# Enhancing Privacy, Censorship Resistance, and User Engagement in a Blockchain-Based Social Network

Myo Thiha[1][a], Halil Yetgin[1][b], Luca Piras[1][c] and Mohammed Ghazi Al-Obeidallah[2][d]

[1]*Department of Computer Science, Middlesex University, The Burroughs, London, NW4 4BT, U.K.*
[2]*Department of CS and IT, Abu Dhabi University, Abu Dhabi, U.A.E.*

Keywords:     Blockchain, Decentralised Social Network, Privacy, Censorship, User Engagement.

Abstract:     In the contemporary digital era, online social networks have become integral to global communication, facilitating connectivity and information dissemination. Millions of people use centralised social media platforms today, which raises concerns about user control, privacy, and censorship. These platforms profit from user data and content, as the single authority of these platforms has complete control over user data. Although peer-to-peer decentralised online social networks were developed to address the weaknesses in centralised platforms, they still have significant limitations in terms of securing privacy, and handling censorship resistance issues. In this work, we propose a novel decentralised online social network leveraging blockchain technology to address these pressing issues in centralised and peer-to-peer online social networks. The proposed system prioritizes user control by decentralizing data storage and network governance, thereby reducing the issues associated with centralized control. By employing blockchain technology, individuals maintain ownership of their data and gain greater control, thereby enhancing user privacy protection. Additionally, the cryptographic security and immutable ledger of blockchain technology protect freedom of expression and information exchange by resisting censorship. Moreover, with the integration of incentivization mechanisms, users are incentivized to contribute to the network's growth and sustainability, as well as promoting engaging content and encouraging ownership among users. The evaluation results show that our blockchain-based decentralised online social network (DOSN) accomplishes the aim and objectives for preserving privacy, censorship resistance and enhancing user engagement in online social network with the use of blockchain technology.

## 1    INTRODUCTION

Nowadays, social networks are the most common platforms on which people share their personal information. There are over 4.5 billion Internet users worldwide, and over 4 billion people utilise social networks. In the upcoming years, social networks will continue to grow and bring in more users. More significantly, they have impacted how people interact with one another and communicate. However, this impact is not always positive (Mohammed, 2022). The business strategy of these platforms is based on providing users services for free in an attempt to attract more users. In return, users' behaviour and everything they share on the platform are used by the

owners in order to make profit through selling advertising (Guidi, 2021). Therefore, the increasing dominance of major industry players such as Meta and Twitter has led to the suppression of opposing viewpoints and discussions about user privacy due to the vulnerability of personal information to data breaches and misuse, as well as the centralisation of control over user interactions and content (Yerby et al., 2019). Furthermore, the centralization of power in a small number of organisations raises concerns about responsibility and the possibility of improper influence over public opinion. One of the primary causes of these issues is because of the dependence on the client-server architecture with proprietary and centralised servers (Tran et al., 2016).

In an attempt to address this issue, researchers have suggested alternative platforms. Over the past ten years, various decentralised online social networks have been developed. These networks are built on various peer-to-peer system architectures. How-

[a] https://orcid.org/0009-0002-3684-2093
[b] https://orcid.org/0000-0003-0994-5839
[c] https://orcid.org/0000-0002-7530-4119
[d] https://orcid.org/0000-0003-4976-1380

ever, due to the limitations and lack of success of peer-to-peer decentralisation techniques, blockchain technology has been considered as a decentralised alternative in a number of research areas to address challenges arising from centralised and peer-to-peer decentralised social networks.

Blockchain is a distributed, decentralised ledger that operates without a central authority to facilitate secure and transparent transactions. Although its main application has been in the field of cryptocurrency, its prospective benefits are not limited to this sector. The application of blockchain technology to social network has been investigated recently in an effort to solve the problems with current centralised platforms. Decentralised social networks provide an alternative to traditional social network by promoting trust and transparency in online interactions, ensuring privacy and communication without restriction or censorship, and giving users more control over their personal information (Zhan et al., 2022).

The principal aim of this paper is to conceptualise, design, and implement a decentralised online social network application by integrating blockchain technology. The integration aims to enhance privacy, provide users with greater control over their personal data, and resistance against censorship, as well as promote an engaging and democratic online community. This will alleviate a great deal of relief from many data-related issues of traditional centralised online social networks. Moreover, the proposed application aims to grow user communities and engaging contents by incentivising them monetarily for their contributions in sharing valuable content. This results in highly personalised feeds and more engaging content. By means of this aim, it will significantly contribute to the decentralisation of social networks, as well as user-centred online communication platforms.

In line with the aim outlined above, the following research questions (RQ) are individuated:

RQ1. *How does the blockchain architecture address potential privacy concerns in centralised OSNs and peer-to-peer decentralised online social networks (DOSNs)?*

RQ2. *How does the decentralised nature of blockchain-based DOSN provide the censorship resistance?*

RQ3. *How can the blockchain-based DOSN enhance the contribution of engaging content than centralised OSNs and peer-to-peer DOSNs.*

To answer the research questions, we performed different phases: (i) *decentralisation with blockchain technology*. Initial research steps with literature review for privacy, censorship-resistance and user engagement in decentralised online social networks and how blockchain combined with other decentralised technology could offer a more efficient solution. (ii) *Requirements Analysis and Design*. Based on the information collected from the literature review, functional and non-functional requirements are analysed and the design of the system architecture is created. (iii) *Implementation*. Based on the requirements and design, the actual implementation of blockchain-based DOSN application is conducted. (iv) *Evaluation*. The viability and effectiveness of the implemented blockchain-based DOSN application is evaluated via observation against the research questions.

The rest of the paper is organised as follows: Section 2 describes the literature review of background and initial research steps (relating to point (i) above). Section 3 describes the requirement analysis and design for the application as well as the actual implementation process by using blockchian and related decentralisation technology (point (ii) and (iii) above). Section 4 describes the evaluation via observation against the research questions, and related works. Section 5 concludes the paper.

