AN INDEPENDENT AND DECENTRALIZED AUTONOMOUS SOCIAL NETWORK POWERED BY BLOCKCHAIN

Dr. D. Madhavi[1], P. Likitha[2], B. Bhavya Sri[3], M. Mounika[4]

Article History: Received: 07.05.2023 **Revised:** 19.06.2023 **Accepted:** 14.07.2023

Abstract

Online social networks (OSNs) are becoming more prevalent in daily life, but because all well-known OSNs are centralised, there are some management, security, and privacy issues that need to be addressed. Decentralised architecture based on blockchain technology gives us the ability to solve the issues. This article creates and illustrates the decentralised operation of an online social network service based on blockchain technology. The Interplanetary File System (IPFS) allows for the decentralised storage of a sizable amount of normally required data with minimal security requirements. Due to a decentralised autonomous organisation that was created for user autonomy, users can democratically self-manage the OSN.

Keywords: Blockchain, Security, Privacy, Online Social Network (OSN), Management, Interplanetary File System (IPFS).

---

[1]Associate Professor, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana.
[2,3,4]B.Tech Final Year, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana.

Email: [1]dasarimadhavi3@gmail.com, [2]Policelikitha59@gmail.com, [3]bobolubhavyasri@gmail.com, [4]muthyalamounika@gmail.com

DOI: 10.31838/ecb/2023.12.s3.699

1. INTRODUCTION

A platform called Online Social Network (OSN) enables people to connect with one another online. It is an important forum where the general public may assemble and exchange knowledge, express their ideas, and reveal personal information. According to research by Chaffey [1], the most popular OSN in the world is the most live, which suggests that engaging with OSN is a very popular online activity for Internet users. Since most OSNs in use today are centralised, it is common for OSN enterprises to fully own all user data and services.

Users typically cannot access the service until they have accepted the OSN agreements that OSN companies have put in place. Nevertheless, a number of agreements permit the OSN companies to access user data for customised services like advertising. If users do not want the companies to use their data and protect their privacy, they often have to submit numerous complex applications or even quit using such OSN.

Due to the centralization of data and services, all user data is now uploaded to and kept on centralised servers under the control of OSN businesses. When servers fall down, users find it difficult to secure their OSN content. To make matters worse, if the servers are hacked, security information including passwords, security holes, and user addresses may be made public. Hackers who use the same password across several websites can swiftly access the accounts of many users by using a method known as a credential stuffing attack [2].

Personal data about users is therefore susceptible to theft and abuse. These problems with centralised OSNs inspire researchers to consider developing an OSN using a decentralised structure. Decentralised OSN users may gain from a more secure and safe social networking environment where their owners have more control over their data and privacy. Services are now offered as a result of the scattered storage of the data and the absence of reliance on centralised servers. Peer-to-peer technology is used to operate a decentralised OSN, with each node supporting the service and maintaining a share of the data.

A breakthrough idea in the field of social media is an autonomous, decentralised, Blockchain-based online social network. Traditional social networks have been dominated by centralised platforms, where members' personal information and content are under the control of a single organisation, frequently raising issues about privacy, censorship, and manipulation.

The adoption of blockchain technology also guarantees tamper-proof content and reliable moderation processes. The decentralised structure of blockchain networks enables community-driven content curation, where participants jointly validate and rank contributions, as opposed to depending on a centralised organisation to control and filter material. This creates a setting that promotes real involvement, inhibits bogus news, and lowers the possibility of censorship.

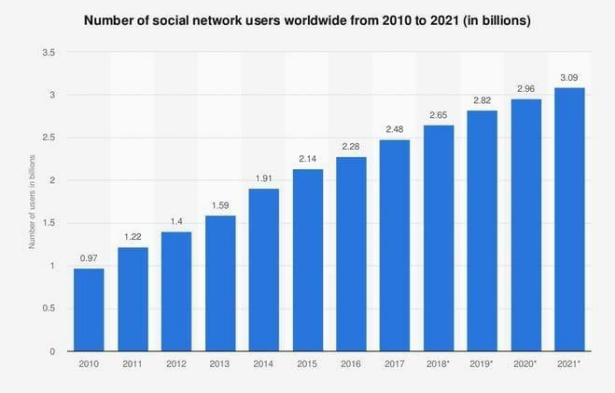

Figure 1 Social Network Users 2010 to 2021

A breakthrough idea in the field of social media is an autonomous, decentralised, Blockchain-based online social network. Traditional social networks have been dominated by centralised

platforms, where a single organisation controls user personal information and content, raising issues with privacy, censorship, and manipulation frequently.

