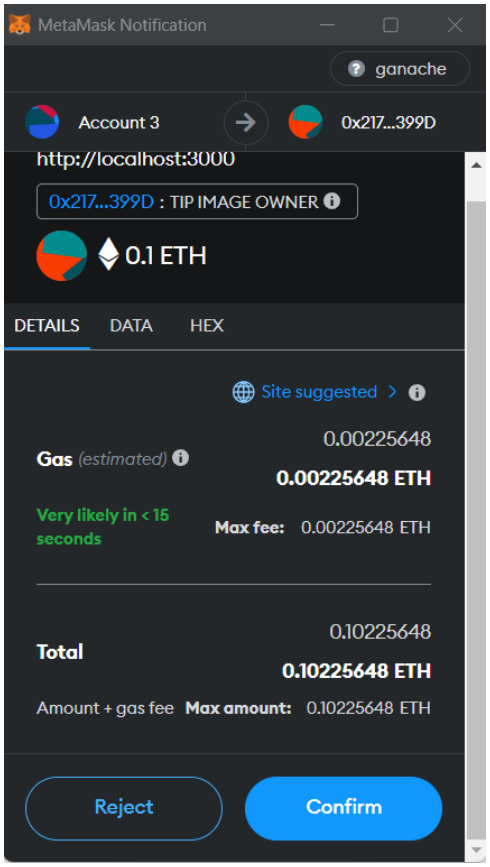

Figure A.4: Post tipping

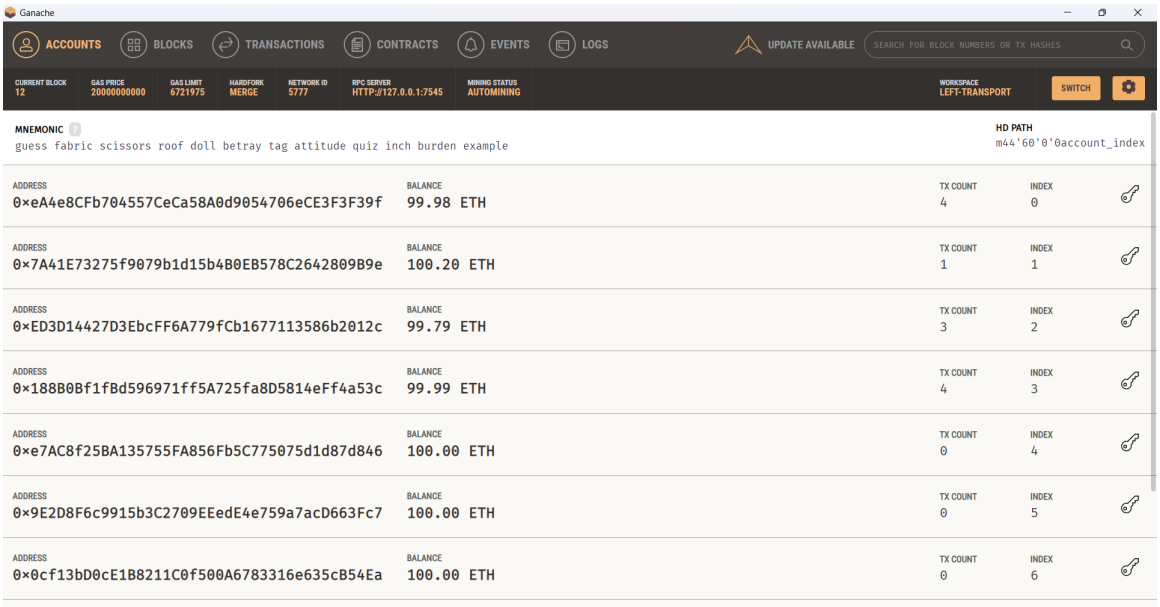

Figure A.5: Ganache blockchain network

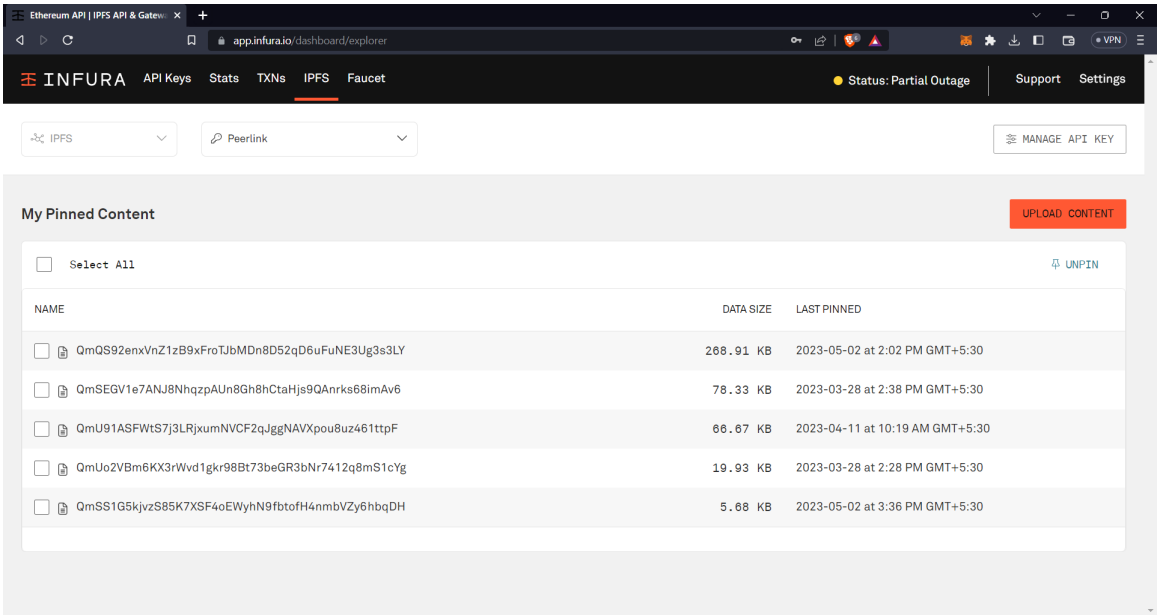

Figure A.6: Infura IPFS