一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2021-17(2021-05)

多層化ブロックチェーンを用いた時空間データ滞留システム監査機構に関する研究

上田　純輝† 　塚本　和也† 　山本　　寛†† 　野林　大起† 　池永　全志†

† 九州工業大学　〒820-8502 福岡県飯塚市川津 680–4
†† 立命館大学情報理工学部　〒525-8577 滋賀県草津市野路東 1 丁目 1-1
E-mail: †ueda.junki453@mail.kyutech.jp †tsukamoto@cse.kyutech.ac.jp, ††hiroyama@fc.ritsumei.ac.jp
†nova@ecs.kyutech.ac.jp †ike@ecs.kyutech.ac.jp

あらまし　IoT 技術の発展に伴い，多くの IoT デバイスや新たなアプリケーションが出現し，大量のデータが生成されることが予想される．それらのデータには，特定の時間・場所でのみ必要とされる時空間データ (STD) が含まれる．先行研究では，時空間データを特定の期間・範囲に滞留し続ける新たなネットワークの構築を目指し，車両を用いた時空間データ滞留システム (STD-RS) を提案してきた．しかし，STD-RS を実空間で動作させた際，位置情報の誤差や受信電波強度，ソフトウェアプログラムのバグなどによる誤動作が原因で，対象とする範囲外に STD が送信される可能性がある．STD-RS を利用するサービス提供者としては，提供範囲の信頼性確保は重要な点といえる．そこで本研究では，下位層では実空間から生成される STD の管理を行う一方で，上位層では STD-RS が誤動作していないか監査する仕組みとして，多層化ブロックチェーンを新たに提案する．STD-RS のリアルタイム監査を実現するには，ブロック探索時間の短縮化が重要となるため，総ブロック数に依存しない効率的なブロック探索手法を考案し，シミュレーション評価実験を通じて有効性を明らかにした．

キーワード　多層化ブロックチェーン，時空間データ，データ滞留

An Audit Mechanism for Spatio-Temporal Data Retention System Using Based on Multi-tier Blockchain

Junki UEDA†, Kazuya TSUKAMOTO†, Hiroshi YAMAMOTO††, Daiki NOBAYASHI†, and Takeshi IKENAGA†

† Kyushu Institute of Technology
680–4 Kawazu, Iizuka-shi, Fukuoka, 820–8502, Japan
†† College of Information Science and Enginieering,Ritsumeikan University
1-1 nojihigashi1choume, kusatsu-shi, Shiga, 525–8577, Japan
E-mail: †ueda.junki453@mail.kyutech.jp †tsukamoto@cse.kyutech.ac.jp, ††hiroyama@fc.ritsumei.ac.jp
†nova@ecs.kyutech.ac.jp †ike@ecs.kyutech.ac.jp

Abstract　With the development of IoT technology, a large number of IoT devices and new applications are expected to emerge, generating a large amount of data. These data include spatio-temporal data (STD), which is needed only at a specific time and place. In our previous research, we proposed a spatio-temporal data retention system (STD-RS) using vehicles, aiming to construct a new network that keeps spatio-temporal data in a specific period and range. However, when STD-RS is operated in real space, there is a possibility that STD is transmitted outside the target range due to malfunctions caused by errors in location information, reception signal strength, bugs in software programs, etc. As a service provider using STD-RS, it is important to ensure the reliability of the provided range. In this paper, we propose a new method for the transmission of STD-RS. In this paper, we propose a multi-layered blockchain as a mechanism to audit STD-RS in the upper layer while the lower layer manages the STD generated from the real space. In order to achieve real-time auditing of STD-RS, it is important to reduce the block search time.

