2024 年度 委託研究

課題 241

高信頼データ流通のための非集中型ネットワーク内ストレージ及びアプリケーションの研究開発

研究計画書

国立研究開発法人
情報通信研究機構

１．研究開発課題

『高信頼データ流通のための非集中型ネットワーク内ストレージ及びアプリケーションの研究開発』

２．目的

サイバー空間とフィジカル空間を高度に融合させるシステムにより、社会的課題をデジタル技術で解決する「Society5.0」のビジョンのもと、いわゆるデータ駆動型社会への変革を目指す取り組みが進んでいる。データ駆動型社会では、地理的に分散し、複数のデータ所有者（組織や個人）が有する膨大な量の分散データを扱う必要がある。しかし、全てのデータを一部のクラウド事業者等のプラットフォームで管理する従来の形態では、機密・プライバシーに関わるデータの意図しない漏洩や、データ公開の一方的な停止等が起こる懸念がある。このため、データの保持・管理を自らが管理するサーバー等を用いて自律的に行い、それらの連携によりデータを流通させる「自律分散型」のデータ流通アーキテクチャの実現を目指した研究開発が盛んに進められている。このデータ流通の形態においては、悪意あるデータ所有者が偽のデータを流通させる等の攻撃を避け、データの真正性・可用性をいかに保つかが大きな課題となる。

全てのデータ所有者が対等な立場で、データの真正性、高い可用性を保ち、単一故障点がなくデータの共用・流通を可能とする技術として、ブロックチェーンに代表される分散台帳技術（DLT: Distributed Ledger Technology）が広く用いられている。DLT は、分散ネットワーク内のすべてのノード（計算機・サーバー）上で同期されたトランザクションデータを認証し、権限の透明性や責任追跡性をサポート可能なシステムであり、仮想通貨の実装等にも用いられている。ブロックチェーンに保存されるデータは、すべてのノードに同期する必要があり、大容量のデータを扱う場合に通信コスト・ストレージコストが大きくなる。このため、ブロックチェーンへはデータのハッシュ値のみを保存し、データそのものを保存する外部のストレージ（オフチェーンストレージ）をブロックチェーンと連携させて利用することで、通信コスト・ストレージコストを抑える形態が一般的となっている。

企業間連携や医療応用等では、機密・プライバシーを保護するため、データ所有者がデータ開示相手を明示的に制御可能とする機能が要求される。また一般にデータを保管する地理的位置が他国や他地域の場合、その位置に依存して法令等の制約の影響を受けるため、データ流通の地理的範囲を制限する機能も必要となる。DLT 上のトランザクションデータは公開が前提となるため、こうしたデータ流通の機能はオフチェーンストレージによって実現する必要がある。しかし、現状のオフチェーンストレージはこれらの機能を十分に有していない。

国立研究開発法人情報通信研究機構（以下、「機構」という。）では、上記課題に対し、属性に基づく暗号処理と Information-Centric Network（ICN）を組み合わせることで、データアクセス効率、流通範囲の制御を可能とするネットワーク内ストレージ構成方式 [1]、ならびに、同方式と、オフチェーンストレージとして広く用いられている InterPlanetary File System (IPFS) [2]と呼ばれる非集中型ストレージシステムとを連携動作させる「NICT セキュアオフチェーンストレージ」の実装を進めている。本委託研究は、この NICT セキュアオフチェーンストレージとブロックチェーンとを組み合わせて利用し、高信頼・高効率のデータ流通機能を有する非集中型ネットワーク内ストレージを実装するとともに、アプリケーション実証を行うものである。

３．内容

ブロックチェーン、「NICT セキュアオフチェーンストレージ」を用いた高信頼・高効率の非集中型ネットワーク内ストレージ、およびアプリケーションの実現に向けた研究開発を行う。

ブロックチェーンは、自由参加型（Ethereum など）と許可型（Hyperledger Fabric など）に分類されるが、NICT セキュアオフチェーンストレージはいずれの型でも連携可能である。後述の実証用テストベッド上ではブロックチェーンとして許可型の Hyperledger Fabric [3]を動作させる。

「NICT セキュアオフチェーンストレージ」は以下の機能要素から構成される。

- IPFS（非集中型ストレージ）

IPFS はオープンソースにより開発が進められている構造化オーバレイネットワーク上で動作する非集中型のストレージプロトコルおよびその実装であり、現在のインターネットで主要なプロトコルである Hyper Text Transfer Protocol (HTTP) を補完または置換するプロトコルとすることを目指している。IPFS では、コンテンツのハッシュ値をコンテンツの ID として利用する方法を採用しており、データの改ざんに強く、正当性の検証が容易となっている。NICT セキュアオフチェーンストレージでは、性能・信頼性を向上させる改造を行った「NICT 版 IPFS」を用いる。NICT 版 IPFS のアプリケーションインターフェースは、Go 版 IPFS（Kubo[4]）に従う。

