Blockchain Based Atonomys De-Centralised Online Social Network

1. Adimulam Sumanth 2. Karubhukta Venu Manikanta 3. Arisenkala Ajay

4. Ripudaman Singh Nanra 5.Dr. K. N. S. Lakshmi, Head of the Department.

Department Of Computer Science Engineering,

Sanketika Vidya Parishad Engineering College, Visakhapatnam, India

Abstract—Online social networks (OSNs) have become integral to daily life, yet the prevalent centralized model of these platforms presents considerable challenges in terms of security, privacy, and management. In response to these concerns, a decentralized architecture underpinned by blockchain technology emerges as a promising solution. This paper delves into the development of an OSN service leveraging blockchain technology to facilitate decentralized operation, thereby addressing the aforementioned issues. Through the utilization of the Interplanetary Filesystem (IPFS), large volumes of low-security data are effectively decentralized, contributing to enhanced data integrity and accessibility. Furthermore, the establishment of a decentralized autonomous organization empowers users with greater autonomy, enabling democratic self-governance of the OSN. This innovative approach not only addresses existing shortcomings but also paves the way for a more resilient, transparent, and user-centric social networking paradigm.

I.INTRODUCTION

The Online Social Network (OSN) serves as a virtual platform where individuals establish connections and engage with one another via the internet. It has emerged as a pivotal medium through which the public accesses and disseminates information, exchanges perspectives, and shares life experiences. Research conducted by Chaffey [1] underscores the prominence of the most widely utilized OSNs globally (refer to Figure 1), highlighting the pervasive nature of engaging with OSNs as a prevalent online activity among internet users.

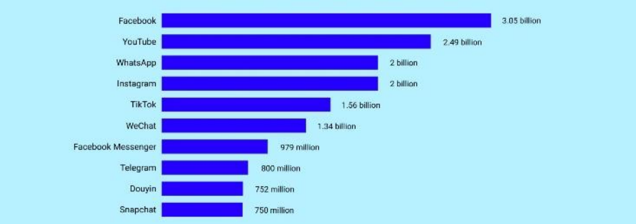

Figure 1. Most used social media platforms in the world

In contemporary times, the prevailing trend in Online Social Networks (OSNs) leans towards centralization, wherein OSN companies typically assert full ownership over user data and services. Users, in turn, are often required to consent to the terms of service dictated by these companies before accessing the platform. However, these agreements frequently grant OSN companies broad rights to utilize user data for personalized services, such as targeted advertising. Consequently, users who prioritize data privacy may find themselves navigating cumbersome opt-out processes or reluctantly forgoing the use of such OSNs altogether.

The inherent vulnerabilities of centralized OSNs have spurred researchers to explore the development of decentralized alternatives. Decentralized OSNs offer the promise of a safer and more user-controlled social networking environment, where privacy and data ownership are prioritized. By distributing data storage and eliminating reliance on centralized servers, decentralized OSNs mitigate the risks associated with centralized platforms.

Traditionally, decentralized OSNs operate on a peer-to-peer mechanism, wherein each node in the network stores a portion of the data and supports the provision of services. However, challenges persist in terms of addressing malicious activities and establishing mechanisms for self-management and sustainable development.

II.BACKGROUND

A. Blockchain

Blockchain technology is widely acknowledged as a transformative innovation with the potential to significantly reshape human existence. Its inception can be traced back to the release of Bitcoin in 2008, marking the first mature implementation of blockchain. Bitcoin, a decentralized public cryptocurrency, operates without reliance on any centralized entity. Participants in the network possess the freedom to join or exit at will, and all operational protocols are delineated within its source code [3]. With a staggering market capitalization of 218 billion US dollars as of August 24, 2020 [4], Bitcoin stands as the preeminent blockchain project, emblematic of the technology's widespread adoption.

Distinguished from conventional database technologies, blockchain boasts a distinctive data structure characterized by a chain of interconnected blocks. The inaugural block in this sequence, known as the genesis block, encapsulates all pertinent information, which is subsequently transformed into a fixed-length hash value through the utilization of cryptographic hashing algorithms. This resultant hash value is then embedded within the succeeding block. Upon the completion of each subsequent block, a new fixed-length hash value is derived from its constituent data, including the hash value of the preceding block, thus perpetuating the chain. Through this iterative process, each block becomes inherently linked to its antecedent. Crucially, the incorporation of hash values from preceding blocks ensures the immutability of the blockchain. Any attempt to alter the contents of a block would necessitate corresponding modifications to all subsequent blocks, thereby safeguarding the integrity of recorded data [5]. This intrinsic property of blockchain technology renders it resistant to tampering, thereby ensuring the permanence and integrity of stored data.