A social network created on a blockchain, however, is decentralised, which means that it isn't run by a single organisation. Instead, to maintain the integrity of the network, a group of users works together to validate transactions. The network's security, transparency, and censorship resistance are all increased by this decentralisation.

An autonomous social network is one that follows a set of established norms that are upheld by self-executing computer programmes known as smart contracts that run on the blockchain. These smart contracts make the network more dependable and predictable by ensuring that it adheres to a set of predetermined rules.

All things considered, a blockchain-based autonomous decentralised online social network has the ability to provide users more control over their data and content while also allowing them to engage in a more open and democratic social network. This innovative idea has the potential to revolutionise how we communicate online.

2. LITERATURE REVIEW

Websites may work together to identify credential stuffing on certain user accounts, according to a strategy outlined in the research by Kee Coby Wang [1] and colleagues. To differentiate between legal login behaviour (such as password reuse, entering the correct credentials into the incorrect websites, etc.) and credential stuffing, our detection engine employs cutting-edge anomaly detection while closely monitoring suspect logins. Websites collaborate utilising an innovative secret membership test methodology to prevent the disclosure of password information. Because it uses cuckoo filters, this protocol is highly scalable and, in a fundamental sense that we specify, is more secure than comparable options.

With a peer-to-peer version of electronic currency, S. Nakamoto [2] shown in their paper that online payments may be done directly from one party to another without going through a banking organisation. Digital signatures help with the problem in some ways, but the main benefits are lost if a trustworthy third party is still required to prevent double spending. A peerto-peer network is what we provide as a remedy for the double-spending problem. The network timestamps transactions by hashing them into a continuous chain of hash-based proof-of-work, generating a record that cannot be changed without repeating the proof-of-work. The longest chain gives evidence for the sequence of events seen as well as the origin of the most CPU power.

In their essay Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich introduced the Argon2 new hash function in their study [3]. Low-entropy secrets can be protected with this method without the use of secret keys. On a typical PC, it runs extremely quickly, but for users who desire to conserve memory, it imposes prohibitive time-memory and computation-memory tradeoffs. Additionally, a certain amount of RAM is needed, which is configurable.It is possible to provide total ASIC- and botnet-resistance by populating the memory in 0.6 cycles per byte using a non-compressible approach.

Concerning the technology that allows for the breach of online users' privacy in their study, Justin Bayan [4] presented recommendations in their article. The design of my "Anonymizer" system, which prevents these invasions of privacy, is then described. Users can maintain their privacy without having to wait for new legal or technical restrictions. In order to conclude, I'll assess the most recent advancements in web privacy.

3. PURPOSE

To give users more privacy, security, and control over their personal data, an independent, decentralised, blockchain-based online social network is being developed. Security and discretion is a network that makes use of blockchain technology to provide enhanced privacy and security features. Users retain ownership of their data, and the decentralised nature of the network reduces the likelihood of security lapses or unauthorised access. Users control and own their data in a social network built on the blockchain. They

have complete control over the information they provide and with whom, and they can always refuse access to their data. People now have more control over their online behaviour because to this.Social networks built on the blockchain frequently contain systems for decision-making and community governance. Users can vote on significant choices, suggest modifications, and participate in the network's development. This guarantees a platform that is more democratic and open.Some social networks built on the blockchain include a native coin or token.

This coin can be used to reward quality content, encourage peer-to-peer exchanges on the platform, and encourage users to contribute to the network. Blockchain-based social networks can make it possible for various platforms and applications to communicate with one another. Users are free to move their information and profiles freely between other decentralised social networks, encouraging an online ecosystem that is more open and linked. Traditional social networks frequently rely on data exploitation and targeted advertising for money. Alternative business models, like user-centric ones where users have ownership over their data and can decide to take part in data-sharing or targeted advertising on their terms, can be investigated in a blockchain-based network. A blockchain-based autonomous decentralised online social network's overall goal is to give users more privacy, control, and autonomy over their data and online activities while developing an online community that is more democratic and transparent.

