A blockchain based autonomous decentralized online social network

Ningyuan Chen, David Siu-Yeung Cho

University of Nottingham
UK | CHINA | MALAYSIA

University of Nottingham Ningbo China, 199 Taikang East Road, Ningbo, 315100, Zhejiang, China.

First published 2021

University of Nottingham
UK | CHINA | MALAYSIA

A Blockchain based Autonomous Decentralized Online Social Network

Ningyuan Chen
Faculty of Science and Engineering
Department of Electrical and Electronic Engineering
University of Nottingham Ningbo China
Ningbo, China
e-mail: ningyuan.chen@nottingham.edu.cn

David Siu-Yeung Cho
Faculty of Science and Engineering
Department of Electrical and Electronic Engineering
University of Nottingham Ningbo China
Ningbo, China
e-mail: David.cho@nottingham.edu.cn

***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.**

Keywords - Blockchain, Online Social Network (OSN), Decentralized Autonomous Organization (DAO)

I. INTRODUCTION

Online Social Network (OSN) is a platform for people to build connections with each other via the Internet. It is a major platform that the public can obtain and disseminate information, exchange views and share their lives on it. Research from Chaffey [1] reveals the liveness of top used OSN in the world (Figure 1), therefore, it can be found that interacting with OSN is a very popular online activity for Internet users.

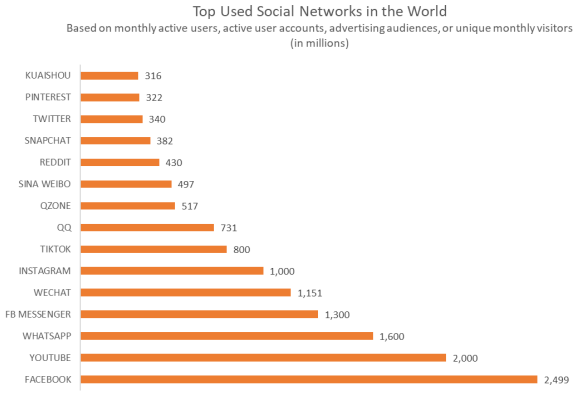

Figure 1. Top used social networks in the world

Nowadays, most of OSNs are centralized, which means the OSN companies often have full ownership of all user data and service. In general, users can only use the service after they agree to the agreements of OSN which are enacted by OSN companies. However, many agreements give the OSN companies right to use user data for personalized services such as advertisement. If users do not allow the companies to use their data and protect their privacy, they usually have to make a series of expatiatory applications or even give up using such OSN. Data and service centralization also caused all data of users is uploaded and stored in centralized servers which are controlled by OSN companies. Therefore, it is hard for users to protect their contents on the OSN when the servers crash down. To make matters worse, if the servers are hacked, security information includes password, security problems, address of users is possible to be leaked. For many users using the same password in kinds of sites, hackers can easily hack their accounts by using a method named credential stuffing attack [2]. This makes personal information of users at risk of leakage and abuse. Such problems of centralized OSNs boost researchers to consider develop an OSN based on the decentralization framework.

Decentralized OSNs have the potential to provide a safer and more controllable social network environment for users where privacy and information are more controllable for their owners. Because the data is stored in a distributed way and service is no longer relied on centralized servers. In general, a decentralized OSN is usually operated by a peer-to-peer mechanism in which each node stores some parts of data and support the service. However, it is not binding on malicious acts, and lack of self-management and sustainable developing abilities.

In this paper, we proposed an autonomous decentralized online social network architecture based on blockchain technology. Blockchain is able to provide a safe and trusted peer-to-peer mechanism where participants have unique identities and private keys. The private key has the highest control right of the corresponding account and is stored in user's own device. Moreover, all transactions in blockchain need to be signed by the private key, so cheating can be avoided. In order to give the system abilities of self-management and sustainable development, a decentralized autonomous mechanism powered by blockchain is embedded in the architecture. The rest of this paper is organized as follows. Firstly, we introduce the background of related technologies used in this architecture. Secondly, a detail description of the architecture is discussed. Thirdly, functions of this project are showed. Finally, a conclusion is made.

II. BACKGROUND

A. Blockchain

Blockchain is widely considered as a revolutionary technology that has the ability to reform human life greatly. The first mature implementation of blockchain is Bitcoin came out in 2008, it is a decentralized public cryptocurrency, it does not rely on any centralized entity, every user can join or leave the network freely and all operation rules are formulated in its source code [3]. The Bitcoin now has 218 billion US dollar market cap (data accessed on 24th Aug. 2020) [4], and is the most popular blockchain project.

