Decentralised Social Media Platform Using Blockchain Technology

Farhan Ali Baig[1] , Hajera Zia[2] and Dr. Mohammed Abdul Bari[3]

UG Scholar[2,3], Head Of Department (CSE)[3]

Department Of Computer Science Engineering, ISL Engineering College, Hyderabad, Telangana

Abstract- Online social networks are becoming more and more prevalent in people's life, but they face the problem of privacy leakage due to the centralized data management mechanism. Evolvement of blockchain technology has greatly changed the network and it makes many applications to be distributed, decentralized without loss of security. Ethereum is an open-source blockchain platform that provides a runtime environment for running smart contracts, which is called Ethereum Virtual Machine (EVM). Ethereum-based applications are usually referred to as Decentralized Applications (DApps), since they are based on the decentralized EVM, and its smart contracts. By combining smart contracts, we use the blockchain as a trusted server to provide central control services. Blockchain helps us incentivise users of the platform with cryptocurrency as a reward for moderation. This is a decentralised application based on Ethereum blockchain built using solidity and react. In this paper, we examine how blockchain and incentivisation can enable more functionalities of traditional social network systems.

Keywords- *blockchain technology, decentralisation, Ethereum, smart contract, social media*

I. INTRODUCTION

Traditional social media networks essentially serve a central authority and are inherently vulnerable to external and internal threats.[1] These include privacy breaches, data leaks, poor moderation of the platform as a whole and censorship problems. While it works well enough for the most part it still suffers from its inherent weaknesses.

We implement blockchain technology to overcome these existing problems - A social media protocol based on blockchain and its features such as smart contracts.[2] Smart contract is essentially a block of code which acts as rules on the chain which is visible to all, and with increasing adoption of the blockchain [3] it is possible to create a decentralized social network which is much more secure than existing applications while maintaining transparency. Decentralized networks enable users to have more control and with the absence of a central figure it secures user data against selling of it by authority.

In this paper, we propose a social media application based on Ethereum platform [4] for recording data and use InterPlanetary File System (IPFS) [5] as distributed data storage service to support a decentralized application. The social media application uses a frontend webpage UI to interact with users and save users' information on blockchain while storing the larger file data in the IPFS system. The purpose of developing this application is to give an brief idea about how blockchain technology can be used to enhance the existing industry.

II. LITERATURE REVIEW

K A number of previous and current works have been working on developing decentralized applications with the use of IPFS or Swarm as distributed data store. We will discuss several applications that make use of these technologies and also work that we have been referring to for insights on development of DApps.

A. AKASHA project

Akasha [6] is another social media application developed using Ethereum and IPFS on dedicated blockchain. The Akasha team has found a suitable technology stack to implement a decentralized and distributed Internet after a lot of study and prototyping work. The cornerstones of the Akasha stack are IPFS and Ethereum, augmented by React with Redux, Node.js, and Electron. The Akasha project provides a guideline of how social media applications can be built with the merits of the blockchain system.

B. DesignCourse

They have provided detailed explanation on how to build a decentralized application with the use of Ethereum platform, web3.js library and ReactJs as the frontend. This provides a brief understanding of how these components can come together to build a successful DApp. Meanwhile, they also provide explanation for other concepts including IPFS system which is currently used in the social media application in this paper. They provide a lot of insights and tips on setting up a private blockchain and make the entire DApp works at a ready stat

B. Social Media, Content Moderation, and Technology

This paper develops a theoretical model to study the economic incentives for a social media platform to moderate user-generated content. The optimal content moderation strategy differs for platforms with different revenue models, advertising or subscription. They provide a platform's content moderation strategy depends on its technical

sophistication. Because of imperfect technology, a platform may optimally throw away the moderate content more than the extreme content. Therefore, one cannot judge how extreme a platform is by just looking at its content moderation strategy. Furthermore, we show that a platform under advertising does not necessarily benefit from a better technology for content moderation, but one under subscription does. This means that platforms under different revenue models can have different incentives to improve their content moderation technology.

III. PROBLEM STATEMENT

Social media has become a huge part of our lives. But centralized social media continues to breach our trust. While social media platforms may connect people better than any other service, it does so at a cost: it gathers troves of data on participants and uses that data to sell targeted advertising.

It's also crucial to talk about censorship, which has become a significant issue on traditional social media platforms. Due to their increased authority, providers can easily delete the posts, restrict the content, and ban users who share different views than theirs.

