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[6] 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。

第 3 章

ブロックチェーン技術

本章では、本研究で用いるブロックチェーン技術について述べる。最初に仕組みや説明を述べ、その技術が持つ問題点や現状の政治的な問題点について述べる。その後、ブロックチェーン技術を最大限に活用するための技術であるオフチェーン技術について述べる。そして、ブロックチェーン技術を用いた暗号通貨の代表的なものについて説明を行う。最後に、本章のまとめを行う。

3.1　仕組み

本節では、ブロックチェーンの仕組みについて述べる。また詳しくは後の**??**項にて後述するが、ブロックチェーンにはいくつかの種類が存在する。ここでは特に指定のない限り、中央集権的な機関の存在しない、パブリック型ブロックチェーンについての説明を行う。

3.1.1　P2P 通信

ブロックチェーンは P2P 通信によって行われる。この P2P 通信とは、対等の端末間で行われる通信のことである。通常のネットワークサービスは、クライアント・サーバ型と呼ばれる通信機能によって運営されている。サーバ側ではサービス運営者がサービスや機能を提供するアクセス可能なコンピュータであるサーバを設置し、このサーバ上でサービスが運営される。例えば慶應義塾大学湘南藤沢キャンパスにて使われている学事システムの SFC-SFS では、履修可能単位の閲覧機能、履修単位申告機能、履修者が過剰になった時の選抜機能などを提供している。この機能を運営しているコンピュータを一般に、サーバと呼ぶ。これに対し、利用者はクライアント側となる。クライアントとは、サーバに対してそれが持つ機能を使わせてもらうためのリクエストを送るコンピュータのことである、SFC-SFS の例では、学生がサービスにアクセスするために使うスマートフォンや PC などがこれに当たる。つまり、サービスの提供者側であるサーバと消費者側であるクライアントで役割が分かれていることが特徴だ。このような形で通常のネットワークサービスは運営されるが、P2P サービスはこれと異なる。P2P サービスでは、通信する端末間の関係が対等である。つまり通信する双方が同じ機能を持ち、相手へサービスを提供する一方で、相手からサービスを受けているという状況が発生しているのだ。P2P サービスの例として、インターネット回線を使った通話アプリが存在する。P2P の通話サービスの場合、A の端末と B の端末で通話を行なっている時、この通話アプリを提供している会社は二人の会話中の通信について関与していない。双方ともが自分の音声を相手へ提供する機能と相手の音声を受け取る機能を持つ、つまりクライアント・サーバ型の両方の機能を双方が持っているのだ。以上が P2P 通信の特

徴である。ブロックチェーン技術は中央集権を持たない環境での分散台帳技術であるが、これには P2P 通信が使われている。したがって、全ての参加者がサービスの使用者としての役割のみならず、サービスの提供者としての役割も持っているのだ。

3.1.2 デジタル署名とアドレス

デジタル署名とは、あるメッセージが署名した人によって作られたかを検証する仕組みである。ここでは「A が自分の 3BTC(Bitcoin) を使いたい」と主張する時に、それが本当に A の発言であるかを担保するのがこのデジタル署名の役割である。代表的なブロックチェーンである Bitcoin や Ethereum では ECDSA(楕円曲線 DSA, Elliptic Curve Digital Signature Algorithm) を利用しており、これについて説明を述べる。(!!! 後に参照する図を挿入のこと！)

$$y^2 = x^3 + ax + b \tag{3.1}$$

以上が楕円曲線について一般的に表される式である。この中でも Bitcoin や Ethereum が用いる規格である secp256k1 曲線は a=0, b=7 であるため、以上の方程式は

$$y^2 = x^3 + 7 \tag{3.2}$$

上記のように表される。また楕円曲線の加算の定義として、点 A と点 B を加算することを考える。この時、加算後の座標は点 A と点 B とを通る直線のもう一つの交点の x 軸に関して対称移動させた点である。したがって点 A と点 B が同一座標の点 G であるとき、その接線と楕円曲線との交点を x 軸に関して対称移動させた点は G + G = 2G となる。secp256k1 は G のベースポイントを定めており、そこから秘密鍵 r を掛け合わせた rG が公開鍵となる。この時、楕円曲線上の離散対数問題によって秘密鍵から公開鍵を導出することは容易であるが、逆の公開鍵から秘密鍵を導出することは難しいことが知られている。この秘密鍵を使い、「自分の Bitcoin を使いたい」と主張することによって、利用者は自分の Bitcoin を使用する事が可能となる。この主張を行う際の署名値は以下の式によって導かれる。

$$S = \frac{h + kR}{q}(modp) \tag{3.3}$$

q：一回のみ使われる乱数 ($1 \leq q \leq 2^256 - 2^32 - 977$)
h：取引情報のハッシュ値
k：送信者の秘密鍵
R:一時的な公開鍵の x 座標
p:楕円曲線の x 座標がこれより大きくならないための値で素数