Apart from other database technologies, the blockchain has its special data structure, it consists of a series of blocks, where the first block is called genesis block, all information of genesis block is converted to a fix-length hash value by using hash algorithm, and then this hash value will be stored in the second block. Once the second block is completely generated, a fix-length hash value is also converted from the second block information which includes the hash value of genesis block, and this hash value is prepared to store in the third block. The blocks are linked one by one by performing this process. Due to each block has a hash value of the former block, any modifications to blocks will result in subsequent block changes, different from the original blockchain (Figure 2). Therefore, this character prevents blockchain from been tampered, makes sure the data will no longer be modified once it is recorded on the blockchain.

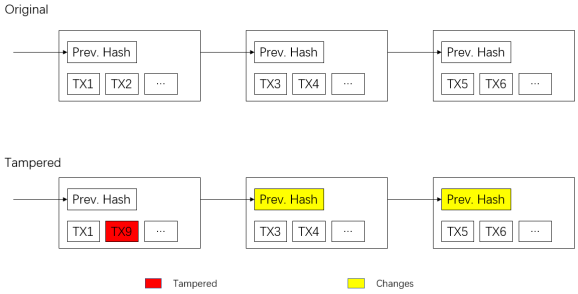

Figure 2. Differences between original and tampered blockchains

A blockchain also has encryption and consensus mechanisms in order to make the blockchain is synchronous in every node. When a user generates a transaction in the user side, the data of the transaction is encrypted by the private key of the user, then the nodes verify the encrypted transaction. After this, the nodes try to get consensus among themselves under a specific protocol, for example, the Bitcoin uses Proof-of-Work (PoS) protocol to get consensus. Once the consensus gets, the new block includes new transactions is shared with other nodes and added in the blockchain. By using these methods, the blockchain can keep synchronous among thousands of nodes without relying on a centralized leader.

Thus, this project uses blockchain technology to implement functions of OSN, including account management, posting tweets, comment tweets, autonomy.

B. Tendermint

Tendermint is a blockchain platform consists of two major technical components: the consensus engine, named Tendermint core, make sure the same transactions are recorded on each machine in the same order; the application interface, named the Application Blockchain Interface (ABCI), it can let the transactions to be processed in any programming language [6]. Tendermint can work well in BFT status (1/3 of the nodes fail arbitrarily) [5], therefore, it is safe enough for this project.

Since Tendermint is an easy-to-use and highly-performance blockchain platform, it is selected for consensus and network part in this project. We can focus more on developing the application part, user client part, and autonomy plan.

C. Decentralized Autonomous Organization (DAO)

The decentralized autonomous organization (DAO) is a virtual entity with a certain number of members or shareholders, where its members or shareholders can operate it through autonomous programs such as voting to spend funds of the DAO and change its code[7]. The DAOs are established and operated based on blockchain and smart contracts, the decentralization of blockchain ensure the DAOs are decentralized, not under someone's control.

DAOs have three classical characteristics:

- The members of a DAO should have a clear definition, including membership entry and exit mechanism. For example, many DAO projects use tokens to identify their members.
- As most DAOs operate 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.
- In DAOs, there are no centralized decision-makers, all decisions should be made after the majority of the DAO members agreements. The decision rules are defined in the code of DAO and the decision is executed rely on the blockchain platform.

Therefore, a DAO is established in this project for autonomy. It is run on the blockchain of this project.

D. Interplanetary Filesystem (IPFS)

In this project, we use Interplanetary Filesystem (IPFS) to store the data that is big volume and has low safety requirements. Most of the data in IPFS are multimedia tweet content. IPFS is a protocol for distributed peer-to-peer data storage. The data stored in IPFS is distributed within an open set of peers using a Kademlia-based distributed hash table (DHT) and addressed through a cryptographically-generated name called CID. IPFS is suitable for blockchain-based applications [8], in which such applications can access the data in IPFS by CID. CID is a multihash value which is small and fixed length, so that the blockchain is able to keep the files of blockchain data small even if there are millions of CIDs stored in blockchain. Besides, the IPFS is a decentralized protocol, which means it meets the

decentralization requirement of the decentralized blockchain application.