## 2 BACKGROUND AND LITERATURE REVIEWS

In this section, we will discuss the relevant literature which other researchers have done in the field of decentralised online social networks and explain the initial research steps on how blockchain technology could offer a more efficient decentralised solution. First, we will discuss the overview of the history of online social networks, along with the evolution of peer-to-peer decentralised online social networks using specific examples. Second, we will examine the pertinent studies that have been conducted on the subjects of preserving user privacy, and resistance to censorship in decentralised online social networks with various architectures, outlining the limitations and challenges of each. Next, we will depict the evolution of blockchain-based decentralised online social networks. Finally, we will explain the core features of our blockchain-based decentralised DOSN that, in comparison to previous peer-to-peer decentralised online social networks, is more effective at addressing the issues of user privacy, and censorship resistance arising from centralised OSNs, as well as enhancing user engagement.

## 2.1 History of Online Social Networks and Their Problems

A new era of networked communication was ushered in 1991 when Tim Berners-Lee successfully integrated hypertext applications with the Internet, which led to the development of the World Wide Web. In addition to revolutionizing the development of online communities, this technology provided offline groups with support. The launch of websites including SixDegrees.com, Classmates.com, and GeoCities in the middle of the 1990 indicated the beginning of innovative social networking sites. Online social networks, or OSNs, have become extremely popular since the mid-2010s. Large corporations such as Meta and X have emerged, allowing users to share text messages, digital images, and videos with their friends. Meta is a well-known online social network that appeals to users of all ages, and currently, it has over 2.9 billion members. OSNs have become an essential component of many users' life (Shilina, 2023).

However, it is also discovered that user privacy in those OSNs is readily compromised. While most OSNs allow users to adjust privacy settings to prevent other users from seeing their data, there are no practical technological ways to restrict OSN providers' access or prevent them from sharing user data with third parties. Massive amounts of personal data, such as demographics, interests, and online activity, are gathered by dominant social networks from their users; this data is frequently breached by attackers. In 2020, almost 25% of records that were exposed came from database breaches on social networking sites such as Facebook and Twitter (Shilina, 2023). But since then, the problems have become worse; in 2022, the percentage increased to almost 41%, showing a substantial increase in data breaches and social networking platform theft. Censorship is another issue with the centralised OSNs that exist currently. Facebook, for instance, prohibits certain content that does not adhere to the platform's policies (Shilina, 2023). Nevertheless, the fact that a single authority determines these rules compromises users' freedom of speech.

## 2.2 Evolution of Peer-to-Peer Decentralised Online Social Networks

In order to accommodate these issues in centralised OSNs, DOSNs have been explored. A DOSN is typically implemented by a peer-to-peer (P2P) manner, whereby independent users collaborate together to form a platform architecture with the goal of empowering them to have greater control over the information they store and can access. According to the survey of (Schwittmann et al., 2013), they have distinguished three main categories of P2P architecture in DOSNs for preserving privacy, user control and censorship resistance.

**Federated Architecture**, which is made up of separate servers, is the most well-known P2P architecture for DOSN. With federated networks, users can choose which server to register with to gain access to the full network, which is dispersed among numerous servers. It allows content sharing with particular contacts or contact groups through a fine-grained access control system. Secure sockets layer/transport layer security (SSL/TLS)-like security is provided via the server-to-server protocol, which regulates the transfer of encrypted and signed messages. By facilitating decentralised cooperation among separate groups, this architecture preserves user autonomy and privacy while giving users control over their data. Furthermore, as the network is federated and lacks a single point of control, it is impossible for a single body to censor or manage the entire network, offering censorship resistance.

**End-to-End Client-Side Data Encryption Architecture**, which implements encryption on the end hosts to protect data content privacy from curious or hostile service providers. In a centralised OSN, the server is responsible for enforcing access control lists. When using user-to-user encryption, access control via cryptography falls under the responsibility of the end host. Persona, Vegas, and SoNet are examples of such types of social networks. To begin with, the Persona network employs an encryption approach called attribute- based encryption (ABE), which permits the sharing of the symmetric content key with specified groups or sets of groups. Compared to conventional hybrid techniques, which encrypt the group key for every recipient, this is more efficient. Persona conceals metadata from the general public as well, although it still permits server providers to view social network graphs (Baden et al., 2009a). Next, to make the process more convenient for users, the Vegas social network leverages QR codes for key exchange (Paul et al., 2014). Additionally, it describes a coupling technique that enables a user to ensure the accuracy of two of his trusted friends' identities by launching friendship authentication between them. Vegas hides the social graph with a rigorous approach. It employs public servers' storage with random names of file and concealed the structures of directory, and it does not let users

view their friends' contact lists. By doing this, the social graph is successfully concealed from friends and server providers. Lastly, SoNet uses aliasing for hidding the social graph from server providers. Users only communicate to their storage provider, which also serves as a proxy for accessing the storage of other users. In order to prevent the storage server from resolving aliases of other storage services to cleartext usernames, both parties generate random IDs when establishing acquaintances (Schwittmann et al., 2013).

**Distributed Hash Table Architecture**, which is utilised to search data in a P2P system with logarithmic routing complexity. By distributed user data among a network of peers, each of whom is in charge of a portion of the data, this architecture is used in PeerSoN, LifeSocial, and Cachet decentralised social networks to assure privacy and censorship resistance (Schwittmann et al., 2013). In a peer-to-peer system with logarithmic routing complexity, PeerSoN employs a distributed hash table (DHT) to locate data. Every participating peer and every data object to be stored is assigned an ID within the DHT key space. Each peer is in charge of the data stored in a specific area of the key space, which includes the IDs that are closest to them. This strategy makes sure that authority and responsibility are distributed among a diverse group of peers. Next, all user content in LifeSocial is stored using a DHT. References to other data items or the actual payload data itself can be contained in data objects (Graffi et al., 2011). Finally, Cachet hides the recipients of data items by using object references. The public keys are stored in encrypted form at their parent objects rather than with the data objects (Nilizadeh et al., 2012). Only friends with permission can view the receivers of the referenced items when they are given a well-known object as an entry point (Urdaneta et al., 2011).

