卒業論文 **2018** 年度 **(**平成 **30** 年度**)**

ブロックチェーン技術とメッセージング技術を使用した **IoT** データ市場 **MIWWG** の提案と実装

指導教員

慶應義塾大学環境情報学部

中澤 仁
村井 純
楠本 博之
中村 修
Osamu Nakamura
Rodney D. Van Meter III
植原 啓介
三次 仁
高汐 一紀
武田 圭史

慶應義塾大学 総合政策学部
井上 義之

tigerman@ht.sfc.keio.ac.jp

学部論文要旨 2018 年度 (平成 30 年度)

ブロックチェーン技術とメッセージング技術を使用した IoT データ市場 MIWWG の提案と実装

論文要旨

日本語で要旨、ベタ書きで ok.

キーワード
ブロックチェーン, IoT, メッセージングシステム

慶應義塾大学総合政策学部
井上 義之

Abstract of Bachelor's Thesis Academic Year 2018

Implementing and Evaluating MIWWG : IoT data market which is made of blockchain and messaging technology.

Abstract

abstract in English.

Keywords
blockchain; IoT; messaging system

Keio University
Faculty of Policy Management
Yoshiyuki Inoue

目次

図目次

表目次

第 1 章

序論

本章では、最初に本研究における背景およびその現状の問題点を述べる。そのあと、これに対する本研究の目的とアプローチについて述べる。そして最後に、本論文の構成について示す。

1.1 背景

私たちの身の回りには様々な IoT 製品が存在している。その最たる例はスマートフォンであろう。Google Now[?] は生活の中において、必要な情報を聞く前に教えてくれる技術である。例えば、夜遅くまで外にいるとき、ユーザがスマホに聞くことなく終電の時間を教えてくれる機能がある。これはスマートフォンの GPS 機能と、現在時刻、交通機関のダイヤを参照した上で通知を与えている。他にも、ウェアラブルデバイスが注目されている。fitbit[?] は腕時計式のウェアラブルデバイスである。アプリをインストールすると、デバイスから取得した歩行数や心拍数、睡眠時間、食事、消費カロリーなどのデータを閲覧できる。他にも、車にカメラを取り付けることで道路上の白線の掠れを検知し、塗り直すべき白線の箇所を取得する研究 [?] がある。これによって、今までは別途調査が必要であった道路の白線の掠れている場所の検知が簡単になった。このように、IoT 製品· サービスは様々な利益を我々に与えてくれている。そしてこれらの IoT 製品· サービスは全て取得した IoT データから我々に有益な情報を与えてくれているのだ。この元データなしに IoT の製品· サービスは決して生まれない。そこでこの IoT データの流動性を高めるため、IoT データ市場というものが近年、考えられている。その市場では IoT データを事業者間で売買できるようになっていて、取引の際の手数料をこの市場を管理する管理者へ払うようになっている。他にも、この市場に参加する際や、参加し続ける際に管理者へ払うようになっている制度も存在する。このように一定の仲介手数料は存在するものの、IoT データをより簡単に調達できるようになる IoT データ市場は、買い手にとって利益をもたらしてくれるものである。またこの IoT データ市場は売り手にとっても、今まで自社でしか活用用途のなかったデータを販売することが可能になる点で、利益を得られる。このように、IoT データ市場は買い手と売り手の双方にとって利益を享受することのできるものであるため、これから IoT 市場全体の成長に伴って出現· 発展していくものと考えられている。

1.2 IoT データ市場に関する問題

この便利な IoT 製品· サービスを支える IoT データの元となり得る IoT データ市場であるが、ここには問題が存在する。問題とは、管理者が存在することだ。この管理者の存在が、市場全体を不健康な状態へと導

く。詳細には、管理者が好き勝手に市場全体をコントロール出来るので、この管理者に敵対する組織はこの市場に入れない或いは入ったとしても利益が出にくいような制約を受けてしまう可能性がある。また国の市場とは異なり、公正な取引がなされているかを監視するインセンティブが管理者に存在せず、公正取引が実現されない可能性がある。また公正取引が実現されなかった場合、偽データでの詐欺などがあった場合でも、それをこのプラットフォーム上で罰することが行われない可能性も存在する。このように、現在の管理者の存在する IoT データ市場には大きな問題点が存在する。