When a company uses centralized storage for user data, any breach of that system exposes enormous troves of data in one fell swoop. We've seen it happen to Facebook, Google+, LinkedIn, and many more companies that store our data this way. We're all vulnerable: every company, every organization, every individual.

IV. PROPOSED SYSTEM

Advances in Blockchain and distributed ledger technologies are driving the rise of incentivized social media platforms over Blockchains, where no single entity can take control of the information and users can receive cryptocurrency as rewards for creating or curating high-quality contents. Once the application is deployed on the blockchain, the network as a whole will always be able to serve clients looking to interact with it, which means zero downtime**.**

On one hand, traditional social media's popularity is increasing exponentially due to the heightened marketing and entertainment experience it offers to its users. However, on the other side, there are rising concerns over the data and privacy breaches to which these platforms are often associated.

Blockchain social media, with its decentralized and distributed networks, offers a plausible solution to such issues. Among other things, they enable users to assert greater control over their data.

WALLETS

Simply put, Web3 wallets are a way to use hardware or software not only to access funds, but to effortlessly allow you to interact with decentralized applications, serve as a gateway to bankless financial services, collect NFTs [7], create on-chain identity, collaborate with communities, and provide substantially more use cases beyond the scope of the traditional wallets we have today.

Just like how people have a physical wallet to store paper money, these wallets help store access to your digital currency instead. In addition, Web3 wallets are capable of storing digital assets such as NFTs and enable users to interact with Decentralized Apps (dApps). This is done all without the necessity of a middleman involved.

Wallets don't actually store the cryptocurrency, but they store the information required for access to your funds which are digital cryptocurrencies.

GAMIFICATION AND EXTRINSIC MOTIVATION

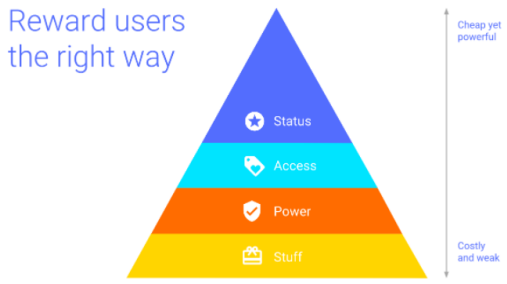
In the era of goldfish-like attention spans, user experience designers are turning to gamification to retain and incentivize users. Virtual swag such as badges and stickers can help increase the stickiness of a product. Badges introduce a sense of competitiveness among users, persuading them to level up and unlock the next badge.

This will help to deter mindless low-quality posting simply for the purposes of challenge completion. The culture of a social network is set from the very beginning, so it's imperative early challenges cultivate the right environment.

This gamification element creates many mutual benefits to both the platform and the user. Challenges can be set to reward content creation, post engagement, labelling content, expanding networks, curating profiles, expanding the user base and moderating the site. This will be particularly useful in early phases of growth to provide some intrinsic value to the platform while the user-base is low.

Points serve as indicators of achievement and progress. Points can reward users with status (if used to rank users against each other) or they can offer tangible rewards (for example, when converted to in-app currency or free items as part of a loyalty scheme).

Badges primarily serve to recognize a user's accomplishments. Badge systems in many apps and games also help align users to shared goals while acting as virtual status symbols, distinguishing badge-holders from others.



SYSTEM STUDY

A. Blockchain

Blockchain is a chain or list of blocks [8]. Each block in the blockchain has its own digital signature or cryptographic hash, which contains digital signature of the previous block, and it has data including state data and transaction data. Each block is generated within a specific epoch (i.e., period of time) and pointed towards its parent in the blockchain, forming a long chain of hashed blocks. Ethereum is a blockchain-based.

B. Ethereum Virtual Machine (EVM)

The Ethereum Virtual Machine is the component on the Ethereum platform that handles the deployment and execution of the smart contract. The EVM is a quasi-Turing complete state machine as all transactions on the EVM involve limit commands and change of the state values due to the gas limit given to the contract execution. EVM has a stack-based architecture, involving ROM, memory and account storage. They are used to store the state values as well as the contract program bytecode. EVM executes its own bytecode instruction set, which can be compiled from a higher level smart contract languages such as Solidity and Serpent. When a transaction involving state changes from contract functions, an EVM will be instantiated to load the program bytecode and execute the function and states will be updated upon successful execution of the transaction.

