# Self-Managed Online Social Network Using Blockchain Technology

**Kommineni Madhuri[1], Praveen Babu G.[2]**

[1]M.Tech. Student, Department of Information Technology (DIT), JNTUH University College of Engineering, Science and Technology, Kukatpally, Hyderabad, 500085, Telangana, India.
[2]Associate Professor of CSE, Department of Information Technology (DIT), JNTUH University College of Engineering, Science, and Technology, Kukatpally, Hyderabad, 500085, Telangana, India.

## Abstract

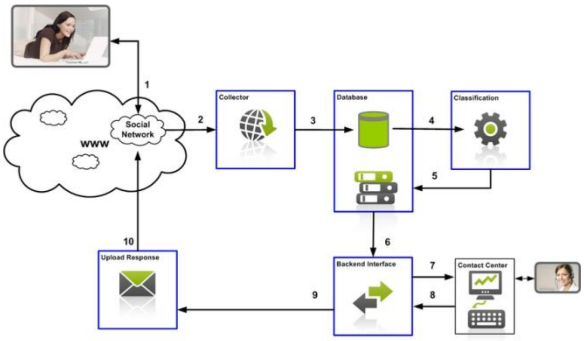
Online social networks (OSNs) are becoming more and more integrated into people's everyday lives. In any case, since all notable OSNs are controlled, there are a few issues with privacy, management, and security. Users are usually restricted to using the services that OSN firms deploy after agreeing the OSN agreements. But a lot of contracts let OSN companies get to user data to provide personalized services like ads. Users typically have to submit a number of elaborate applications or even stop using such Online Social Network (OSN) if they don't let the businesses use their information while protecting their privacy. Blockchain technology combined with a decentralized architecture can address the aforementioned problems. In this architecture, most of the network functions are distributed among the multiple nodes. It means they are responsible for managing their own network policies, security and performance because the network traffic directly flows between those nodes. It is suggested in this project work to create an OSN service based on blockchain technology and demonstrate its decentralized operation. An enormous amount of data with generally low security requirements can be decentralized by storing it in the Interplanetary File system (IPFS). This distributes data to nodes consisting of hundreds of thousands of individual computers connected to the IPFS, rather than storing data in a single centralized server. A decentralized autonomous organization that allows users to democratically self-manage the OSN may be established in order to promote user autonomy.

**Keywords:** Blockchain, Online Social Network (OSN), Decentralized Autonomous Organization (DAO).

## 1. INTRODUCTION

Nowadays, the majority of online social networks (OSNs) are centralized, indicating that all user data and services are often wholly owned by the firms operating these networks. Generally speaking, users can only access the service after accepting the terms set forth by OSN companies. However, under a number of agreements, OSN corporations have the ability to exploit user information for targeted services like advertising. If customers don't want businesses to use their data and keep their private information safe, they usually have to give a lot of reasons or stop using these types of online social networks. When data and services were centralized, customer data was also uploaded and saved on centralized computers that were run by OSN companies. As a result, users find it challenging to safeguard their OSN content in the event that server failure occurs. To exacerbate the situation, user addresses and other security information, such as passwords, may be compromised if the servers are compromised. By employing a technique known as a credential stuffing attack, hackers can readily breach the accounts of numerous users who use the same password on various websites [1]. Users' private information is therefore vulnerable to theft and misuse. Researchers are encouraged to think about creating an OSN based on the decentralization framework by these issues with centralized OSNs.

**Figure 1. Example Figure**



Since decentralized online social networks (OSNs) provide owners more control over information and privacy, they may offer consumers a more safe and controlled social network environment. Due to the fact that services are no longer dependent on centralized servers and data is stored in a distributed manner. Generally speaking, a peer-to-peer mechanism powers decentralized OSNs, where each node keeps part of the data and supports the service. It does not, however, impose obligations on bad deeds, a lack of self-control, or the ability to develop steadily.

