九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Bitcoin プロトコルの拡張による著作権管理方式の提案

北原, 基貴
九州大学

川本, 淳平
九州大学

櫻井, 幸一
九州大学

https://hdl.handle.net/2324/1662106

出版情報：暗号と情報セキュリティシンポジウム. 2014, pp.4F1-, 2014-01-21
バージョン：
権利関係：

Copyright ©The Institute of Electronics,
Information and Communication Engineers

SCIS 2014 The 31st Symposium on
Cryptography and Information Security
Kagoshima, Japan, Jan. 21 - 24, 2014
The Institute of Electronics,
Information and Communication Engineers

Bitcoin プロトコルの拡張による著作権管理方式の提案
Digital Rights Management by using the extended Bitcoin Protocol

北原　基貴 *　　川本　淳平 *　　櫻井　幸一 *
Motoki Kitahara　　Junpei Kawamoto　　Kouichi Sakurai

あらまし デジタル上における著作物は，保存や複製が容易というその特徴から，違法コピーが大量に作られてきた．これを防ぐために用いられるのが著作権保護システムである．コンテンツ提供者が正規購入者を判別するための認証サーバを導入し，コンテンツを一元管理するという手法が多く用いられてきたが，そのサーバにアクセスが集中し，サービスが停止するという問題が存在した．この問題に対する先行研究として，コンテンツの分配に P2P を用いた手法が存在する．P2P 通信によりコンテンツの分配を各ユーザが行うことができるため，配布用サーバにかかる負担を最低限にすることができる．P2P コンテンツ分配における DRM として，我々は，電子マネーの一種である Bitcoin プロトコルを応用した手法を提案してきた． Bitcoin におけるコインを利用権とみなすことで，コインをもつユーザが利用可能としていた．この手法では相互認証が可能で，P2P 分配の実現可能という利点があるが，コンテンツ購入のための金銭の取引を現金で行うことを想定しており，正しく金銭の授受が行われたことをシステムとして確認・保証できないという問題点が存在した．本論文では既存研究で問題であった，金銭の取引に関してシステム化を行った．現在用いられている Bitcoin のプロトコルにコンテンツの利用権となる要素を追加することで，Bitcoin における通信のやりとりのみでコンテンツの購入や金銭の支払いを完結できている．また，P2P コンテンツ分配の特徴である，分散コンテンツ取得に対する提案 DRM の拡張を行った．

キーワード DRM, Bitcoin, P2P ネットワーク

1　序章

1.1　背景

インターネットの普及とコンピュータの発展に伴い，様々なコンテンツが情報媒体として取り扱われるようになってきた．多くのメディアを持ち歩くことができること，コピーが容易なことやインターネットに繋がっていればどこでも購入できるといった利点が存在する．しかし，このデジタル媒体はコピーが容易なため，インターネットを通して不特定多数と媒体を共有できてしまうという問題がある．これを防ぐ，正規の購入者のみが利用可能にするために導入されたのが著作権管理システムである DRM(Digital Rights Management) である．

DRM を使用する場合，利用者が購入できるコンテンツは暗号化されたものとなる．これは，オリジナルのコンテンツを利用者が入手可能な場合，そのコンテンツをコピーし，不特定多数の人に渡してしまう可能性があるためである．よってコンテンツには暗号化を施し，コンテンツを利用する際も利用者がオリジナルのコンテンツを手にすることなく利用するという形式になる．このプロトコルは次のようになる．

まず，正規の利用者はコンテンツ配布者と通信を行い，コンテンツを購入する．この際，コンテンツ提供者は自身のサーバに購入者の情報を保存する．購入者がコンテンツを利用する場合，コンテンツ提供者と通信を行い，自身が正規の購入者であると認証を行う．認証が無事完了したら，コンテンツ提供者は購入者が持つコンテンツ再生用のソフトウェアに対してコンテンツの復号鍵を送る．この復号鍵は再生用ソフトウェアのみが用いることができ，正規の利用者であってもコンテンツ自体の復号はできないとする．この鍵を用いてコンテンツの利用を行う場合は，購入者がコンテンツ再生用のソフトウェアに対して暗号化されたコンテンツを送る．コンテンツ再生用のソフトウェアは，自身が持つ復号鍵を利用し，コンテンツを復号しつつ再生する．コンテンツの再生が終了したらコンテンツの再生用ソフトウェアは復号鍵を廃棄する．実際のシステムにおいては，毎回復号鍵を得るために通信を行うという方式では通信コストが大きくなるため，この復号鍵は一定期間保持するように設定されていることが多い．このため，鍵の認証ではコンテンツ提供者のサーバにとって負荷になることは少ない．正規

* 九州大学, 福岡県福岡市西区元岡 744, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, Fukuoka, Japan

の利用者でもコンテンツを復号しつつ再生するため，暗号化されていないコンテンツを得ることはできない，このことにより，暗号化されていないコンテンツの二次配布を防ぐ事ができるといえる．

この DRM の問題点として，コンテンツの配布によるコンテンツ提供者のサーバに掛かる負担が大きいという点が存在する．正規の利用者がコンテンツを購入する場合，暗号化やデータベースへの登録の観点から，コンテンツ提供者のサーバから直接購入する必要がある．この際，コンテンツ自体の容量が大きいため，コンテンツ提供者のサーバへと負荷が集中することになる．利用者の数が増加すればするほどこの通信は増え，負担も増加する．もしこのサーバに対する負荷が膨大になり，正常なサービスを提供が不可能になった場合，全ての正規の利用者はコンテンツを再生することができなくなる．この点は DRM を利用しない場合と比べて正規の利用者に負担をかける，利便性を低下させるということであり，大きな問題といえる．