4. METHODOLOGIES

A blockchain-based autonomous decentralised online social network needs to be properly designed while taking into account a number of technological and social factors. The important steps that can be taken to develop such a network include the ones listed below.

Identify the use case, Name the desired use case(s) for the social network. This might apply to social networking, content sharing, blogging, and any other online community that requires a decentralised, independent, and safe platform. Select a suitable blockchain. Select a blockchain that can provide the functions and features the social network needs. This may require the ability to create and manage smart contracts, provide rapid and scalable transactions, and ensure data protection and confidentiality. Put smart contracts together Create smart contracts that outline the rules and logic of the social network. This includes user engagement incentives, content filtering, and the network's governance structure. Design of user interfaces Make an intuitive and user-friendly user interface so that individuals can interact with the network with ease.

This category may include features like messaging, notifications, and user profiles. On the chosen blockchain platform, build the network and use it, making sure it can support a large number of users and transactions. Once the social network is operational, launch it and then thoroughly test it to ensure everything is operating as it should. This includes testing for usability, scalability, and security. By gathering user feedback and incrementally modifying the smart contracts and user experience, the social network can be improved. This will ensure that the network will become more effective and relevant over time.

4.1. Existing System:

Today, 80% of people use online social networks to communicate with friends and family, get news, and share their ideas. All social network programmes save user sign-up and post information on centralised servers, thus if one of those servers crashes, services to users would be disrupted and data will be lost. If a server is compromised, the privacy of all users' data will be in jeopardy because the attackers could use it for anything.

Disadvantages:

Centralised social networks may offer connectivity and convenience, but they also come with some significant disadvantages, such as problems with fake accounts and dishonest behaviour, a lack of control and ownership, a concentration of power, addiction and mental health problems, and concentration of power. Users of social media platforms should be aware of these limitations and adopt the appropriate safeguards to protect their privacy and welfare while using these platforms.

4.2. Proposed System:

We offered a blockchain-based architecture in this system for decentralised, autonomous online social networks. A secure peer-to-peer network where members can trade private keys and have unique identities can be provided by blockchain. The private key has the most control over the corresponding account and is stored on the user's own device. In order to prevent fraud, every blockchain transaction must also be signed by the private key.A decentralised autonomous mechanism powered by blockchain is incorporated into the system architecture to give the system the ability to control itself and evolve sustainably.It is incredibly challenging to crash or hack the user's data because the user's to and from addresses are encrypted in the server and the tweet as well.

Advantages:
Distributed online social networks offer a number of benefits in terms of user privacy, data control and administration, censorship resistance, accessibility, connectedness, collective control, and adaptability. These advantages promote a more user-centric, inclusive, and empowering social media experience where users have greater freedom, control, and ownership over their data and online presence.

System Architecture
The basic rough architecture diagram can be represented with the following figure 2.

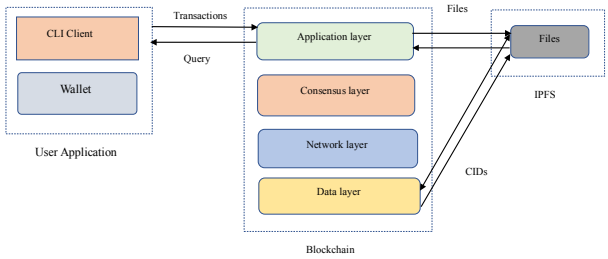

Figure 2 System Architecture

Figure 2 depicts the whole system's structure. The system consists of three parts; on the user side, the wallet, command-line interface (CLI) client, and user application enable user interaction with the system. The blockchain component is in charge of running the OSN service and DAO. Additionally, IPFS is used to store a lot of data with no concern for security.

1. User Application
User interfaces are frequently provided by blockchain user applications, which enable users to interact with the blockchain network by submitting transactions, managing cryptographic keys, setting up and controlling user accounts, and more. These applications may also have user-friendly graphical user interfaces (GUIs) or command-line interfaces (CLIs) to facilitate user interactions with the blockchain network.