1.3 目的とアプローチ

そこで、本研究では管理者の存在しない IoT データ市場を提案、実装することを目的とする。この際、管理者のいない中での合意アルゴリズムが必要となるが、これにはブロックチェーンを使用する。また、データの買い手と売り手の間でのデータ通信が必要となるが、これにはメッセージングシステムを使用する。この二つを統合させ、IoT データ市場を作り出すことが本研究のアプローチである。

1.4 本論文の構成

本論文は本章を含めて 8 章からなる。本章では IoT が我々の生活の役に立っていることと、そのためにはデータが不可欠でその市場が誕生していること、しかしそこには管理者がいるという問題点が存在することを示した。また、それに対する目的とアプローチを述べた。2 章ではこれをさらに詳細に、技術的な観点も含めて論じる。3 章ではブロックチェーン技術について簡単に述べ、今回使用する Ethereum やオフチェーン技術について触れる。4 章では提案する IoT データ市場の機能要件およびそのプラットフォーム上での取引の流れを述べる。5 章では提案する市場に関して、設計と実装を述べる。6 章では提案する市場に関して、トランザクション流通量などの定量評価を行う。7 章では今後の展望について、ブロックチェーン技術の観点と社会的な観点から論じる。8 章では本論文のまとめを述べる。

第 2 章

背景と問題意識

この章では、本研究における背景と問題意識について詳細に述べる。

2.1 背景

最初に、本研究の背景について述べる。

2.1.1 IoT

IoT とは、物理空間の様々なモノがネットワークに繋がり、そのデータに基づいて組織の意思や他のモノの動きが決定される世界の概念を表す言葉である。特にこの一連の流れの際、人間が意図的にデータ入力をしたりデータ送信をしたりする必要がなく、これらをモノが自発的に人間にとってはシームレスに行うことを IoT という言葉で表す。そしてこの IoT は我々の生活に大きな恩恵をもたらしている。例えば既に販売されているサービスとして存在するものとして、道路事業者や交通事業者向けにその会社の自動車の GPS 情報を取得し、交通情報を提示するものがある。[1] これは、道路事業者が利用者に対する利便性の向上を、交通事業者が業務の効率化を測れるようにするものである。また、自宅の外に温度センサ取り付けることでピンポイントで温度や湿度が取得でき、その情報をスマートフォンでスマートフォンから閲覧できる製品がある。[**?**] これにより、屋外に出ることなく手元のデバイスですぐ外の気温を確認でき、例えば屋内で今日の服装を決定することができる。このように、我々は IoT によって様々な利益を得ている。

この便利な IoT であるが、これの思想に基づいてサービスやアプリケーションを作り上げるには、コストのかかる工程が大きく分けて 3 つ存在する。1 つ目は Sensing、情報を取得する必要がある。交通情報の例では、各事業者の車に GPS を設置する部分がこれに当たる。また、もしある交通事業者が直近に通っていない交通区間があったとすると、その区間の交通情報を取得することはできない。温度計センサの例では、自分の家のすぐ外に温度計を設置する部分がこれに当たる。2 つ目は Processing、情報を処理する必要がある。交通情報の例では、GPS から取得した位置情報があまり変わっていないようであればそこが渋滞している可能性があると判断することがこれに当たる。温度計の例では、特定の温度範囲を逸脱した場合、スマートフォンへ通知を送るようになっている部分がこれに当たる。3 つ目は Actuation、情報を活かして行動する必要がある。交通情報の例では、渋滞情報を地図上にマッピングしてわかりやすく提示することがこれに当たる。温度計の例では、スマートフォンや PC 上に温度を表示することがこれに当たる。なお、ここで挙げた二つの例ではどちらもディスプレイに表示することが Actuation に当たるが、他にも「工場内で温度上昇を検知した場合、工場

内の生産機器の稼働率を下げる」ということを自動で行うこともこの Actuation に当たる。以上の流れは一般に SPA(Sensing、Processing、Actuation の略) と称され、これらを経て IoT の様々な製品やサービスは構築される。