## 2.3 Limitations and Challenges of P2P DOSNs

Each of the three architectures — federated server, end-to-end client-side data encryption, and distributed hash table — has limitations and challenges specific to its implementation and use.

### 2.3.1 Limitations of Federated Server Architecture

Even though the architecture in federated server is decentralised, individual user data is not always retained on the server where it was initially stored. If

friends from other servers ask for this information, it will be transferred to their servers and made accessible in plaintext to the service provider. Users must therefore have trust in both their friends and their own service provider (Bielenberg et al., 2012). Moreover, as each user is uniquely identified, the service provider can see every interaction and can use this information to determine the social graph of the people it hosts. Therefore, only having a theoretically decentralised architecture won't be sufficient to protect user data privacy in a single location (Schwittmann et al., 2013). Even with server-side imposed access control and user data distribution across multiple servers, users remain susceptible to privacy attacks. Furthermore, users need to have trust in both the services they receive from friends and their own service provider (Schwittmann et al., 2013). Users have less control over their data since user privacy depends on providers not disclosing user data without authorization.

### 2.3.2 Limitations of End-to-End Client-Side Data Encryption Architecture

World-readable encrypted data stores are nonetheless susceptible to metadata leaks, including timestamps, data object sizes, data structures, and header information. This enables the inference of social graphs and reveals trends of user behavior. Third-party attackers may be able to obtain sufficient information from the metadata linked to the data objects even though the content is encrypted (Greschbach et al., 2012). The computational cost of the encryption procedures is high, particularly when using more intricate systems such as Attribute-Based Encryption(ABE). ABE operations might be 100–1,000 times slower than RSA public-key method operations (Baden et al., 2009a). This can be a major performance bottleneck, especially on mobile devices. Discussion groups and comments that may be viewed by other contacts are not supported by some DOSNs, such as Vegas, which concentrate on obscuring the social graph. This restriction results from the requirement to avoid communication types that disclose interpersonal connections, which forces a trade-off between functionality and privacy functionality (Schwittmann et al., 2013).

### 2.3.3 Limitations of Distributed Hash Table Architecture

Each peer in a DHT is in charge of the information stored in a certain area of the key space. This may lead to an unfair situation where some peers have far more hard drive space allocated to them than the actual amount of data they store in the DHT

(Schwittmann et al., 2013). Data objects can contain pointers to other data objects or actual payload data in DOSN such as LifeSocial (Graffi et al., 2011), which keeps all user content in a Pastry DHT. However, every reference must be resolved in a DHT query, which is typically transmitted to different peers. Since the assignment of data objects to peers seems to be random, neither authorship nor network proximity are taken into consideration. This may impact the retrieval of data, hence decreasing its efficiency. Peers must always communicate with one another according to the DHT architecture, especially while they are signing on and off. When the DHT is employed as payload storage rather than just a data index, there is an overhead in comparison to server federations. As a result, there is a chance that performance will be slower and network traffic will increase (Schwittmann et al., 2013).

## 2.4 Blockchain-Based DOSN and Main Features

Recent years have seen a major transformation towards a more decentralised and user-powered internet ecosystem. Distributed ledger technologies, such as blockchain, can be utilised for addressing privacy and censorship concerns associated with centralised OSNs. The integration of blockchain technology into online social networks has garnered significant attention from researchers in recent times, due to its rapid advancement and enduring popularity. In an attempt to improve privacy, and censorship resistance while addressing the shortcomings of early P2P DOSNs, several research projects are investigating a new generation of decentralised social networks that incorporate blockchain technology.

A blockchain is an expanding distributed ledger that maintains an unchangeable, secure, and chronological record of every transaction that has ever occurred. A person or group going by the name of Satoshi Nakamoto created the first block of the blockchain, known as the gensis block, in 2009 and employed it to create the cryptocurrency known as Bitcoin. The main goal is to protect electronic files from manipulation by encrypting their bit sequence using a cryptosystem. Blockchain is one of the most innovative and promising technologies that powers decentralised applications by giving the network a strong infrastructure. Overall, blockchain is an immutable distributed ledger that records all network interactions and transactions (Yaga et al., 2018).

The main features of the blockchain based DOSN are explained as follow:

**User Privacy -** Online social networks built on blockchain technology eliminate a single point of failure due to decentralisation. In contrast, centralised social networks are susceptible to data breaches because they primarily rely on centralised servers. In fact, because blockchain technology is decentralised, it removes the possibility of control by a single entity. Additionally, because all transactions are encrypted and tracked, user data cannot be tampered with, guaranteeing its integrity and confidentiality (Guidi, 2021).

**Censorship Resistance -** One of the most significant problems with centralised OSNs is censorship. Users specifically oppose the restriction of sensitive topics in order to maintain their freedom of speech and expression. On the other hand, content in centralised OSNs is reviewed and removed if it violates specified guidelines. Blockchain-based DOSNs, in contrast to centralised ones, let users publish and exchange content without worrying about censorship. Content that has been stored on the blockchain is irreversible and cannot be changed or deleted by a central entity. This encourages freedom of speech and offers a potential solution for the censorship issue (Guidi, 2021).

**Reward for Contribution in Engaging Content -** In blockchain-based social networks, a content creator or a regular user might be compensated with incentives for high-quality content. All transactions are documented and audited by everyone, making the rewarding phase transparent thanks to the blockchain. In addition to being one of the main characteristics of a blockchain-based DOSN, rewarding is also thought to be essential for success in adding value to content and creating economic models (Guidi, 2021).

## 3 ANALYSIS AND DESIGN

In this section, the analysis and design phases performed for the blockchain-based DOSN application will be discussed. Firstly, it will discuss the blockchain and its related technologies. Secondly, the system architecture and prototype of the application will be discussed. Finally, it will explain the algorithm and mechanism which are implemented to address the user control, privacy, and censorship resistance limitations in centralised and P2P decentralised OSNs.