そしてこれらの値のうち、S と R が署名となり、ブロックチェーン上で周知される。この主張が本人のみ知り得る秘密鍵を使って行われたものかを確認する際は、以下の式を使って検証する。

$$Q = \frac{hG}{S} + \frac{RK}{S}(modp) \tag{3.4}$$

S, Q, R：送信者から受け取った署名
h：取引情報のハッシュ値
G：secp256k1 のベースポイント
K：送信者の公開鍵

p:楕円曲線の x 座標がこれより大きくならないための値で素数

以上の式において、Q の x 座標が送信者が送信した R の座標と一致する時、この署名は正しいものであると検証される。また、この公開鍵を Bitcoin では HASH160 · Ethereum では Keccak256 ベースのハッシュ関数によってそれぞれハッシュ化し、Ethereum ではそのハッシュ値の末尾 20 バイトを抜き出したものがアドレスとして使われる。そして「そのアドレスに対して、3BTC を送金する」と主張できるようになり、このアドレスの管理者 (つまり元の公開鍵や秘密鍵を持っている者) がその後、「ここで受け取った 3BTC を使う」と主張できるようになるのだ。(!!!後に参照する図を挿入のこと！)

3.1.3 トランザクション

ここでは、Bitcoin を例にとトランザクションについて説明を行う。ブロックチェーン上の記録は、全てトランザクションという単位毎に格納される。つまり、「A が B に 3BTC を渡した」という記録が一つのトランザクションに格納されるということだ。このトランザクションはインプット部分とアウトプット部分、そしてその他の部分が存在する。インプットには、当該トランザクションのトークンの出所が存在している。例えば、「A が 3BTC を使う」と申し出たとしよう。この時、ネットワーク全体が「A は 3 BTC 以上持っている」ということが分からないと、A が 3BTC 使うという行為は認められない。ここで「3BTC 以上持っている」ということは、換言すると「3BTC 以上を誰かから送金された過去があり、その BTC は未だに使用されていない」ということである。この「未だに使用されていなく、その所有者が未だ使える状態」のトランザクションのことを Bitcoin では UTXO(Unspent Transaction Output) と呼ぶ。この UTXO を使おうとする時は、トランザクションのインプットに UTXO の存在する場所を明示することで、UTXO を使う事ができる。つまり、インプットはトランザクションの送金における払い手に当たる情報が入る部分と言える。次に、アウトプットについて説明する。アウトプットはトランザクションの送金における受け取り手に当たる情報が入る部分である。前項で述べたように、受け取り手の情報はアドレスによって表される。したがって、「A が B に 3BTC を渡した」あとで未だに B がこれを使っていない状態の時、このトランザクションのアウトプットの署名欄には Bitcoin アドレスが存在している。その後、「B が C に 3BTC を渡した」とすると、先ほど Bitcoin アドレスが書かれていた署名欄には Bitcoin アドレスの素となった公開鍵とこの公開鍵に対応する署名値が代入される。つまり、あるアウトプットが UTXO であるか否かの判断はこの署名欄に Bitcoin アドレスがあるか公開鍵と署名値が存在するかの違いによって行われる。このようにしてトランザクションは管理される。

3.1.4 ブロックとマイニング

ここではブロックとマイニングについて説明を行う。ブロックチェーン技術は情報の記録を単一の歴史を共有することによって、参加者の合意できる台帳管理を行おうとする技術である。この単一の歴史を刻む歴史書の 1 ページが 1 ブロックに当たる。現在の Bitcoin では 10 分に 1 回、Ethereum では 15 秒に 1 回、それぞれのペースで新しいブロックが生成される。このブロックにはトランザクションが 0 個以上含まれており、その処理内容が単一の歴史として刻まれる。そしてブロックチェーン技術はこの方式によって、二重支払い問題を解決している。A が 3BTC を持っている時、同時に「A が B に 3BTC を払う」と「A が C に 3BTC 払う」というトランザクションを発行しようとしたとする。しかし、ブロックが生成される際にのみ送金の処理は行われるため、ネットワークの遅延等の影響によって二つのトランザクションが承認されることはあり得ない。また、各々のブロックはヘッダに前のブロック情報をまとめたハッシュ値を持っており、どのブロッ