2. Blockchain
The blockchain, which provides the underlying technology and concepts, plays a crucial role in the architecture of the blockchain by enabling a decentralised, open, secure, and immutable record system. It consists of encryption, network protocols, smart contracts, consensus processes, incentives for consensus, and data structures. These elements work together to create a reliable blockchain network.

3. IPFS
IPFS can play an important role in blockchain architecture by providing decentralised storage, content addressing, efficient data sharing, off-chain data storage, and help for the development of decentralised apps. By utilising IPFS, blockchain networks can overcome storage and sharing constraints while enhancing their decentralisation, security, and resilience.

4. Publish Tweets

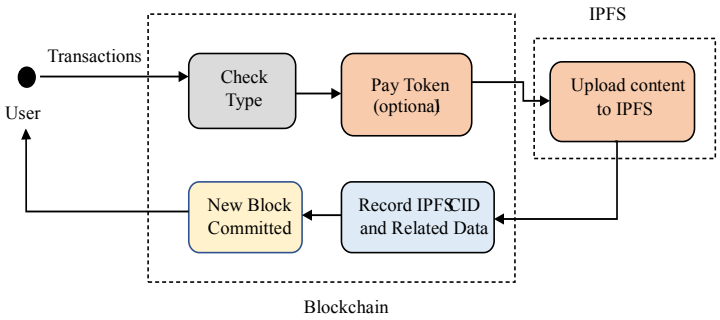

Figure 3 Publish a tweet

Figure 3 illustrates how a user publishes a tweet. Users can send a transaction relating to publishing a tweet by using the CLI client. The blockchain first confirms the transaction type to make sure it is a publishing tweet action when it gets a transaction.

The user is then automatically charged a predetermined amount of tokens to stop resource misuse and spam tweets. Following the posting of the tweet's content to IPFS, the CID and any associated data, including the user's address, the tweet's title, and the amount of gas used, are recorded in the blockchain for subsequent retrieval. The publishing process is complete and the user receives the result once the nodes have committed the transaction. For administrative purposes, each tweet has a hash ID that uniquely identifies it in the blockchain.

Blockchain Technology

Blockchain technology is used to provide a transparent and safe platform for users to connect and share information without depending on a centralised authority in a blockchainbased autonomous decentralised online social network. The usage of blockchain technology in these networks can be summarised in the following fundamental ways:

Every node in the social network holds a copy of the blockchain and functions as a decentralised network of computers known as a node. As a result, there is no longer a requirement for a central server or authority, which makes sure that no one organisation has control over the network. A block in the blockchain is created for each engagement or transaction on the social network, including posting content, liking, and commenting. By connecting these blocks in a chronological manner, an immutable record of all activities is produced. Users can confirm the accuracy of the information by using this transparency, which also protects the integrity of the data.

Users are empowered by blockchain-based social networks because they have complete control over their data and content. Users have ownership over their personal information and have the option to grant or revoke access to others. This measure stops centralised platforms from using unauthorised data mining or exploitation. Blockchain networks encrypt user data and communications using cryptographic methods. While using the network, users can keep pseudonymous identities to safeguard their privacy. Security is improved through encryption techniques, which make sure that only authorised parties can access particular information.

Social networks built on blockchain rely on consensus techniques like Proof of Work (PoW) and Proof of Stake (PoS) to ratify and approve the content and transactions uploaded to the blockchain. These controls guarantee the network's decentralised and reliable operation. To encourage user engagement and contributions, some blockchain-based social networks create their own native tokens or coins. For actions like producing valuable material, interacting with others, or rendering beneficial services, users can earn tokens. These tokens can be traded, exchanged for other digital assets, or used within the network itself.

Blockchain networks are naturally resistant to censorship because of their decentralised structure. Social network content cannot be readily altered or withdrawn by a single authority. This function encourages free speech and guards against the possibility of centralised management of information flow. These autonomous, decentralised online social

networks hope to promote trust, user autonomy, privacy, and security while eliminating dependency on central authority or intermediaries by utilising blockchain technology.

