要 旨

Bitcoin プロトコルを用いた Pure-P2P コンテンツ流通及び課金システムの検討

林 憲佑

P2P 型コンテンツ流通システムはスケーラビリティが高く，耐障害性の高いシステム構築が可能であるため注目されている．従来のシステムでは，コンテンツをカプセル化しユーザ間で流通させる．しかし，二次配布を行う利点が存在しないため負荷分散が行われにくく，流通経路の追跡も困難であった．既存方式として，Bitcoin の全取引履歴であるブロックチェーンが公開される性質を用いて流通経路の明確化を行い，カプセルの二次配布者に利益を与える著作権管理システムが提案されている．しかし，既存方式では配信者が何らかの方法で入金を受けた後，コンテンツ利用権を購入者に与えるという手順をとっている．よって，配信者が信用できることが前提のシステムであり，悪意のあるユーザが参加する恐れのある P2P においては現実的ではない．

そこで本論文では，Bitcoin プロトコルを用いた Pure-P2P コンテンツ流通及び課金システムを提案する．提案システムでは，Bitcoin における取引単位であるトランザクションを 6 種類定義し，コインの情報だけではなくコンテンツに関する情報をブロックチェーンに記録可能にする．これにより，販売したいコンテンツの登録や，コインとコンテンツ復号用鍵の同時取引を可能にする．不正への対策として，購入者がコインを事前に取引用に確保することを必須の動作とすることで，購入者がコインを渡さずにコンテンツ復号用鍵を入手することを不可能にする．また，コンテンツ配信者が，不正なコンテンツ復号用鍵を購入者へ渡す可能性があるため，第三者による鍵の正当性検証を可能にし，不正が認められた場合に返金処理を行うことで，不正を無意味なものにする．これにより，安全なコンテンツ流通シス

テムが実現できることを示す.

キーワード　ピアツーピア, ビットコイン, コンテンツ流通, 課金システム, デジタル著作権管理

Abstract

The Study on the Pure-P2P content distribution and billing system using Bitcoin protocol

Kensuke HAYASHI

A P2P content distribution system has received a lot of attention in recent years, because of its high scalability and high fault tolerance. Conventional system encapsulates a content, and distributes a capsule among users. Conventional system has a problem that users do not have a method to know a distribution route, and load sharing isn't performed because there are no merits by which the user uploads a file. Against this problem, a method of digital rights management based on Bitcoin protocol has considered. In this method, using the mechanism that Blockchain which is all transaction history is shown, can give a benefits to a user. In this method, vendor gives right of use to a buyer after getting money from a buyer. Therefore, when a vendor is not a reliable person, this system can't be usable. For this reason, it is risky to use this system because a malicious user exists in P2P.

In this paper, I propose a new content distribution and billing system using Bitcoin protocol. In this system to define a format for the 6 types of transactions. Then, users can record not only coin but also information of content in Blockchain. Accordingly, it becomes possible to a registration of sale contents, and trade in a coin and a decryption key of contents at the same time. As a countermeasures against dishonest acts, I make a structure that a buyer must reserve some coin beforehand. From this point, when a buyer does not pay a coin to a vendor, buyer can't get a decryption key. Also, a

vendor may hand an illegal decryption key to a buyer. Then, enable to the correctness verification of the decryption key by the third party and enable to refund when it is illegal. I show that a safe contents distribution system can be realized by this method.

key words P2P, Bitcoin, Content Distribution, Billing System, Digital Rights Management