## LITERATURE REVIEW

### Detecting Stuffing of a User’s Credentials at Her Own Accounts:

We provide a way for websites to work together to find situations where each user's credentials have been stuffed with credentials. Our detection method uses contemporary anomaly detection and closely monitors suspect logins to distinguish between credential stuffing and typical login activity (password reuse, proper password entry into incorrect websites, etc.). Websites work together with a special private membership test protocol that uses cuckoo filters to stop password leaks. Compared to comparable scalable options, our protocol is significantly more safe and highly scalable in a critical metric that we specify. Using probabilistic model checking, we evaluate our credential-stuffing detection accuracy over a range of operational points. These methods distinctive application of formal techniques to determine how our design affects usability may be of independent relevance. We demonstrate that our framework's basic infrastructure deployment should already be able to handle the aggregate login traffic that the US retail, airline, hotel, and consumer banking industries experience.

### Bitcoin: A Peer-to-Peer Electronic Cash System:

If electronic currency was the sole form of payment available, payments might be made online directly between parties without going thru a bank. Digital signatures are helpful, but the network creates a permanent timestamp outside of recurring proof-of-work by hashing tasks into an ongoing series of hash-based proof-of-work. This makes the main benefits useless if a reliable third party is still needed to stop double-spending. The fundamental advantages are in conflict. We provide a network-located peer-to-peer solution for the double-spending problem. By turning jobs into a series of hash-based proofs of work, the network creates a timestamp that can't be changed that isn't part of repeated proofs of work. The longest chain shows both where the most processing power came from and the order in which the events were found. Nodes that are broken down together to attack the network will make the longest chain and beat attackers because they control most of the CPU power. The network itself needs very little arranging. Nodes are free to disconnect and rejoin the network whenever they choose, and the endless proof-of-work chain that follows them serves as a reminder of what happened while they were together. Communications are released on a full force action.

**New generation of memory-hard functions for password hashing and other applications:**
We introduce Argon2, a novel kind of hash function that can be used to protect secrets with low entropy without the need for secret keys. It runs very quickly on a standard PC, demands a fixed (but insurmountable) amount of memory, and forces memory-saving users to make unfeasible trade-offs between computation and time. In general, it can offer ASIC and cap resistance by filling the memory in 0.6 cycles per byte in a way that can't be compressed.

**The Anonymizer: Protecting user privacy on the web:**
I start this post by talking about the technology that makes it possible to violate the privacy of web users. Next, I describe how my "Anonymizer" system is built to prevent such privacy infringements and allow users to stay anonymous in the interim until new laws or technological advancements are implemented. I wrap up by evaluating the state of web privacy trends.

## 3. METHODOLOGY

When you use a decentralized OSN, services don't depend on centralized platforms and data is stored in multiple places. This means that users have more control over their data, privacy, and information, and the social network is safer and easier to use. A peer-to-peer system is often used to run a decentralized OSN. In this type of system, each node offers the service and saves a copy of the data. However, it does not apply to malicious behavior, poor self-control, and abilities that will as a lifetime.

**Disadvantages:**

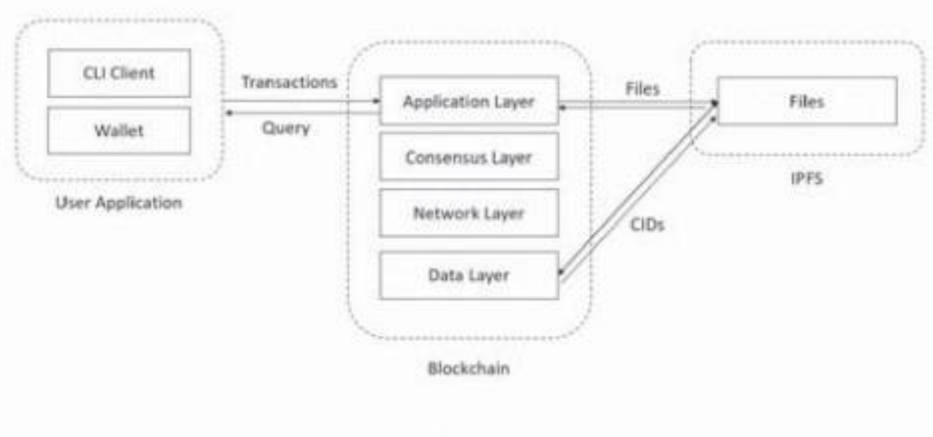
1. Nevertheless, it does not apply to harm full activities.
2. Lack of self-control and capacity for sustained growth.