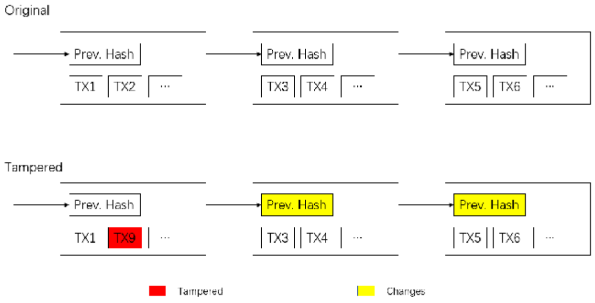

Figure 2. Difference between original and tampered blockchains

In addition to its inherent data structure, a blockchain incorporates encryption and consensus mechanisms to ensure synchronous operation across all network nodes. When a user initiates a transaction, the transaction data is encrypted using the user's private key. Subsequently, network nodes verify the encrypted transaction before collectively striving to achieve consensus through a predetermined protocol. For instance, Bitcoin employs the Proof-of-Work (PoW) protocol to facilitate consensus among nodes. Upon attaining consensus, the newly formed block containing the updated transactions is disseminated to other nodes and appended to the blockchain. Through the utilization of these methodologies, blockchain technology maintains synchronization across thousands of nodes without the need for centralized leadership.

Accordingly, this project harnesses blockchain technology to implement various functionalities of the Online Social Network (OSN), encompassing account management, tweet posting, comment submission, and user autonomy.

B. Tendermint

Tendermint is a comprehensive blockchain platform comprising two primary technical components: the consensus engine, known as Tendermint Core, and the application interface, referred to as the Application Blockchain Interface (ABCI). Tendermint Core is responsible for ensuring that identical transactions are recorded on every machine in the same sequential order, thereby maintaining consistency across the network. On the other hand, the ABCI allows transactions to be processed in any programming language, providing flexibility and compatibility for developers [6].

Tendermint exhibits robust performance even in Byzantine Fault Tolerant (BFT) scenarios, where up to one-third of the nodes may fail arbitrarily [5]. This inherent resilience makes Tendermint a secure and reliable choice for the present project.

C. Decentralized Autonomous Organization (DAO)

The concept of a Decentralized Autonomous Organization (DAO) is central to fostering autonomy within the system. A DAO represents a virtual entity wherein members collectively govern operations through autonomous programs, including voting and code modification [7]. These organizations operate on blockchain platforms, leveraging smart contracts to ensure decentralization and autonomy. Key characteristics of DAOs include clearly defined membership criteria, often utilizing tokens for identification purposes. Additionally, DAO operations are governed by executable code on the blockchain, effectively treating the code as law within the organization. Decentralized decision-making is another hallmark feature, necessitating agreement among the majority of members for major decisions, all of which are executed on the blockchain. Thus, within this project's framework, the implementation of a DAO serves as a mechanism for promoting autonomy and self-governance, operating seamlessly within the blockchain infrastructure.

D. Interplanetary File System (IPFS)

In this project, the Interplanetary File System (IPFS) is employed to store large-volume data with low-security requirements, primarily multimedia tweet content. IPFS functions as a decentralized protocol for distributed peer-to-peer data storage. Utilizing a Kademlia-based distributed hash table (DHT), data is distributed among an open network of peers and accessed through cryptographically generated Content Identifiers (CIDs). IPFS seamlessly integrates with blockchain-based applications, allowing direct access to data via CIDs. With CIDs being small and fixed-length multi-hash values, IPFS ensures efficient storage within the blockchain while meeting decentralization requirements.

III. ARCHITECTURE

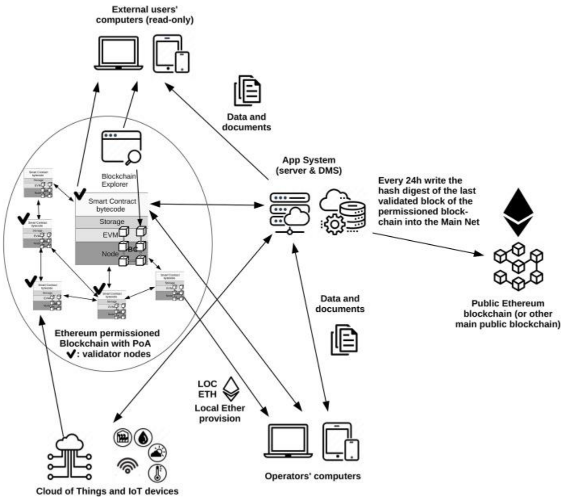
External users' computers (read-only)
Data and documents
Blockchain Explorer
Smart Contract bytecode
Storage
EVM
BC
Node
App System (server & DMS)
Every 24h write the hash digest of the last validated block of the permissioned block-chain into the Main Net
Public Ethereum blockchain (or other main public blockchain)
Data and documents
Ethereum permissioned Blockchain with PoA
✓: validator nodes
LOC ETH
Local Ether provision
Cloud of Things and IoT devices
Operators' computers