Key words　Multilayered blockchain, Spatio-temporal Data, Data Retention

1. はじめに

IoT (Internet of Things) 技術の発展に伴い，多くの IoT デバイスや新しいアプリケーションが爆発的に増加している．IoT デバイスが生成するデータの中には，発生した時間や地理空間に依存するものがあると考えられ，先行研究ではこのようなデータを時空間データ (Spatio-temporal data，STD) と定義している．例えば，交通情報，気象情報，災害情報，時限的な店舗広告などの情報は，その情報が生成された場所に依存しつつもその状況がリアルタイムに変化するため，時空間データであるといえる．

一方で，スマートシティの一環として，様々なサービス提供事業者が STD を収集し，処理を行い，特定の地域を対象としたコンテンツを生成し，サービスとして提供されることが想定される．我々はこれまでに，地域に分散配置された IoT 機器の種類や IoT データの管理者に依存しない二次利用を目的として，地理空間を意識した IoT データの収集，処理，コンテンツ配信を行う地理指向情報プラットフォーム (GCIP:Geo-Centric Information Platform) [1] を提案している．[1] では，自治体などの地理空間の管理組織が STD の収集・管理を一元的に管理する想定だったものの，実環境では複数の事業者が STD を収集・管理することが想定される．この場合，STD のデータ共有空間範囲や時間などの違いを吸収する柔軟な共有手法が必要となる．

また，GCIP [1] では STD の配信機能の一つとして，特定の範囲内を走行する車両を用いた自律分散のデータ滞留システム STD-Retention System(STD-RS) を提案している [2]. [2] では滞留範囲内に存在する車両が自身の位置情報に基づいて，定期的に STD をブロードキャストすることで，滞留範囲内のユーザが STD を受動的に受信可能となる．しかし，STD-RS ではその自律制御に起因して，(a) 車両ノードの位置情報誤差，(b) 受信電波強度の計測誤差による車両間の近さの誤推定，(c) ソフトウェアプログラムのバグ，などにより STD-RS を構成する車両が誤動作することで，本来想定しないエリアから STD が配信されることが考えられる．STD-RS の誤動作による想定外のデータ送信は，帯域の無駄遣いだけでなく，STD 配信者にとっては対象外のユーザに情報を発信することになるため，情報漏洩などのリスクが発生することになる．一方でユーザとしては，不必要な情報受信によって非利益を被る可能性がある．

そこで本研究では，GCIP において STD の配信に STD-RS を用いる状況を想定し，その配信が滞留範囲内で正常に配信されているかを監査する仕組みとして，STD が各エリアで流通された履歴を管理・解析する機能を備えた多層化ブロックチェーンを新たに提案する．これにより，STD の柔軟な共有の実現と STD-RS が誤動作が発見でき，STD-RS の機能向上を図ることができる．STD-RS の誤動作検知性能を評価するために，(1)STD 生成時の作成したブロックの全ノードへの伝搬時間と (2)STD 誤送信をブロックチェーン上で検知するまでの遅延時間，に関して提案手法の有効性をシミュレーション実験によって評価する．

2. 関連研究

本研究では，複数の車両から取得した情報を用いて，ネットワークの端 (エッジ) 部分でブロックチェーンを作成し，情報の共有を実現することを目指す．そのため，本節では複数の車両から安全に交通情報を取得するため，ブロックチェーンを利用したエッジコンピューティングの関連研究について述べる．

[3] では，車両間での通信の信頼性の問題や，車両から生成される情報の取得のため，分散データ管理基盤として機能するブロックチェーンが，RSU と車両により構成される．また，車両が生成した様々な情報の登録を受け付けてブロックチェーンへ登録する機能が，スマートコントラクトとして実装されている．スマートコントラクトとは，ブロックチェーン上で様々な処理を自動的かつ高信頼に実行する仕組みであり，Ethereum などの比較的新しいブロックチェーンに備わっている．車両から生成される情報は RSU に送信され，RSU でブロックが作成される．作成されたブロックはブロックチェーンを構成する全ての RSU・車両へ自動的にブロードキャストされる．ここで，ブロードキャスされたデータが改ざんされていないことは，ブロックチェーンを構成する RSU・車両群により相互に検証されるため，高信頼な情報共有が可能となる．

[4] [5] では，ブロックチェーンで現在問題とされている，「単位時間に処理可能な取引量が少なくなる」スケーラビリティ問題の解決法として，地理的に近いノード同士でドメインを自律的に形成し，ドメイン毎に独自のブロックチェーンを管理する手法が提案されている．特に [5] では，各ドメインに存在するノードの減少ブロックチェーンの改ざん耐性が低下しないように，多数のブロックチェーンが相互に解決する P2P ネットワークを構成し，各ブロックチェーンの状態を相互に記録・検証する履歴交差法を用いることで，スケーラビリティの問題を解決している．

