様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２３ 日現在

機関番号：３２６５７
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１２８０

研究課題名（和文）著作権管理可能なP2P動画配信技術

研究課題名（英文）P2P Video Streaming Method with Copy Protection

研究代表者
小川　猛志（OGAWA, TAKESHI）

東京電機大学・システムデザイン工学部・教授

研究者番号：３０７５００８８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：従来のP2P型データ配信技術は配信データの不正コピーを防ぐことができず，商用の動画配信サービスに適用することはできなかった．我々は，P2P型データ配信システムにおいて，正規ユーザが再生する動画の画面をキャプチャされても流出元を特定できる技術を考案し，SDN環境での実現性を確認していた．本研究では上記技術を拡張しWebRTCと組み合わせることでインターネット環境でも基本動作を実現できることを確認した．また，ブロックチェーン上のアプリケーションとして，本技術を実現することを新たな目標として設定し，そのために必要なブロックチェーンの処理性能向上技術を発明しシミュレーションによりその有効性を確認した．

研究成果の学術的意義や社会的意義
提案する動画配信技術を応用することで，従来大規模なクラウドが必要だった動画配信サービスを，極めて低コストなサーバによりで提供できる可能性があることを確認した．また，ビットコインやイーサリアムなど既存のブロックチェーンの処理性能(1秒あたりのトランザクション承認数)を数100倍に向上できる可能性のある技術を創出した．

研究成果の概要（英文）：The conventional P2P video distribution technology cannot prevent unauthorized copying of distributted video file, and cannot be applied to commercial video distribution services. We have devised a technique that can identify the source of leakage even if the screen of a video played by a legitimate user is captured, and confirmed its feasibility in an SDN environment. In this research, it was confirmed that the basic operation can be realized even in the Internet environment by extending the above technology and combining it with WebRTC. In addition, we set a new goal the realization of this technology as an application on the blockchain, then invented the blockchain processing performance improvement technology necessary for that purpose, and confirmed its effectiveness by simulation.

研究分野：情報ネットワーク

キーワード：p2p　電子透かし　動画配信　HLS　ブロックチェーン　WebRTC

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

既存のストリーム動画配信サービスは，動画電子ファイルをサーバから配信する C/S 型が一般的である．C/S 型動画配信システムにおいては，配信ファイルを再生できる権限のあるユーザのみに視聴を許可するため，Digital Right Management (DRM)技術と電子透かし技術が使用される．DRM 技術では，暗号化した電子ファイルを配信し，配信サーバが認証したユーザ端末内の動画再生ソフトウェアのみに復号鍵を配布する．当該アプリケーションからは復号鍵を取り出せないため，電子ファイルが他のユーザに流出しても，視聴する事はできない．しかし，動画の再生画面はソフトウェアで容易にキャプチャ可能であり，一旦キャプチャされると，復号鍵を持たないユーザであっても視聴可能となる．そこで，ユーザ毎に異なる配布番号(以下，D-ID)を不可視データにより動画電子ファイルに埋め込む技術(電子透かし技術)が実用化されている．同技術は動画のキャプチャやインターネットへのアップロードを防ぐものではない．ただし，同技術で埋め込んだ D-ID はオリジナルの動画からの除去が困難であり，デコード・エンコードを行っても値が変わらない特徴がある．このため，インターネットに流出したファイルが見つかった場合，D-ID を読み出すことで，流出元を特定可能であり，動画の流出を抑止できる．

ところが，C/S 型では，配信サーバの処理性能や通信帯域がネックとなり，同時にストリーム動画を視聴できるユーザ数が制限される問題がある．

２．研究の目的

我々は，ストリーム動画配信サービスに P2P 型通信技術を適用することで，配信サーバを増設せずに多数のユーザに低コストでサービスを提供できる方法を明確化することを目的に研究に取り組んでいる．既に，同一のファイルを共有する P2P 型通信において，動画ファイルのデータを一切加工せずに再生時には異なる D-ID が表示されるという，一見矛盾する要件を解決する手法を考案し，SDN 環境で実装した試作機により基本動作を確認していた[1]. 本研究予算では，配信サーバやユーザから制御できないルータのみで構成されるインターネット環境での実現方法の確立を目的に研究を開始した(目的 1)．また，集中サーバーを設置せずに，端末間での電子マネーの交換や複数の端末に跨ったプログラム(スマートコントラクト)の実行が可能な，パブリックブロックチェーン技術(以下ブロックチェーン)を適用することで配信サーバ自体を不要とすることを研究目的に追加し研究を進めた(目的 2).

