A method of image privacy protection based on blockchain technology

Xueying Dong
Fuzhou University
Fuzhou,China
Email:995385074@qq.com

Abstract--With the rapid development of virtual economy, infringement disputes in intellectual property rights (IP) such as film and television, games, creativity and so on frequently appear. The market urgently needs effective IP protection solutions. There are many problems in the traditional way, and blockchain technology has produced a subversive innovation in IP protection, and thoroughly solve the IP protection problem. This paper proposes a method of image privacy protection based on blockchain technology to protect the copyright of images in the network, and to deal with the privacy content in the image, so as to protect the rights and privacy of image owners.

Key Words: **IP, blockchain, privacy, image.**

Ⅰ.INTRODUCTION

Blockchain[1] technology is a new distributed technology that uses block-chain data structure to verify and store data, it uses distributed node consensus algorithm to generate and update data, and uses cryptography to ensure the security of data transmission and access, and uses intelligent contracts composed of automated script code to program and manipulate data.

Existence certification is the earliest blockchain certification service, which can be used to prove how digital assets are made through the network. The hash algorithm[2] proves the content of a file, and the timestamp proof the time that file was created. Using hash and timestamp, almost any document and digital asset can be identified.

Blockchain is a permanent, open and unalterable global distributed database. Once the transaction is written into the block chain, it will always be stored in the database. This feature is a perfect solution for notarization and IP protection, and it may become an important function of the whole society in the future.

This system will be built on the Ethereum [3]. Ethereum is an open source public platform chain platform with intelligent contract function. Peer-to-peer contracts are handled through its dedicated encrypted currency, the Ether, which provides a decentralized virtual machine. Smart contract[4] is a computer protocol designed to disseminate, verify or execute contracts informationally. It allow for credible transactions without third parties. These transactions can be traced and irreversible.

The purpose of this paper is to propose a method of image copyright management and image privacy protection method based on blockchain. Users can publish pictures in applications. This method uses blockchain technology to protect the copyright of photo authors. At the same time, this method can process the privacy part of the picture, such as face, etc. Users will not be able to get the complete picture without the permission of the author. The author can use the right of privacy, right of use and copyright to trade with others. The overall framework is as follows.

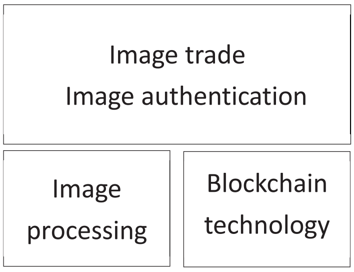

Fig.1 Image module

Ⅱ. SYSTEM ARCHITECTURE

1. Picture uploading

The system is presented to users in the form of website. Users need to register an account on the website.

After registration is completed, users can upload their own pictures. Here the server generates the hash value of the image file through the hash algorithm. If the copyright of the picture is not registered, the user can register his copyright of the picture. Otherwise, the user will be prompted that the copyright has been registered.

The user can process the privacy part in the picture, and the system provides a tool for processing. Users can obscure the privacy part. When the picture is displayed in the user's personal space, the unauthorized user can not see the complete picture, only after paying the corresponding fee to obtain permission to see. This permission requires the photo author to be open when uploading the settings, otherwise other users will not be able to see the image privacy content.

After uploading pictures, users need to set some parameters of the picture. The parameters to be set are as follows:

- Whether permission to transfer picture copyright is allowed.
- Whether the right to use pictures is allowed to be traded.
- Do you allow other users to pay for private content?
- If the parameter 1 is allowed, set the copyright price of the picture.
- If parameter 2 is allowed, set the price of the right to use pictures.
- If parameter 3 is allowed, set the privacy content to pay the cost.

Among them, if users purchase the right or copyright of the picture, the privacy content is open to it by default.

After completion, the remaining steps are completed by the system. Picture transactions are controlled by intelligent contracts. No manual intervention is required.

In order to register the author's copyright on the block chain network, the author must pay a certain fee. In the block chain network, token is used as the currency of payment. The system is built on Ethernet block chain network, so the token here refers to ether currency.

2. Picture preprocessing

After uploading the picture, the system will preprocess the picture.

First calculate the hash value of the image as the unique identification of the picture. The algorithm for calculating hash value is SM3 hash algorithm[5]. The processing of SM3 is:

Step 1: Fill the image data with a fixed length of fingerprint, so that the length of the filled data is an integral multiple of 512;

Step 2: Packet the filled information into groups of 512 bits, divided into N groups, that is

$$b(0), b(1), \dots, b(N-1)$$

Step 3: iterative compression to get the last hash value (hash value).

$$IV(n) = CF(IV(n-1), b(n-1))$$

If the information is divided into N groups, the final hash value is obtained. Picture logo is the only one corresponding to a picture in the system. It is necessary to use picture logo in picture transaction or query.

