Tokenizing and managing the copyrights of digital content on blockchains

Tatsuro Ishida
NTT Service Evolution Labs
tatsurou.ishida.xa@hco.ntt.co.jp

Hiroki Watanabe
NTT Communications Corp.
hirokit.watanabe@ntt.com

Shigenori Ohashi
NTT Service Evolution Labs
shigenori.ohashi.ur@hco.ntt.co.jp

Shigeru Fujimura
NTT Service Evolution Labs
shigeru.fujimura.wg@hco.ntt.co.jp

Atsushi Nakadaira
NTT Service Evolution Labs
atsushi.nakadaira.hy@hco.ntt.co.jp

Kota Hidaka
NTT Service Evolution Labs
kota.hidaka.yk@hco.ntt.co.jp

Jay Kishigami
Muroran Institute of Technology
jay@csse.muroran-it.ac.jp

***Abstract*— This paper proposes a method for managing digital content on blockchains in which content copyrights are distributed in the form of tokens. Our implementation of the proposed method resulted in fast retrieval of the history on the blockchain without relying on an external database.**

Keywords—Content rights, rights management, blockchain, tokenize

I. Introduction

Since digital contents have been digitized and managed, several methods have been devised to prove that the copyrights are being processed correctly. For example, watermarks and DRM are used to prevent unauthorized use [1][2]. Recently, some methods of managing copyrights and contents by using blockchains has been proposed [3][4][5]. The following three features of the blockchain used for crypto assets suggest that it might be suitable for content management: (1) its tamper-resistance is expected to reduce unauthorized use, (2) content copyrights holders can trade content and value directly, and (3) the blockchain can be operated transparently because the system it runs on keeps track of all the past transactions.

II. Problems

There are a few problems when it comes to applying a conventional blockchain to content management. The first problem is copyrights control. In Japan, copyright is considered as a group of small rights. For example, copyright includes the right to reproduce, to transfer, to lend, and to distribute a work. Therefore, digital content needs to be able to handle different rights for different people. The owner (copyright holder) can sell, distribute, and read the work, while the user can only read it. However, conventional crypto assets are dividable by any user: in other words, they work the same as cash. The second problem is the low searchability of transaction history. When managing content, it is necessary to search the history to check whether a user has the proper right for that content. If you want to check this, you have to crawl the entire transaction history and extract the history of a specific user. To improve the efficiency of this process, an attempt has been made to save the transaction history in an RDB and to provide the search function by means of an external service[6]. However, in this case, the accuracy of the information depends on something outside of the blockchain, and thus it is not reliable. To achieve a high-speed search of history while maintaining the decentralized characteristics of the blockchain, we need to improve the searchability of the data in the blockchain without using external services.

III. Proposed Method

The requirements to solve these challenges are as follows. (1) The copyright to handle content is different between the content copyright holder and the user. Thus, the system must recognize users individually and give them proper operation authority. (2) The copyright must have the ability to be transferred. For example, the right to watch content would be buy and sell. (3) Content management requires high searchability in order to confirm the status of copyrights.

We implemented a demo that incorporates the above requirements. Ethereum[7] is used as the blockchain base. Some of the new proposals in the Ethereum Request for Comments (ERC) have been determined as suitable for this implementation. In this work, we have expanded the token design proposed in ERC 721 and ERC 998. ERC 721 [8] has the feature of being able to indicate the owner address and the user address on token. compared to the crypto asset. ERC 998 [9] is an extension of ERC 721 and can bind tokens together by defining parent and child tokens. For example, it enables an advertisement linked to specific content to be played, with its history then stored on the blockchain. Let us briefly describe the retrieval of tokens. Normally, Ethereum does not index token data on its smartcontract (smartcontract is the name of a blockchain implemented in Ethereum). It is common to provide an external database for indexing. This proposal allows for fast search on a smartcontract without an external database.

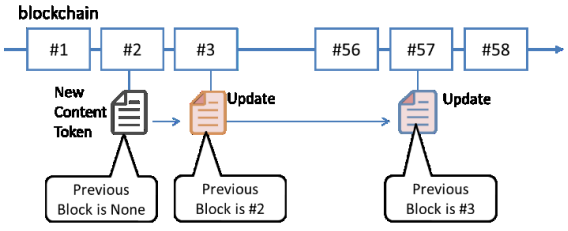

Figure 1 Search procedure in the proposed method.

Specifically, when a change is made to a token in a certain block, the block number is recorded in the token itself. If you want to track token changes, you can scan the smartcontract by specifying a block number within the token. As shown in

978-1-7281-3575-5/19/$31.00 ©2019 IEEE

Figure 1, when a new token is generated, it is recorded in the smartcontract. Here, a token is recorded in the block of number 2. Inside it, the contents that indicate that the person himself or herself has just been made are described. Next, the contents of the token were updated and recorded in the block number 3. Inside, it is recorded that the previous block is number 2. At number 57, a change to the token is recorded. Inside the token, the previous block is recorded as number 3. This makes it possible to search efficiently. An image of the process constructed by including the above technique is shown in Figure 2. There are four characters in this process, advertiser, content rights holder, publisher and viewer. Advertisers pre-populate the blockchain with ads and ad costs. Content rights holders register content rights in the blockchain in the form of tokens. The rights holder gives a part of the right (grant right for advertising) to the publisher, and the publisher attaches the advertisement to the content as child token. Viewers are also given the right to watch, and when they watch, they are automatically allocated a predetermined amount of advertising expenses according to the smart contract. The history can be retrieved later when needed using token search technology.

