International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Blockchain Based Social Media

Rumeet Singh Kohli
Department of Information Technology
Maharaja Agrasen Institute of Technology, India

Dr. ML Sharma
Department of Information Technology
Maharaja Agrasen Institute of Technology, India

Dr. KC Tripathi
Department of Information Technology
Maharaja Agrasen Institute of Technology, India

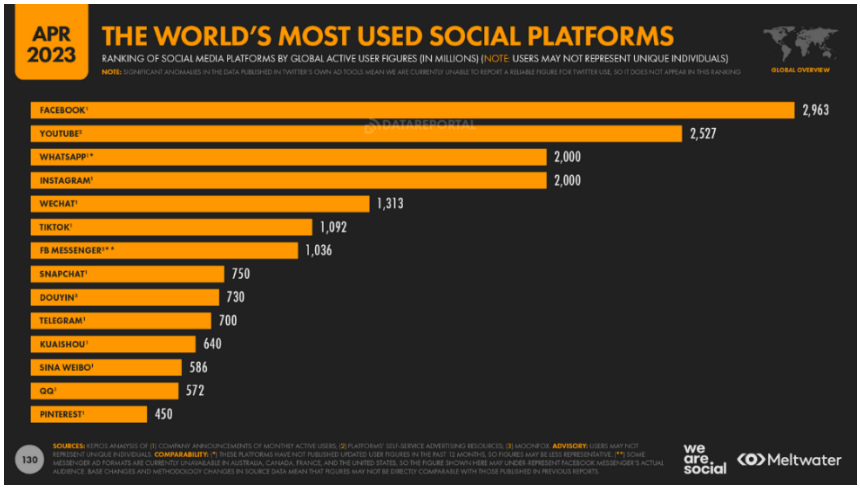
Abstract

Social media sites are becoming more common in people's life. All popular social media sites are centralized which results in privacy and security issues. A decentralized architecture based on blockchain technology is more secure and private. In this paper, a social media based on blockchain technology is created and operated in decentralized manner. Blockchain is not capable of storing large amounts of data; hence, IPFS is used.

Keywords - Blockchain, Social Media, Decentralized

I. Introduction

Social media is a platform for people to build connections and interact with other peoples via the use of internet. It is a major platform that the public can obtain information, exchange views, and share their opinions on it. Hence, Social media platforms have been major sites where the users accessing the internet spend their time on.



Most of the social media platform are centralized, i.e., any data uploaded by the user is owned by the company and could be misused. The companies also make their users accept terms or conditions to use their services which includes collection of users data to serve them advertisements. Due to centralization, the user data is uploaded on companies' servers which cannot be accessed or can be deleted if the company shut downs. If the companies' servers are hacked, the private information of many people using the sites might leak. This can lead to abuse of users' personal information. Such problems faced by users in centralized social media lead to the decentralization of the social media platforms.

Decentralized social media provides more secure environment to the user accessing the platform. The users can control their data because the data is stored in a distributed form and is not stored on a central server. A decentralized platform is most often using the peer-to-peer mechanism where every node stores some part of the data. The decentralized platform however is not foolproof can have malicious attacks.

In this paper, we have introduced a decentralized social media platform based on blockchain technology. Blockchain is peer-to-peer mechanism where every user has unique identification and private keys. The private key is kept on the user's own device and has the most power over the related account. Moreover, every blockchain transaction in order to prevent fraud, documents must be signed using the private key. The design incorporates a decentralised autonomous mechanism driven by blockchain to offer the system the ability to regulate itself and evolve sustainably. The remainder of this essay is structured as follows. The history of the linked technologies employed in this design is presented first. Second, a thorough explanation of the architecture is covered. The project's functions are displayed in the third section. Finally, a decision is reached.

II. BACKGROUND

Blockchain is viewed as a ground-breaking technology with the potential to fundamentally alter how people live their lives. The first fully developed blockchain implementation is Bitcoin, which debuted in 2008. It is a decentralised public cryptocurrency that does not rely on any centralised authority, and all its operational guidelines are outlined in its source code.

The blockchain has a unique data structure that sets it apart from other database systems; it is made up of several blocks. The first block is referred to as the genesis block, and all of its data is turned into a fixed-length hash value using a hash algorithm before being deposited in the second block. Following the completion of the second block's generation, a fix-length hash value is created from the data in the second block, which also contains the genesis block's hash value. This hash value is then ready to be stored in the third block. This procedure involves linking the blocks one at a time. Any changes to blocks will result in following block changes, which is distinct from the original blockchain since each block carries a hash

value of the previous block. Therefore, this character ensures that the data won't be changed once it is recorded on the blockchain and protects the blockchain from being tampered with.

A blockchain also includes encryption and consensus techniques to ensure that the blockchain is synchronised at every node. When a user produces a transaction on the user side, the contents of the transaction is encrypted using the user's private key, and the encrypted transaction is then verified by the nodes. Following that, the nodes attempt to reach consensus among themselves using a specific protocol, such as the Proof-of-Work (PoS) algorithm used by Bitcoin.

Once consensus is reached, the new block, which includes new transactions, is shared with other nodes and put to the blockchain. Using these strategies, the blockchain can maintain synchronisation across hundreds of nodes without depending on a centralised leader. This project employs blockchain technology to accomplish OSN functionalities like as account administration, tweet publishing, tweet commenting, and autonomization.