3. 先行研究

本節では，柔軟な大きさの地理空間を対象に異分野連携を行う GCIP(Geo-Centric Information Platform) の全体概念を説明する．その後，GCIP における STD 配信手法の一つである時空間データ滞留システムについて説明する．

3.1 Geo-Centric Information Platform [1]

GCIP [1] では時空間データ STD に着目し，地理空間を意識して STD を収集し，処理を行い，地理空間向けのコンテンツを生成した上で，配信を行う地理指向情報プラットフォーム (GCIP:Geo-Centric Information Platform) という概念を提案した．この節では，地理を意識したデータ流通プラットフォームである GCIP と，その要素技術についての説明を行う．GCIP では，図 1 のように，ある任意の地理空間範囲内に存在する様々な機器からインターネット上に送信される多種多様なデータを地理空間を単位として集約できる．データの収集は，交換局，携帯電話網の基地局，Wi-Fi のアクセスポイント (AP) 等の様々な機器が設置されるポイントで行う．次に，前述したネットワーク機器が収集したパケットを複製し，空間範

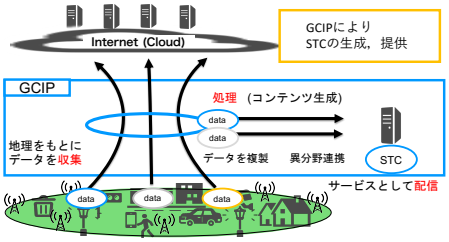

図 1: GCIP

囲を公共的に管理する自治体などの組織が設置するストレージ (以降，データ蓄積サーバと呼ぶ) に随時蓄積する．地理空間範囲は国土地理院が定義したメッシュ ID に基づいて識別されており，データ蓄積サーバが設置された各メッシュ内には，当該メッシュを対象として，時空間コンテンツを提供したい事業者が管理する異分野連携サーバを設置し，データ蓄積サーバから取得したデータを機械学習，統計処理等で分析し，時空間情報を活用したコンテンツを動的に生成する．生成したコンテンツはデータ収集時に利用した各種インフラ網だけでなく，3.3 節で説明するデータ滞留システム STD-RS を用いて配信することで，当該地域内のユーザに向けてサービスを確実に配信する．

3.2 実環境を想定した GCIP の拡張

現在，急ピッチで整備が進められている次世代移動体通信網 5G は，全国を 10km 四方のメッシュ (国土地理院が定義する 2 次メッシュ) に区切り，メッシュ毎に移動体通信事業者が 5G 高度基地局を設置することを目指している．さらに，この 2 次メッシュ内では，より細かいメッシュ単位で，小規模基地局を配置することができる上，任意の範囲を対象にモバイルエッジコンピューティング (MEC) サーバを設置することが予想される．そのため，実際には各空間範囲内には，通信事業者が独立して基地局を設置する上，居住地域には各種アクセスポイント (AP) が設置されると予想される．次にデータ蓄積サーバに着目すると，各通信事業者が設置する MEC サーバに蓄積される上，公共性の高いデータは自治体が管理するデータ蓄積サーバに別途蓄積されることになる．つまり，当初 GCIP で想定していた自治体が設置したデータ蓄積サーバでの一元管理は実現的ではなく，各通信事業者が設置した MEC サーバとデータ蓄積サーバ，異分野連携サーバ間の柔軟なデータ共有を想定したプラットフォームの構築が必要不可欠である．

3.3 時空間データ滞留システム (STD-RS)

3.3.1 前 提 条 件

STD-RS では，コンテンツを配信する空間範囲内に存在する車両 (以降，ノードと呼ぶ) を活用する．各ノードは GPS によって位置情報を取得しており，定期的に自身の ID を含んだビーコンを一定周期でブロードキャスト送信する．加えて，STD は条件に応じて確率的にブロードキャストでコンテンツを拡散する．このデータには滞留エリアの情報 (中心座標，滞留半径 R)，データ送信間隔 d が含まれているため，受信した各ノードは自身の位置情報とデータに含まれる滞留エリア情報から，STD の拡散の可否を自律的に決定する．

