# The Blockchain-Based Digital Content Distribution System

**Conference Paper** · August 2015

DOI: 10.1109/BDCloud.2015.60

**5 authors**, including:

Jay Kishigami
MIT
**21** PUBLICATIONS **189** CITATIONS

SEE PROFILE

Hiroki Watanabe
Nippon Telegraph and Telephone
**5** PUBLICATIONS **101** CITATIONS

SEE PROFILE

# The Blockchain-based Digital Content Distribution System

Jay Kishigami
Muroran Institute of Technology
Hokkaido, Japan
Email: jay@csse.muroran-it.ac.jp

Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, and Akihiko Akutsu
NTT Service Evolution Laboratories
Kanagawa, Japan
Email: fujimura.shigeru@lab.ntt.co.jp

***Abstract*—The blockchain-based digital content distribution system was developed. Decentralized and pear-to-pear authentication mechanism can be considered as the ideal rights management mechanism. The blockchain has the potential to realize this ideal content distribution system. This is the successful model of the Superdistribution concept which was announced almost 30 years ago. The proposed system was demonstrated and got a lot of feedback for the future practical system.**

## I. Introduction

After the commercializing of the Internet in 1994, the digital content delivery services have been increasing rapidly. Especially the music and video delivery would be a dominant of the Internet payload which occupied more than the half of its traffic. There are two kinds of delivery systems; one is protected delivery, and the other is non-protected. The method to protect the digital content has a lot of variation. But the basic technology is the encryption. The variation is depend on how to convey the key to decrypt the content.

DRM, Digital Rights Management, and CAS, Conditional Access System, are applied for almost all commercial-based digital content for the protection. The DRM technology has been mainly adopted to the tele-communication-based services and the CAS technology to the broadcasting services. These two technologies have the similar algorithm based on the encryption. The difference of each service is mainly depend on the way of key handling and the time to decrypt.

The problem of these system is the pirate attacking. There are so many attacks to decrypt or steal the key for taking the content without the legal procedure. The copyright law in each country protect the content from these pirates. Especially, the Japanese copyright law has been said as the technical copyright law because of the too much technical statements.[1] This causes the game of hide-and-seek between the encryption technology and illegal decrypt or get-out of the protection. The encryption technology has been improving the complexity and its algorithm. One of them is the key length. The longer key length makes longer time to decrypt. This means that the longer one realize the high level encryption, and more safe environment.

Back to the year of 1983, the first Superdistribution concept was released.[2][3] The author's idea was the ideal digital content distribution system. The name of Superdistribution was imitated with the Superconductor, because of its no resistance condition. In the case of the digital content distribution, the resistance has been the non-healthy market maturity. This problem has been the most difficult issue for the digital content distribution even today. His core idea was that the usage model would be installed by way of compensation of the ownership model. To realize his idea, there has been a lot of trial. We had established the Content ID Forum(CIDF) in 1999, which was based on the metadata and ID control mechanism using the dual watermark system. [4]

After that, so many trial to realize his Superdistribution idea had been done. But I have to say no successful trial had been undertaken. The main reason should be the center-concentrated rights management system. To keep the consistency and security, each ID should be registered to the authentication center. This centralized service would be the only solution to keep the system in terms of consistency. Many right holder would not ask their authority to any other party, their final and ideal procedure on the copyrights management is that they would operate their right by themselves.

We developed blockchain-based digital content distribution system to realize the rights holder's dream. The most significant point is that this system can be operated by the rights holder themselves. And there are so many convenient features which could not be realized by any other centralized one. This paper describes the concept of the idea and demonstration system for the super high definition video system, called 4K or 8K. And some features are also showed in this paper.

## II. The system

The system has been designed to keep the following features; 1. The content owner can control easily and always. The concept is totally different from the conventional center-operated rights management system. This means owner can control everything. To realize this concept, simple and easy operation would be required. 2. Reasonable security and simplicity can be realized. The conventional Bitcoin system which is the first product to use the blockchain mechanism takes about 10 minutes to mine the Hash value for the calculation. This is because to compete the fastest calculation in order to avoid the pirates. In the case of the digital content distribution, these long mining time will disturb the operation. 3. The first target was assumed the super high resolution video, called 4K or 8K. The capacity of each video was around 1GB through 10GB after HEVC compression. Total encryption for the file is not practical, because the time to decrypt will take a long time.