クの次に繋げられたブロックであるかを明示している。このブロックがチェーンのように何個も連なることによって、ブロックチェーンという分散管理台帳が形成されていく。そしてこのブロックが生成される際に行われることが、マイニングと呼ばれる行為である。そしてブロックの生成を行おうとする者をマイナーと呼ぶ。ブロック情報をまとめたハッシュ値の中には、ナンスと呼ばれるブロックのマイナーが付加する 32bit の数値が存在する。このナンスを含めたハッシュ値が、一定の数だけ頭に 0 を持つようにすることによって、そのブロックは正当なブロックであると承認されるようになっている。例えば、Bitcoin のメインネットワークにおいて 553582 番目に生成されたブロックの情報について見てみる。以下は Bitcoin の現在の統計情報などを提供している https://www.blockchain.com/ja/ から取得した情報である。すると、ハッシュ値は「0000000000000000001b0218ca2b54e9809b5d948864c5bd1e657e5aa09f438f」となっている。そしてこの時のナンスの値は「4142738813」となっている。ブロックの持つトランザクションのハッシュ値などの情報に、このナンス値を足したところ、このように頭にいくつもの 0 がつくハッシュ値を見つけ出せたのである。この時この様々なナンスの値を取り付け、0 が頭に一定数以上つくハッシュ値を見つけ出す行為について、マイニングと呼ぶ。そしてこのマイニングという行為によって、ブロックチェーンにおける改竄可能性を防いでいるのだ。現在 (2018-12-13 00:46:30)、マイニングは 16 進数において頭の 18 文字に 0 が続く場合、ブロックが生成されるようになっている。つまり、最新より一つ前のブロックのハッシュ値をブロックに含めて $16^{1}8$ 回の演算を行うことで最新のブロックを無効にでき、自分の思い通りのブロックを提出する事ができる。しかし、2 つ前のブロックを変更しようとするときはどうだろう。Bitcoin の各参加者は、ブロックがもっとも長く連なったブロックチェーンを信用するように設計されている。つまり 2 つ前を変更するには、新しく 2 つ分のブロックを生成しなくてはならないのだ。この時に必要な計算量は $16^{(}18 \times 2)$ となり、難易度は格段に上昇する。これがさらに 3 つ前、4 つ前.. となっていくと、事実上変更は不可能となる。よって 3BTC を払い、その対価としてのサービスを受けたのちにその支払った BTC を取り返すために新しいブロックを作り直す行為は、ブロックが一定数以上深くなった場合においては不可能である。つまり理論的にブロックの改竄は可能であるが、それは実際にはそれを行うことは極めて難しいということである。これがブロックチェーンの参加者が公開台帳を信用する理由であり、改竄耐性を持つという理由である。そしてマイナーがこのマイニングを行う動機はマイニングを成功した時に成功報酬がもらえることである。この成功報酬はブロック高によって決められており、最初は 50BTC で始まり、2018 年 12 月現在では 12.5BTC である。このようにしてブロックは生成され、ブロックチェーンは管理される。

3.2 問題点

ここでは、前半の 2 項でブロックチェーン技術に関する固有の問題点を述べる。その後、後半の 2 項で現在のブロックチェーン事情に関する問題点を述べる。

3.2.1 スケーラビリティ

ここではブロックチェーンで管理することによる、トランザクション処理数に関するスケーラビリティの少なさについて述べる。Bitcoin では 1 ブロックに含める事が可能なデータ量は 1MB となっている。このデータ量の中にトランザクションに関するデータを含めなくてはならないため、1 ブロックで処理できるトランザクションの数は限られている。そしてブロックの生成ペースは平均で 10 分に 1 回になるように調整されるため、処理できるトランザクションの数は時間当たりで一定であると言える。つまり Bitcoin を 100 人が使おう