2.1.2 IoT データ市場

ところで、現状はこれらを全て一つの主体が行う必要がある。これら全てで IoT サービスが出来上がるので、当然と言えば当然だ。しかし近年、これは IoT データを売買できるプラットフォームである「IoT データ市場」と呼ばれるものが出現している。その中の一つが EverySense[3] だ。EverySense は IoT データを売買できるプラットフォームである。この IoT データ市場について、先の交通情報の例を使い、様々な観点から考えてみよう。最初に、IoT データの買い手の視点に立つ。同じ道路を走る車にいくつもの GPS センサを取り付ける必要は、企業間の垣根を取り払えば存在しない。同じ道路に同一事業者の車がいないので、その区間の交通情報を取得するためにセンサを取り付ける必要があるのだ。もし他の会社の車の GPS 情報を買い、取得することが出来れば、わざわざ GPS センサを取り付ける必要はない。更に、先ほどは自社の車が通っていない交通区間についての情報を取得することはできなかったが、情報を買うことができれば通っていない道の交通情報も分かる。次に、IoT データの売り手の視点に立つ。今までは GPS センサを取り付けることは自社の為のみであった。したがって、GPS センサの代金や取り付けの工事費は全て自社のコストとなり、そのコストは顧客の払った売り上げから賄っていた。しかし GPS センサのデータが売れることが分かれば、このコストの一部はデータの買い手が負担することになり、価格面で顧客サービス向上につながる。最後に、全体を俯瞰する観点に立つ。同じ時刻に同じ場所を走行する別事業者の車両が 1 台ずつ、計 2 台が存在していたとする。片方の会社はもう片方の会社から車両データを買えば良いので、IoT データ市場の出現によって無駄な GPS センサが 1 台減ることとなる。更に、IoT 化を進める上で不可欠なセンサが物理空間に増える可能性を秘めているのだ。データの売り手がデータ取得の費用が全て既存の顧客が払った売り上げから賄うわけではないと分かった場合、更に多くのセンサを車両に取り付ける可能性がある。この時、世の中全体で使える IoT センサ量は増加し、世の中全体の IoT 化が今までより容易に進むようになる。このように、様々なステークホルダに利益をもたらし得るのがこの IoT データ市場である。

2.1.3 ブロックチェーン技術

ブロックチェーン技術の詳細については後の 3 章にて述べるが、ここではこの技術の背景と概要について述べる。詳細な理由については後述するが、IoT データ市場は管理主体が存在しないほうが望ましい。そして管理主体のいない市場を作る際は、その市場の金の流れについて全員が合意に達する必要がある。この合意に達するためのアルゴリズムがブロックチェーン技術である。合意アルゴリズムに関する研究は、現在最も有名な Bitcoin[4] の開発以前も行われてきた。完全に管理主体の存在しない研究として挙げられる'b-money'[5] では、参加者の全員が受け取れる単一の歴史を示す元帳が必要であるとした。これは現在の Bitcoin をはじめとするブロックチェーンのアイデアの中心となるものである。さらに、計算問題によって金を創造するという現在のブロックチェーンに使われているアイデアもこの論文にて導入されたが、提案が不十分であったため実装がなされなかった。これらのアイデアを Proof Of Work という具体的な手法で具現化し実装可能となり、作られたのが Bitcoin であり、ここで使われている技術や後に更に考案された技術が総称されてブロックチェーン技術と呼ばれている。現在ではチューリング完全で様々な暗号通貨の基軸暗号通貨プラットフォーム

として使われている Ethereum[?] やギャンブルのチップとして使われる Augur[7], 半中央集権的な Ripple[8] などもこのブロックチェーン技術によって存在している。

2.2 IoT データ市場に関する問題

IoT データ市場は前述の背景を経て作られることとなったが、ここには大きな問題点が存在する。ここでは、政治的な問題点と技術的な問題点の 2 点に分けてその問題点を説明する。