Implementation

Today, 80% of people use online social networks to communicate with friends and family, get news, and share their ideas. All social network programmes save user sign-up and post information on centralised servers, thus if one of those servers crashes, services to users would be disrupted and data will be lost. If a server is hacked, the security of all users' data will be at jeopardy since attackers could misuse the data of all users.

Moving all social media programmes to decentralised (data will be preserved at multiple nodes or servers) Blockchain servers is the idea put up by the paper's author as a solution to the issues. Each piece of information or transaction will be saved in a block, and the blockchain will validate the hash codes of all previously stored blocks across all active nodes before saving any new blocks. Only new blocks will be added if all prior block hash codes are validated; if any node verification fails, information will be obtained from other live nodes, and the attacked system will be restored. Because no attacker has ever been able to modify any blocks, blockchain is viewed as being immutable.

By using Blockchain, OSN networks can retain data across many nodes and eliminate the possibility of server failure and hacking. Because the author of the article suggests utilising Blockchain to store social media postings, all large content, including as movies and photos, will be saved at IPFS (inter planetary file system) servers. Because of this transaction/block hash code verification and immutable data storage, blockchain is widely regarded as being safe and dependable in the business.

Dataflow Diagram

In terms of the data that is input into the system, the various processing operations that are carried out on this data, and the output data that is created by this system, DFD is a simple visual formalism that may be used to represent a system. The data flow diagram (DFD) is one of the most important modelling tools. It is used to represent the system's component parts. These components include the internal operations of the system, the data supporting those operations, a third party using the system, and the information flows inside the system. DFD illustrates the different transformations that are applied to data as it moves through the system. It makes use of images to demonstrate how data is modified and how it moves from input to output.

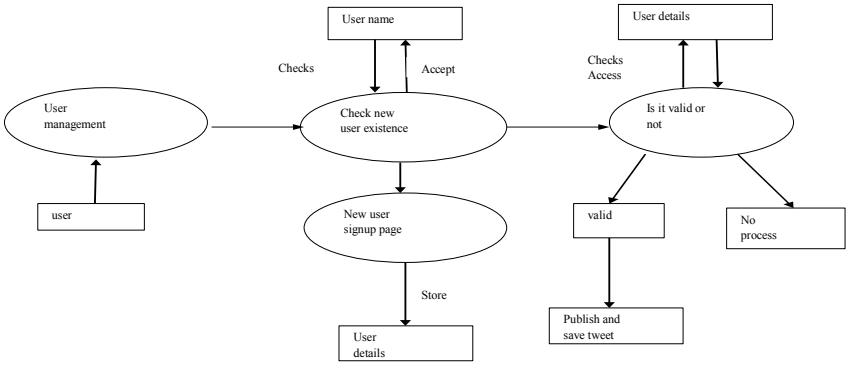

Figure 4 Dataflow Diagram

5. RESULTS

The outcomes of are as follows: Implementing an independent, decentralised, blockchainbased online social network has the potential to increase community governance, censorship resistance, user privacy, and empowerment, among other things. It might need widespread adoption and run into technical issues in order to achieve its goals.

Figure 5 User Login Screen

In the above screen user need to login the account by entering credential like username and password.

Figure 6 Post Tweet Screen

In the above screen user can enter post message and then upload post related image and then click on 'Open' and 'Submit' button to save post data in Blockchain and get below output

Figure 7 Output Screen

In the above screen all users can see one and other tweets with all post details and images.

6. CONCLUSION

A blockchain implementation for OSN is demonstrated in this paper. Users preserve their security information in their own possession to avoid security information leaking from centralised systems. Due to its decentralised nature, users do not have to worry about a centralised body crashing the social network service. A DAO also gives each member the ability to independently run their social network. Without a centralised leader, an OSN can continue to grow. The blockchain technology employed in this project not only provides OSN with a decentralised environment but also permits users to autonomously manage their social networks.Finally, blockchain-based autonomous systems have the ability to completely change how we communicate and distribute information online. These networks seek to overcome important problems with traditional centralised social media platforms including privacy, data ownership, and censorship resistance by utilising blockchain technology. The lack of a centralised organisation in charge of user data is one of the main benefits of social networks powered by

blockchain technology. Instead, information is dispersed and kept in a decentralised network of nodes, ensuring openness and lowering the possibility of data breaches and unauthorised access. Without relying on a centralised platform, users have more control over their data, choosing what information to disclose and with whom.