が、100 万人が使おうが、同じだけの処理能力しか存在しないのである。例えば Web サービスであれば、受け付けるリクエストに対する処理能力を上げる方法はたくさんある。Web サーバの台数を増やし、ロードバランサで負荷を振り分ける。DB を分散処理させ、データモデリングを見直してよりレスポンスの速い DB にする。JavaScript を後から読むようにし、思い画像は最初のトップページ範囲を表示してから順に Ajax で取得する。など、様々な方策を打てる。しかし、ブロックチェーンは時間をかけてマイニングを行い、複数のチェーンが同時並行で存在していくことを防いでいる。もし 3 秒に 1 回のペースでブロックが生成される場合、同じ長さのチェーンが大量にできてしまい、どれが本当の台帳とみなして良いかわからなくなる。また、ブロックには一定のサイズしか入らないことで最新のブロックが変更された時の巻き戻されるトランザクションの数を減らしている。もし大量のトランザクションを 1 つのブロックに入れた場合、それはブロックを広報する際の遅延が生じる。この時、最新のブロックからマイニングを行いたいマイナーは、ブロックの遅延によって不利を受ける。これが続いた場合、マイナーが少なくなり、マイナーの一極集中を招く恐れがある。このことによる弊害については 3.2.4 にて後述する。つまり、仕組みそのものに固有のスケーラブルになり得ない要素が含まれているのだ。勿論、マイニングには参加者が多い方がマシンパワーが大きいので、変更されにくいブロックを生成する事が可能である。しかしながら、それは改竄耐性が上がるのみであり、トランザクションの処理能力は上がらない。どれだけ沢山の参加者が増えたとしても、それはセキュリティ性を高めるために使われてスループットを犠牲にしている、ここにブロックチェーンの大きな問題点の一つが存在する。

3.2.2　手数料とマイクロペイメント

全世界では大量のトランザクションが生成されている。従って、生成された全てのトランザクションが直ぐに最新のブロックに入るとは限らない。この時、早くマイナーにブロックへ入れて貰うため、トランザクションの送信元は手数料を設定することができる。この手数料はマイナーが得る成功報酬にプラスして、マイナーへと渡る。よって、より多くの手数料を指定した方が早くトランザクションが処理される可能性が高まるのだ。またブロックサイズの上限が決まっているため、トランザクションの大きさが大きい程、多くの手数料がマイナーへのインセンティブに必要となる。1MB の内 500KB を使うトランザクションを処理して 0.01BTC の手数料のトランザクションと、1MB の内 50KB を使うトランザクションを処理して 0.01BTC の手数料のトランザクションとでは残りのブロックに入れられるトランザクションの大きさが変わってくるためである。残りでより大きなトランザクションを捌ける方が、より多くの手数料を獲得できるためである。しかしこの仕組みは、小さな買い物に使うためには適していない。手数料はトランザクションベースで決まるため、少額の支払いであれば手数料が少なくて済むという性質のものではないためである。つまり、Bitcoin で 10 円にあたる飴を買う際も 1000 万円にあたる高級車を買う際も、同じ速度で処理してもらうには同じ手数料が必要なのだ。よってここまで記したのブロックチェーン技術では、マイクロペイメント (少額取引) には適さないという問題点がある。

3.2.3　マイナーの一極集中

ブロックはブロックチェーンにおける歴史書の 1 ページであり、マイナーはそのブロックを承認する役割を持っている。即ち、マイナーは取引の歴史の承認者、ブロックチェーンの管理者と換言できる。そしてそもそも、ブロックチェーンは完全に分散された記録システムであった。中央集権な機関が存在しないので、その完全に透明性が保たれたプラットフォームを信用する人が参加するものとして作られた。しかしながらこの

前提を覆すようなことが Bitcoin では起こったと、Bitcoin のコア開発者で Blockstream の共同設立者である Pieter Wuille 氏は言う。(http://nonem.hatenablog.com/entry/2017/10/14/182226) マイナーの中にはマイニングプールと呼ばれるものを作り、ブロックを生成している集団がある。彼らは自宅の PC などでマイニングをしたいものの、成功する確率が少ないので大勢でマイニングを行っている。そして例えば各人の計算能力が同じ 100 人で 12.5BTC を採掘した場合は、1 人あたり 0.125BTC ずつ分配する。このいくつかのマイニングプール間で、生成したブロックを送信する前にブロックヘッダのみを共有しているようなのだ。これにより、情報を共有するマイニングプールは他のマイナーよりも早くマイニングに取りかかることができる。これは計算能力を信用しているのではなく、共有の相手のマイニングプールを社会的に信用していることであり、これは Bitcoin の基本理念に反する。それと同時に、これらのマイニングプール間でのマイニングが有利となり、他のマイナーがマイニングに参加する際に不利となってしまう。ここで、これからマイニング参加するにはこのマイニングプールに所属する方法が一番良い方法となる可能性がある。その際マイナーは歴史の承認者であるため、一極集中するとその間でメインの Bitcoin とは別の取り決めを作ってしまい、それが Bitcoin のルールとなってしまう可能性がある。この時、本来の目的と離れて Bitcoin に中央集権的な機関が存在してしまう可能性がある。以上の理由から、マイナーの一極集中は望ましいことではなく、現在の Bitcoin を取り巻く状況の問題点の一つである。