3.3.2 STD-RS の問題点

STD-RS の目標は，滞留エリア全体にデータを定期的に拡散し，滞留させることである．よって，システムユーザが滞留エリア内に入ると自動的にデータを受信できる．しかし，STD-RS は，時空間データを滞留させる車両の送信制御が完全に自律分散化しているため，(a) 車両ノードの位置情報の誤差 (b) 電波伝搬強度の変化誤差 (c) ソフトウェアプログラムのバグにより想定外の動作が発生する可能性がある．この場合，滞留エリア外でのコンテンツ配信 ((a) と (b)) やパケットロスの増大 ((c)) が発生する事になる．これまでに提案した STD-RS では，(a) (c) に起因する各種誤動作を検出・監査できる仕組みがないため，STD 配信の信頼性・効率性の低下だけでなく，無線資源の利用効率の低下を招くことになる．そのため，STD-RS の信頼性・効率性の向上を実現する誤動作の検出・監査システムが必要不可欠である．

4. 提案手法：多層化ブロックチェーン

前述した STD-RS における問題点を解決するために，多層化ブロックチェーンによる STD-RS の誤動作検知機構を提案する．多層化ブロックチェーンでは，4.1 節で記載するようなネットワーク環境に対して 2 層のブロックチェーンを構成する．その上で，4.3 節で説明する探索手法を用いて，上位層ブロックチェーンのブロック探索時間の短縮を実現する．

4.1 ネットワーク構成

今回は共通に定義されたメッシュエリア単位に独立管理の形で各通信事業者が独立して管理する基地局 (メッシュルータ) を設置した上で，データを収集し，そのデータを保管する MEC サーバを設置する環境を想定する．この想定環境を図 2 に示す．MEC サーバは収集した情報を元にコンテンツを生成，管理する．これに加えて GCIP に従って地理空間毎に収集したデータは行政機関が保持するため，情報をデータ蓄積サーバにて保管，管理する．例えば，地域内に存在する店舗が発信する広告，交通などの公共性の高いコンテンツなどがデータ蓄積サーバに保管される．

そこで図 3 に示すように，各種通信事業者が保持するコンテンツと行政機関が保持するコンテンツを共有し，ユーザに STD-RS を利用して配信するため，本研究では RSU を MEC サーバ，異分野連携サーバとして活用する．本研究では，各エリアに配備されている複数の RSU 間でコンテンツを共有するために，RSU 群がブロックチェーンを構築する (下位層ブロックチェーン)．この下位層ブロックチェーンを活用することで，各機関が保持する独自コンテンツに加えて，共有によって新しいコンテンツが生成できる．さらに GCIP では RSU を介して，STD-RS を活用することで作成したコンテンツを配信できるため，その情報を GCIP により再度収集するサイクルを構築することで，高度な STD の生成，処理，配信システムの構築が可能となる．

4.2 多層化ブロックチェーン間の連携手順

上位層のブロックチェーンは下位層に MEC サーバを設置した通信事業者や行政機関間の STD，コンテンツの共有や，3.3.2

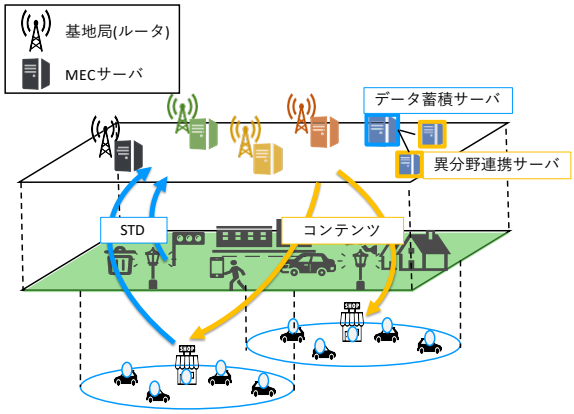

図 2: メッシュ内の想定

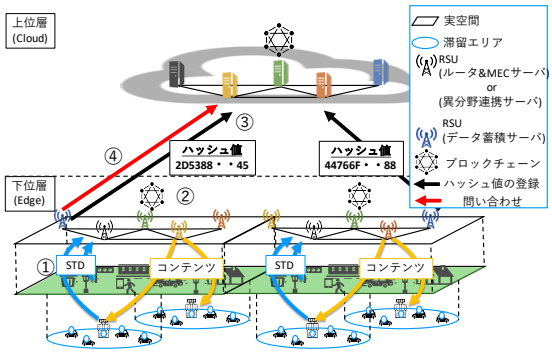

図 3: 多層化ブロックチェーン間の連携

節で述べた STD-RS の問題が発生していないかを検知することを目的としてグローバルに構築される．STD-RS の問題が発生してないか検知できるまでの流れは以下の通りとなる．

