

令和 6 年 6 月 13 日現在

機関番号：11301

研究種目：基盤研究(C)（一般）

研究期間：2021～2023

課題番号：21K11862

研究課題名（和文）安全で実用的な個人データ活用のためのスマートコントラクト技術の開発

研究課題名（英文）Development of smart contract technology for secure and practical personal data utilization

研究代表者

酒井 正夫（SAKAI, Masao）

東北大学・データ駆動科学・AI教育研究センター・准教授

研究者番号：30344740

交付決定額（研究期間全体）：（直接経費） 1,500,000円

研究成果の概要（和文）：本研究では、安全で実用的なスマートコントラクトを実現するための主要要素である「スマートコントラクト連携・支援機能を有する非中央集権型P2Pストレージ」を実現するための技術群を開発した。これら研究成果は現在特許出願を検討・準備中であり、その完了を待って学術発表を行う予定である。また、本研究では、不特定多数のスマートフォン等が発信するBLE（Bluetooth Low Energy）ビーコンを観測することで地域の人流を推計する「IoTセンサ」装置を開発した。また、地域の産学官の機関と連携し、その性能を評価する実証実験を行い、開発装置が有効に動作することを確認した。

研究成果の学術的意義や社会的意義

本研究で開発した「スマートコントラクト連携・支援機能を有する非中央集権型P2Pストレージ」関連の技術群は、スマートコントラクトの普及と個人データの積極的な活用を実現する上での幾つかの未解決問題を克服するものであり、社会的意義が大きい。また、本研究で開発したIoTセンサ装置群は、地域の人流・移動を、低プライバシー侵害リスク・低コスト・高精度で推計できるものである。地域の産学官関係者と共同で実施した実証実験により、その有効性と性能が確認され、実際に行政・商店街によるイベント等の効果検証指標としても採用されており、社会的に貢献している。

研究成果の概要（英文）：In this research, I developed technologies to realize “decentralized P2P storage with smart contract coordination and support functions,” which is a key element to realize secure and practical smart contracts. The results of this research are currently under consideration and preparation for patent application, and will be published in academic publications pending the completion of the patent application. I also developed “IoT sensor” devices that estimates the human flow rate in an area by observing BLE (Bluetooth Low Energy) beacons sent by many unspecified smartphones and other devices in the area. In collaboration with local industry, academia, and government organizations, I conducted a demonstration experiment to evaluate the performance of the device and confirmed that the developed device works effectively.

研究分野：Information Security and Data Use

キーワード：プライバシー保護 データ活用 人流 新型コロナウイルス接触確認アプリCOCOA ブロックチェーン
Peer to Peer スマートコントラクト

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

1. 研究開始当初の背景

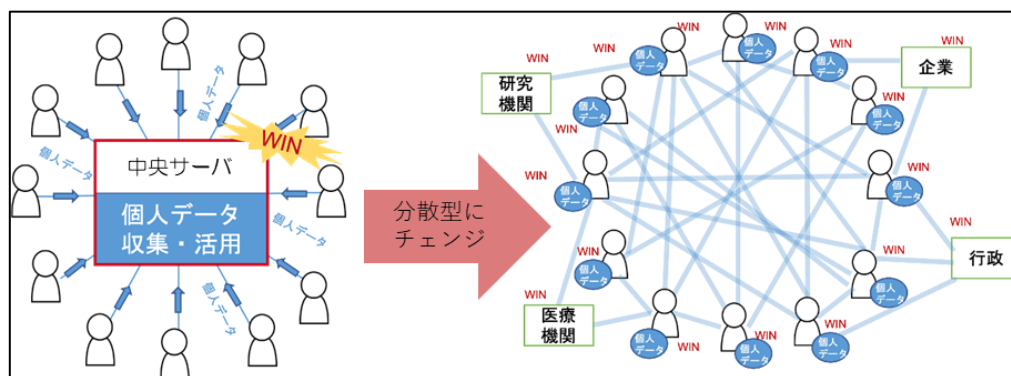
データ科学・AI 技術の発展に伴いデータの重要性が高まっている。個人に紐づく個人データはその活用範囲の広さから特に重要であるが、現状、個人データのビッグデータは GAFKA 等の外資系企業が独占的に保有・活用しており、社会全体で誰もが容易に活用できる状況ではない。日本でもこの状況を改善するために、本人から承諾を受けて個人データの活用を促進するための法改正や関連プロジェクトの支援に取り組んでいる。「情報銀行」はそのような取り組みの一つであり、不特定多数の個人から信託を受けて個人データを預かりビッグデータとして社会全体で活用できるようにすることを目指している。しかし、情報銀行はサービス事業者側で個人データを集約して管理する中央集権型であるため、事業者側での大規模情報漏洩リスクがあり、また、個人データを預けることに対するユーザの心理的抵抗感も解消されておらず、そのことが普及の妨げになっている。そのため、預かる個人データの種類、提供先、利用形態が制限されており、情報銀行の普及と発展の妨げになっている。

