A Method of Digital Rights Management based on Bitcoin Protocol

Kitahara, Motoki
Kyushu University

Kawamoto, Junpei
Kyushu University

Sakurai, Kouichi
Kyushu University

https://hdl.handle.net/2324/1498293

出版情報：Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. 84, pp.1-6, 2014. ACM
バージョン：
権利関係：

A Method of Digital Rights Management based on Bitcoin Protocol

Motoki Kitahara
Kyushu University
744, Motooka, Nishi-ku
Fukuoka, Japan
kitahara@itslab.inf.kyushu-u.ac.jp

Junpei Kawamoto
Kyushu University
744, Motooka, Nishi-ku
Fukuoka, Japan
junpei@inf.kyushu-u.ac.jp

Kouichi Sakurai
Kyushu University
744, Motooka, Nishi-ku
Fukuoka, Japan
sakurai@inf.kyushu-u.ac.jp

ABSTRACT

In the digital world, so many copyrighted works are made in an illegal way because it is easy to keep and copy. Digital Rights Management has proposed to prevent this theft. Contents providers often bring in one server who has charge of managing the normal user, but there are some problems that it flocks to the server. Against this problem, P2P based DRM system has considered. All users can transfer the encrypted content to other users, so the content server does not have to load so much traffic from users. As a problem with this method, it is hard to figure out usage situation of contents because P2P based system is divided into many pieces of users. In this paper, we propose a new P2P based DRM system using Bitcoin protocol, which is one of the electric commerce. Bitcoin protocol, timestamp server saves all transactions to prevent double spending. We can bring out all usage situations to apply this system.

Categories and Subject Descriptors

K.5.1 [Hardware/Software Protection]: LEGAL ASPECTS OF COMPUTING; M.6.4 [System Management]: MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS

General Terms

Digital Rights Management

Keywords

Digital Rights Management, Bitcoin. P2P network

1. INTRODUCTION

1.1 Background

With the development of computers and spread of the Internet, many kinds of contents have been treated as information data. Major examples are music data and picture data. These data have the value of themselves, and we can use them as a digital media. As an advantage that we can bring out a large amount of data with a small terminal, digital data has spread especially in audio data. However, digital media has a problem that it is easy to upload and share the data with general public through the Internet. Digital Rights Management has proposed in an effort to prevent this problem and become usable only by a normal user.

1.2 DRM's state and problem

DRM is defined that holding the contents secure by preventeing the illegal copying, imposing fees, processing payments, tracking contents, and protecting each principal's right and profit[1]. In the use of DRM, the content that user can buy is encrypted one. The steps of using this encrypted contents are as follows;

1. normal buyer communicates with the contents provider's server directly and verifies himself or herself,
2. after he completes the verification, contents provider's server sends the decryption key to the user's playback software of its media, even if a normal buyer cannot use this decryption key and get an unencrypted content,
3. when a user uses the contents, he or she use the media playback software and use the contents,
4. the media playback software running the contents in concurrence with decrypting the contents with the decryption key,
5. if the contents ends, the media playback software discards the decryption key.

As the above, normal user also cannot get the unencrypted contents because the content is run by user's playback software in concurrence with decrypting. This means that no user can do illegal distribution of unencrypted media. As a problem of this DRM, it is hard to computerize all traffic for the contents provider's server. The more people want to use the media, the harder the contents provider's server computerizes traffic because when a people decrypt the contents, he or she must communicate with the contents provider's server. If the contents provider's server is out, no users can get the decryption key and use the media.

This means that DRM system imposes an enormous drain on the normal users. In fact, existing DRM system, such as MPEG-21, almost focus on two relationships, contents provider and buyer[2].

IMCOM (ICUIMC) ’14, January 9-11, 2014, Siem Reap, Cambodia
Copyright 2014 ACM 978-1-4503-2644-5 ...$15.00.

