BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain

Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, Tomokazu Yamada, Akihito Akutsu
NTT Service Evolution Laboratories
Yokosuka-City, Kanagawa, Japan

Jay (Junichi) Kishigami
Muroran Institute of Technology
Muroran-City, Hokkaido, Japan

Abstract—**We propose a concept for a new rights management system based on the blockchain technology, which is famous for supporting the reliability of the bitcoin. We clarify problems that occur when we apply the blockchain technology to the rights management system, and we also describe our trial implementation.**

Keywords— blockchain; content delivery; DRM(Digital Rights Management)

I. Introduction

The bitcoin [1], which is the first and most popular cryptocurrency, has been receiving a lot of attention [2]. One of its technical features is that it enables reliable transactions without a centralized management mechanism even if there are unreliable participants in the network, and this feature is obtained by the invention of blockchain technology. A blockchain is something like a ledger in which all transactions have been recorded, and it is shared by the participants of a bitcoin network. The structure of a blockchain is that a block that consists of multiple transactions is connected with a previous block in chain-like form. To ensure reliability, when a new block is added to the previous block, a little special process of solving a puzzle, called proof-of-work (POW), is needed and this puzzle is not easy. This is because this process can prevent attackers from forging the blockchain on their own. With the number of bitcoin transactions becoming larger and larger, discussion of blockchain applications other than currency have been thrust into the spotlight because its reliability has been securely kept among the large-scale use. Sometimes the approach of these applications that take advantage of the features of blockchain is called “bitcoin 2.0”.

Blockchain technology has great potential for application to video rights management systems because it is completely different from the conventional method in which a centralized management mechanism is normally adopted. The potential is especially great for high-quality videos such as 4K/8K videos which, if copied with the original image quality, would create serious problems. A video rights management system controls what users use videos in various way such as “playing” or “editing”. Rights management service providers have to spend a lot of money to keep their systems safe from attackers and the costs they incur are inevitably reflected in their service fees. On the other hand, in a rights management system based on blockchain technology, the blockchain itself is strong against attack and its service provider doesn’t have a responsibility to maintain the blockchain alone. This creates the possibility of lowering users’ service fees. As a result, the services become easier to use for semi-professional video creators who cannot use them now.

The rest of this paper is as follows. The next section describes issues of applying the blockchain technology to a rights management system. Our approach to these issues and our trial implementation, named “BRIGHT (Blockchain based RIGHTs management system)”, are described in Section 3. The paper is concluded with a mention of future work in Section 4.

II. Discussion about applying the blockchain technology to a rights management system

Since the blockchain technology was developed for cryptocurrencies, a specialized portion of it is for exchanges of currency. In applying it to a rights management system, there are several issues to discuss. Two of the most important are given below.

A. Coupling videos with rights information on the blockchain

In cryptocurrencies, information exchanged between users is about exchanges of currencies. On the other hand, information in rights management systems is about exchanges of rights or license information. Both types of information should be recorded in the blockchain and be able to be transmitted securely. Unlike cryptocurrencies, however, there is one more point to consider in rights management systems, that is, how to treat video securely.

If the average file-size of videos is taken into consideration, trying to record videos themselves to the blockchain is entirely inappropriate. Therefore, the methods for delivering videos and rights information should be separated. This is why the method that couples videos themselves with rights information on the blockchain tightly is important.

B. Latency of reflecting the rights information

In the blockchain technology, it requires a certain time to add a new transaction to the blockchain as a new block. It takes an average of ten minutes in bitcoin, and it is strongly recommended that the transaction not be approved until six blocks have been coupled after the block which includes the

978-1-4799-8748-1/15/$31.00©2015IEEE

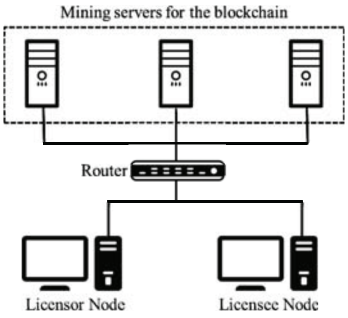
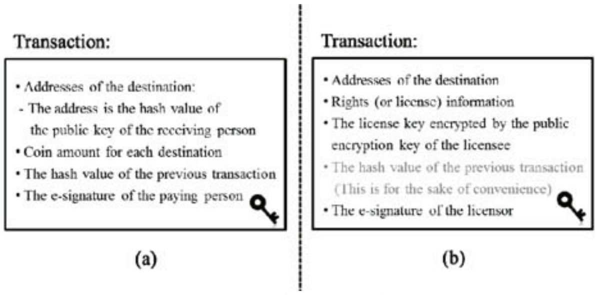