## 3.1 Blockchain-Based Decentralised Technologies

Blockchain is a unique data structure that stores data across numerous nodes or computers in the form of a sequence of blocks. According to Figure 1, the initial block, known as the genesis block, has its data transformed into a fixed-length hash value using a hash algorithm. The following block then stores this hash value. Every time a new block is generated, this process is repeated, creating a fixed-length hash value based on the data in each block, which includes the hash value of the block that preceded it, to be stored in the subsequent block. The blocks are chained in this way, so any changes made to one will also affect all of the blocks that come after it. As a result, once recorded data is placed on the blockchain, it cannot be changed because the original blockchain is impervious to manipulation. Blockchains fall into three primary categories, according to (Guidi, 2021) Public Blockchains (everyone can join the network), Private Blockchains (members are selected subject to certain criteria), and Consortium Blockchains (semi private blockchains restricted to a group). Furthermore, permissioned (private blockchain), permissionless (public blockchain), or both (consortium blockchain) can be used for all three types. Therefore, blockchain is characterised by audibility, privacy, confidentiality, consistency, decentralisation and integrity.

### 3.1.1 Ethereum Blockchain and Smart Contract

Ethereum's blockchain is particularly appropriate for implementing blockchain-based social networks due to a number of significant features and benefits. To begin with, Ethereum is decentralised, meaning that no single entity can control the network as a whole. Because of this, it is resistant to interference and censorship, which is a major benefit for social networks where freedom of speech and expression are essential. Second, social networks built on Ethereum could provide users with better privacy and more control over user data. It is impossible to gather and utilise personal data without permission in the absence of a third-party central authority. All data is stored in separate blocks as unique immutable hashes, considerably decreasing the risk of data breaches and identity theft. Furthermore, social networks and other sophisticated applications can be created with Ethereum's smart contracts. These contracts can automate a number of tasks, including user transactions and content monetization, among others. In addition, the interoperability of Ethereum facilitates data sharing and interaction between various apps, building a more integrated and effective ecosystem. Finally, Ethereum en-

ables the generation of native tokens that can be employed for a variety of purposes inside the social network, such as incentivising individuals for their contributions or facilitating network transactions. This may encourage user involvement and engagement. Due to the aforementioned reasons, the Ethereum Blockchain is selected for our decentralised online social network based blockchain network.

### 3.1.2 InterPlanetary File System (IPFS)

Interplanetary File System (IPFS) is a decentralised protocol to address, route, and transfer content-addressed data in a decentralised network. The way it operates is by using a hash to identify files and enabling a peer-to-peer network to locate the nearest copy of the file using that hash. Data is represented by IPFS as content-addressed content identifiers (CIDs), which are specific to the data they were computed from. This facilitates the retrieval of data by considering its content instead of its location. The protocol employs interplanetary linked data (IPLD) to operate with CIDs to represent relationships between data. Blockchain-based social networks can be implemented using IPFS thanks to its features, which include data control, portability, and integrity. It can be used to store messages and posts in a decentralised online social network, allowing for decentralisation and censorship resistance. Furthermore, integrating IPFS with blockchain technology can facilitate the management of encryption/decryption keys and the recording of associations of user credentials, both of which are critical for developing secure social networks (Xu et al., 2018). In our blockchain-based DOSN, all the user's media data such as images, and videos will be stored on the IPFS, and only the hash value returned from the IPFS is stored on the blockchain. In this way, it allows the application to become more scalable, and reduces the storage demand on the blockchain. In other words, by leveraging Ethereum's smart contracts, IPFS enhances secure and cost-efficient storage solutions within the blockchain ecosystem, thereby boosting the overall performance of Ethereum.

## 3.2 System Architecture and Smart Contract Design

### 3.2.1 System Architecture

The proposed blockchain-based DOSN application forms a three-layer architecture according to the Figure 2.
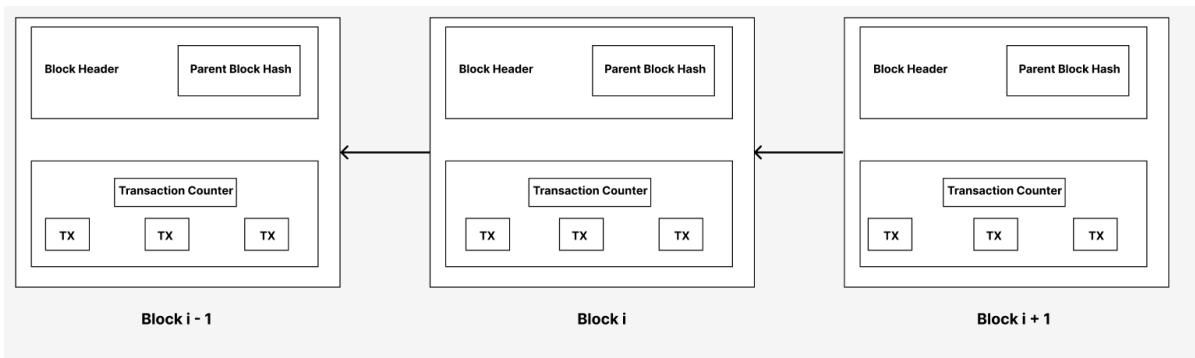
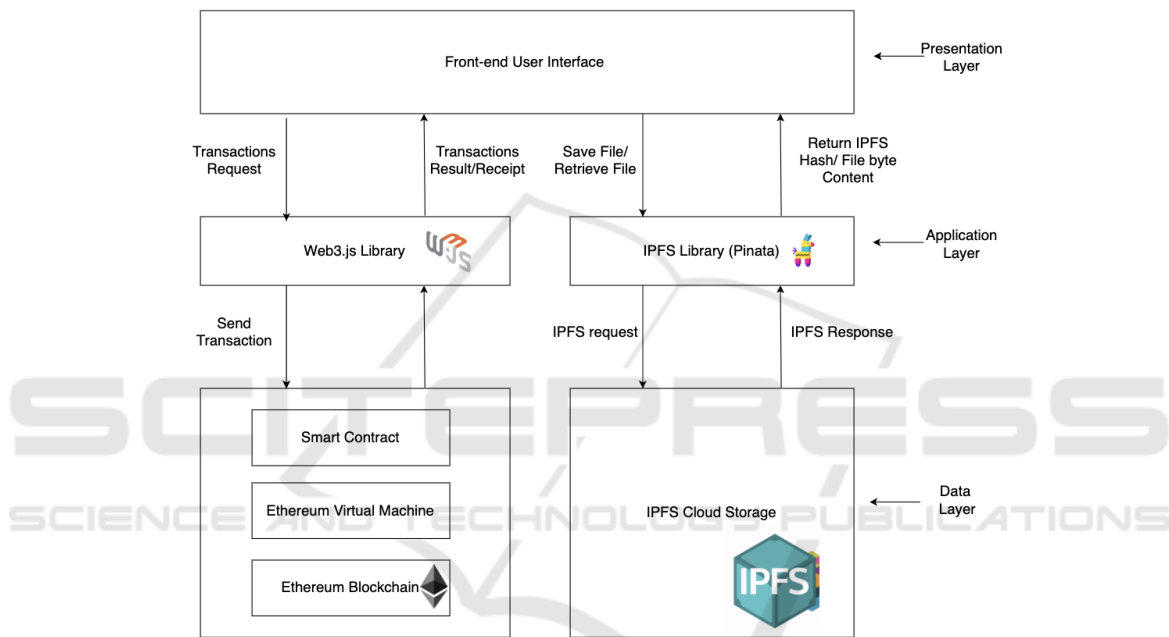Figure 1: Blockchain consisting of a continuous sequence of blocks.