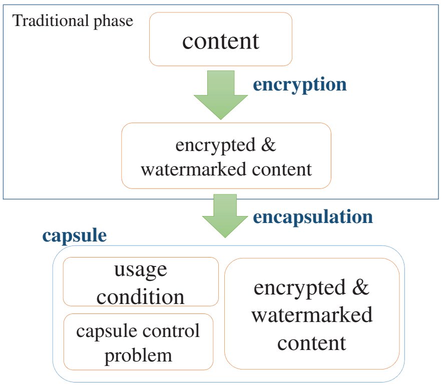

Figure 1: Content encapsulation.

1.3 Related work

In DRM system, two kinds of methods, client-server computing based system and peer-to-peer based system have proposed. In this section, we compare these two systems about the implementation methodology and its differences. DRM system has two steps in encryption of contents. In first step, it encrypts the contents. In second step, it encapsulates the encrypted contents adding a usage condition and capsule control problem. The figure 1 shows the normal encryption method and the DRM's encapsulation method.

In the normal encryption method, we show the traditional phase of 1, content is encrypted to prevent the illegal usage. In the DRM's encapsulation method, legally buyer may become the attacker and he or she may outpour the plain content to general public as an attacker. To prevent this illegal use, in the DRM's capsule system, normal user cannot get the plain content. The all part of 1 shows the DRM's capsule system. First, it encrypts the content and adds a watermark. And then, it encapsulation with usage condition and capsule control problem. The usage condition is the permission that user has the right of use the content or not. The capsule control problem decrypts the content and gives us the content with streaming method. By this work, we can use the content without getting the plain content itself.

1.3.1 *Client-server computing based DRM system*

In early introduction times of DRM, this client-server computing based DRM system was major method. In this method, content's provider must prepare the dedicated server for management of contents provide, which manages all users such that it distributes decryption key for decrypting contents or verifies users, whether they are authorized one or not. contents distributor and contents manager is the same, but in that system, contents and its DRM are separated and finally encapsulated[3]. The condition for using the contents in this approach is to receive a secret key from the server. The advantages over these methods are that the management can be centralized, and it is easy to manage the billing and research of user's usage situation.

However, there was a problem that the more people use the contents, the more the server has to verify a user and upload a decryption key. It may cause the server is out. For this reason, we create more than one server for verification and reduce the traffic. By increasing the number of servers depending on the users, it can respond dynamically scalable. However, it is hard to forecast the number of users and extend the server, so it does not become a fundamental solution to the problem, and the following P2P based DRM system have been proposed.

1.3.2 *P2P based DRM system*

The DRM system utilizing P2P, there is no need to rely on the management server to distribute the content itself because each user can distribute the contents for each. DRM management server exchanges a permission to use of each user's contents for the money. Further, in the P2P based DRM system has the advantage that by registering the content with copyright for DRM management server, any user can become a contents provider. Not only it is possible to provide contents easily even in private, but also each company is to provide a system of its own over the cost is eliminated for utilizing a large system.

As an example of the implementation of DRM, it is considered that the validation is done by using the ID of the user[4]. The content playback software sends the ID of the owner at their first time of using a content to the management server, and the contents provider claim price at a later for the registered ID. In this technique, the usage condition is to send his or her own ID to the management server. Through the specification as such, it is possible to freely distribute by each user. Even if a large amount of users wishes to content at one time, the download is possible by using the P2P from the contents holder, so the overload on the server is eliminated. There is no usage condition because there is no need to send money in advance, but when it comes to preventing an unauthorized use of the contents, it relies on the point that the user sends his or her ID at first time to use contents. To save this protection and avoid the activating without sending his own ID, it is encrypted and encapsulated.

In addition, they propose three kinds of P2P based DRM system, one is similar to client-server computing based DRM system, another method is distributed P2P based DRM system which the contents provider manages the authorized user DB, and the other one is semi-distributed P2P based DRM system, which relies on the DRM management server for the authorized user DB.Further, it is also mentioned that trading system one user and others. It is necessary to introduce DRM management server for encapsulating the contents in any methods. A contents provider sends the usage condition and contents to the DRM management server and gets the encapsulated contents. The contents provider distributes this capsule. After other users who want to use the contents get this capsule and satisfy its usage condition, the user can use the contents. For more information about the differences of each approach, it is following.