この問題を解決するため，P2P による通信を用いてコンテンツの分配を行う DRM 方式が複数提案されている．認証方式や復号方式に変更を加え，P2P を用いてコンテンツの分配を行うことでコンテンツ提供者への負荷集中問題の解決している [3]．それらの手法の一つとして，電子現金の一種である Bitcoin に着目した手法が存在する [8]．この手法では Bitcoin のプロトコルを利用し，Bitcoin におけるコインを利用権と定義した新たなシステムの構築を行う．この利用権を持つ利用者だけがコンテンツの利用が可能になるというシステムである．Bitcoin プロトコルは，すべてのトランザクションが全利用者に対して公開されるという特徴がある．この仕組みにより，参加者全員で互いに検証しあうという P2P の利点を活かしたシステムとなっている．この方式における問題点として，コンテンツ購入における金銭の授受をシステム外のものとしていた．取引における利用権の取引は提案するプロトコルを用いるとしており，それらの通信は参加者全員で検証することができる．しかし，実際にコンテンツを購入する際の金銭の支払いが検証できないため，最終的に金銭が支払われたかの認証はコンテンツ提供者にしか出来ないシステムであった．また，P2P を用いているが，コンテンツを分割して多人数から集めることができないという問題もある．現状用いられている多くの P2P システムでは，最終的にコンテンツが完成できれば，コンテンツは部分的に多数の場所から得ても問題はない．しかし既存研究ではこの点が実現できていない．このため，P2P を利用する目的である負荷分散が，部分的にしか実現できてないといえる．

1.2 提案手法における貢献

本論文では，P2P をベースとした DRM システムにおいて，既存研究の拡張を行う．金銭の支払いが可能であり多人数から集めることのできるシステムを提案する．Bitcoin プロトコルに対し，コンテンツ利用権として用いる要素を追加する．この要素を取引に用いるとともに，金銭の取引は Bitcoin 本来のコインを用いる．これにより，支払う金銭と利用権の両方を参加者全員で認証可能になる．また，コンテンツ分割数と同じだけ利用権を分割することで，分割されたコンテンツを多人数から集めた場合でも分配による利得付けを実現している．このため，P2P システムにおける負荷分散を，既存研究より高い次元で実現化できたといえる．

2 関連研究

DRM は違法なコピーを防ぎ，手数料を課し，支払いの処理を系統立てし，コンテンツを追跡し，利権者の権利と利益を守ることでコンテンツをセキュアに保つことと定義されている [7]．よって，DRM システムを考える場合はこれらの要素を満たすシステムを考える必要がある．

実際に，著作権管理方式として規格化を目指しているものの一つとして，MPEG-21 があげられる [2]．これは違法コピーに対して，従来の規格では実現出来なかった DRM の基本要求や規格における開発のマルチメディアフレームワークを実現することを目的としている．そのため，コンテンツのカプセル化や分配を行う機関に関してより詳細に定義を行っている．しかし，この方式ではより現実世界に則した，様々な分配のモデルまで網羅できていないという問題が存在している．実現不可能な例として，超流通と呼ばれる複製防止を行わずに改変の防止を防ぐシステムや，小売店を考慮した，仲介を行う売買システムなどがあげられる．

Lee らはこれらの手法に対し，より現実世界にそった，利用を促す目的でコンテンツ配布参加者にロイヤリティを与えるフレームワークを考案している [5]．この手法では，ビジネスモデルや配布の詳細には触れず，ロイヤリティの与え方やライセンスの付加，パッケージングについて考察を行っている．最終的に，先ほど述べた著作権保護のための手法である MPEG-21 の欠点に関して実例を挙げ，その改善となる新たなモデルとその前提となるとして三つの考えを提案している．そのうち，一つ目としてインターネット上には大量のデータが存在しているが，優先度の高いものは多くはないということ．二つ目として，全ての有りうる分配モデルを網羅することはできないため，何を選択するかが大事であるということ．三つ目として，不正利用の技術も日々進歩していくことを考慮すべきということ．これらの要素を踏まえ，今の

世界における優先度をもたせた手法を提案している．また，著者らはこの手法の問題点として，重要な情報，すなわち権利者の情報や暗号化に用いる鍵の管理方法と標準化として設立させることをあげている．

また，コンテンツの分配について細かく見た場合，コンテンツを一元配布するサーバ・クライアント型と利用者同士でコンテンツを交換し合う P2P 型が存在する．上記で述べた MPEG-21 や Lee らの手法ではどちらも考えた，大きな枠組みとしての提案だったが，実際に DRM を行うことを考えた場合，サーバの負荷という観点で差が存在しているため，個々に見ていく必要がある．

2.1 サーバ・クライアント型 DRM

サーバ・クライアント型 DRM 方式はコンテンツ配布者が管理用のサーバを導入し，そのサーバが全利用者の管理や，正規利用者であるかの検証，暗号化コンテンツを復号するための鍵の送信を行うシステムである．利便性の観点から，すでに存在しているコンテンツに対しても簡単に DRM で用いることができるよう，コンテンツと DRM を別に扱い，カプセル化するという方式が取られることが多い [4]．この手法におけるコンテンツを利用するための条件は「サーバから秘密鍵を受け取ること」となる．利点として，管理が一元化でき，ユーザの調査や課金の管理が容易であるという点がある．