The opportunity for monetization and incentive is a further important advantage. Token economies are frequently used in blockchain-based social networks, where individuals are compensated with tokens for their contributions to the network, such as producing content, curating data, or offering worthwhile services. Bypassing conventional advertising-based income methods, this incentivization strategy enables users to directly monetise their contributions while encouraging active involvement and improving content quality.Additionally, by offering encrypted protocols and decentralised identity systems, blockchain-based social networks improve user privacy. Users can keep pseudonymous or anonymous profiles, which lowers the chance of personal information being exposed and promotes free speech without concern for repercussions.In conclusion, while autonomous, decentralised, blockchain-based online social networks present interesting alternatives to the shortcomings of centralised platforms, their development and uptake are still in their infancy. To overcome the difficulties and fully realise the potential of these networks, additional study, technology breakthroughs, and user adoption are required.

Future Enhancements

A user-friendly interface will be developed to replace CLI clients because they are less than optimal for regular users going forward. Since a public IPFS network will be utilised in this project, a private IPFS network will be built to boost data security. Since the simulation method can employ tokens to motivate users to produce more valuable content to OSN and invest their time in the autonomy component, it will be necessary for the continued development of the autonomous part. Users may decide what data they wish to share and with whom thanks to blockchain technology, which gives them total control over their data. Users have more control over their privacy settings and can keep ownership of their data with a decentralised social network, which lowers the possibility of data breaches and unauthorised use of personal information. Strong security measures are offered by blockchain's cryptographic algorithms, which can shield user data from hacking and unauthorised access. Attackers find it harder to penetrate the network by decentralising data storage and encryption. The increased security might contribute to user confidence and trust. Traditional social media platforms are centralised, which means that a single organisation or authority controls them. A decentralised social network, in contrast, lacks a central point of control and runs on a distributed network of nodes. By removing the possibility of censorship, algorithm manipulation, and biassed content moderation, users are given access to a platform that is really democratic and impartial. Blockchain's decentralised structure enables more effective procedures for content verification and fact-checking. The immutability and transparency of blockchain can be used to promote reliable material, fight fake news, and track down the source of information. This may result in a setting where information sharing is more trustworthy and credible.

7. REFERENCES

1. J. Blocki, B. Harsha, and S. Zhou. On the economics of offline password cracking. In 39th IEEE S&P, May 2018.
2. Biryukov, D. Dinu, and D. Khovratovich. Argon2: New generation of memory-hard functions for password hashing and other applications. In 1 st IEEE Euro S&P, March 2016.
3. M. Bartsch, T. Dienlin, in: Control your facebook: an analysis of online privacy literacy, 56, Elsevier, 2016, pp. 147–154.
4. M. Qamar, M. Malik, S. Batool, S. Mehmood, A.W. Malik, A. Rahman, Centralized to decentralized social networks: factors that matter, in: Managing and Processing Big Data in Cloud Computing, IGI Global, 2016, pp. 37–54.
5. S. Taheri-Boshrooyeh, A. Kupcu, O. Ozkasap, Security and privacy of distributed online social networks, in: Proceedings of Distributed Computing

Systems Workshops (ICDCSW), IEEE, 2015, pp. 112–119.

6. N.B. Ellison, D. Boyd, Sociality through social network sites, in: The Oxford Handbook of Internet Studies, Oxford University Press, 2013, pp. 151–172.
7. H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh. Kamouflage: Loss-resistant password management. In ESORICS, volume 6345 of LNCS, September 2010.
8. A. S. Brown, E. Bracken, S. Zoccoli, and K. Douglas. Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 2004.
9. J. Boyan. The Anonymizer: Protecting user privacy on the web. Computer-Mediated Communication Magazine, 4(9), September 1997.
10. S.D. Warren, L.D. Brandeis, The right to privacy, Harv. Law Rev. 4 (5) (1890) 193–220.