- UCINC（セキュアネットワーク内ストレージ機能）

機構が研究開発を進めている、ブロックチェーンで管理されたデータへのアクセスを安全かつ高速に行えるネットワーク内ストレージ機能 [1]。ICN によりデータの名前や対応するコンテンツの ID をもとにネットワーク内にキャッシュとして保存する機能を持ち、データ送信元の配信負荷削減と応答遅延の向上が可能。また、Ciphertext-Policy Attribute-Based Encryption (CP-ABE)と呼ばれる属性暗号を用いて、ユーザーの属性に基づくアクセス権限に応じたデータの開示・非開示の設定が可能である。さらに、許可されたネットワーク外ではキャッシュを保持しない域外キャッシュ管理機能を有し、データ流通範囲の制御が可能となっている。本機能は、機構開発のオープンソースである Cefore [5]を用いて実装されており、Cefore が有するインターフェースを通じて利用可能である。

- Authority （トラストアンカー機能）

許可型ブロックチェーン、IPFS ネットワークに参加するための証明書の発行、およびユーザーの属性に応じた CP-ABE の暗号鍵の発行等を行う。Authority の各機能は HTTP・REST インターフェースを通じて利用できる。

本委託研究では、ブロックチェーンおよび NICT セキュアオフチェーンストレージを組み合わせ、以下の項目の研究開発を行う。

研究開発項目１ 非集中型ネットワーク内ストレージフレームワークの研究開発

研究開発項目２にて実証するアプリケーションで活用可能とする非集中型ネットワーク内ストレージのフレームワークを研究開発する。ブロックチェーンおよび NICT セキュアオフチェーンストレージを活用し、高信頼かつ高効率なデータ流通アプリケーションを実現する上で必要

な機能（ブロックチェーン上のスマートコントラクトを含む）を、ソフトウェアフレームワークとして設計・実装する研究開発を行う。
具体的には、以下の方法についての研究開発を行う。

- 安全性・プライバシーを維持する計算処理方法
  NICT セキュアオフチェーンストレージが有する属性暗号機能およびデータ流通範囲制御機能を活用し、データの安全性、プライバシーを維持しつつ、アプリケーション固有の計算処理を実行する方法
- 性能の確保
  NICT セキュアオフチェーンストレージが有するキャッシュ機能等の利点を活かし、高い応答性能やスループットを実現可能とするアプリケーションデータ制御（検索、処理、送受信などを含む）方法

上記を、既存アプリケーションやデータ基盤との互換性、法令等との適合性を確保しつつ、アプリケーション共通の基盤となるソフトウェアフレームワークとして設計・実装すること。
当該フレームワークは下記を満たすこと。

- NICT セキュアオフチェーンストレージを構成するソフトウェアのうち、IPFS および UCINC のソフトウェアを組み込み、属性暗号により暗号化されたデータの登録・取得を行う機能を有すること。NICT セキュアオフチェーンストレージのデータへ、IPFS および UCINC 両方のインターフェースを用いてアクセスするアプリケーションソフトウェアを実装すること。IPFS および UCINC のインターフェースをそれぞれ異なるアプリケーションソフトウェアが用いる形でも良い。
- IPFS、UCINC、Cefore、Authority の各機能要素は、基本的に機構より提供または貸与されるソフトウェアを用いること。Hyperledger Fabric は、オープンソースソフトウェアとして公開されているのでそれを用い、後述のテストベッド上で動作する Hyperledger Fabric のネットワークに接続して動作させること。品質担保や課題解決のために必要であれば、各機能要素を改良・拡張すること。また、各機能要素は機構と協議の上、独自の実装に置き換えても良い。その場合もインターフェースの互換性に留意すること。
- 将来の外部システム連携を考慮し、外部の IPFS のデータを標準的な API を用いて取り込む機能を有すること。連携が可能であることを、研究開発項目２の実証において示すこと。