しかし，この手法の問題点として，コンテンツを利用するユーザが増えれば増えるほどそのサーバに対する負荷が増大するという問題がある．このため，利用者が正規コンテンツ購入者であるかの検証用サーバを複数作成し，負担を減らすという手法が取られてきた．利用者数の増加に合わせてサーバ数を増やすことで，利用者の増加にある程度の対応はできる．しかし，利用者の増加に備えてある程度冗長性を持たせる必要があり，無駄の多いシステムとなっている．このため，サーバに負荷のかからない P2P 型の DRM が提案された．

2.2 P2P 型 DRM

P2P を利用した DRM 方式では，コンテンツ自体の配布は各ユーザがそれぞれで行うことができるため，管理サーバに依存する必要がない．コンテンツ提供者のサーバはそれぞれの利用者が持っているコンテンツに対して，金銭を受け取ることと引き換えに利用許可を与える．また，P2P 型 DRM システムでは，DRM 管理サーバに対して自分が著作権を持つコンテンツを登録することで，任意のユーザがコンテンツ提供者になることも出来るという利点がある．コンテンツ提供が個人でも容易に可能になるだけでなく，信頼できる大きなシステムが一つあれば，各企業がコストをかけて自前のシステムを用意する必要もなくなる．

P2P 型 DRM の実現の一例として，ユーザの ID を用いて検証を行うという手法が考えられている [3]．コンテンツの初回利用時に自身の ID を管理サーバへ送信するコンテンツ再生用ソフトウェアを用い，管理サーバは登録されている ID に対して後日代金を請求するというものである．この手法では，利用条件は ID を送ることとなる．このような仕様にすることで，自由に配布することが可能となる．コンテンツを希望するユーザが一度に大量に出たとしても，コンテンツ保持者から P2P ネットワークを利用してダウンロードが可能であり，サーバ負荷を削減できる．利用条件はコンテンツの初回起動時に自分の ID を送るという点であり，コンテンツの不正利用を防ぐことに関しては，この点にかかっているため，この部分を迂回してコンテンツが起動できてしまわないよう暗号化・カプセル化を施している．この手法では，認証をコンテンツ提供者が一手に引き受けなければならないという問題と，コンテンツの配布状況が不透明であるという問題がある．これは DRM の定義の一つであった，「コンテンツを追跡する」という点を満たすことができず，コンテンツ配布者にとって得られる情報が少なく，マーケティングを行いづらい，不完全な DRM 方式であるといえる．また，認証においても ID のみの方式となっており，十分に安全であるとは言いづらい．

また，別の P2P を利用した DRM 方式として，我々は，Bitcoin プロトコルを用いた手法を提案した [8]．この手法において，利用者がコンテンツを購入する場合，同時にコンテンツの利用権を得る．このコンテンツの利用権を持っている利用者のみがコンテンツを利用可能になる．このコンテンツの利用権は Bitcoin プロトコルにおけるコインと同等に扱うため，参加者全員が常に「誰が利用権を持っているのか」の検証を行うことが出来る．よってコンテンツの利用条件を「利用権を持ったことがあること」と定義することで，P2P 型の DRM が構築できる．また，利用権の受け渡しトランザクションが全員に明示されるため，トラッキングが行いやすいという利点と，分配者に利得を与えることができるという利点，そして不正を働いた利用者が全員に公開されるという利点がある．この手法では，分散ダウンロードを考慮していなかったため，コンテンツを分割し，複数人からコンテンツを部分的に得る事ができないという問題と，金銭の受け渡しが考慮されていないという問題点が存在する．

2.3 Bitcoin

Bitcoin は，電子現金の一種である [6]．Bitcoin は現実世界における金と同様に，そのコインの価値をコインとなるデータ列が有限であることにより保証されている．

Bitcoin の利用者は自分の ID から公開鍵を作成する．この公開鍵に対してコインが紐付けられる．コインの情

報は全員が共有しており，誰もがコインがどの公開鍵に紐付けられているか確認することができる．Bitcoin において，コインの受け渡しは相手の公開鍵による暗号化と自身の秘密鍵の署名により行う．すなわち Bitcoin システムでは, コインは電子署名の連鎖によって表されている． コインを持つ利用者が別の人にコインを渡す場合，まず送りたい相手の公開鍵を用いて自身の持つコインを暗号化する．次に得た値に対して自身の秘密鍵で署名を行う．最終的に得られたデータをネットワーク上にブロードキャストを行い，全員がこのデータを更新することでコインの受け渡しは完了する．コインの所有者の正しさ確認は，コインの前所有者の署名を検証することにより行う．最終的にルートまでたどることができればコインは正当な手続きにより現在の所有者に渡ったと検証できる．コインは全ネットワーク上で公開されており, その正当性も参加者全員が検証可能となっている．