３．研究の方法

(1)目的１：インターネット環境での実現性の確認

初年度(2018 年度)から研究室内に構築した実験環境で実装と検証をすすめた．ただし，2020 年度と 2021 年度は実機検証が困難であったため，仮想環境で実装を進めた．

(2)目的２：ブロックチェーン適用方法の研究

現状のブロックチェーン技術では処理性能(単位時間あたりの平均トランザクション承認数)が著しく不足すること，及びノードで保存が必要なデータ量の削減が必要であることが分かったため，2020 年度からそれらを解決する方式の検討とシミュレーションによる検証を進めた．

４．研究成果

(1)目的１：インターネット環境での実現性の確認

提案方式の概要を図 1 に示す．提案方式では，配信する動画ファイルを n 個にコピーしそれぞれに異なる数値(0～n-1)を不可視電子透かし情報(Copy-ID)として埋め込み，その後既存の HLS 配

信技術によりそれぞれを数秒単位の動画ファイル(チャンクファイル)に分割する．配信サーバからの制御により，Copy-ID の組み合わせが視聴端末ごとに異なる ID(D-ID)となるように各チャンクファイルのダウンロード元端末を切り替えることで「同一のファイルを共有する P2P 型通信において，動画ファイルのデータを一切加工せずに再生時には異なる D-ID が表示される」ことを実現している．なお図 1 では n=4 の場合の例を示しており， 5 端末め以降の端末には既に視聴を開始していた他端末から，配信サーバからの指示によりチャンクファイルがダウンロードされる．

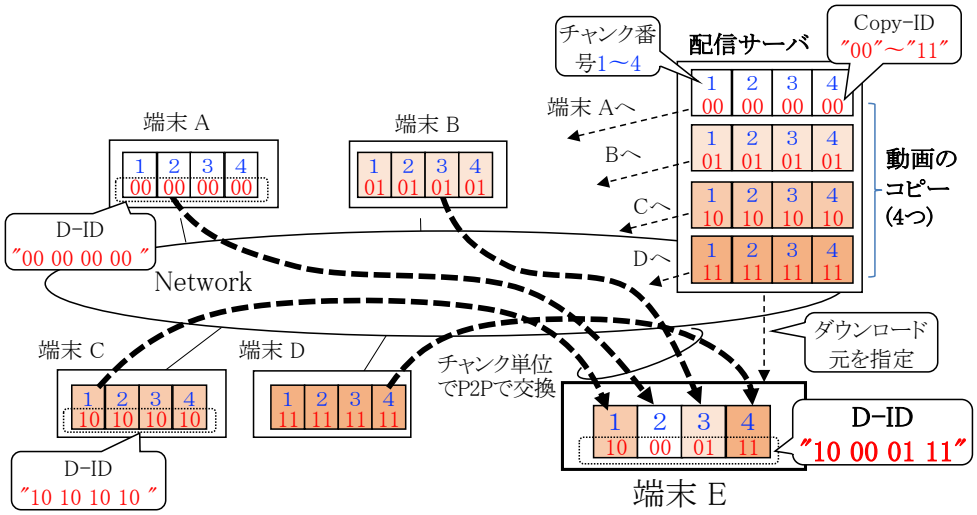

図1 提案方式の概要

従前の研究では送信元端末の切り替えを SDN 対応ルータにより実施していたが，視聴端末自身に切り替えさせることで，SDN 非対応の IP ネットワーク(ただし NAT なし)環境内で基本動作を実現できることを確認し学会で発表した．さらに，WebRTC と組み合わせることで NAT があるインターネット環境でも動作可能と考えている．現在，事前に視聴を予約した複数の端末に対して NAT を透過してチャンクファイルを転送し，画像に乱れなく視聴できること仮想環境内で確認している．コロナ感染予防のため実機での作業に遅れが生じており，実機による動作検証及び性能測定は今後の課題である．

(2)目的２：ブロックチェーン適用方法の研究

ブロックチェーンでは，p2p 網を構成する全てのノードが同一のデータベース(台帳)と後述するブロックチェーンを保持し，台帳を更新したい場合は，更新コマンド(トランザクション)を作成し全ノードに放送する．ランダムなくじで決定されるブロック生成者(ビットコインの場合平均して 10 分に 1 回決定)は未実行のトランザクションをサイズに制限のあるブロック(ビットコインの場合平均 4,000 トランザクション程度格納可能)に収め，ブロックが生成された順に保持しているブロックチェーンの末尾(最も新しいブロック)に接続し，当該ブロックを全ノードに放送する．各ノードはブロックを受信すると当該ブロック内のトランザクションを格納されている順番で実行する．非常に高い確率で全てのノードが保持するブロックチェーンが一致する特性をもつため，台帳の更新結果も一致することが確率的に保証されている．なお，各ノードは最新の台帳データの正当性を検証できるようにするため，最初のブロックから最新のブロックまで全てのブロックを保持する必要がある．本技術の問題と提案する解決策の概要を以下に示す．