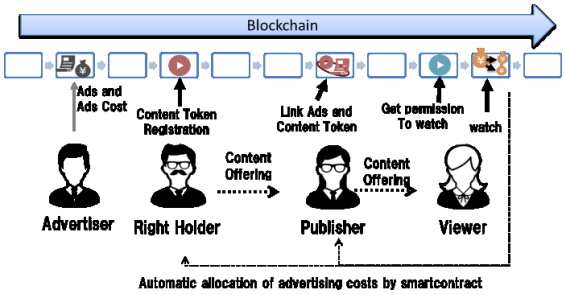

Figure 2 Token processing method

IV. Evaluation and Discussion

After implementation, we evaluated the proposed method. All evaluations were conducted using a private chain built on Ethereum. Content was registered on the smartcontract, and it was confirmed that different copyrights were granted to different roles and that copyrights could be transferred. We also analyzed the cost change of the proposed method and the retrieval speed as non-functional requirements. First, the cost change investigation is described. In Ethereum, Gas exists as a fee to execute a transaction. It is paid to users who approve the transaction. Gas cost is determined by the number of steps of computational procedure that constitutes a token, so it can vary depending on the token complexity. We confirmed that when a token is created with 20 rights to view, Gas becomes too high, exceeding Ethereum's Gas limit (the maximum amount of GAS you can spend on a transaction. The generator of the new block determines the value as above or below. As of January 2019, the upper limit is approximately 8 million Gas), and processing is delayed. This problem can be solved by reworking the implementation. In the first implementation, several tokens for the right to view are generated as child tokens of the content token by the ERC 998. The token right is rewritten each time the right is purchased. In the next implementation, when a user with the right to view occurs, the system generates a right token and makes the right token a child of the content token. In the former method, it is easy to control the upper limit of use of the content. On the other hand, since the size of the token is constant regardless of the number of users, there is a cost. In the latter method, the process is initially a lightweight token, but the process of creating a token is required each time a right is generated, and the process becomes heavier as time passes. If the number of changes to the token exceeds a certain number of times, additional control is required to generate a new content token. Next, we investigated the search speed of a token. Tokens were created in accordance with the ERC 998, and 10 viewing rights were registered for each token. 1 block was generated in 15 seconds, and about 10,000 blocks were registered on the blockchain. Data was input approximately every 100 blocks. The proposed method took about 0.3 seconds to do this, while the existing method took about 4.7 seconds; as such, the proposed method is 16 times faster than the existing method.

TABLE I. Speed Measurement Results

	Proposed method	**Existing method**
Average	***287***	***4688***
Standard Deviation	***10***	***57***

(Unit: milliseconds)

Our implementation was experimental and requires some additional features before starting a commercial service. For example, (1) there is no mechanism for excluding unauthorized content in this implementation, (2) it should perform long-term operation and conduct performance surveys, so we have to consider the possibility that the processing will become heavier and heavier, and (3) from the viewpoints of freedom of thought and conscience and privacy, the system needs to be equipped with appropriate disclosure control technology to determine who has what copyrights in what content. This is outside the scope of the current system.

V. Conclusion

We have implemented a system for managing and distributing digital content by registering it as a token on a blockchain. By tokenizing complex copyrights agreements, smart contracts enable automatic profit sharing and efficient historical searching. The constructed system was able to address the problems and requirements in managing and distributing digital content on blockchains.

References

[1] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 87–96, Mar. 2013.

[2] Q. Liu *et al.* "Digital Rights Management for Content Distribution" ACSW Frontiers '03 Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21. Pages 49-58.

[3] S. Cho *et al.* "A blockchain for media: Survey" 2019 International Conference on Electronics, Information, and Communication (ICEIC) , 22-25 Jan. 2019.

[4] N. Herbaut *et al.*, "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains", IEEE Communications Magazine, Vol. 55, Issue 9, pp. 70-76, Sep. 2017.

[5] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. Kishigami, "BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain", 5th IEEE International Conference on Consumer Electronics, pp. 345- 346, 2016.

[6] Ethereum (ETH) Blockchain Explorer https://etherscan.io/

[7] Ethereum Project https://www.ethereum.org/

[8] EIPs/eip -721 .md at master ethereum/EIPs GitHub

https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

[9] ERC -998 Composable Non-Fungible Token Standard Issue # 998 ethereum/EIPs GitHub https://github.com/ethereum/eips/issues/998