Bitcoin には所有者の匿名性をもたせる機構として，利用者と公開鍵の対応を匿名化している．利用者は自身の持つ ID から作成した匿名の公開鍵を用いることで, ネットワーク上に全て情報を公開しつつも自分がいくらコインを持っているかの情報を秘匿することが出来る. ただし, 完全な匿名性は毎回公開鍵を使い捨てにしなければ実現できない [1]．また，Bitcoin の安全性はハッシュ関数の一種である SHA-256 に依存している．もしこのハッシュ関数が破られてしまった場合，コインの違法作成が可能となる．Bitcoin におけるコインは二重使用を防ぐため，タイムスタンプサーバを用いて全ての取引が記録されている．受け取ったコインに対して同じコインが過去別の誰かに送られていないか取引を調べることで，ひとつのコインを二度使用することを防いでいる．

3 定義

本論文では以下の定義を用いる．$a \parallel b$ は二つの文字列 a, b の連結を表す．$\mathrm{SIG}(x, y)$ は y を署名に用いる秘密鍵, x を署名する文書とした時の出力を表す．$\mathrm{HASH}(x)$ は x をハッシュ関数に入力したときの出力を表す．$\mathrm{ENC}(x, y)$ は y を暗号に用いる秘密鍵，x を暗号化する文書とした時の出力を表す．$\mathrm{DEC}(x, y)$ は y を復号に用いる秘密鍵，x を復号したい文書とした時の出力を表す．$\mathrm{ENCAP}(x, y, z)$ はカプセル化関数にコンテンツ x，利用条件 y，動かすプログラム z を入力した時の出力を表す．

Bitcoin プロトコルにおいて，以下が用いられている．利用者 A は PK_A という公開鍵と，SK_A という秘密鍵を持つ．ある Bitcoin ネットワーク上には，$C_0, C_1, ..., C_n$ という n 個のコインが存在する．全てのコインは最初はルートに存在しており，発掘に成功した利用者がこのコインの所有者となる．本論文では，コイン C_0 をユーザ A が持つ場合，$C_{0,A}$ と書く．コインがルートにある場合，$C_{root,0}$ と書く．ユーザ A が持つコイン $C_{0,A}$ をユーザ B に送る操作を，$\mathrm{SEND}(SK_A, PK_B, C_{0,A})$ と書く．この際 $\mathrm{SEND}(SK_A, PK_B, C_{0,A})$ は

$$\mathrm{SIG}(\mathrm{HASH}(C_{0,A} \parallel PK_B), SK_A) \parallel C_{0,A}$$

を意味する．利用者 B が利用者 A から真に正しいコインを受け取ったかの確認をする場合，$\mathrm{HASH}(C_{0,A} \parallel PK_B)$ の値と $\mathrm{VERIFY}(PK_A, C_{0,B})$ が等しいことを確かめる．この際，$\mathrm{VERIFY}(PK_A, C_{0,B})$ は

$$\mathrm{DEC}(\mathrm{SIG}(\mathrm{HASH}(C_{0,A} \parallel PK_B), SK_A), PK_A)$$

を意味する．この値が正しかった場合，更に一人前の取引において，同様の検証を行う．最終的にコインがルートまでたどることができれば利用者 B が持つコインは正規に利用者 A から授与されたと証明できる．これらの検証の連鎖を，$C_{B,0} \vdash C_{A,0} \vdash ... \vdash C_{root,0}$ で表す．

4 提案手法

この章では，P2P をベースとした，金銭の支払いが可能でありコンテンツを多人数から部分的に集めることのできる DRM システムを提案する．既存の Bitcoin プロトコルに対し，利用券とそれを扱う関数を追加する．コンテンツ購入代金の支払いには，Bitcoin 本来のコインを用いる．コンテンツ分配の際は，分配者はこの利用権となる値を送るとともに，購入者は Bitcoin におけるコインを受け取るという取引を行う．既存の Bitcoin における取引に，利用権となる要素を送るというステップを加えるだけで本提案手法は実現可能となる．これらの取引はすべて公開されており，誰もが閲覧可能である．よって，支払う金銭と利用権の両方が正しく行われているか参加者全員が認証可能になる．仮にコンテンツの一次購入者 U_A が二次購入者 U_B にコンテンツを分配し，U_A はコインを得たが，コンテンツ提供者 U_P にコインを送らなかった例を考える．この場合，U_A が U_B にコンテンツを分配し，U_B が U_A にコインを送ったというトランザクションが公開されているが，U_A が U_P にコインを送ったというトランザクションが公開されていない．よって，U_A が不正にコインを得たと検知可能である．

本提案手法では既存の Bitcoin のプロトコルに加え，以下の要素を追加する．あるコンテンツ提供者 A は最大で l 個のコンテンツを販売可能とし，i 番目のコンテンツを $M_{A,i}$ と書く．あるコンテンツ提供者 A が提供するコンテンツ M に対して m 個のコンテンツ利用権を発行するとし，i 番目のコンテンツ利用権を $T_{A,M,i}$ と書く．l や m は実用上問題無いサイズを選ぶものとする．コンテンツ再生ソフトウェアが検証する，コンテンツの利用条件を D_d と書く．d は，コンテンツ利用権の検証操作を何世

代分行うのかを表している．すなわち，ここで，$d = root$ の場合，D_{root} は，利用券の検証操作を root まで行うことを表す．言い換えれば,D_{root} は $T_{A,B,i}, 0 \leq i \leq m$ に含まれる $T_{x_1,i} \vdash T_{x_2,i} \vdash ... \vdash T_{root,i}, 0 \leq i \leq n$ を検証する．$d = 1$ の場合，x_1 検証する．コンテンツのカプセル化を行う場合，ENCAP(M, D_d) を行う．カプセル化されたコンテンツを再生する場合，OPEN(ENCAP$(M, D_d), T)$ によりコンテンツを再生する．