3.2.4 現在の OSS ブロックチェーンの運営

”Decentralization in crypto is a myth. It is a system more centralized than North Korea: miners are centralized, exchanges are centralized, developers are centralized dictators” 「暗号通貨が中央集権的でないと言うのは神話である。そのシステムは北朝鮮よりも中央集権的である。マイナーは中央集権的で、交換所は中央集権的で、開発者は中央集権化された独裁者である。」以上の言葉はニューヨーク大学の Nouriel Roubini 教授が twitter で発言した言葉である。確かに、現在のブロックチェーンはパブリック型であってもその仕様の決められ方は決して民主的なものではない。Ethereum は 2019 年の 1 月にハードフォークが行われることが決まったが、これは開発者会議によって決まったものだ。それ以前でも、Ethereum は The DAO 事件の時のハードフォークから中央集権的であると批判を集めてきた。The DAO という Ethereum 上で動くトークンの資金集めに 150 億円分の Ethereum が集められた。しかし、Ethereum 上で動かす solidity と言う言語のフォールバック関数の仕様に関しての見落としがあり、3 分の 1 が攻撃者によって抜き取られてしまった。その際、Ethereum コミュニティは歴史書であるブロックチェーンの巻き戻しを行い、攻撃者が利益を得ることを阻止した。このような対策が一プロジェクトのバグに対して行われること自体が、中央集権的であることの証左である。ここにマイナーや ETH(Ethereum の通貨単位) を持っている人間の意思は反映されていない。マイナーの件に関しては前項で述べたものがそのままこのツイートの論拠となる。このように、現在の OSS ブロックチェーンはパブリック型と謳いつつ、とても中央集権的であるという側面を持っている。

3.3 オフチェーン技術

ここではオフチェーン技術について述べる。今までのブロックチェーンに関する説明はこれに対応してオンチェーンと呼ばれることがある。オンチェーンはトランザクションの制限が厳しく、全世界で使われる通過の処理が 10 分に 1 回しか行われない。Bitcoin が始まって以来、一日のトランザクションが 45 万を超えたことはない。これは、秒間 5.2 トランザクション以上が処理されたことがない計算になる。VISA を始めとし

た決済システムは遥かに多い TPS(Transaction Per Second) を実現しており、世界中の決済を目的とするには 5TPS は明らかに少ない数字である。この制約を緩やかにするため、オフチェーン技術と総称される技術が存在している。例えば 1 曲 100BTC で楽曲を配信するサービスを考えてみる。最初に、ユーザは使いたい BTC をオンチェーン上にデポジットする。10 曲分配信サービスを受けたいと予定したすると、1000BTC をデポジットする契約をトランザクションとして広報する。その後 1 曲の配信サービスを受けるとき、支払い側は 100BTC 分を払うという署名を行ったトランザクションを受け取り側へ送る。受け取り手はこのトランザクションを確認次第、1 曲の楽曲を配信する。そして支払い側がもう 1 曲楽曲が欲しい時は今度は 200BTC を払う署名を行ったトランザクションを受け取り側へ送る。というこの繰り返しを行い、もう支払い側が要らないと思った時、このオフチェーンでのやり取りを終える。この時の実際の操作としては、受け取り側が精算する旨をトランザクションとして広報することを行う。そしてもし 6 曲の配信サービスを受けた時、600BTC が受け取り側に、400BTC が支払い側に支払われる。この時、最初と最後の 2 つのトランザクションのみオンチェーンには広報したが、実際にはオフチェーンによって 6 曲分の支払いがなされている。オンチェーンのみでは 6 つのトランザクションが必要なところを 2 つのトランザクションのみで同じ機能を提供できたということである。これがオフチェーン技術の概略であり、これに対する細かな実装はブロックチェーンの種類によって違う。各々が Bitcoin と Ethereum のオフチェーン技術の一つである、ペイメントチャネル技術と μ Raiden 技術については後の 3.5.3 項と 3.6.4 項にて行う。