① 処理性能問題と提案する解決策

上記技術では，トランザクションの単位時間あたりの平均処理数の上限がブロックの最大サイズと平均生成間隔により制限され，ビットコインの場合 4,000 個/600 秒=7 個/秒程度となる．このため，提案するストリーム動画配信サービスの基盤としては性能が不足すると判断した．

なお，ブロックの最大サイズを大きくしたり平均生成間隔を短くするとブロックチェーンが分岐し合意形成が不安定になることが知られており，それらを変更せずに性能を向上できる手法が必要である．

IoTA[2]ではブロックチェーン構造を採用せず，トランザクション自体にグラフ構造をもたせることで，上記処理性能問題を解決する手法が提案されている．ただし，矛盾するトランザクションが複数生成された場合にどちらを有効とみなすかについてノード間で判断を統一するために，特権を持つ集中サーバが周期的に発行する特殊なトランザクション及びそこからグラフ構造で接続されたトランザクションのみを全ノードが有効と判断する手法を採用しており，集中サーバが排除されていない．

このため，我々は，IoTA の手法とビットコインの手法を組み合わせることで，双方の課題を同時に解決する手法を考案し，特許出願及び学会発表を行った．具体的には，IoTA 同様にトランザクション自体にグラフ構造をもたせることで，各ノードが受信するトランザクションを同期するが，有効なトランザクショングラフの末尾の指定は集中サーバではなくブロックチェーンで実施する．既存のブロックチェーンではブロック内にトランザクションが全て格納される必要があるが，提案手法ではトランザクショングラフの末尾の ID(以下末尾 ID)のみ格納する．本提案では，トランザクションの 1 秒あたりの発生数が大きくなるほどブロックに格納される末尾 ID 数は増大し，1 つのブロックに格納される末尾 ID 数がブロックサイズの上限(1MB で最大 31,250 個の末尾 ID を格納可能)に達した際に, 方式上の最大処理性能になると見込んでいる．なお，ネットワーク内の伝搬遅延時間が長いほどトランザクショングラフの末尾数は増加する傾向がある．そこで，シミュレータを開発し，1 つの PC(Dell PowerEdgeT330)内に 100 ノードによる p2p ネットワークを構成し，ノード間の 1 ホップの伝搬遅延時間を実網より十分長い 1.5 秒とした環境を構築した．本環境で，1 秒あたりのトランザクション発生数を 40 個/s から，当該 PC の性能上限であった 300 個/s まで変化させて，1 ブロック内の平均末尾 ID 数を測定した．結果を図 2 に示す. 図 2 より単位時間あたりのトランザクション発生数とブロック内末尾 ID 数はほぼ線形関係があることが分かった. また線形関係を外挿すると方式上の上限は約 3,850 トランザクション/s になることが分かった. 以上から, 提案手法は既存のブロックチェーン技術に比べて少なくとも 40 倍(300÷7)の処理性能を実現できることを確認できたと考えている．また，外挿による推定値では 500 倍(3,850÷7)の性能向上の可能性がある事がわかったが，1 台の PC では 300 トランザクション/s 以上の処理の確認が困難である．よって提案方式による最大処理性能の確認のためには，実サービスに近い多数の端末で構成した実験網を構築し測定する必要であり，今後の課題である．

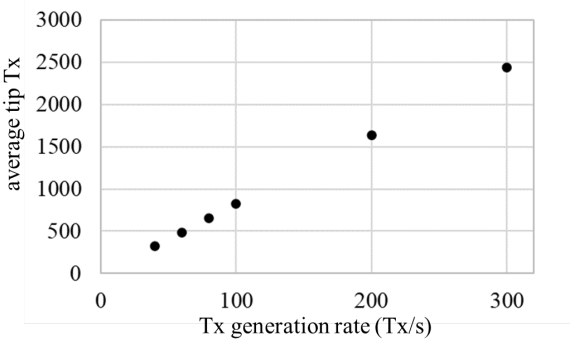

図2 単位時間あたりのトランザクション(Tx)発生数とブロック内に格納されたTx末尾ID数 の関係

② データ量問題と提案する解決策

代表的なブロックチェーンの一つであるイーサリアムでは 2022 年 4 月時点で既にブロックチェーンデータ量が 616G に達している[3]. 我々はスマートフォンでの動画視聴を前提としているが, 一般的なスマートフォンの容量を既に大幅に超過している. データ量は処理を完了したトランザクション数にほぼ比例するため，今後処理性能が向上するとますます大きな問題になると考えた．