III. ARCHITECTURE

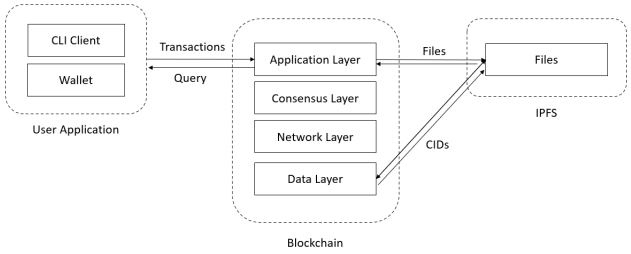

Figure 3. System structure

Figure 3 is the structure of the whole system. There are three parts of the system, in the user application part, there are command-line-interface (CLI) client and wallet, they are on the user side and help users to interact with the system. The blockchain part takes responsibility for the operations of OSN service and DAO. Moreover, IPFS is used for store big volume data that has low-security requirements.

A. User Application

In the user application part, there is a command-line interface (CLI) Client for users to interact with the blockchain, and all security operations such as private key storage and management, signature a transaction, are processed by wallet. For this part is in the user side, all security information e.g., private keys are stored in users' own devices. This avoids security information leakage from a centralized server which may happen in centralized OSNs. This information is fully controllable for users, but users also need to take responsibility for their security information.

B. Blockchain

Blockchain is the core of the system, there are four layers in the blockchain: application layer, consensus layer, network layer, and data layer. For Tendermint is used for this part and it already has the consensus, network and data mechanisms, these layers are implemented by Tendermint directly, the application layer is fully customized in Golang to implement OSN service and DAO operations.

C. IPFS

As mentioned before, all low-security requirement big volume data are stored in IPFS. When a file is stored in IPFS, the related address named CID is returned to blockchain in order to get the file in IPFS when it is needed.

IV. FUNCTIONALITY

A. Initial Setup

Each user who wants to use this system should use CLI client to generate a private key at the first time. The private key is vital important security information for users, it is used to sign transaction, confirm the identification of users and evident the ownership of the account. The encryption algorithm for private key is ED25519. And the private key file is stored in the same path where CLI client is.

B. Publish Tweets

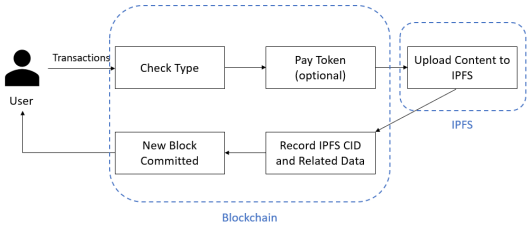

Figure 4. Publish a tweet or comment

Figure 4 is the workflow of users publishing a tweet. Users can send a transaction which is about tweet publishing by using CLI client. Once the blockchain received the transaction, it checks the transaction type first, ensure it is publishing tweets action, then, a certain amount of tokens are paid from user automatically to prevent spam tweets and resource abuse. Next, the tweet content is uploaded to IPFS, and the CID and related data (address of the user, tweet title, gas used) is recorded in blockchain for further query. Once the transaction is committed by nodes, the publishing process is completed and user gets the result. Each tweet has a hash ID to identify itself in the blockchain for further management.

C. Publish Comments

The workflow of publishing comments is similar to publishing tweets (Figure 4). But users need to indicate the hash ID of the tweet that they want to comment on when they send a transaction for commenting. After the comment is successfully published, a mapping is added in the related tweet to indicate the comment based on the comment hash ID (

Figure 5.).

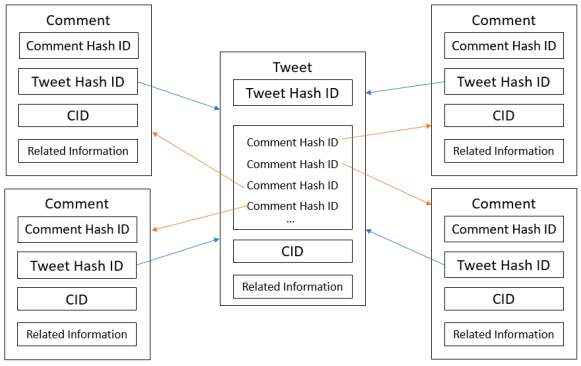

Figure 5.Principle of comments mapping to tweets

D. Vote Tweets and Comments

Users can upvote the tweet that they like, or downvote the tweet that they dislike. Sending a tweet or comment vote transaction can implement this process. This can reflect a user's contribution to the social network.

E. Read Tweets or Comments

For each tweet or comment have a unique hash ID, users can use the hash ID to read the tweet or comment through the CLI client. The reading process nearly has no system resource consumption, so, this process is fast and users need not pay tokens for it.