### *A. Block diagram of the high resolution video content distribution system*

Considering a various requirement, we have been carefully designing the public and private key operation system with blockchain mechanism. The first priority is the usability from the customer viewpoint. The basic mechanism is very similar with the conventional Bitcoin one. The most significant difference between them is that our system will not convey the money at this moment. Figure 1 shows the main mechanism. There are two functional stakeholders in terms of the trading. In the case of the digital content distribution model, the licensor is mostly content rights holder, and the licensee is a user. The typical Superdistribution model requires the authority who handles the right management. The blockchain model has no authority. The miner will generate the latest rights blockchain. All transition are recorded as a history and all user share these information. 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, is needed and this puzzle is not easy. This is because this process can prevent attackers from forging the blockchain on their own.

These mechanism is the same with the existing Bitcoin system basically. Another big difference between the Bitcoin and the proposed system is the incentive and the media. Each miner will consume his own computer resource to get a reward when he find the conditional hash value faster than any other miners. Generally this rewards gives by the Bitcoin itself (BTC). The proposed system takes the digital content not the money. Our hypothesis is that the incentive for the miner will be discussed in conjunction with the business model, that is the out of scope of this paper. The biggest merit to adapt the blockchain mechanism to the digital content distribution model is the authentication scheme. The system requires no centralized rights management organization. All participants have the all transaction history, aka blockchain. This scheme could be said the ideal and ultimate system.

The encryption technology will be adapted to the proposed system also as the same manner with the conventional DRM system. The balance of the decrypt cost and the security level will require the combination of the secret and public key technology. The proposed system is also use the same mechanism. The security level can be deeper by the longer key. The length will be determined considering the calculation time. The proposed system takes ultra-high resolution video content. The file size would be more than 20GB. Therefore, the conventional entirely encrypt/decrypt technique is not a practical solution because of the data size.

The first target of this system is to show the possibility and potential of the Blockchain-based digital content distribution system. The encryption mechanism, therefore, is relatively simple. Each header of the H.265 compression data was modified in conjunction with key management. The data with the right secret key can be played.

*1) Licensor:* The main two function of this module are the permission control for each owned content and upload the content file. The only licensor can control his own content with permission management. The unique characteristics of this system is that the licensor can change the permission anytime; even after the content distributed. From the content owner viewpoint, this anytime-off function is very important, because the contract between owner and users is the limited. For example, the limitation of the content usage is by the expiration, limited number of play, or some owner's will. When the owner finds any inadequate expression on his works, he have to delete it and modify it. The existing content management system is not easy to satisfy this requirement.

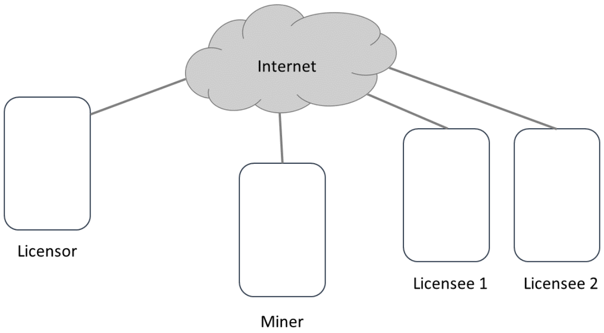


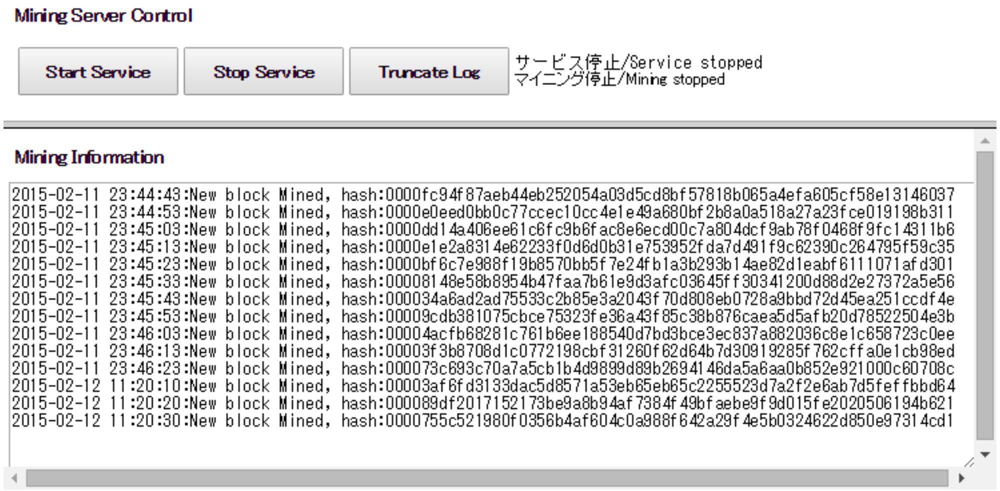
Fig. 1. The main bloackchain-based content distribution system