4.1 分配可能な DRM システム

一般的な DRM システムとして，分配可能な DRM の実装について考える．P2P システムにおいて，コンテンツ提供者以外の利用者からコンテンツの分配ができることは前提条件となるため，第一に考える．この手法では，コンテンツ購入者が別の利用者にコンテンツを分配したとしても引き続きコンテンツを利用可能である．一次購入者 U_A が二次購入者 U_B にコンテンツを配る場合，コンテンツとコインの取引が利用者間で行われる．その後 U_B が得た Bitcoin におけるコイン C_B をコンテンツ配布者 U_P へ送信するという流れになる．この手法において，コンテンツ提供者はコインを送ってきた利用者，すなわちコンテンツ購入者のリストを公開する．コインに刻まれた履歴により誰がコンテンツを分配したかは明確であり，公開されている．よって誰もがコインの不正取得の検知を行うことができる．U_B が U_P へコインを送らなければならないという点は U_B に負担を強いるという点で欠点となるが，一度 U_B にコインが渡ることによる利点も存在する．ファイルサイズの大きなコンテンツの配布を行うという行為に貢献した U_B に対して，コイン C_B のうち $\alpha\%$ を U_P に送り，$100 - \alpha\%$ を得てよいというシステムが考案できる点である．P2P でありながら配布することに利用者自身の得が生まれ，ファイルの送受信が活発に行われる積極的な P2P システムが期待できるためである．

コンテンツの送信は，まず始めにコンテンツの提供者 U_P がコンテンツのカプセル化を行い，カプセル化されたコンテンツを作成する．その後，購入希望者が現れた場合，そのカプセル化されたコンテンツを購入希望者 U_A へ利用権と共に渡す．その後 U_A は二次購入者 U_B にコンテンツと利用権を転送することでコンテンツの分配を行うという流れで広まる．まず，コンテンツの提供者 U_P が利用者 U_A へとコンテンツを販売する流れについて説明を行う．U_P は，正規の利用者でもコンテンツ M 自体を得られないようにするため，コンテンツ M 自体のカプセル化 ENCAP(M, D_{root}) を行う．その後，U_P は U_A に ENCAP(M, D_{root}) を送る．ENCAP(M, D_{root}) はそのままでは使えないため，U_P はこれを使用可能にする，コンテンツの利用権 $T_{0,P}$ を U_A に対して SEND$(SK_P, PK_A, T_{0,P})$ を行い，送る．U_A は正しく利用権が送られたことを VERIFY$(PK_P, T_{0,A})$ を行い確かめると，コイン $C_{A,0}$ を U_P に対して SEND$(SK_A, PK_P, C_{A,0})$ を行い，送る．最終的に，提供者 U_P がコインが送られたことを VERIFY$(PK_A, C_{0,P})$ を行い確かめることにより，コンテンツの送信は終了する．このプロトコルを 1 に記述する．

Algorithm 1 コンテンツの送信

1: C_0，T_0，M,SK_A,PK_B を入力とする．
2: U_P は ENCAP(M, D_{root}) を行い，コンテンツをカプセル化する．
3: U_P は ENCAP(M, D_{root}) を購入者 U_A に送る．
4: U_P は SEND$(SK_P, PK_A, T_{0,P})$ を行い，コンテンツの利用権を U_A に渡す．
5: U_A は VERIFY$(PK_P, T_{0,A})$ を行い，コンテンツの利用権が正しく送られたことを確かめる．
6: U_A は SEND$(SK_A, PK_P, C_{A,0})$ を行い，コインを U_P に渡す．
7: U_P は VERIFY$(PK_A, C_{0,P})$ を行い，コインが正しく送られたことを確かめる．

Algorithm 2 コンテンツの使用

1: U_A,ENCAP(M, D_{root}),$T_{U_P,M_0,i}, 0 \leq i \leq m$ を入力とする．
2: コンテンツ再生ソフトウェアは利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に含まれる $T_{x_1,i} \vdash T_{x_2,i} \vdash ... \vdash T_{root,i}, 0 \leq i \leq n$ を検証し，U_A がこの中に存在するか確認する．
3: M = OPEN(ENCAP$(M, D_{root}), T_{U_P,M_0,i}, 0 \leq i \leq m)$ を行い，コンテンツを開く

次に，コンテンツの一次購入者 U_A がコンテンツを利用する場合について考える．U_A がコンテンツを利用する場合，まずはカプセル化されているコンテンツ ENCAP(M, D_{root}) に対し，利用条件 D_{root} のチェックを行う．このチェックは再生用ソフトウェアによって行われる．この際，利用条件 D_{root} を満たす，すなわち利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に U_A が含まれている場合はコンテンツの利用が可能となる．もし利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に U_A が含まれていない場合，コンテンツの利用は不可能である．このプロトコルを 2 に記述する．

次に，二次購入者 U_B に分配する場合について考える．U_A が U_B にコンテンツの分配を行う場合，自分の持つ利用権 $T_{0,A}$ を，Bitcoin におけるコインの転送と同様に SEND$(SK_A, PK_B, T_{0,A})$ を用いて U_B に転送する．U_B はコンテンツの利用権 $T_{0,B}$ が正しく送られてきたことを VERIFY$(PK_A, T_{0,B})$ により確認し，その代金となるコイン C_B を U_A に送る．U_A は送られてきたコイン C_B のうち，$\alpha\%$ を U_P に送り，分配に貢献したということか