In this project work, a blockchain-based architecture is proposed for an independent decentralized online social network. In order to run decentralized open source networks (OSNs), peer-to-peer systems where each node retains a piece of the data and maintains the service are frequently employed. Additionally, in order to guard against fraud, the private key must be used to sign every block chain transaction. The design includes a decentralized autonomous system that is driven by blockchain technology. This lets the system handle itself and grow over time.

**Advantages:**

1. The blockchain that is being used in this project will give OSN a decentralized setting and let people run their social networks without needing anyone else to do it.

**Fig.2: System architecture**



In order to carry out this project, I created the modules listed below:

1. IPFS data storage: IPFS is a data storage server and we can upload any post related image and these images will be saved in IPFS server and each image will have one hash code as its address. This address will be stored in Blockchain while retrieving post data.
2. Signup Module: Using this module user can sign up with application and Each and every signup will be stored in Blockchain.
3. Login Module: With the help of this module, a user can log into an application and then carry out the tasks listed below.
4. Publish & Save Tweets in Blockchain: Using this module user can post and upload image to application and application will save post data to Blockchain and image data to IPFS server.
5. View Tweets: Using this module all users can see tweets of one and other by retrieving from Blockchain.

## 4. IMPLEMENTATION

Now-a-days 80% people are using online social networks to post their opinions or to get news information or to keep himself/herself in touch with friends and relatives. All social networks applications are using centralized servers to store user’s signup and post details and if that server crash, user services will be interrupted, and data will be deleted. All user data security will be at risk if a server is hacked because hackers may misuse all user data.

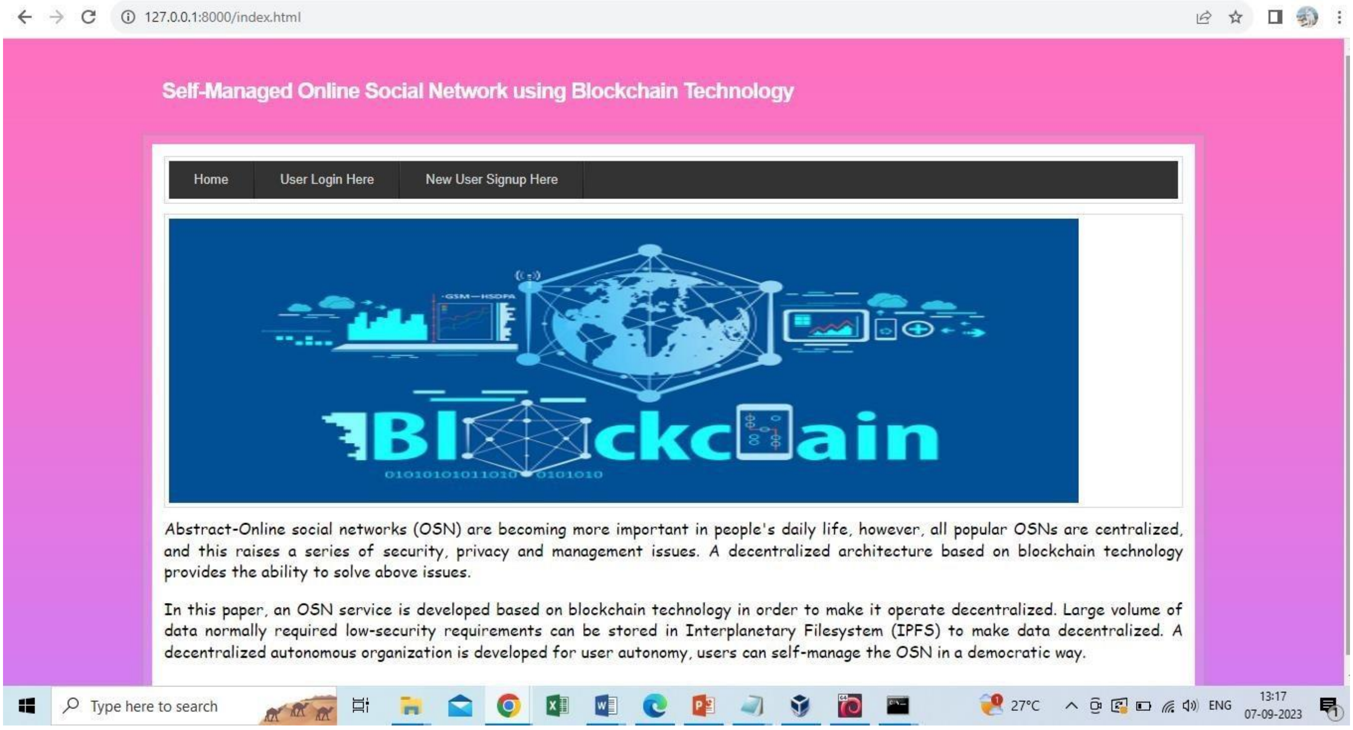
To overcome from above issues in this project work a concept to divert every social media platform to become decentralized (Data will be kept on several servers or nodes.) Blockchain servers are put into use. On the blockchain, each transaction will be kept in the form of a block. Before storing a new block, the block chain checks the hash codes of all the blocks that have already been saved on all the current nodes. If every block hash code is correct, then only a new block will be added. If node verification fails, information will be gathered from other working nodes in order to fix the system that was hacked. Blockchain never allowed any attacker to modify blocks so it will consider as immutable.