Fig. 2. Actual demo system. Each display represents the mining server, licensee 1 and 2

*2) Licensee:* Two major application are running at the licensee client. One of these is the license control application, which get the rights information from the Blockchain and control the player based on the result. The other is the content player, which would play the 4K high-resolution digital content with decoding the H.265. This player can run only if the license certificated.

*3) Mining server:* This is the main module of this system. The mining function is described as follows; To generate the new block which include the rights information, To add the nonce with some calculation, and to broadcast the new generated block on the network.

Figure 3 shows the result of each transaction hash value with nonce. The hash value should keep the condition that first four digit should be 0. This limitation is to control the mining time as 10 second. This hash would be calculated just after new transaction done.



```
サービス停止/Service stopped
マイニング停止/Mining stopped
```

```
2015-02-11 23:44:43:New block Mined, hash:0000fc94f87aeb44eb252054a03d5cd8bf57818b065a4efa605cf58e13146037
2015-02-11 23:44:53:New block Mined, hash:0000e0eed0bb0c77ccec10cc4e1e49a680bf2b8a0a518a27a23fce019198b311
2015-02-11 23:45:03:New block Mined, hash:0000dd14a406ee61c6fc9b6fac8e6ecd00c7a804dcf9ab78f0468f9fc14311b6
2015-02-11 23:45:13:New block Mined, hash:0000e1e2a8314e62233f0d6d0b31e753952fda7d491f9c62390c264795f59c35
2015-02-11 23:45:23:New block Mined, hash:0000bf6c7e988f19b8570bb5f7e24fb1a3b293b14ae82d1eabf611071afd301
2015-02-11 23:45:33:New block Mined, hash:0000814 8e58b8954b47faa7b61e9d3afc03645ff30341200d88d2e27372a5e56
2015-02-11 23:45:43:New block Mined, hash:000034a6ad2ad75533c2b85e3a2043f70d808eb0728a9bbd72d45ea251ccdf4e
2015-02-11 23:45:53:New block Mined, hash:00009cdb381075cbce75323fe36a43f85c38b876caea5d5afb20d78522504e3b
2015-02-11 23:46:03:New block Mined, hash:00004acfb68281c761b6ee188540d7bd3bce3ec837a882036c8e1c658723c0ee
2015-02-11 23:46:13:New block Mined, hash:00003f3b8708d1c0772198cbf31260f62d64b7d30919285f762cffa0e1cb98ed
2015-02-11 23:46:23:New block Mined, hash:000073c693c70a7a5cb1b4d9899d89b2694146da5a6aa0b852e921000c60708c
2015-02-12 11:20:10:New block Mined, hash:00003af6fd3133dac5d8571a53eb65eb65c2255523d7a2f2e6ab7d5feffbbd64
2015-02-12 11:20:20:New block Mined, hash:000089df2017152173be9a8b94af7384f49bfaebe9f9d015fe2020506194b621
2015-02-12 11:20:30:New block Mined, hash:0000755c521980f0356b4af604c0a988f642a29f4e5b0324622d850e97314cd1
```

Fig. 3. Mining Information example

### B. Possible Functions

We shows three possible functions on the blockchain-based digital content distribution system. These funstions are the limited demonstration to make the content owner understand the system. Based on the response from the content owner or any other stake holder, we will improve the system in near future.

*1) Control each-by-each licensee:* The content owner, aka licensor, can control the licensee each-by-each. This function will be realized by the metadata which attached the content also. And licensor can control each permission in the real time manner.