Figure 2: Three-layer system architecture encompassing presentation, application and data layers.

**Presentation Layer -** The presentation layer of the application is made up of its user interface. To provide rapid and consistent access to the application, a decentralized content distribution network (CDN) will serve the user interface. Through the user-friendly and intuitive interface, users can easily interact with features and functionalities of the application.

**Application Layer -** Application Programming Interface (API) requests from the frontend application to the backend blockchain and IPFS storage are handled by the Web3 and Pinata IPFS APIs at the application layer. User input is sent to the appropriate Web3 API and Pinata IPFS API, including user profiles and post data from the frontend client. The underlying blockchain system will then communicate with the

Web3 API to provide function calls, contract deployment, and fund transfers. When a user creates a post with an image or video, the Pinata IPFS API will upload that image or video file to the IPFS cloud storage and return only the IPFS hash value to the blockchain.

**Data Layer -** The application's data layer consists of a decentralised storage network that stores user data, post content, and social interactions. The storage network, which will be accessible via the Ethereum blockchain, will make use of an IPFS decentralised protocol to guarantee data consistency and availability. To protect user privacy and control, data will be stored in an encrypted format with the user's private keys.

### 3.2.2 Smart Contract Design

The smart contract that is deployed on the Ethereum blockchain for this application consists of two main structs, which is an object data structure in Solidity programming language, in order to store information about user, and post. First of all, the "Profile" struct will store information about each user including their account address, username, biography, hash value returned from the IPFS storage for the profile picture, the time at which the account is created, unique Id, total number of posts created, followers, followings, account addresses of followers, and followings. Secondly, the "Post" struct will store information about each post including post id, creator's account address, hash value returned from the IPFS storage for the profile picture of the creator, post type, hash value returned from the IPFS storage for the image or video file contained in the post, description of the post, the time at which the post is created, the total tip amount, likes and dislikes.Next, the smart contract includes two arrays: one is for the list of users who created account on the application and the other is for the list of posts created by users. Also, it includes four mappings, which are similar to a hash-table or dictionary data structure in other programming languages. They are used to store the data in the form of key-value pairs. The first mapping "profiles" is to map from the user account address to related "Profile" struct. This is to make sure that each user account is registered only once and to quickly search user information by address, similar to locating a person by ID in the relational database. The second mapping "posts" is to map from the account address of the post creator to the array of related "Post" struct so that it stores the list of related posts that the specific user created. The last two mappings: "likedPosts" and "dislikedPosts" are to map from the account address of the user to the array of related post IDs that are liked or disliked by that user. In this way, it can store separately the list of related posts that the user liked or disliked by the account address.

### 3.3 Algorithm and Mechanism

The login and authentication process in the application is validated with the user Ethereum account wallet address provided via Metamask rather than traditional username and password validation used in centralised OSNs. When the user attempts to login, the wallet address of the user will be directly connected with the application and validated. The authentication will be carried out with the account wallet address, to decide whether the username already exists or not.

If the username already exists, the user information will be fetched from the blockchain. If the username, which attempts to login, has not been registered on the blockchain, the application will ask to create a user account. In order to handle the user account registration, all the user information including username, biography and profile picture will be stored on the blockchain. However, to store the profile picture of the user to the blockchain, the file of the profile picture is first uploaded to the IPFS decentralised cloud storage. Then, only the hash value returned from the IPFS storage is stored on the blockchain. In this way, it prevents the size of the blocks to store.

In terms of post creation, the user can create post including post description, and media contents such as images or videos. Unlike, centralised OSNs, all the information regarding the post is stored on the blockchain and decentralised storage, IPFS so that there is no central entity who can alter or censor user posts. Moreover, users can give likes as well as dislikes to the posts which mean the content moderation is only powered by community driven approach. Also, the users can tip the post which is engaging, so that the owner of the post can acquire incentives. In this way, it promotes the creation of more engaging content and filtering the inappropriate content. Also, the feed algorithm of this social network is based on popularity sorting based on three main factors, likes, dislikes, and tips. Popularity sorting ensures that high-quality and relevant content is prominently featured, while low-quality or inappropriate content is pushed down in the feed. This helps users discover valuable content more easily and reduces the visibility of harmful or irrelevant content.