Figure 3. System architecture

In Figure 3, the structure of the entire system is depicted, comprising three distinct components. The user application segment encompasses the Command-Line Interface (CLI) client and wallet, situated on the user's side to facilitate interaction with the system. These user-facing elements serve as interfaces through which users can engage with the system's functionalities.

The blockchain component assumes responsibility for overseeing the operations of the Online Social Network (OSN) service and the Decentralized Autonomous Organization (DAO). Within this segment, the blockchain infrastructure serves as the backbone of the system, orchestrating the execution of OSN-related tasks and facilitating the governance mechanisms of the DAO.

A. User Application

Within the user application segment, a Command-Line Interface (CLI) Client is provided to enable users to interact seamlessly with the blockchain. Concurrently, all security-related operations, such as private key storage and management, as well as transaction signing, are handled by the wallet component. Placed squarely on the user's side, this setup ensures that critical security information, including private keys, remains securely stored on users' own devices. By decentralizing the storage of security information, the risk of security breaches commonly associated with centralized OSNs is mitigated. This approach affords users full control over their security information, thereby minimizing the likelihood of unauthorized access or data breaches. However, users must assume responsibility for safeguarding their security information to ensure the integrity and confidentiality of their data.

B. Blockchain

At the heart of the system lies the blockchain, comprising four integral layers: the application layer, consensus layer, network layer, and data layer. Leveraging Tendermint for this purpose, the consensus, network, and data mechanisms are seamlessly integrated as part of the blockchain infrastructure. Tendermint handles these layers directly, providing a robust foundation for the system's operations. Meanwhile, the application layer is custom-built in Golang to accommodate the specific requirements of the Online Social Network (OSN) service and Decentralized Autonomous Organization (DAO) operations.

C. IPFS

As previously mentioned, the Interplanetary File System (IPFS) serves as the repository for large-volume data with low-security requirements. Upon storing a file in IPFS, a corresponding address known as a Content Identifier (CID) is generated. This CID is then relayed to the blockchain, enabling retrieval of the file from IPFS when necessary. By leveraging IPFS for data storage, the system ensures efficient and decentralized access to large data sets, enhancing scalability and resilience.

IV. FUNCTIONALITY

A. Initial Setup

The initial setup process for users of this system begins with the utilization of the Command-Line Interface (CLI) client to generate a private key upon their first interaction. This private key serves as crucial security information, enabling users to sign transactions, authenticate their identity, and assert ownership of their accounts. The private key is encrypted using the ED25519 encryption algorithm for enhanced security. Subsequently, the private key file is stored in the same directory as the CLI client, ensuring convenient and secure access for users.

B. Publish Tweets

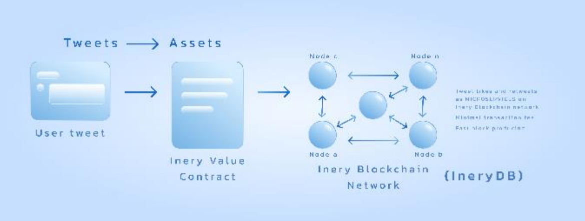

Figure 4. Publishing a tweet

Figure 4 illustrates the tweet publishing workflow within the system. Users initiate a tweet publishing transaction via the CLI client. Upon receipt, the blockchain verifies the transaction type and deducts tokens to deter spam. The tweet content is uploaded to IPFS, and its CID and metadata are recorded in the blockchain. Once validated by network nodes, the tweet is assigned a unique hash ID for identification and management.

C. Publish Comments

The process of publishing comments mirrors that of publishing tweets (Figure 4). However, users must specify the hash ID of the tweet they wish to comment on when submitting a transaction for commenting. Once the comment is successfully published, a mapping is added to the relevant tweet to associate it with the comment using the comment hash ID. This streamlined workflow ensures seamless integration of comments within the system, enhancing user engagement and interaction.

D. Vote Tweets and Comments

Users can upvote or downvote tweets and comments based on their preference. This action is executed by sending a transaction to vote on a tweet or comment, enabling users to contribute to the social network by expressing their opinions and preferences.

E. Read Tweets or Comments

Each tweet or comment is assigned a unique hash ID, allowing users to retrieve specific content using the CLI client. This reading process is efficient and incurs minimal system resource consumption, ensuring swift access to content without requiring users to expend tokens. Consequently, users can effortlessly navigate through tweets and comments, enhancing their overall experience within the network.