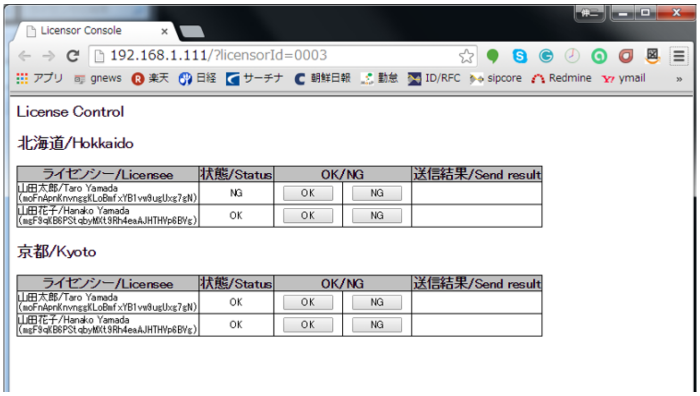
*2) Control each content:* First, the licensor set the content ID as one of the metadata. The licensor can give the permission information based on each content ID.

Figure 4 shows the permission control dashboard. On this GUI, the licensor can control the permission of the right to watch based on content and the terminal, even after the content distributed.

*3) Off-line control:* When the licensee browser, which has a decoding function of the digital content, goes off-line, the internal digital content can not be reproduced because it requires the transaction ID generated from the blockchain mining server through the network.

## III. Results

We showed the proposed blockchain based system at the semi-closed forum. Totally around 100 people checked our system. Most of them were creator, content owner and digital content stake holders. They suggested a lot of ideas to improve this system. The most impressive and attractive point for them was the decentralized mechanism. The current DRM system is the centralized architecture, which requires an authentication mechanism. And at the same time, this center has a lot of power to control the content distribution. The typical example is the broadcaster. Many countries adopts a DTT: Digital Terrestrial Television system in these 20 years. These broadcasting system forged CAS: Conditional Access System to protect from the illegal copy and control the content. The independent producer should make the content based on the broadcaster's request. Otherwise they lose the media of distribution.



License Control

北海道/Hokkaido

| ライセンシー/Licensee | 状態/Status | OK/NG | | 送信結果/Send result |
|---|---|---|---|---|
| 山田太郎/Taro Yamada<br>(moFnApnKnvnggKLoBmfxYB1vw9ugUxg7gN) | NG | OK | NG | |
| 山田花子/Hanako Yamada<br>(mgF9qKB6PStqbyMXt9Rh4eaAJHTHVp6BVg) | OK | OK | NG | |

京都/Kyoto

| ライセンシー/Licensee | 状態/Status | OK/NG | | 送信結果/Send result |
|---|---|---|---|---|
| 山田太郎/Taro Yamada<br>(moFnApnKnvnggKLoBmfxYB1vw9ugUxg7gN) | OK | OK | NG | |
| 山田花子/Hanako Yamada<br>(mgF9qKB6PStqbyMXt9Rh4eaAJHTHVp6BVg) | OK | OK | NG | |

Fig. 4. Permission control system

The blockchain system advocates the ideal decentralized architecture for the digital content distribution. The information of each transaction is added to the blockchain by the mining technology and nonce. The proof-of-works insists the security of the blockchain itself. No one can not control this mechanism entirely. Of course, there are some weak points on the mechanism recently reported. But these technology is improved year by year.

Another comments were some applications of this system. Most practical application would be the office system, where a lot of files are controlled because of each confidentiality. Even though, it is not easy to control all files internally and externally at the same time.

## IV. Conclusion

Decentralized blockchain-based digital content distribution system was proposed, and developed a prototype for the easy understanding its concept.

The proposed system has no incentive mechanism for the mining calculation at this moment. This means no cost can be covered if each minor calculates the hash value. Some BTC would be paid to the minor as a incentive in the case of the Bitcoin system. We consider that the incentive mechanism should be discussed in the business model. The future work would be that more sophisticated system and other field applications. These future model will be discussed soon.

## Acknowledgment

The authors would like to thank the Barnard Software Co. in Sapporo through the developing the system. And we also express a great appreciation to Dr. Asada. The system could not be developed without his fruitful advices.

## References

[1] Nobuhiro nakayama, *Choskukenhou (Copyright Law)*, 2nd ed. Japan: Yuhikaku, 2014.

[2] Ryoichi Mori, *about Software Service*, JECC Journal, No.3, pp.16-26, 1983 in Japanese

[3] Ryoichi Mori, *What Lies Ahead*, Byte Magazine, Jan 1989

[4] Koichi Sakanoue, Junichi Kishigami, et al., *New Sevices and Technologies Associated with Metadata*, NTT Technical Review Vol.1 No.3, pp.46-50 , 2003