2. 研究の目的

スマートコントラクトとはブロックチェーンによる非中央集権型の自動契約技術のことであり、暗号資産取引のような一方向の送金だけではなく、送金とその対価提供がセットになった双方向の契約処理にも対応できる。スマートコントラクトにおける対価を「自身の個人データの活用許可」とすることで、前述の中央集権型に起因する問題を根本的に解消可能であり、データ提供者は自身の個人データをサービス事業者に預けることなく、権利の購入者のみに必要最低限の範囲でオンデマンドで活用させることができる。

ただし、個人データ活用のためのスマートコントラクトには、販売者が不特定多数であることに起因する実用面での課題がある。それは契約成立時に販売者がオフラインの場合、代金が販売者に即時に送金される一方で、販売者から対価が提供されず取引が完了しない点と、データ提供者によるデータ偽造・改ざんなどの不正に対して根本的かつ効果的な対策が実施困難な点である。

本研究の目的は、これらの課題の解決するスマートコントラクト技術を開発することである。また、本研究では、開発技術の社会実装も目的とするため、プライバシー侵害リスクの低い個人データ収集技術の開発とその活用にも積極的に取り組む。



3. 研究の方法

本研究では、安全で実用的なスマートコントラクトを実現するための主要要素として「スマートコントラクト連携・支援機能を有する非中央集権型 P2P ストレージ」の存在を仮定している。研究代表者らは、これまでに独自の非中央集権型 P2P ストレージ技術を開発済みであり、本研究ではそれを基幹として、追加で必要な新しい連携・支援のための技術・機能の開発を行い、さらに、それら開発技術の有効性を理論的に検証した。

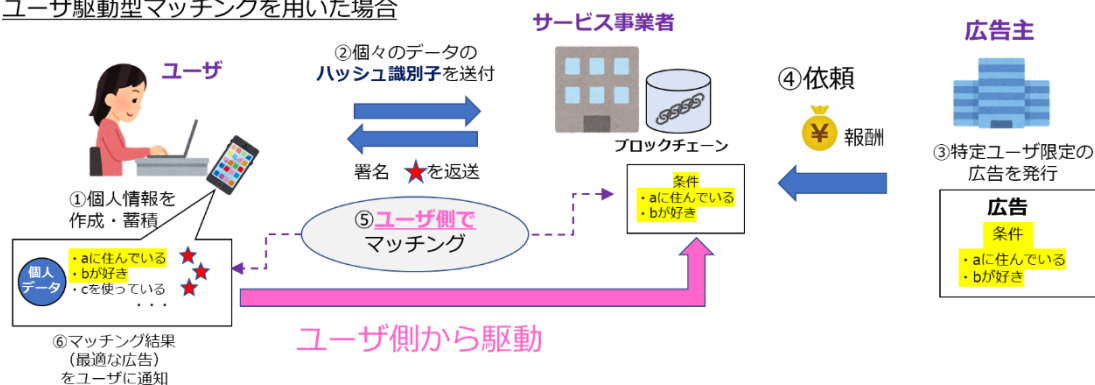
また、本研究で開発する技術を実装する P2P ノード、また、個人データ収集支援の役割を担う IoT センサ装置の開発も行った。本研究期間中は、コロナ禍であったこともあり、多くの市民が当時自身のスマートフォンに新型コロナウイルス接触確認アプリ (COCOA) をインストールしており、その COCOA が継続的に匿名性を考慮した BLE (Bluetooth Low Energy) ビーコンを発信していた。そこで、本研究では不特定多数のユーザが所有するスマートフォンが周囲に発信する COCOA の BLE ビーコンを、プライバシー侵害リスクが低く、また、社会全体で有効活用資する個人データとして選定し、それを収集・解析して人流情報を推計する機能の開発も行った。さら