1. まず，メッシュ内の実空間において，各種デバイスから生成される STD や STD-RS の稼働状況に関する情報がメッシュルータを通して，データ蓄積サーバや MEC サーバに送信される．

2. MEC サーバやデータ蓄積サーバ，異分野連携サーバは共有可能な STD のみを下位層のブロックチェーンに登録する．

3. データ蓄積サーバは下位層ブロックチェーンに登録された STD からハッシュ値を生成し，上位層のブロックチェーンに登録する．

4. そして，コンテンツ配信者からの依頼があった場合，上位層のブロックチェーンに登録されているハッシュ値を読み出し，複数のエリアから登録されているハッシュ値を特定する．

上位層のブロックチェーンに登録されるハッシュ値は STD やコンテンツ毎に異なるため，同一のハッシュ値が登録された場合，そのハッシュ値に対応する STD が特定のエリア外に送信されたと判断できるため，STD の誤送信を検知できる．

下位層から上位層に登録されるトランザクションのデータ構造を表 1 に示す．トランザクションのデータ構造はトランザクションを識別するトランザクション id と STD のハッシュ値，

表 1: トランザクションのデータ構造

要素	説明
index	トランザクション id
hash	STD のハッシュ値
timestamp	トランザクションの生成時刻
area	STD の流通が確認されたエリア
company	STD の配信を管理する組織

表 2: ブロックのデータ構造

要素	説明
index	ブロック id
timestamp	ブロックの生成時刻
transaction	含まれているトランザクション
previoushash	前ブロックのハッシュ値

トランザクションが作成された時間のタイムスタンプ，どのエリアから生成されたか判別する area，どの管理主体が管理しているか判断するための company で構成される．今回，STD が誤送信された事だけを検知したいためシンプルなデータ構造としている．

下位層のブロックチェーンには STD やコンテンツ共有を目的として，STD やコンテンツ本体を登録するものの，上位層のブロックチェーンでは，STD やコンテンツの誤送信を検出する事のみを目的とするため，ハッシュ値のみを登録する．また，データ蓄積サーバからの問い合わせを受け付ける機能はスマートコントラクトとして実装され，上位層ブロックチェーンに配備されている．

4.3 多層化ブロックチェーンでの探索手法

STD をメッシュ内で共有するデータ蓄積サーバは，上位層のブロックチェーンに STD を誤送信していないか検証依頼を行う．この際，上位層ブロックチェーンではブロック探索が必要となるが，完全性が確保されているブロックチェーン内部のデータを参照するために，全ブロックを探索することが望ましい．しかし，図 4 のように，1 ブロックの検証に 1 秒要する場合，n ブロックによってチェーンが構築された状況で、全てのブロックを探索して該当するトランザクションが存在するかを検索する全探索手法では n ブロックの探索が必要となるため，計 n 秒時間がかかる．つまり，登録トランザクション数の増加に比例して探索時間が増加してしまう．

そこで，本研究では完全性は一定程度犠牲にはするものの，STD の誤送信検知時間を短縮するために，前回探索したブロックまでの検証結果を保持した上で，次回探索時には新しく追加されている未検証であるブロックのみを探索の対象とする手法を新たに提案する．提案手法の動作を図 4 を用いて説明する．

1. 下位層のデータ蓄積サーバではこれまでに上位層ブロックチェーンに検証依頼を行った事があり，上位層ブロックチェーンの n-1 ブロック目まで検証が終了しているとする．

2. 上位層ブロックチェーンで n ブロック目が生成された段階

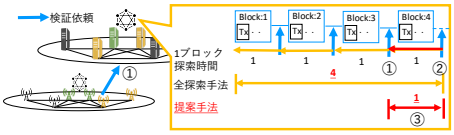

図 4: 提案手法

表 3: ブロック伝搬のパラメータ

パラメータ	数値
ブロックサイズ [byte]	1000000
帯域幅 (送信帯域幅，受信帯域幅)[bps]	10000000
ノード間の遅延 [ms]	5,10,50,100
ノード数	4,16,64,256,1924,4096