一方，関連研究[4][5]では，ブロックチェーンを多数のブロック群に分割して，ブロック群ごとに，一部のノードのみが保持することで，ノードあたりのデータ量を削減する手法が提案されている．しかしながら，ブロックのヘッダ情報はすべてのノードが保持する必要があり，スマートフォンを想定するとまだ不十分である．

このため，我々は各ブロック群内のブロックヘッダを集約したブロック群ヘッダを新たに定義し，各ノードはブロッグヘッダの代わりにブロック群ヘッダを保持することで最新の台帳データの正当性を検証可能とする手法を考案し，特許出願を行っている．現在見積もっている従来手法と提案手法の 1 ノードあたりのデータ量を比較結果を表 1 に示す．表 1 より，提案手法により大幅にデータ量を削減できることが分かった．今後は詳細設計を進め，実機による動作確認を行う予定である．

表 1　従来手法と提案手法の 1 ノードあたりのデータ量比較結果

	従来技術		関連研究[5]		提案手法	
	フルノード	ライトノード	フルノード	ライトノード	フルノード	ライトノード
ブロック数 (データ量)	14.5M個 (616.2GB)	ー	2k個 (85.0MB)	ー	2k個 (85.0MB)	ー
ブロックヘッダー数 (データ量)	14.5M個 (7.5GB)	左同	左同	左同	2k個 (1.0MB)	左同
ブロック群ヘッダー数 (データ量)	ー	ー	ー	ー	14.5k個 (0.9kB)	左同
データ量合計	616.2GB	7.5GB	7.6GB	7.5GB	86.0MB	1.0MB

文献

[1]Takeshi Ogawa, Manato Oishi, and Noriharu Miyaho, "P2P video streaming method with Copy protection based on SDN technology." International Conference on Digital Arts, Media and Technology (ICDAMT), IEEE, pp. 52-57, Mar. 2017. (最優秀論文賞)

[2]IOTA Foundation, "The Coordicide", (https://files.iota.org/papers/Coordicide_WP.pdf), 2022.6.22.

[3] Ethereum ， ”Ethereum Full Node Sync (Default) Chart”, (https://etherscan.io/chartsync/chaindefault)， 2021.6.11.

[4]金子勇大，朝香卓也, "ブロックチェーンにおけるストレージを考慮した DHT 負荷分散クラスタリング", 信学技報, vol. 118, no. 371, NS2018-161, pp. 29-34.

[5] Y. Xu and Y. Huang, "Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain," in *IEEE Access*, vol. 8, pp. 17434-17441, 2020.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 島津　俊輝　小川　猛志	４．巻 J104-B No.7
２．論文標題 ブロックチェーンにおけるトランザクション処理性能向上技術	５．発行年 2021年
３．雑誌名 電子情報通信学会和文論文誌B，7月号	６．最初と最後の頁 613-618
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transcomj.2020BLL0015	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Toshiki SHIMAZU,　Takeshi OGAWA	４．巻 -
２．論文標題 Proposal of Transaction Processing Performance Improvement Technology of Blockchain	５．発行年 2020年
３．雑誌名 IEICE International Conference on Emerging Technologies for Communications　2020	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.63.E1-3	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 柿沼翔太，小川猛志
２．発表標題 IPネットワークにおける著作権管理可能なP2P動画配信方式の提案
３．学会等名 電子情報通信学会東京支部学生会
４．発表年 2019年

１．発表者名 柿沼翔太，小川猛志
２．発表標題 IP ネットワークにおける著作権管理可能な P2P 動画配信方式の検討
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2019年

〔図書〕　計0件

〔出願〕　計2件

産業財産権の名称	発明者	権利者
ノード及び分散合意形成システム	小川猛志，島津俊樹	同左
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2022-069495	2019年	国内

産業財産権の名称	発明者	権利者
合意形成システム	小川猛志，大林正樹	同左
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2019-153098	2022年	国内

〔取得〕　計0件

〔その他〕

視聴者制限可能なP2P動画配信技術
https://www.inl.aj.dendai.ac.jp/works3.html
著作権管理可能なP2P配信技術
https://www.iri-tokyo.jp/uploaded/attachment/5827.pdf

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	宮保　憲治 (MIYAHO NORIHARU) (10366396)	東京電機大学・システムデザイン工学部・教授 (32657)	
研究分担者	冬爪　成人 (FUYUTSUME NARITO) (30328520)	東京電機大学・システムデザイン工学部・講師 (32657)	
研究分担者	松井　加奈絵 (MATSUI KANAE) (30742241)	東京電機大学・システムデザイン工学部・助教 (32657)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関