## 4 EVALUATION AND DISCUSSION

In this section, we will assess the viability and effectiveness of our blockchain-based DOSN application in relation to the research questions. This evaluation intends to examine whether the project accomplishes the aim and objectives for preserving privacy, and censorship resistance as well as enhancing user engagement in online social network with the use of blockchain technology.

**(RQ1).** *How Does the Blockchain Architecture Address Potential Privacy Concerns in Centralised OSNs and Peer-to-Peer DOSNs?*

The underlying blockchain technology of the application can address privacy concerns in centralised OSNs and peer-to-peer DOSNs through several mechanisms. In traditional centralised OSNs, user data is

stored on centralised servers controlled by a single entity, making them vulnerable to data breaches and unauthorized access. Also, while peer-to-peer networks aim to distribute data across multiple nodes, there's still a risk of data leakage if one or more nodes are compromised. In this blockchain- based DOSN, as the Ethereum blockchain maintains an immutable ledger of transactions or data regarding user interactions on the blockchain in a tamper-proof manner. Once data is recorded on a blockchain, it is extremely difficult to alter without consensus from the network. Therefore, it provides a strong level of transparency and integrity to the data stored on the blockchain, which is helpful for preserving the privacy of social network interactions and transactions. Peer-to-peer technologies and blockchain technology are both decentralized, however the blockchain network offers a more advanced level of decentralisation. It also uses strong encryption methods to protect user communications and data. End-to-end encryption protects user privacy from unauthorised access by ensuring that only the intended receivers may access and decrypt information. Moreover, the combination of end-to-end encryption and smart contract logic used for social connection between users help secure the privacy between users' information. For example, according to the Figure 3, users cannot view the content of the other user, who does not have any social connection between them. Unless the post of the user is available public, other users cannot view the content. The content can only be decrypted and viewed by the authorized user, who is the creator of the content, and other users who share social connections with that particular creator can view his or her posts. This is achieved through the use of Ethereum smart contract validation rules. In this way, our solution addresses the privacy problems which are vulnerable in centralised OSNs, and peer-to-peer networks.

### (RQ2). *How Does the Decentralised Nature of Blockchain-Based DOSN Provide the Censorship Resistance.*

Underlying technologies: Ethereum blockchain, IPFS storage, and smart contract which are used to implement this online social network, provide censorship resistance for users. As Ethereum blockchain and IPFS are decentralised systems, they don't rely on a single central authority to function. Instead, they operate on a network of nodes spread across the world. Once data is written onto the Ethereum blockchain, it becomes immutable. Similarly, content stored on IPFS is distributed across multiple nodes, and once uploaded, it remains immutable. This immutability ensures that no central authority

can censor or remove content on blockchain and IPFS without user's consent. Also, social network functionalities are deployed as smart contracts on the Ethereum blockchain, users can interact with the network without relying on a centralised intermediary. Moreover, Ethereum blockchain network is governed by decentralised consensus mechanism, Proof of Stake (PoS), meaning that decision-making power is distributed among network participants rather than being controlled by a single authority. As shown in Figure 4, users can participate in the governance of the network, influencing decisions related to data management policies, such as giving likes to valuable content, and dislikes to harmful content. Based on the number of likes and dislikes, all the content is sorted, and only the valuable content will be on top of the news-feed, and harmful content will be pushed down and unable to view. In this way, this reduces the risk of censorship by eliminating single points of control, and enhances the community driven approach on content moderation and filtering.

### (RQ3). *How Can the Blockchain-Based DOSN Enhance the Contribution of Engaging Content than Centralised OSNs and Peer-to-Peer DOSNs.*

The implemented Ethereum blockchain-based DOSN enhances the contribution of engaging content compared to peer-to-peer DOSNs through several mechanisms. In peer-to-peer DOSNs, there is no chance to integrate incentivisation for social interactions, and thus, user's engagement is only enhanced through traditional ways of liking, commenting, and sharing posts. However, in this blockchain-based DOSN, incentivisation mechanism is implemented to reward users with incentives for creating engaging content. As shown in Figure 5, users incentivise each other through giving likes, dislikes, and tips for valuable contributions. By incentivizing users to contribute valuable content, the network motivates users to actively participate in the network and produce engaging content. Moreover, in this social network, decentralised content curation algorithm is implemented that rely on user interactions and community consensus to surface engaging content. This algorithm prioritizes content based on factors such as likes, dislikes, tips, and reputation scores, ensuring that the most relevant and interesting content is prominently featured. Also, through decentralized decision-making process or incentive-based rewarding system, users can collectively determine what constitutes engaging content and how it should be promoted without relying on centralised authorities, which addresses unfair monetization mechanism, such as boosting in centralised OSNs.
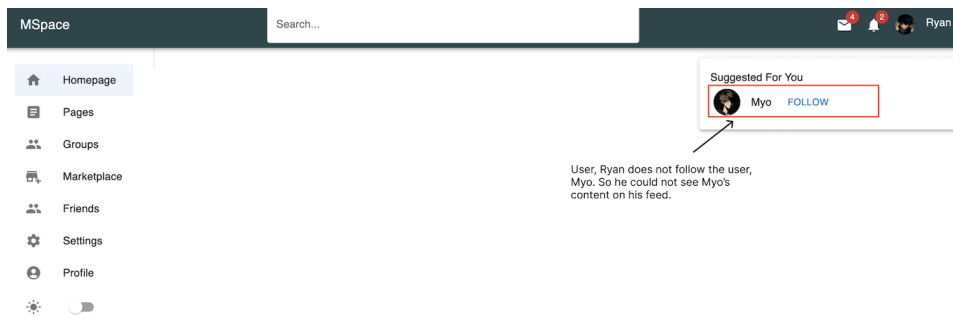
Figure 3: Feed showing that users cannot view posts of other users unless they are publicly shared.
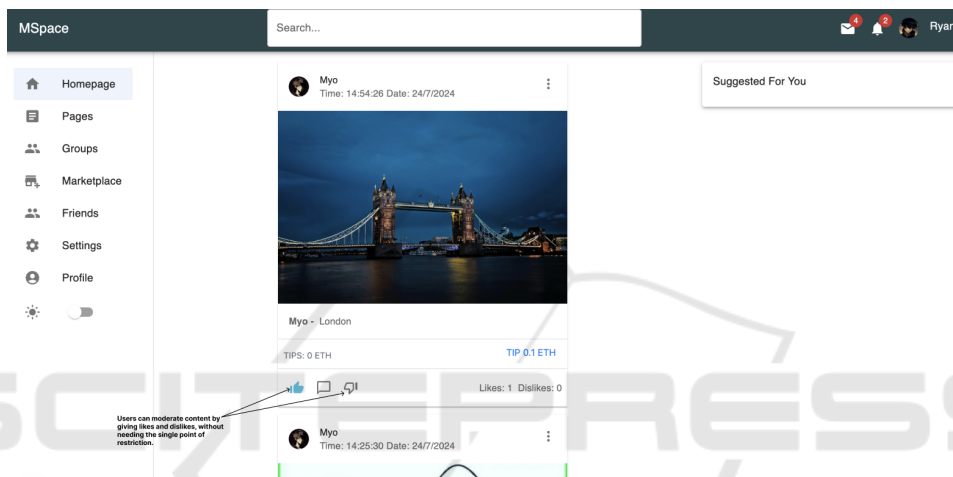