C. Smart Contract

A smart contract is a piece of program which runs on the blockchain and its execution is examined and enforced by the relevant consensus protocol. Smart contract is a special protocol designed to contribute, verify or implement the negotiation or performance of the contract. Smart contracts allows automatic execution of transactions without any supervision from third parties. Users invoke a smart contract in present cryptocurrencies by sending transactions to the contract address deployed on the blockchain. Transactions sent by the user to the blockchain will cause a state change that will be reflected in the change of account balance or the state value of the contract. These transaction calls to the smart contract are traceable and immutable, and they can be verified by any participants in the blockchain network.

D. InterPlanetary File System (IPFS)

IPFS is a protocol designed to create a content-addressable, P2P method of storing and sharing hypermedia in a distributed file system. IPFS attempts to address the deficiencies of the client-server model and HTTP web through a novel P2P file sharing system. This system is a synthesis of several new and existing innovations. It combines a self-certifying namespace, an incentivized block exchange, and a distributed hash table (DHT). IPFS has no single point of failure, and nodes do not need to trust each other not to tamper with data in transit. The IPFS can be accessed via many approaches such as HTTP. After local file is transmitted to the IPFS system, it is available to the entire network and can be traced and identified by its content hash. In this case, IPFS offers a high-throughput content-addressed block storage model to provide support for many use cases.

```
pragma solidity ^0.4.21;

contract User {
    address[] follow;
    address owner;
    Tweet[] tweets;
    struct Tweet {
        string comment;
        string ipfsHash;
        string timeStamp;
    }

    modifier onlyCreator() {
        require(msg.sender == owner);
        _;
    }

    constructor() public payable {
        owner = msg.sender;
    }

    function postTweet(string _comment, string  _ipfsHash, string _timestamp)
    public onlyCreator {
        tweets.push(Tweet(_comment, _ipfsHash, _timestamp));
    }

    function getLatestTweet() public constant returns (string, string, string) {
        if (tweets.length > 0) {
            Tweet memory latest = tweets[tweets.length - 1];
            return (latest.comment, latest.ipfsHash, latest.timeStamp);
        } else {
            return ('', '', '');
        }
    }

    function getNumTweets() public constant returns (uint) {
        return tweets.length;
    }

    function addFollow(address _following) public onlyCreator {
        follow.push(_following);
    }

    function deleteFollow(address _unfollow) public onlyCreator {
        for (uint i=0; i< follow.length; i++) {
            if (follow[i] == _unfollow) {
                while (i < follow.length-1 ) {
                    follow[i] = follow[i+1];
                    i++;
                }
                follow.length--;
            }
        }
    }

    function checkIfFollowing(address _follow) public constant returns (bool) {
        for (uint i=0; i< follow.length; i++) {
            if (follow[i] == _follow) {
                return true;
            }
        }
        return false;
    }

    function getNumFollow() constant public returns (uint) {
        return follow.length;
    }

    function getFollowAddress(uint idx) constant public returns (address) {
        require(idx < follow.length);
        return follow[idx];
    }

    function () public payable {
    }
}
```

V. CONCLUSION

Blockchain-based social media represent a good alternative to current Online Social Networks. Users gain full control of their content and are rewarded in order to encourage engagement, participation, and, in particular, the production of valuable content. Indeed, users make contributions, promote and monetize their content through tokens, and receive rewards for their contributions. This drives the social network's tokenized economy, creating more profit for business owners.

This system prototype has demonstrated the idea of using IPFS and smart contracts together on the Ethereum blockchain and further work needs to be done to examine the performance and improve the smart contract based on the real needs of the social media network

We are planning to extend this analysis in different directions. First, we want to investigate new reward strategies based on the social scenario, and examine how the current reward strategies can be further improved.

VI. REFERENCES

[1] State of social media, https://velasblockchain.medium.com/the-future-of-social-media -is-decentralized-12f875cd1835

[2] What are smart contracts, https://ethereum.org/en/developers/docs/smart-contracts/

[3] Evolution towards web 3.0, https://coinmarketcap.com/alexandria/article/what-is-web-3-0

[4] Ethereum project, https://www.ethereum.org/

[5] What is IPFS, https://docs.ipfs.io/

[6] Akasha project. [Online]. Available: https://akasha.world/

[7]NFTs explained, https://ethereum.org/en/nft/

[8]]What is Blockchain, https://www.investopedia.com/terms/b/blockchain.asp

[9] Yi Liu, T. Pinar Yildirim, Z. John Zhang "Social Media, Content Moderation, and Technology", https://www.researchgate.net/profile/Pinar-Yildirim-6/publication/348427172_Social_Media_Content_Moderation_and_Technology/links/6036e563a6fdcc37a84da548/Social-Media-Content-Moderation-and-Technology.pdf?origin=publication_detail