2.2.1 政治的な問題

最初に政治的な問題点について説明する。政治的な問題、それは市場に単一の管理者が存在することだ。そして管理者の存在は主に以下の 2 つの問題を孕む。1 つ目は市場の管理者が市場全体に対して巨大な力を持ってしまうこと。2 つ目は公正な市場の担保が難しくなることである。1 つ目、市場の管理者が巨大な力を持つことについて考察する。市場の管理者のビジネスモデルの代表的なものの一例としては、市場参加者がデータの売買をする際、プラットフォーム提供料として販売手数料を徴収する方法である。この販売手数料が例えば 10% で設定されているとする。すると、データの売り手は「10% の販売手数料であれば例えば A 円で販売し、このデータが B セット売れると考えられるので A × B 円が売り上げになる。そのためには 円のセンサを取り付けることによって最大の利益が得られる。」という計画で販売計画を立てる。この販売計画の根底にあるものは「10% の販売手数料」という前提である。市場の管理者は他の誰の同意を得ることなしに、この 10% という値を 30% へ値上げすることが出来るのだ。勿論、この値上げについては基本契約書での取り決めや、この市場に参加するまでのやりとりによっては参加者が法的に拒否することは可能である。但し、法的に解決するには長い期間や訴訟のための費用がかかる上、今回の IoT データ市場において司法がどのような判断を下すかは不明瞭である。換言すると、管理者の存在が IoT 市場において本格的に商売をしようとする事業者にとっての SPOF(Single Point Of Failure, 単一障害点) なのである。つまり、この管理者が全ての善意の IoT 市場の参加者にとって「正しく」機能する必要があるが、このことについて確実に担保する術は存在しない。2 つ目、管理者の存在によって、公正な市場の担保が難しいという点について考察する。一般には、公正な市場を守るために、以下の流れが存在する。以下については、スライド作成時、証券取引等監視委員会事務局の特別調査課長であった目黒克幸氏のスライド [9] を参照した。

1. 立法権を持つ国会が公正な市場を実現するための法整備を行う。
2. 金融庁の証券取引等監視委員会が、法律にもとづいて実際の市場の監視· 調査を行い、問題があれば告発する。
3. 告発された内容に基づいて地方検察庁が起訴を行い、裁判所によって裁判が行われる。

もし IoT 市場においてもこの流れを踏襲する場合、この流れにおける全てのステップを、今回の IoT 市場は市場の管理者が担当することとなる。我が国では立法権、行政権、司法権と独立した 3 権の行う権利行使を一つの市場管理者が行使するのだ。これで公正な取引が担保される可能性は大きく減る。例えば市場の管理者にとって、ビジネス的に敵対する事業者が市場に参入しようとしたとする。あるいは、市場において有力な参加者がある事業者を排除しようと、市場の管理者に何らかの方法で参入しないように圧力を加えたとする。これに応じた管理者は、新規参入しようとした特定の企業を排除するような制約を参加する企業に課すことが出来る。もしこのようなことを立法が行おうとし、それが憲法に違反しているようであれば司法がこれを許すこと

はない。しかし、三権が一つの管理者に集中しているこの IoT 市場は、この参加制約を簡単に作り出せてしまう。さらにもう一つの例を考えてみる。偽データと思われるデータを販売していたある事業者がいたとしよう。そのデータを買っていた被害者と思われる事業者が市場の有力者であれば、管理者は参加者の風評などを恐れて調査· 処罰に乗り出すかもしれない。ただ、偽データ販売の規模が小規模で被害者が小さな力の持たない事業者であった場合、管理者がこれを調査· 処罰するインセンティブは存在しない。むしろ、調査はコストがかかるので、調査にはマイナスのインセンティブが存在する。証券取引等監視委員会であれば、小規模であっても風評等に関わらず、調査する。ここにも証券取引等監視委員会が調査するインセンティブは存在しないが、法律によって調査することが義務付けられているので調査を行う。それに対し IoT データ市場が偽データ販売について調査を行うことはあくまでサービスであり、法律によって義務付けられているものではない。つまり、現状の IoT データ市場では公正なデータの流通について必ず調査や監視が行われ、処罰される仕組みを作ることは不可能であるのだ。以上、管理者の存在による IoT データ市場の政治的な問題点を大きく分けて二つの観点から述べた。