By applying Blockchain OSN, networks can maintain data at multiple nodes and avoid risk of server crashing and hacking. In this project, social media posts will be stored on blockchain. however, as blockchain is not designed to store large amounts of data, all heavy information, including videos and photographs, will be stored on IPFS (interplanetary file system) servers.

Because blockchain is immutable at a storage facility and allows for transaction/block hash code verification, it is safe and dependable in the present market.

## 5. EXPERIMENTAL RESULTS

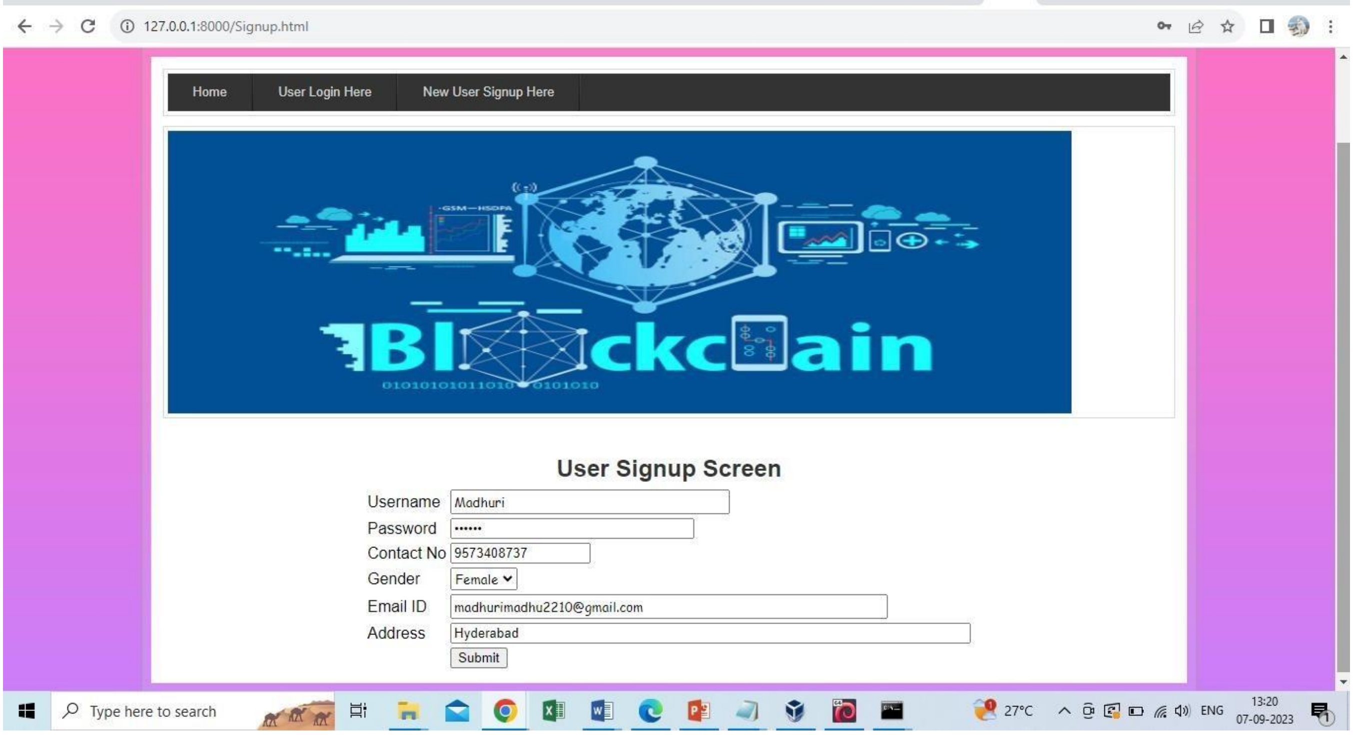
Figure 3. Home Screen



Abstract-Online social networks (OSN) are becoming more important in people's daily life, however, all popular OSNs are centralized, and this raises a series of security, privacy and management issues. A decentralized architecture based on blockchain technology provides the ability to solve above issues.

In this paper, an OSN service is developed based on blockchain technology in order to make it operate decentralized. Large volume of data normally required low-security requirements can be stored in Interplanetary Filesystem (IPFS) to make data decentralized. A decentralized autonomous organization is developed for user autonomy, users can self-manage the OSN in a democratic way.

