5E-02

ブロックチェーン上で柔軟なトークン設計によって実現するコンテンツの管理手法

石田 達郎† 渡邊 大喜† 大橋 盛徳† 藤村 滋† 中平 篤†
日本電信電話株式会社 NTT サービスエボリューション研究所†

1. はじめに

ブロックチェーンを用いてデジタルコンテンツを管理する方法が模索されている[1][2][3] [4]。コンテンツ管理にブロックチェーンを用いる理由は主に 3 つある。(1)コンテンツ権利者により、直接的なコンテンツおよび代価の取引が実現される、(2)ブロックチェーンの耐改ざん性を、権利処理に適用することで不正な利用の減少が期待される、(3)コンテンツの利用料を、暗号通貨を介して透明性高く分配が可能となる、である。これらの特徴を有するコンテンツ管理システムのプロトタイプ実装を通じてシステム要件の整理を行う。

2. 課題

一つ目の課題として、従来の暗号通貨用ブロックチェーンは、そのままコンテンツ管理に適用できるものではない。暗号通貨は、現金のようにどのユーザにとっても同じように扱うことができる代替可能な性質がある。しかし、コンテンツは権利の有無によって異なる制御ができる必要がある。たとえば、コンテンツの権利者は配布や販売が可能な一方、コンテンツの利用者は勝手に配布・販売ができないように制御できるようにするといったことである。

二つ目の課題として、取引履歴の検索性が低いことが挙げられる。コンテンツを管理する際には、あるユーザがあるコンテンツに関わる権利を有しているかを調べるなど、履歴を検索することが必要になる。あるユーザを示すアドレスに関係する取引の履歴を取引履歴全体から抽出する場合、すべての履歴を参照したうえで関連する履歴を整列させる必要がある。この効率を上げる方法として、取引履歴を RDB 等に転記し検索機能を外部サービス化する試みもある[5]が、この場合、情報の正確性を外部のサービスに依存することとなる。ブロックチェーンの非中央集権的な特性を保つためには、外部サービスを用いず、ブロックチェーンに登録されたデータそのものの検索性を高める工夫が必要になる。

3. 提案方式

課題を解決するための要件は以下のとおり。

(1) コンテンツ権利者と利用者では扱える権限が異なるため、コンテンツを扱う人によって異なる権限制御ができることが必要となる。
(2) 権利の移転ができること。たとえばコンテンツを視聴する権利を売買する際に利用する。
(3) コンテンツ管理においては、権利状況の確認のため、高い検索性が求められる。

今回、ブロックチェーン基盤としてイーサリアム[6]を用いて実装を行った。ブロックチェーン上で暗号通貨以外のものを扱う共通仕様を、イーサリアムではトークンと呼んでいる。Ethereum Request for Comments(ERC)によって新たなトークンの提案が行われており、一部の提案が今回の要件を満たす実装に適していると判断したためである。

今回は ERC721、ERC998 で提案されているトークン設計を拡張することで課題の解決を試みた。

ERC721[7]を利用してコンテンツにかかわる権利をトークン化した。ERC721 は分割できない資産を表現するトークンに対し、所有者アドレスや、利用者アドレスの明示を可能とする。さらに ERC998[8]により、トークン同士を紐付けることも可能した。ERC998 は ERC721 の拡張で、トークンに紐付く子トークンを記述することができる。これにより、「デジタルコンテンツを視聴する際に、必ず広告を見るように紐付ける」といった表現も可能となる。

トークンの検索について記述する。トランザクション履歴を検索するときに、特定 ID のトークンに関する履歴のみを抽出することができれば効率よく検索が可能となる。今回、トークン内に、「トークンに変更があったブロック番号」を記載するよう設計した。これにより、変更点のブロックのみをしらべることで、トークンに変更のある履歴だけを効率よく検索していくことを可能とした（図 1）。

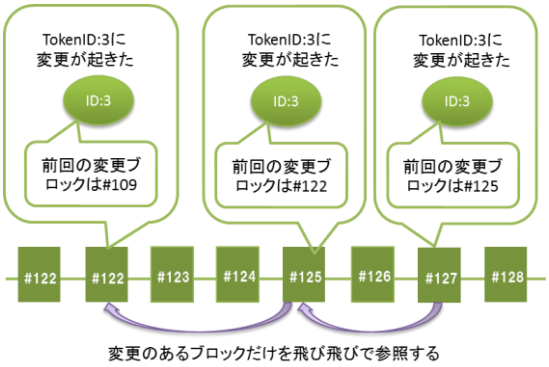

図 1 提案手法における検索手順のイメージ

† TATSURO ISHIDA, Nippon Telegraph and Telephone Corporation
† HIROKI WATANABE, Nippon Telegraph and Telephone Corporation
† SHIGENORI OHASHI, Nippon Telegraph and Telephone Corporation
† SHIGERU FUJIMURA, Nippon Telegraph and Telephone Corporation
† ATSUSHI NAKADAIRA, Nippon Telegraph and Telephone Corporation