研究開発項目２　高信頼データ流通アプリケーションの研究開発

研究開発項目１の非集中型ネットワーク内ストレージフレームワークを用いて、具体的なアプリケーションを実装し、実証を行う。受託者は、ブロックチェーンおよびオフチェーンストレージを組み合わせたデータ流通が有効となるアプリケーションを一つ以上選択し、動作を実証する。アプリケーションの分野は限定しないが、医療・ヘルスケア分野、IoT・ロボット分野、物流・サプライチェーン分野、MaaS・モビリティ分野、コンテンツ・データ取引分野、エネルギー分野、ゲーム・エンターテイメント分野など、ブロックチェーンおよびオフチェーンストレージを利用する意義が明確な分野を選択す

ること。また、複数の対等な組織・ユーザーが参画し、データの所有権が明確であり、かつ、容量が大きいデータを扱うアプリケーションが適している。受託者が既に有している、あるいは、既存のアプリケーションを改造しても良い。

機構は本委託研究向けの実証用テストベッドを 2025 年度１Q より受託者へ提供する。本テストベッドは、機構が構築・提供しているテストベッド設備[6]上で稼働する。実証用テストベッドでは以下のホストが複数動作する。

- Hyperledger Fabric がインストールされ、動作するホスト
- IPFS、UCINC、Cefore がインストールされ、動作するホスト

また、Authority がインストールされ、動作するホストが１つ動作する。実証用テストベッドには上記のいずれもインストールされていないホストも複数用意する。これらのホストへは受託者のソフトウェア等をインストールして動作させることが可能である。
受託者は、研究開発項目２のアプリケーションを実証用テストベッドのホストのいずれかで動作させ、上記の通り実証用テストベッドで動作する Hyperledger Fabric、IPFS、UCINC、および Authority と接続させること。

４．アウトプット目標

研究開発項目１ 非集中型ネットワーク内ストレージフレームワークの研究開発

- 研究開発項目１のフレームワークによって、属性暗号機能およびデータ流通範囲制御機能を利用したアプリケーションを開発可能であることを示すこと。
- CP-ABE により暗号化されたオフチェーンデータの取得要求を行ってから、アプリケーションとして表示完了するまでにかかる応答時間が、実証用テストベッド上で 100ms 以内となることを示すこと。あるいは、達成できることを論理的に示すこと。通信および CP-ABE の暗号処理にかかる時間は概ね 50ms 以内と想定して良い。

研究開発項目２ 高信頼データ流通アプリケーションの研究開発

- 受託者が選択したアプリケーションの動作を確認すること。機構が提供する実証用テストベッド上で動作する Hyperledger Fabric、IPFS、UCINC、および Authority と接続した研究開発項目１のフレームワークを用いて、受託者開発のアプリケーションの動作を確認すること。
- ユーザーが持つ権限、および、その変化に応じてアプリケーション上で実行できるデータの操作（表示・更新等）も変化することをデモンストレーションにより示すこと。
- 10 以上のユーザー（または組織）が、1000 以上のデータを収容し、連携するアプリケーションの実証を行うこと。
- アプリケーションとして利便性高くわかりやすいインターフェースを実現すること。アプリケーションのユーザビリティや受容性をアンケートや定量評価により評価・報告すること。

5．アウトカム目標

2027 年　研究開発項目１のフレームワークのソフトウェアおよび受託者開発のアプリケーションの開発版リリース。受託者開発のアプリケーション以外の分野の企業間データ連携サービスへの適用性を実証。

2028 年　研究開発項目１のフレームワークのソフトウェアおよび受託者開発のアプリケーションの商用版リリース。商用サービスの実施にあたっては、非集中型ネットワーク内ストレージおよび受託者開発のアプリケーションの管理・運用を受託者にて実施する前提とする。

研究開発項目 1 の非集中型ネットワーク内ストレージフレームワークを 20 以上のデータ連携サービスに適用。

2030 年　欧米のブロックチェーン・IPFS を活用するデータ連携技術（例：Horizon Europe の TRUSTEE [7]）との接続。

6．採択件数、研究開発期間及び研究開発予算等

採択件数　　：1 件

研究開発期間：2025 年度（4 月 1 日または契約締結日）から 2026 年 9 月 30 日

研究開発予算：1 件あたり、2025 年度、総額 50 百万円（税込）、2026 年度は総額 25 百万円（税込）を上限とする。

（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

研究開発体制：単独の提案も可能であるが、産学官連携等による複数の実施主体からなる体制とすること。選択するアプリケーション分野の商用サービスを実施している、あるいは、実施する予定がある企業が受託者として参加する体制とすること。