3.4 Bitcoin

ここではブロックチェーン技術を使って作られた最初の実装物である Bitcoin について述べる。3.1 節で説明したことと重複することが多いが、のちの Ethereum と対比するために述べる。通貨単位は BTC である。

3.4.1 トランザクションベースの一元管理

Bitcoin は全てトランザクションベースで管理される。3.1.2 項で述べたように、自分の BTC を使いたい時はその BTC をもらった過去のトランザクションを指定する。そしてそのトランザクションを指定して BTC を使った過去がないことを承認ノードが確認 (UTXO であることを確認) した上で、その BTC は使用される。ここで、仮に 10BTC を貰ったトランザクションを使って 3BTC を使いたいとする。すると支払い側は生成されるトランザクションは 3BTC を支払い相手へ渡し、残りの 7BTC は自分のアドレスへ送るように指定することで 3BTC のみを使うことが可能となる。この工夫が一般的である理由は、トランザクションベースの一元管理であることに存在する。もし 7BTC を明示しない場合、お釣りの 7BTC がそのまま送信者のアドレスに紐づけられたままできるのであればトランザクションのサイズを減らし、トランザクション送信の際の手数料を少なくできる。お釣りのアドレスを指定することは送信相手を複数指定するためにトランザクションのサイズが大きくなることを招き、このことがトランザクション送信の際の手数料増大を招くためだ。もしアカウントベースで Bitcoin が管理されていれば、この方式を行うことに一定の負のインセンティブが存在するのだ。また、トランザクションベース管理ではこのお釣りであるという情報を秘匿する工夫も考えられている。もし同じ Bitcoin アドレスへ 7BTC を送った場合はこの 7BTC がお釣りであることが明確であり、本来は公開されるべきでない支払い情報の一部が全世界にバラされてしまう心配がある。よって、これに対する一般的対策として BIP(Bitcoin Improvement Proposal)-32 で提案された、拡張鍵生成が知られている。これはチェーンコードやインデックスの数字を用い、新しく秘密鍵· 公開鍵· Bitcoin アドレスを生成する方法の一

般的方法である。これを使うことで、同じく自分が管理しているアドレスでありながらマイナーや他の参加者からはどちらがお釣りでどちらが本来の支払いに使われたのか、あるいはどちらも別々の支払いに使われたのかが分からなくなる。このようにして、支払い情報についてなるべく公開されないような工夫が一般的に行われている。また、Bitcoin が徹頭徹尾トランザクションベースで管理されていることがこれらの振る舞いや工夫から分かる。

3.4.2 script 言語とチューリング不完全

Bitcoin の署名に関して、具体的な方法について今まで言及してこなかったが、これが script 言語と呼ばれるもので行われているという具体的プロセスをここで記す。UTXO の使用時、script 言語と呼ばれる言語によって記述されたプログラムが正を返す時、その UTXO は使用可能となる。Bitcoin の使用例としてもっとも代表的である、Bitcoin をあるアドレスからあるアドレスへ移動させる場合を考える。その際のプログラムは以下のようになる。

ソースコード 3.1: script 言語

```
<sig> <pubK> DUP HASH160 <pubKHash> EQUALVERIFY CHECKSIG
```

<sig>：秘密鍵でトランザクションに署名したもの
<pubK>：公開鍵情報
DUP：一つ前の内容をコピーする命令
HASH160：公開鍵からアドレスを BASE58 でデコードしたものを導く関数
<pubKHash>：アドレスを BASE58 でデコードしたもの
EQUALVERIFY：スタックに積まれている一つ前ともう一つ前が同じであることを確認する命令。異なればその時点でプログラム全体の返り値が False となる。
CHECKSIG：二つ前の署名値が一つ前の公開鍵情報に対して正しいか否かを判断する。

この script 言語は逆ローランド記法であり、順に命令がスタックに積まれて実行されていく。なお、この時トランザクションのアウトプットに記述される、トランザクションをロックするためのプログラムが以下である。

ソースコード 3.2: ロックを行う script 言語

```
DUP <HASH160> <pubKHash> EQUALVERIFY CHECKSIG
```

そしてインプットに記述されるトランザクションをアンロックするためのプログラムが以下である。

ソースコード 3.3: アンロックを行う script 言語

```
<sig> <pubK>
```

つまり、「アンロックのためのプログラム」と「ロックのためのスクリプト」をこの順番で続けて実行することでトランザクションへの署名が正しいかの判断は行われる。以下にその時の様子を示す。