Figure 4: Users participate for the governance of the network, such as adding likes and dislikes, which reduces the risk of censorship by eliminating single point of control.
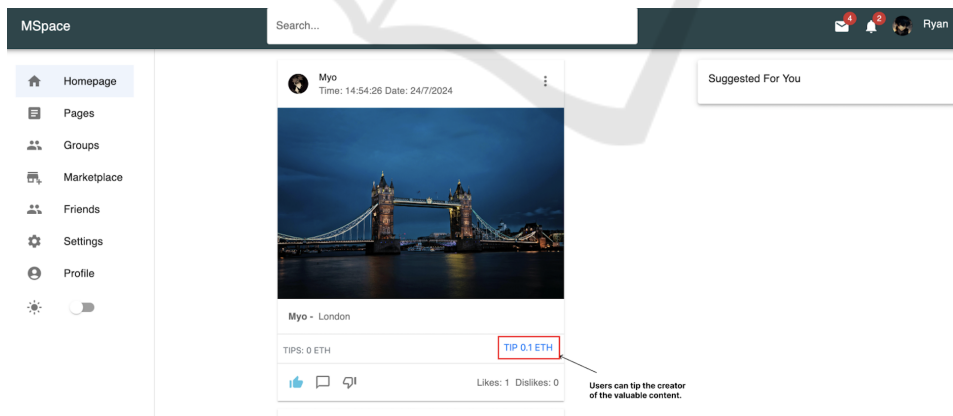


Figure 5: Users can incentivise other users to encourage participation.

# 5 RELATED WORK

In order to accommodate the privacy, censorship resistance and user engagement issues in centralised OSNs, various decentralised solutions have been ex-

plored. The first detailed architecture for the decentralised peer-to-peer (P2P) online social network, PeerSon, was proposed by Sonja Buchegger in 2009 (Buchegger et al., 2009). They developed the Peer-SoN system, which combines a P2P infrastructure

with encryption and direct communication between users' devices, in an effort to strengthen OSNs while protecting users' privacy. The two-tier system architecture of the prototype consists of a distinct look-up service and peers interacting with one another. They created protocols for sharing data directly between peers as well as between peers and the lookup service. However, since the service provider can view every interaction and use this data to ascertain the social graph of the users it hosts, maintaining the mechanism in PeerSoN is a crucial problem. Therefore, protecting user data privacy in a single location won't be possible with just a theoretically decentralized design. Moreover, Randy Baden and Adam Bender proposed a decentralised OSN called Persona, which allows user to have more control over their information (Baden et al., 2009b). Persona uses attribute-based encryption (ABE) to hide user data, giving users the ability to impose strict guidelines on who can access their information. Persona offers a powerful tool for developing apps where users, not the OSN, set access rules for personal information. They present novel cryptographic techniques that improve ABE's broader application. Although, the Persona OSN secure user information, metadata including timestamps, data object sizes, data structures, and header information still leak. This makes it possible to infer social graphs and exposes user behavior patterns. Even when the content is encrypted, third-party attackers might still be able to gather enough information from the metadata attached to the data objects. Two initiatives that investigate blockchain technology for social networks are Akasha7 and Synereo (Chakravorty and Rong, 2017). These solutions are all still in their initial stages of development. Using Ethereum as its blockchain network, Akasha seeks to create a knowledge architecture for social human advocacy within the framework of social networks, freedom of speech, creative perpetuity, and privacy for an improved Internet that benefits all people. A distributed, decentralized social network built for the attention economy is offered by Synereo (Chakravorty and Rong, 2017). It provides more of a social marketplace platform. These blockchain-based solutions protect user privacy and withstand censorship, but they still have limits when it comes to moderation and content filtering.

Unlike these above decentralised solutions, the integration of Ethereum blockchain, smart contract, and IPFS storage solution in our blockchain-based DOSN, offers several advantages. In centralised OSN, the single authority owns the user data. Although users may be able to modify their privacy settings, the network controls what information is gathered and how it is used. Also, in peer-to-peer DOSNs, although it al-

lows users to have control over data, users still need to trust peers and service providers and also distribution of user data may not ensure complete control. In this blockchain-based DOSN, users have complete ownership of their data with the use of cryptographic keys that grant them control over who can access their data and under what conditions. Because the user's crypto wallet is connected to this social network, providing public and private keys for network access, authentication and authorization are implemented through that connection. Hence, only authorized users with the corresponding private keys can decrypt and view the content. Public keys stored on the blockchain facilitate secure communication between users. In contrast, users of peer-to-peer DOSN and centralised OSN have to share personal information in order to participate, as authentication and permission are handled through email and password mechanisms. Additionally, because Blockchain transactions are immutable and transparent, users can simply validate how their data is being accessed or used. On the blockchain, every transaction is recorded and cannot be changed without the users' permission. This transparency gives users greater control over their data compared to peer-to-peer networks where data handling practices might not be as transparent, and depends on the network operator of a specific node. This social network application utilises smart contracts to give users control over how they participate. Users can specify rules for accessing their data or interacting with their content, and the smart contract rules will be automatically enforced without the need for intermediaries. Also, the smart contract manages core functionalities of this social network application, by facilitating privacy-enhancing rules such as zero-knowledge proofs or selective disclosure of information. Therefore, users can selectively share only the necessary details required for specific interactions, preserving their privacy and having more control over data.