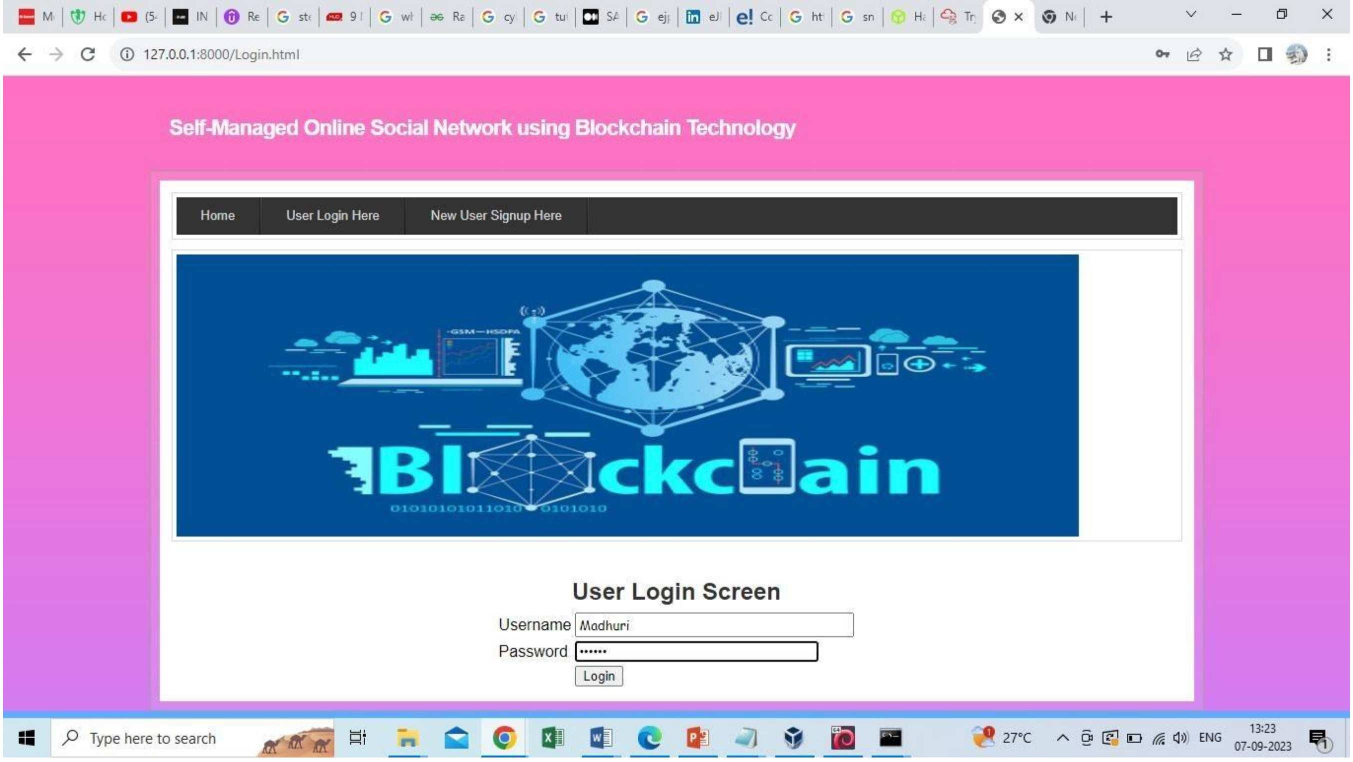
Figure 4. User Registration



User Signup Screen

| | |
|---|---|
| Username | Madhuri |
| Password | •••••• |
| Contact No | 9573408737 |
| Gender | Female |
| Email ID | madhurimadhu2210@gmail.com |
| Address | Hyderabad |