Algorithm 3 コンテンツの分配

1: $SK_A, PK_A, T_{0_A}, PK_B, SK_B, C_{B_0}, PK_P$, ENCAP$(M, D_{root})$ を入力とする．
2: U_A は SEND(SK_A, PK_B, T_{0_A}) を行い，コンテンツの利用権を受信者 U_B に渡す．
3: U_A は ENCAP(M, D_{root}) を U_B に送る．
4: U_B は VERIFY(PK_A, T_{0_B}) を行い，コンテンツの利用権が正しく送られたことを確かめる．
5: U_B は SEND(SK_B, PK_A, C_{B_0}) を行い，コインを U_A に渡す．
6: U_A は VERIFY(PK_A, C_{0_A}) を行い，コインが正しく送られたことを確かめる．
7: U_A は SEND$(SK_A, PK_P, C_{A_0}\alpha)$ を行い，コインを U_P に渡す．
8: U_P は VERIFY$(PK_A, C_{0_P}\alpha)$ を行い，コインが正しく送られたことを確かめる．

ら，$100-\alpha\%$ を得る．このプロトコルを 3 に記述する．

4.2 転売可能な DRM

次に，転売可能な DRM について考える．この手法では，コンテンツを購入した利用者 U_A が自身の持つコンテンツを別の利用者 U_B に転売した場合，U_A はコンテンツを使用不可となる．一般的な転売可能なシステムでは，コンテンツ提供者 U_P は中古売買が行われたとしても利得を得ることはできない．転売時にも U_P に U_A が転売によって得たコイン C_B のうち $\beta\%$ を U_P に送り，$100-\beta\%$ を得てよいというシステムを考えた場合，Bitcoin のプロトコルを用いた通信ではすべての通信が公開されているため，不正転売は不可能となり，このシステムの実現が可能となる．この方式の実現は，Bitcoin システムにおけるコインと同様に，利用権においても二重使用が不可能なシステムを用いる．タイムスタンプサーバの導入を行い，一度手放したコインに関しては手放した記録が残るようにする．コインを持っている間のみコンテンツが利用可能とし，コインを売ってしまうとその時点からコンテンツの利用はできなくなるシステムである．

コンテンツの送信は，コンテンツの提供者 U_P がコンテンツのカプセル化を行い，利用者 U_A へ利用権と共に渡す．その後 U_A は U_B にコンテンツと利用権を転送することでコンテンツの分配を行うという流れで広まる．

まず，コンテンツの提供者 U_P が利用者 U_A へとコンテンツを販売する流れについて説明を行う．U_P は，正規の利用者でもコンテンツ M 自体を得られないようにするため，コンテンツ M 自体のカプセル化 ENCAP(M, D_1) を行う．その後，U_P は U_A に ENCAP(M, D_1) を送る．ENCAP(M, D_1) はそのままでは使えないため，U_P はこれを使用可能にする，コンテンツの利用権 $T_{0,P}$ を U_A

Algorithm 4 コンテンツの送信

1: C_0，T_0，M,SK_A,PK_B を入力とする
2: U_P は ENCAP(S, D_1, P) を行い，コンテンツをカプセル化する．
3: U_P は ENCAP(S, D_1, P) を購入者 U_A に送る．
4: U_P は SEND$(SK_P, PK_A, T_{0,P})$ を行い，コンテンツの利用権を U_A に渡す．
5: U_A は VERIFY$(PK_P, T_{0,A})$ を行い，コンテンツの利用権が正しく送られたことを確かめる．
6: U_A は SEND$(SK_A, PK_P, C_{A,0})$ を行い，コインを U_P に渡す．
7: U_P は VERIFY$(PK_A, C_{0,P})$ を行い，コインが正しく送られたことを確かめる．

Algorithm 5 コンテンツの使用

1: U_A,ENCAP(M, D_1),$T_{U_P,M_0,i}, 0 \leq i \leq m$ を入力とする
2: コンテンツ再生ソフトウェアは利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に含まれる $T_{x_1,i} \vdash T_{x_2,i} \vdash ... \vdash T_{root,i}, 0 \leq i \leq n$ のうち，x_1 を確かめ，U_A がこの中に存在するか確認する．
3: M = OPEN(ENCAP$(M, D_1), T_{U_P,M_0,i}, 0 \leq i \leq m$) を行い，コンテンツを開く

に対して SEND$(SK_P, PK_A, T_{0,P})$ を行い，送る．U_A は正しく利用権が送られたことを VERIFY$(PK_P, T_{0,A})$ を行い確かめると，コイン $C_{A,0}$ を U_P に対して SEND$(SK_A, PK_P, C_{A,0})$ を行い，送る．最終的に，提供者がコインが送られたことを VERIFY$(PK_A, C_{0,P})$ を行い確かめることにより，コンテンツの送信は終了する．このプロトコルを 4 に記述する．

次に，コンテンツの一次購入者 U_A がコンテンツを利用する場合について考える．U_A がコンテンツを利用する場合，まずはカプセル化されているコンテンツ ENCAP(M, D_1) に対し，利用条件 D_1 のチェックを行う．このチェックは再生用ソフトウェアによって行われる．この際，利用条件 D_1 を満たす，すなわち利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に U_A が含まれている場合はコンテンツの利用が可能となる．もし利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に U_A が含まれていない場合，コンテンツの利用は不可能である．このプロトコルを 5 に記述する．