In the process of uploading pictures, if the author allows the pictures to be traded, the system will automatically generate intelligent contracts for the transaction, including the transfer of copyright, the right to use the transaction, the payment of image privacy content viewing and so on. All transactions will be strictly controlled by code. No intervention will be made to ensure the reliability of the transaction and save the cumbersome transaction steps.

We need to carry on the privacy content in the picture, use the image processing technology to process. Ensure that the author's personal privacy is not leaked. After publishing a picture, the author can manually open access to some users so that they can view a complete picture without paying for private content. When the author does not open to see permission, the picture is only open to the author. Authors have the right to revoke the privacy status of the pictures and turn them into public pictures. No fees will be charged for the pictures after they are made public.

The original image, the system generates different resolutions of the picture. The pictures displayed in the author's personal space are low resolution pictures, which prevent other users from illegally obtaining picture resources through screenshots and other means. The author can also customize the personal space to display the resolution of the picture. Hash values between images of different resolutions are associated. The copyright of derivative pictures is also recorded under the author's name.

After processing the picture, the system initiates transactions to the block chain network and records the copyright of the author. After the block is confirmed, the corresponding information will be written to the database without tampering. The block chain network of this system uses workload proof mechanism pow (Proof of Work)[6].

3. Picture transaction

Other users browse the pictures through the author's personal space.

You need to view the privacy picture, then initiate the transaction, pay the corresponding fee and get the right. But only the user can view the picture, and the right of privacy can not be resold.

When you want to get the right to use a picture for a profit, you have to pay the photographer for the right to use the picture. After the transaction is completed, users can download the original picture and use it. The right to use can not be resold. Other users should pay the corresponding fee to the copyright owner of the picture if they want to use the pictures.

Users can also purchase the complete copyright of the picture, become the actual owner of the picture, with the right to complete the picture. After the user completes the transaction of the copyright of the picture, the original author of the picture will lose the copyright of the picture and can not use the picture to obtain the corresponding rights and interests, and the user who purchases the copyright of the picture will have the right to benefit from the picture and trade the right of privacy. The copyright of the picture can be changed again. The cost of various rights can be re calibrated by the copyright owner of the picture.

After the user initiates the transaction and pays the cost, the transaction record is written in the block. The transaction is officially completed.

Picture delivery will use asymmetric password to encrypt the content of the picture, the user holds his own key SK, the user's public key PK is published outside, after the transaction is completed, the system will use the user's public key PK to encrypt the picture resources, the user receives the encrypted file, using SK to decrypt the file, get the picture.

$$E(PK, M) = C$$
$$D(PK, M) = C$$
$$D[SK, E(PK, M)] = M$$

E is the encryption algorithm, M represents the picture plaintext, D is the decryption algorithm, and C is encrypted ciphertext.

4. Picture query

Because block chains are traceable. The system makes use of this feature to enable the use of pictures to be queried. Uploading pictures on the website allows you to check its copyright ownership and record of usage. You can also check the original author of the picture.

Ⅲ. SUMMARY

The invention relates to a picture privacy protection method based on blockchain technology. First, the user uploads pictures to his personal space and sets the parameters of the pictures. Then the server preprocesses the pictures uploaded by the user and generates an intelligent contract for trading pictures. Then the server moves to the number based on block chain technology. The Word Money Network initiates a transaction to record the copyright of the author to the picture and save the transaction information to the database; other users view the thumbnail of the picture through the author's personal space, and complete the transaction by paying the corresponding amount of the smart contract. The invention uses the block chain technology to protect the copyright of the image author, and processes the privacy content in the image, so as to protect the rights and privacy of the image owner.

REFERENCES

[1]. Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]// Security and Privacy. IEEE, 2016:839-858.

[2]. Eastlake Rd D, Jones P. US Secure Hash Algorithm 1 (SHA1)[J]. RFC3174, 2001, 37(2):105-113.

[3]. Sixt E. Ethereum[J]. 2017.

[4]. Clack C D, Bakshi V A, Braine L. Smart Contract Templates: foundations, design landscape and research directions[J]. 2017.

[5]. Kircanski A, Shen Y, Wang G, et al. Boomerang and Slide-Rotational Analysis of the SM3 Hash Function[J]. 2012, 7707:304-320.

[6]. Liu D, Camp J. Proof of work can work[J]. Weis, 2006.