で下位層のデータ蓄積サーバから検証依頼があったとする．この時，提案手法では n-1 ブロック目までの検証は終了しているため，1(n-(n-1)) ブロックのみの検証となる．

3. 結果として，計 1 秒の探索時間で済む

提案した探索手法では，未検証ブロック数のみを探索するため，未検証ブロック数が一定の場合，検証時間は一定となることが予想される．

5. シミュレーション評価

5.1 評価指標と評価環境

本節では，STD-RS の誤動作検知手法を評価するために，多層化ブロックチェーンを用いた際の STD の検知にかかる時間を評価する．この時間はブロックが生成されてから同じハッシュ値検証が完了するまでの時間となるため，大まかに (1) ブロック生成と伝搬時間，(2)STD 誤送信の検知時間，の二つの時間に分類される．(1) の時間では，ブロックチェーン内で対象とする STD のハッシュ値を含むブロックが生成され，ブロックチェーンに参加する全ノードにブロックが伝搬されるまでにかかる時間を評価する．評価には自作したシミュレータと simblock [6] [7] を組み合わせて用いた．具体的には，未確認のトランザクションのブロック内への格納，マイニング，及びブロックチェーンへの連結処理時間を自作ブロックチェーンで行い，その後のブロック伝搬時間を simblock で評価した．評価時のパラメータを表 3 に示す．伝搬時間への影響があると予想される，ノード間の遅延とノード数を変更パラメータとし，その影響を調査する．ノード数は GCIP で定義した階層化メッシュに基づき，メッシュ階層に関する次数 k のメッシュ数 4^k 毎にエッジサーバが設置されるものとした．また，マイニング時間はノード間がある程度の信頼関係があるものとし，一想定として平均 7 秒の標準正規分布に従う値を用いている．

(2) の時間では，上位層のブロックチェーンにおいて誤送信された情報のハッシュ値をブロックチェーンで検知できるまでの時間としてトランザクションを全探索する手法と前回探索した値を保持する提案手法の評価を行った．評価には自作シミュレータを用いる．また，従来の GCIP の想定する行政機関が

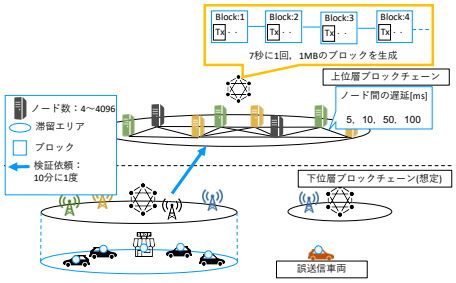

図 5: 検証トポロジ

管理するデータ蓄積サーバ，異分野連携サーバでコンテンツ管理を行うとし，STD-RS に関する情報のみを登録する事を目的とする想定をしたプライベートネットワークと各通信事業者と行政機関が相応な関係としてブロックチェーンを構成し，STD-RS に関する情報以外からも情報が登録される事を想定したパブリックブネットワークでの 2 パターンの評価を行った．

プライベートネットワークでは 7 秒間に 1 回，STD-RS に関する情報のみが登録されたとし，STD 数に応じたブロックサイズのブロックを生成を行う．パブリックネットワークでは上位層のブロックチェーンで STD-RS 以外からも様々な情報が登録されているとし，7 秒に 1 度，現在のビットコインネットワークのブロックサイズ上限である 1MB のブロックを作成しているとする．また，ブロックチェーンでは，ブロックに含まれている各トランザクションに付与されているデジタル署名を検証する処理などのために，ブロックに記載されているデータの読み出しには一定の時間を要する．そのため [8] より，平均ブロック検証時間 Td は，ブロックサイズ Sb と検証定数 kd=0.3796 より，平均ブロック検証時間は式 (1) となる．

$$Td = 0.3796 * sb \tag{1}$$

パブリックブロックチェーンでは 1 ブロック，1MB とするので，式 (1) より 1 ブロックの検証に 0.3796 秒かかる．また，一想定として，6 メッシュエリアから平均 5，7，10，30，60，300 秒の STD 送信間隔で 60 分間のデータ量でブロックを探索するとし，検証依頼の間隔は 10 分間に 1 回行うとしている．