Fig. 1.System overview



- Addresses of the destination:
  - The address is the hash value of the public key of the receiving person
- Coin amount for each destination
- The hash value of the previous transaction
- The e-signature of the paying person

- Addresses of the destination
- Rights (or license) information
- The license key encrypted by the public encryption key of the licensee
- The hash value of the previous transaction (This is for the sake of convenience)
- The e-signature of the licensor

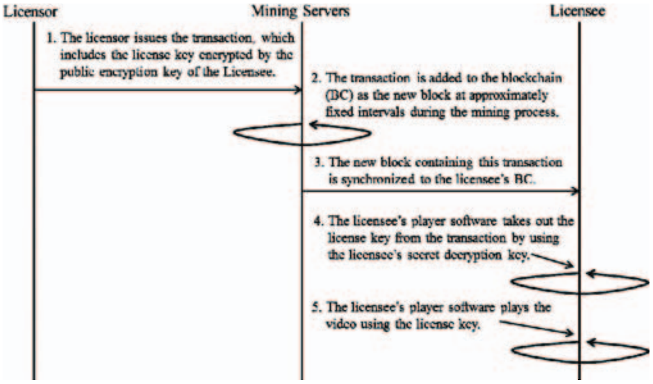
Fig.2. The transaction of (a) bitcoin / (b) our trial rights management system

target transaction. As a result, users using the blockchain technology in the same way they use bitcoin are forced to wait for the video use which is allowed by the blockchain based rights management system. Therefore, it is necessary to devise a way to shorten the delay of reflecting the rights information in the blockchain.

III. Our Approach and system overview

To verify the applicability of the blockchain technology to a rights management system, we developed a trial system based on the Bitcoin Core software [3]. The system overview is shown in **Fig.1**. Our trial system is constructed on a small peer-to-peer network, and there are three blockchain mining servers, which is the smallest number needed to maintain the blockchain. Here, mining means the calculation work performed for connecting a new block to the blockchain; in other words, solving a puzzle to do this. The licensor and the licensee nodes have the blockchain too, but mining is not carried out on these nodes. In these nodes, the blockchain is utilized to issue or receive the transaction.

To take the discussions of the previous section into account, our approach for solving those issues is as follows. First, to couple videos with rights information on the blockchain tightly, we devised player software. Regarding the use of videos, a variety of functions such as playback and editing was considered, but we targeted the control of playback in our trial system. We customized the Media Player Classic - Home Cinema [4] and this customized player always follows rights information addressed to the user. Rights information, i.e. playback license, is included in the transaction which is issued from the licensor. The transaction of our trial system is shown along with that of bitcoin in **Fig.2**. We also customized the specifications for the transaction of the Bitcoin Core software so that the licensor can write the XML-based metadata describing the use conditions of videos.



1. The licensor issues the transaction, which includes the license key encrypted by the public encryption key of the Licensee.
2. The transaction is added to the blockchain (BC) as the new block at approximately fixed intervals during the mining process.
3. The new block containing this transaction is synchronized to the licensee's BC.
4. The licensee's player software takes out the license key from the transaction by using the licensee's secret decryption key.
5. The licensee's player software plays the video using the license key.

Fig. 3. The processing flow of the usage of the license key

In addition, our trial system takes into account the transfer of the license key needed for decrypting encrypted videos. The encryption of video raises the level of security and it is ensured that the rightful owner of the video issues the license of use, unless the license key has been leaked. The processing flow of the usage of the license key is shown in **Fig.3**. The important point in this process is using the licensee's public encryption key and secret decryption key. This ensures that only the licensee can see the license key even if the license key is on the public place of the blockchain.

To address the second issue discussed in the previous section (in other words, to shorten the latency), we customized the Bitcoin Core software. In the POW algorithm of bitcoin, the average interval between the adding of new blocks can be adjusted by the difficulty of the puzzle. We adjusted it so that the average interval is five seconds.

Using our trial system, we verified that the following use cases can be controlled. First, the licensor can control the permission for a particular licensee to use a particular video. Second, the licensor can change the permission for a particular licensee to use a particular video at a certain point in time. These controls are enabled by the rights information on the blockchain and the player software that follows this information.

IV. conclusion

In this paper, we described the applicability of the blockchain technology to a rights management system in proposing a concept for a new rights management system. To develop this concept, we will try to verify its large-scale applicability.

References

[1] S. Nakamoto, "Bitocoin: A Peer-toPeer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.

[2] J. Bonneau et al, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in 36th IEEE Symposium on Security and Privacy, May 18-20, 2015.

[3] "Bitcoin Core integration/staging tree," https://github.com/bitcoin/bitcoin.

[4] "Media Player Classic - Home Cinema," https://github.com/mpc-hc/mpc-hc