1. <sig>がスタックに積まれる
2. <pubK>がスタックに積まれる

3. DUP によって<pubK>が複製される
4. HASH160 によって 3 番目で複製された公開鍵情報がアドレスのデコードされた状態の値になり、スタックに積まれる
5. <pubKHash>がスタックに積まれる
6. EQUALVERIFY によって 4 番目でハッシュ化されてスタックに積まれたものと 5 番目でスタックに積まれたものとを比較する。同じであった場合は実行中のプログラムが続行され、異なっていた場合は実行中のプログラムは中止する。
7. CHECKSIG によって、1 番目でスタックに積まれた署名値と 2 番目でスタックに積まれた公開鍵情報を検証し、正しいものであれば真を返し、間違っていれば偽を返す。

以上が script 言語の実行内容である。また、この script 言語の特徴として、チューリング不完全であることが挙げられる。このことにより、チューリング完全である時と比べてセキュリティホールが少なく済むことが知られている。その一方で、このスクリプト言語によりユーザが望む様々な処理が実現できるとは限らない。

3.4.3 ペイメントチャネル

Bitcoin におけるオフチェーン技術であるペイメントチャネルは、トランザクションの持つロックタイム機能とマルチシグ機能を併用して実現される。ロックタイムとは、定めた時間になった時までそのトランザクションが実行されない機能のことである。マルチシグとは、ある UTXO を使う際に複数の署名値が要求できる機能のことで、「N of M のトランザクション」などと表される。これは M 個のアドレスの内、N 個のアドレスの署名値が必要となる UTXO であるということを示す。例えば A が消費者· B が販売者とし、A から B へ 1000BTC のデポジットを最初のトランザクションとして持っておき、そこから 100BTC ずつで楽曲を買うことのできる状況を想定してみる。

1. A は A と B の署名値が必要な 2 of 2 のマルチシグのトランザクションを生成し、ブロードキャストする。同時に、2of2 のマルチシグなので Bob が音信不通になった時の保障のため、B が何も行わない場合 A に全ての BTC が戻るトランザクションをマルチシグのインプットから提出する。この際、この戻るトランザクションに関しては一定期間が過ぎた後に実行されるようにロックタイムを掛けておく。
2. A が 1 曲の楽曲を買うため、マルチシグのトランザクションに A のみが署名し、アウトプットとして A に 900BTC· B に 100BTC を支払うトランザクションを B へ送る。
3. A が更に 1 曲の楽曲を買うため、マルチシグのトランザクションに A のみが署名し、アウトプットとして A に 800BTC· B に 200BTC を支払うトランザクションを B へ送る。

この時、B は自分に 100BTC でも 200BTC でも送ることが可能な権利を持つが、通常は 200BTC を貰う方を選択する。このようにしてチェーンの外での取引が実現される。そして、A が払うという範囲においては、B の方から A へ BTC を送ることも可能である。ここでは先ほどの例のシチュエーションにプラスして、1 ヶ月ごとに抽選があり、それに当たると 50BTC が帰ってくるという場合を想定してみる。

1. A は A と B の署名値が必要な 2 of 2 のマルチシグのトランザクションを生成し、ブロードキャストする。同時に、2of2 のマルチシグなので Bob が音信不通になった時の保障のため、B が何も行わない場合 A に全ての BTC が戻るトランザクションをマルチシグのインプットから提出する。この際、この戻るトランザクションに関しては一定期間が過ぎた後に実行されるようにロックタイムを掛けておく。

2. A が 2 曲の楽曲を買うため、マルチシグのトランザクションに A のみが署名し、アウトプットとして A に 800BTC· A と B のマルチシグに 200BTC を支払うトランザクションを B へ送る。そして同時に、A と B のマルチシグに A が署名を行い、そのマルチシグから B へ送るようにする。この際、B へのトランザクションには 1 番目に生成したロックタイムより前に設定されたロックタイムを設定しておき、B のアドレスは今回のみ使われる一時的なアドレスを使用する。
3. ここで A が抽選にあたり、B は A へ 50BTC を支払おうとする。しかし A が 850BTC を持ち、B が 150BTC を持つトランザクションを作ったとしても、B が先ほどの 200BTC を貰えるトランザクションを提出しない保証はない。そこで、B は一時的に利用したアドレスの秘密鍵を A へ送る。これによって、B は A に前の契約より少ない BTC の契約に同意したことを示す。