次に，二次購入者 U_B に転売する場合について考える．U_A が U_B にコンテンツの転売を行う場合，自分の持つ利用権 $T_{0,A}$ を，Bitcoin におけるコインの転送と同様に SEND$(SK_A, PK_B, T_{0,A})$ より U_B に転送する．U_B はコンテンツの利用権 $T_{0,B}$ が正しく送られてきたことを VERIFY$(PK_A, T_{0,B})$ により確認し，その代金となるコイン C_B を U_A に送る．U_A は送られてきたコイン C_B

Algorithm 6 コンテンツの転売

1: $SK_A, PK_A, T_{0_A}, PK_B, SK_B, C_{B_0}, PK_P$, ENCAP$(M, D_1)$ を入力とする
2: U_A は SEND(SK_A, PK_B, T_{0_A}) を行い，コンテンツの利用権を受信者 U_B に渡す.
3: U_A は ENCAP(M, D_1) を U_B に送る.
4: U_B は VERIFY(PK_A, T_{0_B}) を行い，コンテンツの利用権が正しく送られたことを確かめる.
5: U_B は SEND(SK_B, PK_A, C_{B_0}) を行い，コインを U_A に渡す.
6: U_A は VERIFY(PK_A, C_{0_A}) を行い，コインが正しく送られたことを確かめる.
7: U_A は SEND$(SK_A, PK_P, C_{A_0}\beta)$ を行い，コインを U_P に渡す.
8: U_P は VERIFY$(PK_A, C_{0_P}\beta)$ を行い，コインが正しく送られたことを確かめる.

のうち，β% を U_P に送り，コンテンツを売った代金として $100-\beta$% を得る．このプロトコルを 6 に記述する.

5 利用権の部分的利用可能な方式

この章では，コンテンツと利用権を多人数から得ることができる方式について説明を行う．P2P ネットワークでは，多くのノードがコンテンツの分散を行うことで負荷分散をするというのが目的である．このため，一つのコンテンツ自体を分割し，多くの分配者からコンテンツを部分的に得，最終的に合成し，コンテンツを得るということがしばしば行われている．本提案方式においても，複数の分配者からコンテンツを得た場合について対応できるよう，拡張を行う．本提案方式では，分配を行った利用者が利得を得ることができるシステムである．このため，部分的に分配に貢献した利用者も，部分的に利得を得ることができるようにしたい．このため，ここではコンテンツの分割に応じた利用権の分割を行い，送ったコンテンツの分だけ利用権を送るというシステムを考える．コンテンツ M を $M_0, M_1, ..., M_k$ と分割したとする．この場合，利用権 T も $T_0, T_1, ..., T_o$ と分割される．利用する場合は T を o 個すべて集めた場合のみ利用可能である．分配に貢献した利用者は分配したコンテンツの量に比例して利得を得ることができる.

コンテンツ提供者 A が提供するコンテンツを $M_{A,i,j}$, $0 \leq i \leq l, 0 \leq j \leq o$ とする．ここで，i はそれぞれのコンテンツの種類，j はコンテンツを分割した際の番号である．コンテンツ提供者 A がコンテンツ M に対して発行するコンテンツ利用権を $T_{A,M,i,j}, 0 \leq i \leq m, 0 \leq j \leq o$ とする．ここで，i は発行した利用権の数，j はコンテンツを分割した際に分割された利用権の数である.

Algorithm 7 コンテンツの送信

1: C_0，T_0，M_0,SK_A,PK_B を入力とする.
2: U_P は ENCAP(M_0, D_{root}) を行い，カプセル化する.
3: U_P は ENCAP(M_0, D_{root}) を購入者 U_A に送る.
4: U_P は SEND$(SK_P, PK_A, T_{0,P,0})$ を行い，コンテンツの利用権を U_A に渡す.
5: U_A は VERIFY$(PK_P, T_{0,A,0})$ を行い，コンテンツの利用権が正しく送られたことを確かめる.
6: U_A は SEND$(SK_A, PK_P, C_{A,0})$ を行い，コインを U_P に渡す.
7: U_P は VERIFY$(PK_A, C_{0,P})$ を行い，コインが正しく送られたことを確かめる.

コンテンツの送信は，コンテンツの提供者 U_P がコンテンツのカプセル化を行い，利用者 U_A へ利用権と共に渡す．その後 U_A は U_B にコンテンツと利用権を転送することでコンテンツの分配を行うという流れで広まる.

まず，コンテンツの提供者 U_P が利用者 U_A へとコンテンツを販売する流れについて説明を行う．ここでは，コンテンツ M の中の M_0 を渡す場合を考える．まず U_P は，正規の利用者でもコンテンツ M_0 自体を得られないようにするため，コンテンツ M_0 自体のカプセル化 ENCAP(M_0, D_{root}) を行う．その後，U_P は U_A に ENCAP(M_0, D_{root}) を送る．ENCAP(M_0, D_{root}) を使用するため，U_P はこれを使用可能にするコンテンツの利用権 $T_{0,P}$ を U_A に対して SEND$(SK_P, PK_A, T_{0,P})$ を行い，送る．U_A は正しく利用権が送られたことを VERIFY$(PK_P, T_{0,A})$ で確かめ，コンテンツの量に応じたコイン $C_{A,0}$ を U_P に対して SEND$(SK_A, PK_P, C_{A,0})$ を行い，送る．最終的に，提供者がコインが送られたことを VERIFY$(PK_A, C_{0,P})$ を行い確かめ，コンテンツの送信は終了する．このプロトコルを 7 に記述する.