7．提案に当たっての留意点

- 2025 年度１Q より機構が提供する実証用テストベッドの各機能要素を、いつ頃、どのように利用する想定か、提案書に明記すること。
- 研究開発期間中に、テストベッド設備[6]の更改等により動作環境が変化する可能性がある。その場合は設定変更等が必要となるため留意すること。
- 受託者は、機構が開発した NICT セキュアオフチェーンストレージを構成するソフトウェアを、研究開発期間中は無償で利用することができる。
- 実証において対象とするアプリケーション分野および受託者がこれまでに実施してきた当該アプリケーション分野での商用サービスの実施時期（または実施予定時期）を明記すること。
- スマートフォン等を用いて一般のユーザーが参加できるアプリケーションを対象とした実証を行う提案を高く評価する。
- 実証で得られるデータ等の中に、パーソナルデータ（個人情報を含む）が含まれる場合、どのように扱う計画かを示すこと。
- 本委託研究にて開発する非集中型ネットワーク内ストレージフレームワークのインター

フェースや機能について複数の受託者間で調整を行う可能性があることに留意すること。

- 本委託研究の成果となる非集中型ネットワーク内ストレージフレームワークのソフトウェアは、可能な限りオープンソース公開すること。オープンソースとして公開する際のソフトウェアライセンスは改変したプログラムソースの開示義務がない MIT 等のライセンスとする。
- NICT セキュアオフチェーンストレージのソフトウェアの改良・拡張を受託者にて行った場合は、変更箇所のプログラムソースは可能な限り機構へ提供するものとする。
- 具体的目標に関しては、定量的に提案書に記載すること。
- 研究開発成果の情報発信を積極的に行うこと。
- 2026 年度については、機構の次期中長期目標の状況※によっては、実施スケジュールや実施内容等の変更、調整が必要となる場合があることをあらかじめご了承ください。
  ※次期中長期目標において、目標に含まれない研究開発課題については委託研究を終了することもあります。

８．運営管理

- 機構と受託者の連携を図るため、代表提案者は、プロジェクトオフィサーの指示に基づき定期的に連絡調整会議を開催すること。
- 複数の機関が共同で受託する場合には、代表提案者が受託者間の連携等の運営管理を行い、受託者間調整会議を定期的に開催すること。
- 社会情勢や研究環境の変化等、必要に応じて、プロジェクトオフィサーが研究計画書を変更する場合があるので、留意すること。

９．評価

- 機構は、2026 年度に終了評価を実施する。また、機構は、本委託研究終了後に成果展開等状況調査を行い、追跡評価を行う場合がある。
- 機構は、上記以外にも本委託研究の進捗状況等を踏まえて、臨時にヒアリングを実施することがある。

１０．成果の社会実装等に向けた取組

- 非集中型ネットワーク内ストレージおよび研究開発項目２のアプリケーションの商用サービス化に向けた計画を明確にすること（委託研究終了後のシステム・運用体制の構築を含めた事業化等の内容を明確に示すこと）。
- 本委託研究で得られた成果のオープン化（例えば、成果発表やそれに留まらずコミュニティ先導のための国際ワークショップや国内特別セッション主催、展示、標準化等）を行う等、成果の社会展開に向けて必要な取組を行うこと。
- 産学官連携体制の構築、研究開発の成果を参加企業等が実用化・事業化につなげる仕組みをビルトインすること。

１１．プロジェクトオフィサー

ネットワーク研究所　ネットワークアーキテクチャ研究室　寺西　裕一

参考

[1] Hiroaki Yamanaka, Yuuichi Teranishi, Yusaku Hayamizu, Atsushi Ooka, Kazuhisa Matsuzono, Ruidong Li, and Hitoshi Asaeda, “User-centric In-network Caching Mechanism for Off-chain Storage with Blockchain,” IEEE International Conference on Communications (ICC), pp. 1076-1081, 2022.

[2] Dennis Trautwein, Aravindh Raman, Gareth Tyson, Ignacio Castro, Will Scott, Moritz Schubotz, Bela Gipp, and Yiannis Psaras, “Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web,” ACM SIGCOMM 2022 Conference, pp. 739-752, 2022.

[3] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” Proceedings of the thirteenth EuroSys conference, pp. 1-15, 2018.

[4] Kubo, https://github.com/ipfs/kubo/

[5] Cefore, https://cefore.net/

[6] 高信頼・高可塑 B5G/IoT テストベッド, https://testbed.nict.go.jp/

[7] Sarwar Sayeed, Nikolaos Pitropakis, William Buchanan, Evangelos Markakis, Dimitra Papatsaroucha, and Ilias Politis, “TRUSTEE: Towards the Creation of Secure, Trustworthy and Privacy-preserving Framework,” ACM International Conference on Availability, Reliability and Security (ARES) 2023, pp. 1-10, 2023.