上記の技術を含めて構築した処理フローのイメージは、図 2 のようになる。広告主、コンテンツ権利者、配信者、視聴者の 4 名が登場する。あらかじめ広告主がブロックチェーンに広告と広告費用を登録する。コンテンツの権利者がコンテンツの権利をトークンの形でブロックチェーンに登録する。権利者が権利の一部（広告を付与する権利）を配信者に渡し、コンテンツの配信者がコンテンツと広告を紐付する。また、視聴者には視聴の権利が渡され、視聴するとスマートコントラクトに従ってあらかじめ記載した広告費用の自動配分が実行される。過去の履歴は、トークンの検索技術によって必要な時にあとから検索できるようになっている。

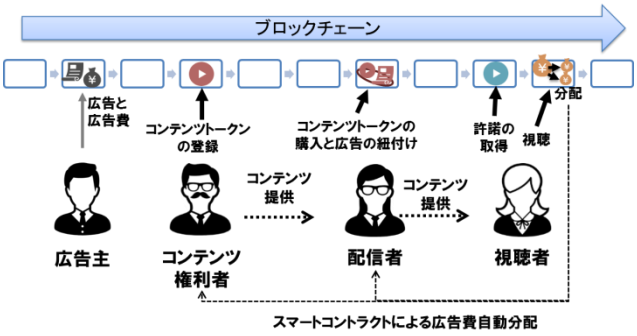

図 2　処理フローのイメージ

4.　評価と考察

実装後、提案手法の評価を行った。なお、評価はすべてイーサリアムでプライベートチェーンを構築して行った。コンテンツをブロックチェーン上に登録し、異なる役割に異なる権利が付与されていること、権利の移転が可能であることが確認できた。さらに、非機能要件として提案手法のコスト変化の分析と、検索速度の分析を行った。

まずコスト変化調査について記述する。イーサリアムにおいては、取引を実行するための手数料として Gas が存在する。Gas は取引を承認したユーザに手数料として支払われる。Gas はおおむねトークンの処理に費やす計算ステップ数によって決まるため、トークンの作り方次第で Gas に変化が出る。ひとつのトークンに対して視聴の権利を 20 個付与したトークンを作る場合、Gas が大きくなりすぎイーサリアムの Gas Limit（一取引で費やせる Gas の上限値。新規ブロックの生成者が値の上下を決められる。2019 年 1 月現在、上限は約 800 万 Gas）を上回り、処理が滞ることが確認された。視聴ごとに視聴の権利をトークンに発生させる方式を用いることでこれを解決することができた。

次に、検索速度に関する調査を行った。トークンは ERC998 に従って作成し、ひとつのトークンにつき 10 個の視聴権を登録した。ブロックは 15 秒で 1 ブロック生成し、1 万ブロック程度を登録した。おおむね 100 ブロック程度ごとにデータを投入した。10 回計測し、平均を求めたところ、今回の実装では提案手法が約 0.3 秒、既存手法では 4.6 秒程度かかり、約 16 倍の速度差があった。

表 1　速度測定結果（単位は ms）

	提案手法	従来手法
平均	287	4688
標準偏差	10	57

今回の実装では、コンテンツの不正利用を防ぐ実装を入れていない。これは今回の検証の範囲外であるが、必要な機能と考えられ、システム構築を行う際にはさらに処理が重くなる可能性を考慮する必要がある。また、誰がどのコンテンツにおいて何の権利を有しているかについては、思想・良心の自由やプライバシーの観点から、適切な開示制御技術をシステムが具備する必要がある。今回のシステムにおいては範囲外としている。

また、映像のストレージを別に構築する必要がある。

5.　おわりに

デジタルコンテンツをブロックチェーン上のトークンとして登録することで、管理流通させる方式のシステムを実装した。複雑な権利契約をトークン化し、スマートコントラクトによる利益の自動配分や履歴検索が実行可能となった。

構築したシステムにより、デジタルコンテンツをブロックチェーン上で管理流通する際の課題と必要要件を整理した。

参考文献

[1] AlphaNetworks https://alphanetworks.io/

[2] Audius https://audius.co/index.html

[3] N. Herbaut et al., "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains", IEEE Communications Magazine., vol. 55, Issue. 9, pp. 70-76, Sept. 2017.

[4] Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, J. Kishigami, "BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain", 5th IEEE International Conference on Consumer Electronics, pp. 345-346, 2016.

[5] Ethereum (ETH) Blockchain Explorer https://etherscan.io/

[6] Ethereum Project https://www.ethereum.org/

[7] EIPs/eip-721.md at master · ethereum/EIPs · GitHub https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

[8] ERC-998 Composable Non-Fungible Token Standard · Issue #998 · ethereum/EIPs · GitHub https://github.com/ethereum/eips/issues/998