In the method similar to client-server computing based DRM system, DRM management server manages the DB for an authenticated user. The users who get an encapsulated content communicate with the DRM management server and get the permission for usage condition. The difference between this type and existing work lies over the delivery system of contents, which is encapsulated that can be freely between all users. Therefore, we may be able to distribute and get the encapsulated contents over-concentration, but there are some problems that when a user gets the permission, it concentrated in the DRM management server in terms of obtaining a use permission user as more and the difficulty of recognition to the distribution status for contents provider.

In the method of distributed P2P based DRM system, the contents provider manages the authorized user DB. The users who get the encapsulated contents communicate with the contents provider and get the permission for usage condition. The contents provider can use any DRM management server, so there is no problem in content distribution even if the user increased. It means that this system fulfills the complete P2P based DRM system. Disadvantages of this method are that the permission of usage and exchange of permission and money is done only by contents provider, and no user can look out over the whole. The former takes much cost to the contents provider in private, and later takes that no one can get statistic data.

In the method of semi-distributed P2P based DRM system, the DRM management server manages the authorized user DB. The users who get the encapsulated contents communicate with the contents provider to get the permission for usage condition, but the contents provider does not have it, so the contents provider communicates with the DRM management server to get the verification and usage condition. And then, the users get the permission of the contents. Each contents provider can separately communicate with any DRM management server, so it is strong against the overload of server. Moreover, it is convenient for contents provider in case of the billing exchange because we can rely on the management server. It can be said that this method is inheriting the advantages of server-client type and increasing as much as possible availability.

Thus, this method can deal with the increasing of users, but this system has some problems in a possibility of realization because it is hard to figure out the usage situation and the lack of advantage for user to distribute the encrypted contents. A more practical method is proposed against this problem as a framework[5]. In this paper, the distributed user is paid to take some costs as a royalty. The author considered how to give some royalty, add the license, and packaging the contents, did not consider so much the Business model or detail of distribution. As a final contribution, they point out the weakness of MPEG-21 and give some improvements. However, they said there are unsolved issues are remained. One of the issues is the difficulty of standardization.

1.4 Contribution

In this paper, we consider a new DRM system based on P2P network. We focus on the Bitcoin protocol which keeps the security only with the users' communication, and we add in this protocol to the DRM system. This means that a new DRM system is constructed specialized on the P2P network, and it is easy to standardization by using the existing protocol. Bitcoin is one of the electronic-commerce systems and has the protection against double spend that a user uses one coin in twice and gets two products. We draw on this protocol in DRM system to bring out the detail of the transaction or distribution. This will enable that we can give some value to someone who distributes many encapsulated contents and analysis the total traffic or usage situation.

1.5 Comparison with existing works

In this section, we make a comparison with the existing method of P2P based. In the method of Iwata et al. which we mentioned above, the verification was done by the ID which is gathered in the server[4]. It does not care who distribute the contents, so all we can find from that is who used the contents. This is simplified method, and it has minimum function. In the proposed method, it passed a coin as the usage condition. All users who can use the contents have this coin, and the user who has the coin is registered by preventing the double spending. For searching these log files. We can figure out who distribute the contents. In fact, contents distribution has no advantage for the user in P2P network, so it is important for users to get the advantage of not only contents download but also contents distribution for realization. In our method, anyone can figure out who distributes the contents, so it is possible to give some advantage to such users. We show the comparison table in table 1. Our proposal method is similar to P2P based DRM system and has some advantage of the visualization.

2. ELECTRONIC COMMERCE AND DRM

Electronic-commerce system is that we can use the specific data as a money on the Internet. Users buy the data with cash, and then, they can buy some products for using the specific data. This data is ensured by the generator of its value.

2.1 P2P based Electronic-commerce system

Iwata et al.'s method is famous as a P2P DRM. In this method, the contents is covered to the capsule and normal user cannot get the plain contents. All user can get the capsuled one and the time using the contents, they send his ID. However, in this system, it is convenient for sending Electronic money instead of user's ID. The manager do not have to retrieve the money and can get the money surely.