F. DAO structure

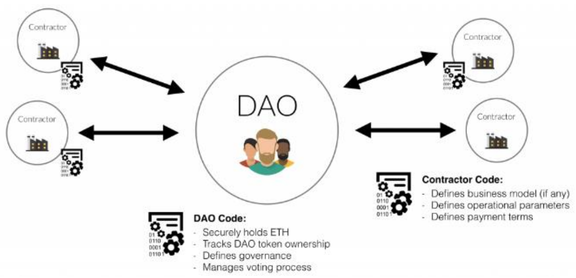

Figure 5. Structure of DAO organization

Figure 5 illustrates the organizational structure of the Decentralized Autonomous Organization (DAO), comprising two key entities: the management team and users. The management team, comprised of selected individuals from the user base, is responsible for overseeing tweets and comments management, including the deletion of illegal content and proposing changes to DAO operation rules. Users participate in the selection process to choose members of the management team. Additionally, any proposed changes to DAO operation rules must undergo user voting for approval.

G. Tweets and Comments Management

Members of the management team have the authority to propose the deletion of illegal tweets or comments. Subsequently, other team members can review the proposal before voting to accept or reject it. If the number of accepted votes exceeds the specified threshold during the voting period, the proposal is automatically accepted and executed. Conversely, if the proposal fails to garner sufficient acceptance votes, it is automatically rejected. This structured approach ensures transparent governance and decision-making within the DAO, facilitating effective management of tweets and comments while upholding community standards and regulations.

H. Selection

Selection occurs automatically at predefined intervals on the blockchain. Users have the opportunity to vote for candidates by creating proposals in their name. Once the selection process concludes, new members of the management team are appointed according to established autonomy rules.

I. Impeach

In instances where a member of the management team engages in misconduct, users retain the right to initiate impeachment proceedings by creating a relevant proposal. To prevent abuse, each user is allocated a limited number of impeachment chances. Impeachment proposals are subject to a vote by all users within the OSN community.

J. Autonomy Rules

Members of the management team possess the authority to propose changes to autonomy rules. These changes may pertain to various aspects, such as the number of team members, tenure duration, voting procedures, and impeachment protocols. Proposals for autonomy rule changes require approval through a community-wide vote, with a high agreement ratio prerequisite for acceptance. This democratic process ensures that significant alterations to governance protocols align with the consensus of the OSN user community.

V. CONCLUSION AND FUTURE WORK

This paper presents an implementation of blockchain technology within Online Social Networks (OSNs), focusing on user empowerment, decentralization, and self-governance. By allowing users to retain control over their security information, the system mitigates the risk of data breaches associated with centralized servers. Moreover, the decentralized nature of the social network service eliminates concerns regarding service disruptions caused by centralized entities. The inclusion of a Decentralized Autonomous Organization (DAO) empowers users to collectively self-manage the social network, fostering sustainability without reliance on centralized leadership. The blockchain implementation not only facilitates a decentralized OSN environment but also enables decentralized management of the network by its users.

For future endeavors, enhancing user experience is paramount, with plans to develop a more user-friendly interface to replace the Command-Line Interface (CLI) clients. Additionally, efforts will be directed toward bolstering data privacy by establishing a private IPFS network. In the autonomy realm, simulation plans will be explored to incentivize users to create high-quality content within the OSN and actively participate in the autonomy processes, potentially through token-based incentives. These initiatives aim to further advance the decentralization and user-centric principles embedded within the OSN framework, paving the way for a more robust and inclusive social networking ecosystem.

REFERENCES

[1] D. Chaffey, "Global social media research summary 2020 | Smart Insights", Smart Insights, 2020. [Online]. Available: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/. [Accessed: 03- May[2020].

[2] L. Constantin, "Credential stuffing explained: How to prevent, detect and mitigate", CSO Online, 2019. [Online]. Available: https://www.csoonline.com/article/3448558/credential-stuffing-explained-how-to-prevent-detect-and-defend-against-it.html. [Accessed: 30- Apr- 2020].

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Bitcoin.org, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 16- Feb- 2020].

[4] "Cryptocurrency Prices: Coins Market Cap Live Coin Prices for All Coins", Blockonomi. [Online]. Available: https://blockonomi.com/market-cap/. [Accessed: 24- Aug- 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.

[6] "What is Tendermint | Tendermint Core", Docs.tendermint.com, 2020. [Online]. Available: https://docs.tendermint.com/master/introduction/what-is-tendermint.html. [Accessed: 26- Aug- 2020].

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

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