**Figure 5. User Login**



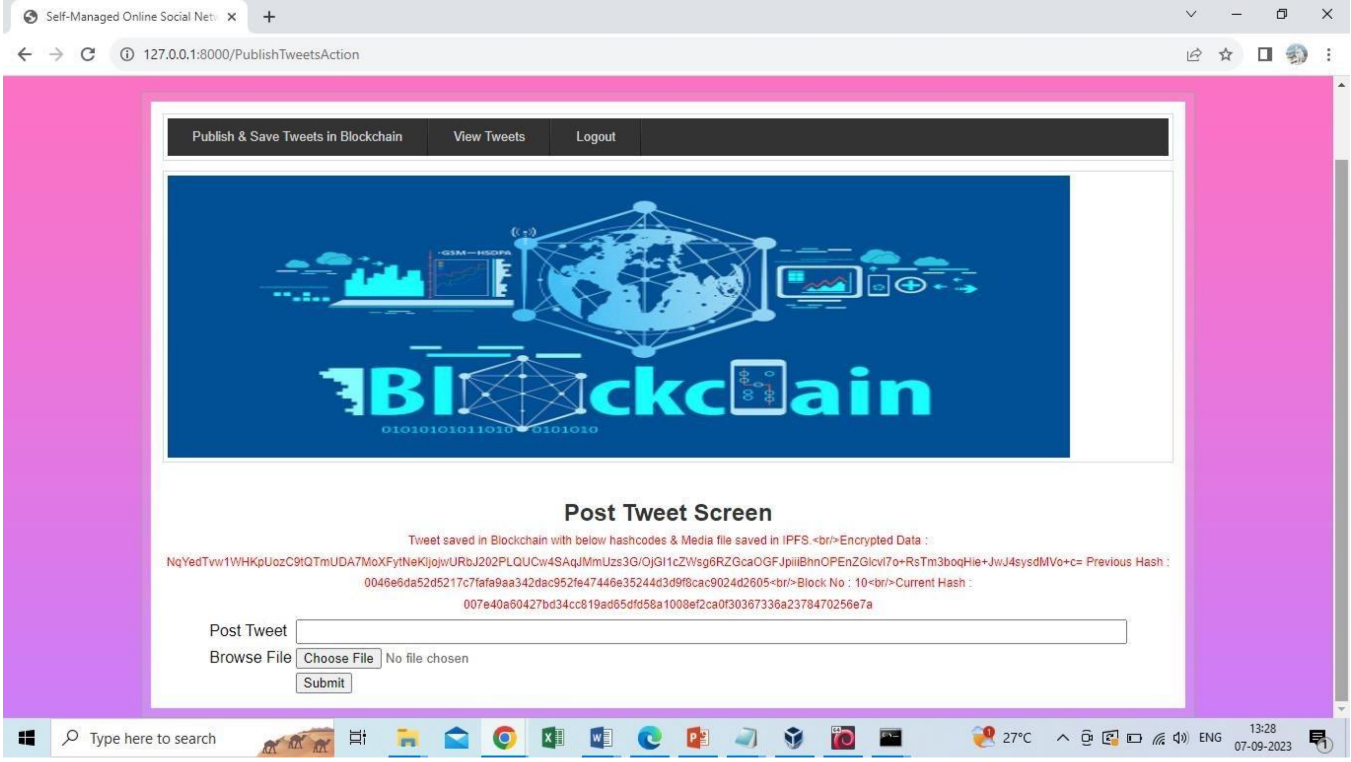
User Login Screen

Username Madhuri

Password ••••••

Login

**Figure 6. Publish & Save Tweets Blockchain**



Self-Managed Online Social Netw
127.0.0.1:8000/PublishTweetsAction
Publish & Save Tweets in Blockchain
View Tweets
Logout
Blockchain
Type here to search
27°C
ENG
13:28
07-09-2023

Post Tweet Screen

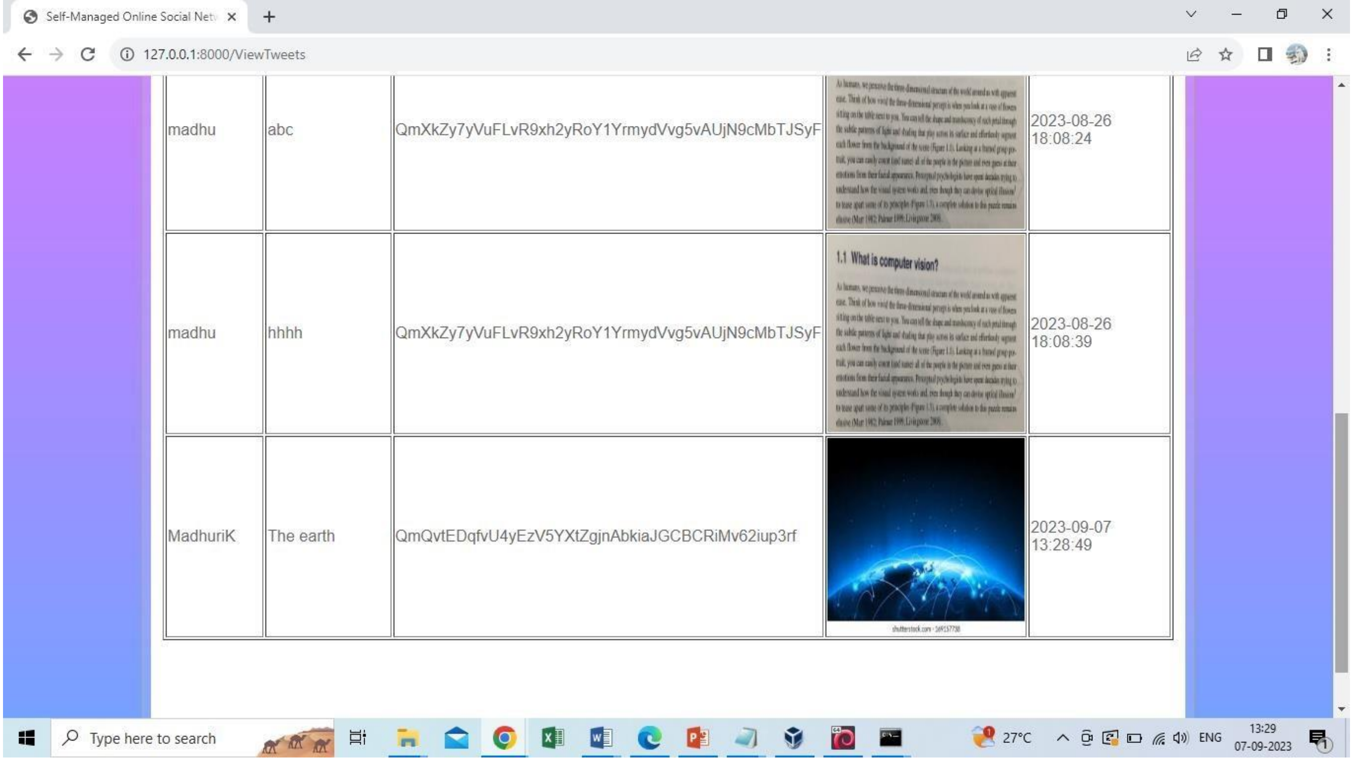
Tweet saved in Blockchain with below hashcodes & Media file saved in IPFS.<br/>Encrypted Data : NqYedTvw1WHKpUozC9tQTmUDA7MoXFytNeKljojwURbJ202PLQUCw4SAqJMmUzs3G/OjGI1cZWsg6RZGcaOGFJpiiiBhnOPEnZGlcvl7o+RsTm3boqHie+JwJ4sysdMVo+c= Previous Hash : 0046e6da52d5217c7fafa9aa342dac952fe47446e35244d3d9f8cac9024d2605<br/>Block No : 10<br/>Current Hash : 007e40a60427bd34cc819ad65dfd58a1008ef2ca0f30367336a2378470256e7a