Normal Electronic money is considered for this so far, but now, we think new Electronic-commerce system based on P2P network which we can deal with the right of use and paying money together. It is Bitcoin. In this system, no one ensures the value of coin, just data[6].

2.2 Bitcoin

Bitcoin is one kinds of electronic-commerce systems, and has the paticular features.

As a main feature of this method, it does not have a centralized server. Bitcoin transaction is on P2P network. So, all participants are the same standpoint and the coin's value is depend on the participants. It means that no one ensure the value of the data, but everyone believe that the data has the value.

In another feature, a transaction of coin is done by signature. A transaction which exchanges coin for money is that sender signs his own coin and the receiver's waller(public key) with his private key. In Bitcoin system, the coin is represented by a chain of digital signatures. The public key written in the coin ensure who is the owner of the coin, and the signature of the previous owner in it ensure the validity of the coin. For this reason, coin owners do not have to hold each coin, it can be published on all networks. Moreover, all participants have become verifiable its validity.

In Bitcoin protocol, privacy keeps by using the anonymous public key. The users can hide information how much he has the coin as a bitcoin by using the public key of anonymous created from given ID, even if he shows all coin he has. However, he must not use the same public key[7].

Table 1: Comparison with existing works.

	Similar to client-server computing	Distributed P2P	Semi-distributed P2P	Proposal method
Tolerance of users increase	low	high	high	middle
Load on the server	large	small	middle	small
Complexity of the billing	easy	hard	easy	complex
Speed of processing on the server	slow	fast	fast	fast
Account management	easy	hard	easy	easy
Tracking of the distribution	no	no	no	yes

Algorithm 1 sending contents

```
require $C$ : contents, $M_1$ : coin, $P_k$ : contents buyer's public key
send $C$ to the contents management server and get encapsulated $E$
$M_2 \leftarrow M_1 \parallel P_k$
$M_2 \leftarrow$HASH$(M_2)$
$M_2 \leftarrow$SIGNATURE$(M_2) \parallel M_1$
get money from the buyer
return $E, M_2$
send $E, M_2$ to the contents buyer
```

Algorithm 2 encapsulation

```
require $C$ : content
$S \leftarrow$ENCRYPT$(C)$
$D \leftarrow$"having a coin on the Bitcoin network"
$P \leftarrow decryption_program$
$E \leftarrow$ENCAP$(S, D, P)$
return $E$
```

Different from the traditional electronic cash, coins in Bitcoin is treated the same as real money.

2.3 Bitcoin protocol

In Bitcoin protocol, there are some features different from the normal Electronic-commerce system, as follows:

- a user generate a public key from his own ID and this public key is anonymous and he can generate any number of keys,
- in Bitcoin system, coin is being public on the Internet and everyone can verify all coins associated with which public keys,
- in case of sending own coin, sender encrypts the coin with receiver's public key and adding signature by signing with own secret key,
- validation check of coin's owner is done by verifying the the previous owner's signature,
- to prevent the double spending, all transaction is registered by timestamp server,
- the first coin is automatically generated, and the first person who find the coin can get it.

3. PROPOSAL METHOD

In this section, we consider a new DRM system using the Bitcoin protocol. DRM system has some kinds depend on the situation, so we consider some kinds of DRM systems. In addition, we only focus on the on-line method.

At this time, we propose two systems based on Bitcoin system. In both systems, we consider the coin as a right to use of contents and all users can verify whether other users have the coin or not.

We use following notations in this paper. $a \parallel b$ denotes concatenation of two strings a, b. M denotes the coin on the Bitcoin network. C denotes the contents. P denotes the public key. E denotes the capsule of contents. D denotes the usage condition. HASH(x) denotes the output of hash function adding x. SIGNATURE(x) denotes the sign that output of signature function adding x. ENCRYPT(x) denotes the output of encryption method adding x. ENCAP(x, y, z) denotes the output of capsule x by adding the usage condition$y$ and control program z. OPEN(x) denotes the plain contents in encapsulated contents x.