Moreover, to address content moderation and filtering inappropriate content issues in peer-to-peer and other blockchain-based DOSNs, community-based moderation is used in this social network, where users can collectively give likes, dislikes, incentives to posts, and sorting by popularity. Users can indicate their approval of content by liking it. This serves as a positive signal indicating that the content is relevant, valuable, or appropriate. Conversely, users can express their disapproval of content by disliking it. This serves as a negative signal indicating that the content may be inappropriate, misleading, or harmful. Moreover, users can financially reward content creators by tipping their posts. This incentivizes the cre-

ation of high-quality content and encourages users to contribute positively to the network. Then, posts are sorted based on its popularity, which are determined by factors such as the number of likes, dislikes, and tips. Popularity sorting ensures that high-quality and relevant content is prominently featured, while low-quality or inappropriate content is pushed down in the feed. This helps users discover valuable content more easily and reduces the visibility of harmful or irrelevant content. Also, with the proof-of-stake consensus mechanism of Ethereum blockchain, it helps prevent spam, and other forms of abuse. By leveraging the community-driven moderation mechanism, the blockchain-based social network empowers users to collectively filter and moderate content according to community standards and preferences, while preserving censorship resistance.

# 6 CONCLUSIONS

In conclusion, the development of a decentralised online social network powered by Ethereum blockchain is an important advancement toward protecting users' privacy, and encouraging resistance to censorship. With the help of blockchain technology's integrated security and transparency, we have developed this decentralised online social network that allows users to actively participate in creating their online experiences rather than just being passive consumers. The network ensures that user data is secure and tamper proof by mitigating the weaknesses of peer-to- peer and centralised OSNs through the use of blockchain technology. The implemented online social network gives users control over who can access their information and under what circumstances by utilizing smart contracts, cryptographic and decentralized techniques in authentication and interaction. Furthermore, users' trust is increased by the immutability of blockchain transactions, which ensures accountability and transparency. Moreover, the social network promotes censorship resistance by offering an environment where people may express themselves freely without worrying about repression or manipulation. Additionally, by integrating incentives and promoting user engagement, the implemented blockchain-based DOSN has successfully addressed issues with both centralised and peer-to-peer OSNs. This is evidenced by the results of the evaluation against research questions. Overall, the principal aim of our work is successfully accomplished. In the future, in terms of features improvement of this social network application, more advanced functionalities such as decentralised commenting, sharing, messaging, creating

stories, creating Non-fungible Tokens (NFTs), and integrating with other decentralized applications, will be included.

# REFERENCES

Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. (2009a). Persona: An online social network with user-defined privacy. volume 39, pages 135–146.

Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. (2009b). Persona: An online social network with user-defined privacy. volume 39, pages 135–146.

Bielenberg, A., Helm, L., Gentilucci, A., Stefanescu, D., and Zhang, H. (2012). The growth of diaspora - a decentralized online social network in the wild.

Buchegger, S., Schiöberg, D., Vu, L.-H., and Datta, A. (2009). Peerson: P2p social networking: early experiences and insights. In *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, SNS '09, page 46–52, New York, NY, USA. Association for Computing Machinery.

Chakravorty, A. and Rong, C. (2017). Ushare: user controlled social media based on blockchain. In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, IMCOM '17, New York, NY, USA. Association for Computing Machinery.

Graffi, K., Gross, C., Stingl, D., Hartung, D., Kovacevic, A., and Steinmetz, R. (2011). Lifesocial.kom: A secure and p2p-based solution for online social networks. pages 554 – 558.

Greschbach, B., Kreitz, G., and Buchegger, S. (2012). The devil is in the metadata—new privacy challenges in decentralised online social networks.

Guidi, B. (2021). An overview of blockchain online social media from the technical point of view. *Applied Sciences*, 11:9880.

Mohammed, A. B. (2022). Decentralised social media platform using blockchain technology.

Nilizadeh, S., Jahid, S., Mittal, P., Borisov, N., and Kapadia, A. (2012). Cachet: A decentralized architecture for privacy preserving social networking with caching. *CoNEXT 2012 - Proceedings of the 2012 ACM Conference on Emerging Networking Experiments and Technologies*.

Paul, T., Famulari, A., and Strufe, T. (2014). Survey on decentralized online social networks. *Computer Networks*, 75, Part A:437 – 452.

Schwittmann, L., Boelmann, C., Wander, M., and Weis, T. (2013). Sonet – privacy and replication in federated online social networks. pages 51–57.

Shilina, S. (2023). *The Promise of Blockchain-Based Decentralized Social Networks: Enabling Privacy, Censorship Resistance, and User Control*, pages 172 – 198.

Tran, M., Nguyen, S., and Ha, S. (2016). Decentralized online social network using peer-to-peer technology. *REV Journal on Electronics and Communications*, 5.

Urdaneta, G., Pierre, G., and van Steen, M. (2011). A survey of dht security techniques. *ACM Comput. Surv.*, 43:8.

Xu, Q., Song, Z., Goh, R., and Li, Y. (2018). Building an ethereum and ipfs-based decentralized social network system. pages 1–6.

Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018). Blockchain technology overview.

Yerby, J., Koohang, A., and Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, 7:1–13.

Zhan, Y., Xing, X., and Xiong, Y. (2022). A conceptual model and case study of blockchain-enabled social media platform. *Technovation*, 119.