に、本研究の実施拠点である仙台市の行政・商店街・地域団体と連携して、開発したIoTセンサー装置を地域の中心街に積極的に多数設置して、その有効性検証にも取り組んだ。

4. 研究成果

本研究では、前述の「スマートコントラクト連携・支援機能を有する非中央集権型P2Pストレージ」を実現するために必要な追加技術として「ユーザ駆動型マッチング技術」、さらに、その補助技術として「スマートコントラクトの契約成立後の不特定多数のP2Pノード群が連携・協力して対価の納品代行を可能にする技術」、「前述の納品代行等の役割を担ったP2Pノード群への報酬の支払いを可能にする技術」、「個人データ活用のスマートコントラクトにおいて、データ提供者の匿名性とプライバシーを過度に損なうことなくデータ購入者がデータに偽造・改ざんが無いことを検証できる技術」等を開発した。これら研究成果は現在特許出願を検討・準備中であり、その完了を待って学術発表を行う予定である。

ユーザ駆動型マッチングを用いた場合



また、本研究では前述の「IoTセンサ」装置を実際に開発した。本研究では、地域の行政（仙台市まちづくり政策局）・商店街（仙台市一番町商店街・仙台商工会議所）・まちづくり団体（一般社団法人「まちくる仙台」）と積極的に連携し、開発した装置を仙台市中心街の屋外に多数かつ長期間（3期に分けて通算1年程度）設置して、地域の人流や地点間の移動量を調査する実証実験も行った。その過程では、データ活用者（行政職員や地域商店主等）からのヒアリングを行い、積極的なデータ活用に資するための「解析結果をリアルタイムで視覚化する独自ダッシュボード」の作成と公開等も行った。

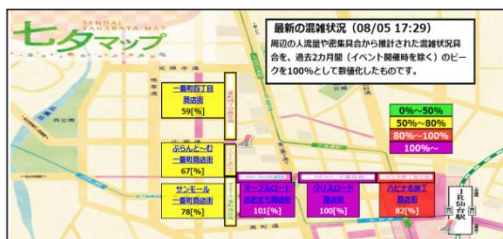
実証実験で得られた人流推計結果は、仙台市商工会議所が毎年実施する人の目視による交通量調査の結果とも比較され、当該装置が非常に高い性能を有する（両者の相関値が0.9以上となる）ことを確認した。その性能と有効性が地域関係者にも評価され、当該センサ装置が推計する人流データが「仙台七夕まつり2022」イベント中（開催：2022年8月6-8日）の混雑状況表示サイトに使用された。さらに、当該センサ装置群により観測される人流・移動量が、仙台市が運営する「SENDAI データダッシュボード（<https://data.city.sendai.jp/>）」においてほぼリアルタイムでWeb公開できるようにした。



仙台市内で段階的に実施された実証実験



第3期に使用されたIoTセンサ装置 (左：屋内用, 右：屋外用)



仙台七夕まつり2022において実際に使用された混雑状況表示サイトの画面キャプチャ

5. 主な発表論文等

〔雑誌論文〕 計0件

〔学会発表〕 計0件

〔図書〕 計0件

〔産業財産権〕

〔その他〕

本研究では、不特定多数のスマートフォン等が発信するBLE (Bluetooth Low Energy) ビーコンを観測することで地域の人流量を推計する「IoTセンサ」装置を開発した。当該IoT装置は大学発ベンチャーにより商品化されており、地域における継続的な人流解析に実際に利用されている。

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
---------------------------	-----------------------	----

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
---------	---------