次に，コンテンツの一次購入者 U_A がコンテンツを利用する場合について考える．U_A がコンテンツを利用する場合，まずはカプセル化されているコンテンツを o 個集める必要がある．全て集めた場合は，ENCAP$(M_i, D_{root}), 0 \leq i \leq o$ に対し，利用条件 D_{root} のチェックを行う．このチェックは再生用ソフトウェアによって行われる．この際，利用条件 D_{root} を満たす，すなわち利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に U_A が含まれている場合はコンテンツの利用が可能となる．もし利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に U_A が含まれていない場合，コンテンツの利用は不可能である．このプロトコルを 8 に記述する.

次に，二次購入者 U_B に分配する場合について考える．この場合，カプセル化されたコンテンツをすべて集める必要はなく，部分的にしか持っていない場合でも送ることができる．今回は M_0 を分配するとする．U_A

Algorithm 8 コンテンツの使用

1: U_A,ENCAP$(M_i, D_{root}), 0 \leq i \leq o$ を入力とする
2: コンテンツ再生ソフトウェアは利用権 $T_{U_P,M_0,i}, 0 \leq i \leq m$ に含まれる $T_{x_1,i} \vdash T_{x_2,i} \vdash ... \vdash T_{root,i}, 0 \leq i \leq n$ のうち，$x_1, x_2, ..., x_{root}$ 全員を確かめ，U_A がこの中に存在するか確認する．
3: $M =$ OPEN(ENCAP$(M_i, D_{root}), T_{U_P,M_0,i}, 0 \leq i \leq m), 0 \leq i \leq o$ を行い，コンテンツを開く

Algorithm 9 コンテンツの分配

1: $SK_A, PK_A, T_{0_A,0}, PK_B, SK_B, C_{B_0}, PK_P$ $, ENCAP(M_0, D_{root})$ を入力とする
2: U_A は SEND$(SK_A, PK_B, T_{0_A,0})$ を行い，コンテンツの利用権を受信者 U_B に渡す．
3: U_A は ENCAP(M_0, D_{root}) を U_B に送る．
4: U_B は VERIFY$(PK_A, T_{0_B,0})$ を行い，コンテンツの利用権が正しく送られたことを確かめる．
5: U_B は SEND(SK_B, PK_A, C_{B_0}) を行い，コインを U_A に渡す．
6: U_A は VERIFY(PK_A, C_{0_A}) を行い，コインが正しく送られたことを確かめる．
7: U_A は SEND$(SK_A, PK_P, C_{A_0}\alpha)$ を行い，コインを U_P に渡す．
8: U_P は VERIFY$(PK_A, C_{0_P}\alpha)$ を行い，コインが正しく送られたことを確かめる．

が U_B にコンテンツの分配を行う場合，自分の持つ利用権 $T_{0,A,0}$ を，Bitcoin におけるコインの転送と同様に SEND$(SK_A, PK_B, T_{0,A,0})$ を用いて U_B に転送する．U_B はコンテンツの利用権 $T_{0,B,0}$ が正しく送られてきたことを VERIFY$(PK_A, T_{0,B,0})$ により確認し，その代金となるコイン C_B を U_A に送る．U_A は送られてきたコイン C_B のうち，α% を U_P に送り，分配に貢献したため，$100 - \alpha$% を得る．このプロトコルを 9 に記述する．

また，多人数から分散ダウンロードが可能な方式において，分配可能な DRM 方式から転売可能な DRM 方式へは 4 章と同様の変更で実現できる．変更点は，コンテンツ配布ではコンテンツ提供者が利用条件 D_{root} を D_1 に変更し，利用者に送る点が異なる．コンテンツの利用では，コンテンツ再生用ソフトウェアが利用者を確認する際，x_1 のみ確かめる点が異なる．コンテンツの転売では，転売して得たコインのうち，$100 - \alpha$% ではなく $100 - \beta$% をコンテンツ提供者に転送する点が異なる．

6 まとめ

本論文では，P2P ネットワークにおける分配方式をベースとした DRM 方式の提案を行った．既存研究と比較し，金銭の支払いを含めた DRM システムを構築できている点，そして多人数から分割されたコンテンツを集めることができる点が利点である．この手法の欠点として，暗号化の方式を Bitcoin に依存していないため，再生用ソフトウェアに組み込まれた暗号が破られてしまった場合を考慮できていない点があげられる．

今後の課題として，利用権を持っている利用者のみが復号できる暗号方式の考案を行っていく予定である．

謝辞

本研究の一部は，日本学術振興会 科学研究費補助金 基盤 B（課題番号 23300027）による補助のもとで行われた．

参考文献

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

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

[3] 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*, Vol. 2, pp. 806–811. IEEE, 2003.

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

[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*, Vol. 25, No. 6, pp. 423–436, 2003.

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

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

[8] 北原基貴, 川本淳平, 櫻井幸一. 電子現金プロトコルを用いた著作権管理システムの提案. コンピュータセキュリティシンポジウム 2013(CSS2013), 2013.