検証トポロジを図 5 に示す．上位層ブロックチェーンと下位層ブロックチェーンで多層化ブロックチェーンが構成されており，下位層では STD-RS の対象とするエリアの RSU で構成されたブロックチェーンと，STD-RS の対象としないエリアの RSU で構成されたブロックチェーンがあることを想定している．また，今回 STD-RS では STD を受信した車両が，誤ってエリア外の RSU に共有してしまったことを想定する．

5.2 評　　価

5.2.1 ブロック生成と伝搬時間

(1) ブロック生成と伝搬時間についての結果を図 6 に示す．ノード間の遅延 5ms と 100ms の時のノード数 4096 での伝搬時間を比べると，遅延 5ms に比べて，遅延 100ms では約 1.5 倍の伝搬時間が経過していることから遅延による伝搬時間の影響は大きいことを確認できた．また，ノード数 4 とノード数 4096 の場合のノード間遅延 100 での伝搬時間を比べると，ノード数

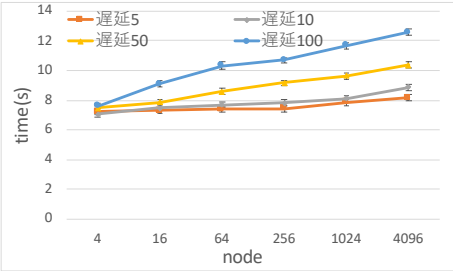

図 6: ブロック生成時間

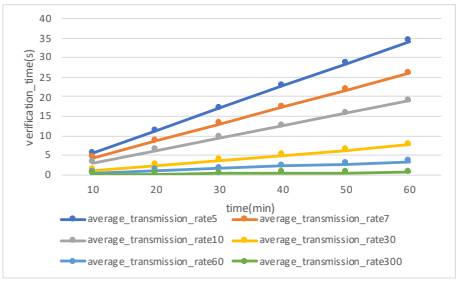

図 7: プライベートネットワーク-全探索手法

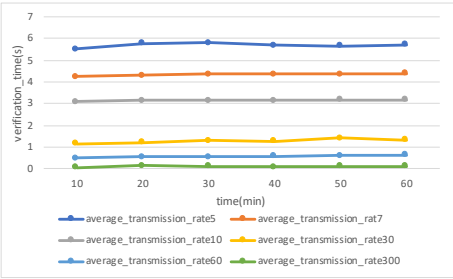

図 8: プライベートネットワーク-提案手法

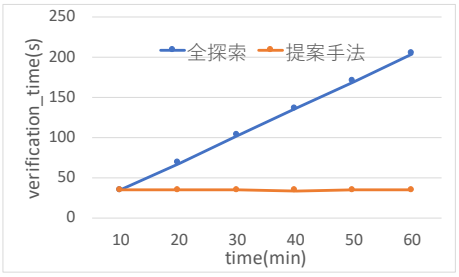

図 9: パブリックネットワーク-全探索と提案手法

4 に比べて，ノード数 100 が約 1.5 倍の伝搬時間が経過していることから，ノード数も伝搬時間への影響が大きいことも確認できた．また，ノード 4 の時の伝搬時間を見ると，ノード間の遅延が大きい場合でも遅延が小さい場合の検証時間よりも短くなっているが，これは数秒しか違わないため，マイニング時間の影響を受けたものだと考えられる．この結果により，ノード数とノード間遅延によるブロックチェーン性能の影響を確認できた．

5.2.2 STD 誤送信の検知時間

まず，STD-RS に関する情報のみを登録する，プライベートネットワークでの全探索手法による検証結果を図 7 に示す．プライベートネットワークでの提案手法による検証結果を図 8 に示す．

プライベートネットワークでは 7 秒間 1 回，ブロックが生成される．しかし，特定のノードのみで構成され，STD-RS が生成する STD の管理を目的としているため，パブリックネットワークに比べて登録される STD 数は少なくなり，ブロックサイズが小さくなる．そのため，検証時間も少なくなり，ブロック探索時間も平均 5 秒の間隔で STD が送信された場合だと，約 34 秒程度の時間となっている．また，特にデータ量が多い場合，全探索手法に比べて提案手法では，ブロック探索にかかる時間を大きく減らすことができるため，有効な手段であると言える．