Post Tweet

Browse File Choose File No file chosen

Submit

**Figure 7. View tweets**



127.0.0.1:8000/ViewTweets

| | | | | |
|---|---|---|---|---|
| madhu | abc | QmXkZy7yVuFLvR9xh2yRoY1YrmydVvg5vAUjN9cMbTJSyF | | 2023-08-26 18:08:24 |
| madhu | hhhh | QmXkZy7yVuFLvR9xh2yRoY1YrmydVvg5vAUjN9cMbTJSyF | 1.1 What is computer vision? | 2023-08-26 18:08:39 |
| MadhuriK | The earth | QmQvtEDqfvU4yEzV5YXtZgjnAbkiaJGCBCRiMv62iup3rf | | 2023-09-07 13:28:49 |

## 6. CONCLUSION

This project showcases an OSN-specific blockchain implementation. To prevent security information from being leaked from centralized servers, users maintain ownership over their security information. Furthermore, because social network services are decentralized, users have expressed concern about centralized entities crashing their services. Moreover, a Decentralized Autonomous Organization (DAO) allows all members to independently administer their social network. An OSN can grow sustainably even in the absence of a central leader. In addition to offering a decentralized environment for OSN, the blockchain used in this project enables users to administer their social networks decentralized.

## 7. FUTURE SCOPE

The CLI clients will be replaced in future work with a user-friendly interface because they are not ideal for typical users. As this project uses a public IPFS network, a private IPFS network will be created to increase the degree of data protection. In order to incentivize users to create more top-notch content on OSN and reward themselves for their contributions in the autonomous section, the simulate strategy will be necessary for future development.

## REFERENCES

1. M. Bellare, P. Rogaway, “Introduction to modern cryptography,” https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf
2. A. Biryukov, D. Dinu,D. Khovratovich, “Argon2: New generation of memory-hard functions for password hashing and other applications,” in 1st IEEE EuroS&P, March 2016.
3. J. Blocki, B. Harsha,S. Zhou,“On the economics of offline password cracking,” in 39thIEEE Symposium on Security and Privacy (S&P), May 2018.

4. 4.H. Bojinov, E. Bursztein, X. Boyen,D. Boneh, “Kamouflage: Loss-resistant password management,” ESORICS, vol. 6345 of LNCS, September 2010.
5. J. Boyan,“The Anonymizer: Protecting user privacy on the web,” Computer-Mediated Communication Magazine, vol. 4, no. 9, September 1997.
6. A. S. Brown, E. Bracken, S. Zoccoli,K. Douglas, “Generating and remembering passwords,”Applied Cognitive Psychology, vol. 18, no. 6, 2004.
7. W. E. Burr, “Electronic Authentication Guideline,” NIST Special Publication 800-63-2,August 2013.http://dx.doi.org/10.6028/NIST.SP.800-63-1
8. Certicom Research, “SEC 2: Recommended elliptic curve domain parameters,” Standards for Efficient Cryptography,2000, https://www.secg.org/SEC2-Ver-1.0.pdf
9. K. Collins, “Facebook buys black market passwords to keep your account safe,”November 9,2016.https://www.cnet.com/news/privacy/facebook-chief-security-officer-alex-stamos-web-summit-lisbon-hackers/