3.1 Proposal method 1: normal DRM

As a first example, we consider the new DRM system that if a user who bought the contents sends the contents itself to another user, the sender cannot use the content after that. This means that it is possible for the user who bought the content to sell to others. In this case, the sender who sold the contents cannot use the contents itself after that. In addition, it can be said that it is possible for everyone to check all the transactions, it pays a certain amount to the contents providers in every trade. To realize this method, the user does the transaction of money and coins in the same way as Bitcoin system. For this, we introduce the timestamp server, and record all transactions to remain regarding coins. A user can use contents only while with the coin, and it becomes no longer possible to use the content after the user gets out the coin.

3.1.1 Protocol

We shows the protocol of our proposed method 1 in this section. Algorithm 1 shows the steps of sending contents. Who want to sell the contents such as contents provider does this algorithm. In this algorithm,he convert his coin to the buyer's coin in exchange for money. It means that buyer becomes to be able to use the contents. Algorithm 2 shows the steps of contents encapsulation. In this algorithm, he convert the contents to the capsule by adding the usage condition and control program. We do not care who do this encapsulation. It is possible to capsule for the seller himself and for the contents manager. And Algorithm 3 shows the steps of use and resell contents. In the resell step, seller convert his own coin to the buyer's coin and get money. The only thing to converting the coin means selling the contents.

And then, we points out the particular topics of this method as follow:

Algorithm 4 sending contents

```
require $C$ : contents, $M_1$ : coin, $P_k$ : contents buyer's public key
send $C$ to the contents management server and get encapsulated $E$
send $E$ to the buyer
$M_2 \leftarrow M_1 \parallel P_k$
$M_2 \leftarrow$HASH$(M_2)$
$M_2 \leftarrow$SIGNATURE$(M_2) \parallel M_1$
get money from the buyer
return $E, M_2$
send $E, M_2$ to the contents buyer
```

Algorithm 5 encapsulation

```
require $C$ : content
$S \leftarrow$ENCRYPT$(C)$
$D \leftarrow$"to have had a coin on the Bitcoin network"
$P \leftarrow decryption_program$
$E \leftarrow$ENCAP$(S, D, P)$
return $E$
```

Algorithm 3 use and resell contents

```
require $E$ : capsule, $M_2$ : coin and $P_k$ : second contents buyer's public key
if want to play the contents then
    $D \leftarrow$OPEN$(E)$
    check the usage condition $D$
    if satisfy $D$ then
        $C \leftarrow$OPNE$(E)$
        return $C$
    else
        return 0
    end if
else if want to sell the contents then
    communicate with the user who want to buy the contents
    $M_3 \leftarrow M_2 \parallel P_k$
    $M_3 \leftarrow$HASH$(M_3)$
    $M_3 \leftarrow$SIGNATURE$(M_3) \parallel M_2$
    get some money $G$ from buyer
    return $E, G$
    send $E$ to the second contents buyer
end if
```

- a contents provider generate some coins or the number of products to sell and it can be the time he sell the contents,

- the contents can be used by using the latest coin. It means that the usage condition is having the latest coin,

- when a user use the contents, the permission accept if the user has the latest coin on the Bitcoin protocol in all network by using timestap server,

- the first buyer directly exchange the contents from the provider, giving the cash and getting the coin and contents,

- in case the first buyer sells the contents to others, the first buyer change over his coin to receiver's coin so the contents has no change,

- the second buyer getting from first buyer gives cash to first buyer and gets the contents and coin,

- coin is public on the Internet, so everyone can verify the latest coin and the previous owner's signature.

3.2 Proposal method 2: Resellable DRM

As a second example, we consider the new DRM system that we do not care the resale contents system. In this system, we can distribute by copying the coins and change over its coin to receiver's one. However, the user who distributes the contents must send the cash which getting from the exchange to the contents provider. Everyone can verify these conditions is satisfied or not. As a result, we impart a function similar to digital watermarking of all users. In this approach, when the user distributes the content, the transaction is not directly financial transaction to the provider but to the user. Everyone can figure out who has been distributed by the content history that was engraved on the coin, so we can send back the money in accordance with its history. In this point, it imposes a burden on the user is a disadvantage, but if we have a system that a user who contributed to the distribution may get some money, aggressive market can be expected, even this system is P2P based one.