Tendermint is a blockchain platform comprised of two major technical components: the consensus engine, known as Tendermint core, ensures that the same transactions are recorded on each machine in the same order; and the application interface, known as the Application Blockchain Interface (ABCI), which allows transactions to be processed in any programming language. Tendermint works well in BFT state. therefore, it is suitable for this project. Tendermint was chosen for the consensus and network component of this project because it is an easy-to-use and high-performance blockchain platform. We can devote more time to building the application, user client, and autonomy strategy.

The decentralised autonomous organisation (DAO) is a virtual entity with a certain number of members or shareholders that may manage it using autonomous programmes such as voting to spend DAO cash and changing its code. The DAOs are created and run using blockchain and smart contracts; the decentralisation of blockchain ensures that the DAOs are not controlled by anybody.

DAOs are distinguished by three characteristics:

- A DAO's members should be defined clearly, including membership admission and departure mechanisms. Many DAO projects, for example, use tokens to identify their members.
- Because most DAOs rely on blockchain and smart contracts, the code about a DAO plays like law; every operation must be expressed as a set of executable code, run on the blockchain platform, to ensure the operation can be executed without any hindrance.
- There are no centralised decision-makers in DAOs; all choices should be taken once most DAO members agree. The decision rules are written in the DAO code, and the decision is carried out via the blockchain platform.

In this project, we use the Interplanetary Filesystem (IPFS) to store large amounts of data with low safety requirements. The majority of the data in IPFS is multimedia tweet content. IPFS is a distributed peer-to-peer data storage mechanism. IPFS data is disseminated over an open network of peers using a Kademlia-based distributed hash table (DHT) and is identified by a cryptographically created name called CID. IPFS is appropriate for blockchain-based apps [8, which may access data in IPFS through CID]. CID is a multihash value that is short and fixed in length, allowing the blockchain to keep blockchain data files small even when there are millions of CIDs recorded on the blockchain. Furthermore, the IPFS protocol is decentralised, which implies it fits the decentralisation criteria of the decentralised blockchain application.

III. ARCHITECTURE

The system is divided into three parts: the user application, the command-line interface (CLI) client, and the wallet, which are on the user side and allow users to interact with the system.

The blockchain component oversees the operations of the social media services. IPFS is utilised to store large amounts of data with low security needs.

Users can communicate with the blockchain via a command-line interface (CLI) Client in the user application section, and all security procedures like private key.

The wallet handles transaction processing, storage, and management. All security information, such as private keys, are saved on the user's own devices for this phase. This prevents security information from a centralised server from being leaked, which may occur with centralised OSNs.

Users have complete authority over this information, but they must also assume responsibility for their security information.

The system's fundamental component is the blockchain, which has four layers: the application layer, the consensus layer, the network layer, and the data layer.

All large volumes of data with modest security requirements are kept on IPFS. When a file is stored in IPFS, the associated address known as CID is sent back to blockchain so that it may be retrieved in IPFS when required.

IV. FUNCTIONALITY

To create a private key for the first time, each user who wishes to utilise this system must use the client. The private key is essential user security information that is used to sign transactions, validate user identity, and demonstrate account ownership.

Users need to complete a transaction to publish the data to the site. When a transaction is received on the blockchain, a fixed number of tokens are first distributed once the transaction's nature and publishing

action have been verified. The tokens are deducted from the user automatically to stop resource abuse and spam tweets. The tweet content is then posted to IPFS, and the CID and related information (such as the user's address, the title of the tweet, and the amount of gas consumed) are stored in the blockchain for later retrieval. Once the nodes have committed the transaction, the publishing procedure is finished, and the user receives the outcome. Each tweet has a hash ID to uniquely identify it in the blockchain for administrative purposes.

The process for posting comments is like that for posting content. However, when users send a transaction for commenting, they must provide the hash ID of the tweet that they wish to comment on. Following the successful publication of the remark, a mapping is added to the associated tweet to identify the comment based on the comment hash ID.

Users can upvote the tweets they like or downvotes the ones they don't. This method can be carried out by sending a tweet or a vote transaction in a remark. This may demonstrate a user's involvement with the social network.

Users can use the site to read a tweet or comment through the site because each tweet or comment has a distinct hash ID. Since the reading process uses almost minimal system resources, it is quick and does not require a transaction.

V. CONCLUSION AND FUTURE WORK

This paper is an implementation of blockchain based social media. Users have full control over their data due to blockchain being decentralized. The blockchain technology provides a decentralized environment and users can take benefit of the all the advancements it brings.

For Future Work, we can implement more security measures like using a private IPFS instead of publicly available ipfs api. The simulate strategy will be required for autonomous part's ongoing development since it can use tokens to encourage users to add more high-quality material to OSN and contribute their time to autonomy part.

REFERENCES

[1] V. Buterin, Ethereum White Paper - A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. 2014, p. 23

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Bitcoin.org, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[3] World's most used social platforms worldwide. Available: https://datareportal.com/social-media-users

[4] S. Henningsen, M. Florian and S. Rust, "Mapping the Interplanetary Filesystem", arXiv preprint, arXiv:2002.07747, 2020

[5] M. Di Silvestre, P. Gallo, M. Ippolito, E. Sanseverino, G. Sciume and G. Zizzo, "An Energy Blockchain, a Use Case on Tendermint", 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2018. Available: 10.1109/eeeic.2018.8493919.