2.2.2 技術的な問題

可用性とセキュリティの観点から、管理者の存在する IoT 市場の問題点について述べる。最初に、可溶性の観点から述べる。IoT 市場は一瞬であろうと市場取引やデータ送信が止まる事は望ましくない。だが、特定の一つの管理者のプラットフォーム上で動く以上、稼働率 100% を担保することは難しい。例えば、クラウドサービスとして有名な AWS(Amazon Web Service) の EC2 などの稼働率に関する SLA(Service Level Agreement) は最高で 99.99% である。この 99.99% を割り込んだ場合、サービスクレジット率の 10% がこれから AWS の製品を使う上で使える金となる。仮に稼働率をこの SLA の 99.99% とした時、1 年間で AWS が稼働していない時間は 52.56 分である。オンプレミス環境と比べて可用性に比較的信頼が置かれているクラウドでさえ、1 年単位で考えると 1 時間弱程度のダウンタイムは仕方がないと AWS は考えている。この 1 時間弱の間にどれほどの裁かれるべきデータ送信が滞るのか。IoT データは逐次飛んでくるものであるので、この時間の間に大量のデータ送信が滞ってしまうことは想像に難くない。また今回はクラウドを想定したが、管理者がクラウドサービスを使い可用性を 100% に限りなく近づけるような努力がなされているかどうかは市場の参加者からはチェックすることができない。このように逐次的に大量のデータが流れ、それが止まってしまうと大きな問題の起こる IoT データ市場においては、単一の管理主体がその市場全体を管理することは望ましくない。次に、セキュリティの観点から述べる。当然、管理者であっても買っていないデータを勝手に閲覧することは許されない契約を市場の参加者と管理者間で結ぶだろう。ただ、それであっても管理者が売買データを見ることが可能である。また、どの企業がどのようなデータを買っているかについても、管理者は全て見ることができる。これは管理者が悪意を持っていない前提ならば問題のない話であるが、悪意を持っていた場合は参加している事業者の IoT 戦略が全て管理者に筒抜けであることを意味する。またセキュリティの脆弱性を突かれた場合、取引データが管理者のデータベースから抜かれた時には事業者間のプライバシーである取引履歴が、IoT データが抜けれた時には販売価値のある IoT データがそれぞれ不特定多数の人間によって見られる可能性を含んでいる。このように、単一の管理者が多くの流出を避けるデータを持つことはなるべくあってはならない。以上 2 点について、単一管理者の存在する IoT 市場の問題点について技術的観点から述べた。

2.2.3　まとめ

本章では IoT が我々の生活の役に立っていることと、そのためにはデータが不可欠でその市場が誕生していることを述べた。しかしそこには管理者がいるという政治的な、技術的な問題点が存在することを示した。そしてこの状況を改善するために、ブロックチェーン技術というものがあることを示した。

参考文献

[1] 株式会社日立製作所, 交通データ利活用サービス, http://www.hitachi.co.jp/products/it/lumada/solution/lumada_s_010044.html (参照 2018-12-13)

[2] 株式会社セラク, Thermo-Cloud, http://www.seraku.co.jp/iot-ps/thermo.php (参照 2018-12-13)

[3] EverySense,Inc., EverySense, https://every-sense.com/ (参照 2018-12-13)

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", http://wfc-knowledgecentre.com/wp-content/uploads/2016/07/Bitcoin-A-Peer-to-Peer-electronic-Cash-System.pdf(参照 2018-12-15)

[5] W. Dai, "b-money", http://www.weidai.com/bmoney.txt, (参照 2018-12-15)

[6] Vitalik Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM", https://whitepaperdatabase.com/wp-content/uploads/2017/09/Ethereum-ETH-whitepaper.pdf, (参照 2018-12-15)

[7] Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander, "Augur: a Decentralized Oracle and Prediction Market Platform", https://www.augur.net/whitepaper.pdf, (参照 2018-12-15)

[8] David Schwartz, Noah Youngs, Arthur Britto, "The Ripple Protocol Consensus Algorithm", https://ripple.com/files/ripple_consensus_whitepaper.pdf, (参照 2018-12-15)

[9] 目黒 克幸, 証券市場と市場監視の役割 証券市場と市場監視の役割－真の規律が効いた市場の実現を目指して－, https://www.fsa.go.jp/sesc/kouen/kouenkai/20101117-1.pdf (参照 2018-12-14)