今回パブリックネットワークは STD-RS 以外からも様々な情報が登録されてるとし，7 秒に 1 度，1MB のブロックを作成していると想定しているので，検証時間はどの STD 送信間隔でも同じ値になった．今回は平均 5 秒の間隔で STD が送信された場合の結果を図 9 に示している．ブロック探索時間では全探索では STC が送信されるにつれ，時間経過とともに探索時間がかかっており，60 分経過時のデータ量では，探索時間は約 205 秒となっている．プライベートネットワーク全探索手法と提案手法と比較すると，共に 60 分経過時のデータ量でのブロック探索時間に比べて約 6 倍ブロック探索時間が多くなることを確認できた．また，提案手法では，どの時間のデータ量でも約 34 秒になっている．60 分経過時の探索時間を比べると約 6 分の 1 となっており，特に時間が経過した際や実環境を想定した場合に有効な結果が示せている．

6. ま と め

本研究では，STC の誤送信検知のための多層化ブロックチェーンを新たに提案した．提案手法では，上位層と下位層の 2 層のブロックチェーンで構成される．下位層のブロックチェーンは特定のエリア内で構築され，異なる事業者間の STD 共有を目的とする．一方，上位層のブロックチェーンは STD 誤送信検知を目的としてグローバルに構築される．下位層では異なる事業者間のデータ共有のためにデータ自身をブロックチェーンに登録するものの，上位層のブロックチェーンにはハッシュ値のみを登録する．上位層のブロックチェーンに登録されるハッシュ値は STD 毎に異なるため，同一のハッシュ値が登録された場合，情報が特定のエリア外に送信された場合に，誤送信として検知できる．また，シミュレーション実験を通じて、本提案手法によって STD 誤送信の検知が異なる管理主体がデータを共有するパブリックネットワークにおいて、ノード数 4096 台の規模のネットワークにおいても約 34 秒程度で誤送信を検出できる事を明らかにした．

今後は多層化ブロックチェーンを実機に実装した上で，エ

ミュレータを用いて検証結果とシミュレーション結果を比較し，有効性を評価する．

謝　　辞

本研究の一部は，JSPS 科研費 19H04103，及び国立研究開発法人情報通信研究機構の委託研究による成果を含む．ここに記して謝意を表す．

文　　献

[1] K. Tsukamoto, H. Tamura, Y. Taenaka, D. Nobayashi, H. Yamamoto, T.Ikenaga, and M. Lee, “Geolocation-centric Information Platform for Resilient Spatio-temporal Content Management,” IEICE Trans.Commun. , Online ISSN 1745-1345, Print ISSN 0916-8516, Sep.2020. DOI: 10.1587/transcom.2020NVI0003 (Early publication)

[2] Daiki Nobayashi, Ichiro Goto, Hiroki Teshiba, Kazuya Tsukamoto, Takeshi Ikenaga, Mario Gerla, "Adaptive Data Transmission Control for Spatio-temporal Data Retention over Crowds of Vehicles," IEEE Transactions on Mobile Computing, Early Access, Mar. 2020.

[3] Maoqiang Wu, et al. "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks",IEEE Internet of Things Journal October 2018.

[4] A. Fujihara, “PoWaP: Proof of Work at Proximity for a crowdsensing system for collaborative traffic information gathering,” Internet of Things, 100046, Elsevier (2019).

[5] 柳原貴明，藤原明広, "ブロックチェーン履歴交差法の実験的性能評価" IN 研究会, 2020 年 3 月.

[6] 青木優介，首藤一幸，"SimBlock: ブロックチェーンネットワークシミュレータ"，IA 研究会，2019 年 3 月.

[7] 永山流之介，首藤一幸，坂野遼平，"コンパクトブロックリレーとインターネット高速化を考慮したビットコインネットワークシミュレーション" NS 研究会 2020 年 3 月.

[8] Motlagh, S.G., Mišić, J. and Mišić, V.B. An analytical model for churn process in Bitcoin network with ordinary and relay nodes. Peer-to-Peer Netw. Appl. 13, 1931–1942 (2020).