3.2.1 Protocol

We shows the protocol of our proposed method 2 in this section. Algorithm 4 shows the steps of sending contents. Who want to sell the contents such as contents provider does this algorithm. In this algorithm,he convert his coin to the buyer's coin in exchange for money. It means that buyer becomes to be able to use the contents. Algorithm 5 shows the steps of contents encapsulation. In this algorithm, he convert the contents to the capsule by adding the usage condition and control program. We do not care who do this encapsulation. It is possible to capsule for the seller himself and for the contents manager. And Algorithm 6 shows the steps of use and distribution of contents. In the distribution step, distributer convert his own coin to the buyer's coin and get money. The only thing to converting the coin means giving the use right of the contents.

And then, we points out the particular topics of this method are as follows:

- a contents provider generate some coins or the number of products to sell and it can be the time he sell the contents,

- the contents can be used by using any coin and it means that the usage condition is having a coin,

- when a user use the contents, the permission accept if the user has a coin on the Bitcoin protocol in all network,

- the first buyer directly exchange the contents from the provider, giving the cash and getting the coin and contents,

- the second buyer getting from first buyer gives cash to first buyer and gets the contents and coin, Algorithm 6 use and distribute contents

```
require $E$ : capsule, $M_2$ : coin and $P_k$ : second contents buyer's public key
if want to play the contents then
    $D \leftarrow$OPEN($E$)
    check the usage condition $D$
    if satisfy $D$ then
        $C \leftarrow$OPEN($E$)
        return $C$
    else
        return 0
    end if
else if want to distribute the contents then
    communicate with the user who want to buy the contents
    $M_3 \leftarrow M_2 \parallel P_k$
    $M_3 \leftarrow$HASH($M_3$)
    $M_3 \leftarrow$SIGNATURE($M_3$) $\parallel M_2$
    get some money $G$ from buyer
    return $E$, $G$
    send $E$ to the second contents buyer
    send the part of $G$ to the contents provider
end if
```

- the money which the first buyer got sends back to the contents provider in accordance with its history, and in this time, who contributed to the distribution may get some money can be possible,
- coin is public on the Internet, so everyone can verify a coin and the previous owner's signature.

4. CONCLUSION

We proposed a new DRM system based on Bitcoin protocol. In this method, it has three features. One is the transparent to the network, another is the aggressive market in P2P system, and the other is the reutilization applying for the existing Bitcoin network. First, about the transparent to the network, all people can verify the transaction, so all users can use it with relief. Second, about the aggressive market, it is easy to give the royalty. All people want to get the royalty, so they may tend to distribute the contents themselves. Finally, about the reutilization, it may be possible to be standardization, because the Bitcoin network is ensured its security. Everyone can reutilize the network in DRM.

Acknowledgment

This work is partially supported by Grant-in-Aid for Scientific Research(B) (23300027) from the Japan Society for the Promotion of Science (JSPS).

5. REFERENCES

[1] Bill Rosenblatt, Bill Trippe, and Stephen Mooney. Digital rights management: business and technology. New York, 2002.

[2] Ian S Burnett, Fernando Pereira, Rik Van de Walle, and Rob Koenen. The MPEG-21 book. Wiley Online Library, 2006.

[3] William Ku and Chi-Hung Chi. Survey on the technological aspects of digital rights management. In Information Security, pages 391–403. Springer, 2004.

[4] Tetsuya Iwata, Takehito Abe, Kiyoshi Ueda, and Hiroshi Sunaga. A drm system suitable for p2p content delivery and the study on its implementation. In Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on, volume 2, pages 806–811. IEEE, 2003.

[5] Junseok Lee, Seong Oun Hwang, Sang-Won Jeong, Ki Song Yoon, Chang Soon Park, and Jae-Cheol Ryou. A drm framework for distributing digital contents through the internet. ETRI journal, 25(6):423–436, 2003.

[6] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 15:2012, 2008.

[7] Elli Androulaki, Ghassan Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in bitcoin. IACR Cryptology ePrint Archive, 2012:596, 2012.