F. DAO structure

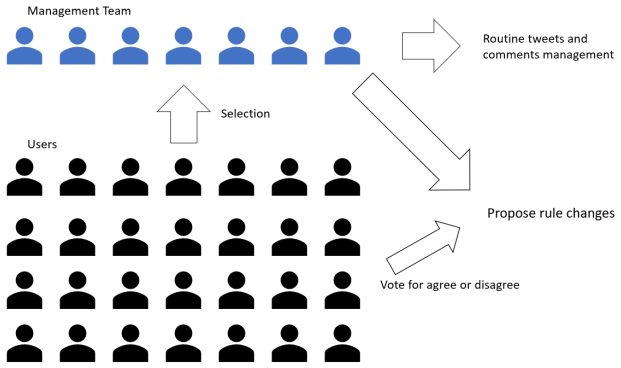

Figure 6. The structure of DAO organization

Figure 6. is the organization structure of the DAO. The DAO has two parts, management team and users. The management team is selected from users, users do selection to select management team members. The management team take responsibility for tweets and comments management (e.g., delete illegal tweets and comments), and creating proposals of DAO operation rule changes. All created proposal should be voted by users for approval.

G. Tweets and Comments Management

The management team members have the right to come up with a proposal about delete an illegal tweet or comment (Figure 7.). Then, the other team members can query the proposal (Figure 8). Next, team members vote for accepting or rejecting this proposal (Figure 9). If the number of accept votes is more than the regulated number in voting period, this proposal will be accepted and execute automatically, otherwise, it will be rejected automatically.

```
ningyuan@ubuntu:~/                    dev/wallet$ ./wallet Pproposal 02 test_add
ress testcid
resp status code:[200]
Your proposal hash:  5d06bd7db8d2015c47a14bbbfefa9b45fa1ec316730d8a00929737da122
62317
```

Figure 7. Come up with a proposal

```
ningyuan@ubuntu:~/                    /dev/wallet$ ./wallet query proposal 5d06bd
7db8d2015c47a14bbbfefa9b45fa1ec316730d8a00929737da12262317
resp status code:[200]
{"Type":2,"CID":"testcid","From":"593A6E7B9224D999981A62FEDDBCFFC4D8CFC32F","Arg
1":"test_address","Arg2":null,"Arg3":0,"Arg4":null,"Arg5":false,"A_addr":["593A6
E7B9224D999981A62FEDDBCFFC4D8CFC32F"],"D_addr":null,"Timestamp":1591197209,"EndT
ime":1591283609,"End":true}
```

Figure 8. Query a proposal

```
ningyuan@ubuntu:~/                    /dev/wallet$ ./wallet vote 5d06bd7db8d2015c
47a14bbbfefa9b45fa1ec316730d8a00929737da12262317 agree
resp status code:[200]
Your vote result:  Vote successfully, Proposal Agreed
```

Figure 9. Vote

H. Selection

Selection is taken place at set intervals automatically on blockchain, users can vote for somebody by creating a proposal within its name. When the selection ends, new management team members will be awarded under autonomy rules.

I. Impeach

If a member of the management team does evil, every user has the right to impeach it by creating a related proposal. In order to avoid abusing, each user only has a small number of chances to impeach. The impeach proposal will be voted by whole users in the OSN.

J. Autonomy Rules

The management team members have the right to create a proposal for autonomy rules changing. The rules which can be changed are fellows: the number of management team members, tenure of the management team, the ratio of agree vote, voting period, the number of impeaching chances. When such proposal came up, it should be voted from all users, and have a high agreement ratio requirement to be accepted.

V. Conclusion and Future Work

This paper presents an implementation of blockchain used in OSN. Users keep their security information under their control, in order to avoid security information leakage from centralized servers. Additionally, since the social network service is decentralized, users do not need to worry about service crash down by centralized entity. Furthermore, there is a DAO for the whole users to self-manage their social network. It is possible for an OSN to develop sustainably without a centralized leader. The blockchain implemented in this project not only provides a decentralized environment for OSN, but also make it possible for users to manage their social network in a decentralized way.

For future work, a user-friendly interface will be developed in order to replace the CLI clients since they are not very suitable for normal users. As a public IPFS network is used in this project, in order to improve the data privacy level, a private IPFS network will be developed. In autonomy part, the simulate plan will be needed in further development, the simulate plan can use tokens to motivate users to create more high-quality content in OSN and pay their effort in the autonomy part.

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