もし B が 200BTC のトランザクションをブロードキャストした場合は、A はその後に続くトランザクションがロックタイムに到達する以前に A と B(一時的なアドレス) のマルチシグから A へ 150BTC を送るトランザクションを発行できるので、B はそのためのトランザクションをブロードキャストしない。B がブロードキャストしなければ、A に全額が渡るトランザクションはインプットが存在しなくなるためだ。このようにして Bitcoin のオフチェーンは実現される。

3.5 Ethereum

ここでは本研究で用いるブロックチェーン技術である Ethereum について述べる。3.4.1 と 3.5.1 が、3.4.2 と 3.5.3 が、3.5.3 と 3.5.4 がそれぞれの特徴に対応している。通貨単位は ETH である。

3.5.1 トランザクションベースとアカウントベースの二元管理

Ethereum はトランザクションに基き、アカウント毎に Ethereum を管理している。もちろん、Bitcoin と同様に「3ETH を持っている」=「3ETH を過去に送ってもらったことがある」という考えのもと、A が 3ETH 持つには A に 3ETH を送ったトランザクションが存在しなくてはならない。しかし、このトランザクションの結果、A の持つアドレスに 3ETH が紐づくのだ。つまり、3ETH を使う際は前のトランザクションに署名をして使うのではなく、「3ETH 使います」ということを A のアカウントの署名で提出すれば 3ETH が使えることになるのだ。これは面倒なお釣りの処理を行う必要も無くす。A が 3ETH 持っていて、B に 2ETH を送信した時、別途自分用のお釣りのアドレスを用意せずとも残りの 1ETH は自分のアドレスに紐づいているのだ。問題点としては、ハードフォークが起こった時にバージョンや ChainID を変更ことができないことが起こってしまうと、リプレイアタックの攻撃の可能性があることである。The DAO 事件を発端に、Ethereum は急遽 Ethereum と Ethereum Classic にハードフォークすることとなった。ブロックの巻き戻しを行うか否かで意見が割れ、巻き戻したほうが Ethereum、巻き戻さなかった方が Ehtereum Classic となったのだ。そしてこの事件より前から所持していた Ethereum を送金しようとすると、それと同じトランザクションを Ethereum Classic ネットワークでも送信できるようになる。よってこの際、Ethereum Classic は持っている人の意思とは無関係に Ethereum 送金と同時に Ethereum Classic も送金されてしまう可能性を持ってしまうのだ。これはトランザクションベースの一元管理では起こり得なかったことである。アカウントベースでの管理を加えたことは、複雑な処理を可能にしたと同時に、セキュリティ面では厄介な問題を引き起こす原因を作った。

3.5.2 スマートコントラクト

Ethereum のアドレスは EOA(Externally Owned Account) アドレスとコントラクトアドレスが存在する。Bitcoin のアドレスと同様に、所有者に紐付くアドレスが EOA アドレスである。EOA アドレスからは採掘や送金などを行うことができる。Bitcoin アドレスと異なる存在が、コントラクトアドレスである。Ethereum ではスマートコントラクトと呼ばれるものが作成できる。これは人が持つものではなく、コードとして定義された関数である。Ethereum はそれそのものがブロックチェーンでありながら、Ethereum ネットワーク上でコードによって支配された世界を築く土台であろうとしている。そしてコードによって支配された世界に当たるものがこのスマートコントラクトである。また、このスマートコントラクトにつけられた Ethereum ネットワーク上でのアドレスがコントラクトアドレスとなる。スマートコントラクトはよりフレキシブルな非中央集権の世界を作ることができる。Bitcoin は金にあたるトークンのやりとりのみが行われているのみだった。その一方で、スマートコントラクトは例えば管理会社のいないギャンブル市場を作ることが出来るのだ。ここでは Augur という Ethereum 上で動いているスマートコントラクトを例に述べる。Augur の参加者はまず、賭けに関するトピックを生成し、それをブロードキャストする。それに興味を持った参加者が賭けを行うため、作成されたトピックに存在する選択肢から一つを選び、賭けたい量の Augur トークンを賭ける。もしこれが競馬のレースであったとするならば、レース終了後にこの事実を認定するフェーズに入る。事実はレース終了後に選択肢の中から正しい選択肢に対して賭けることで行われ、レース終了後でもっとも多く賭けられた選択肢が事実として認定される。その後、争議ラウンドが設けられ、これに対する異議申し立てを行える期間がある。そして最終的な決着を見た結果に基づいて払戻金が支払われるという仕組みになっている。この際、トピックを生成することに関してインセンティブとなるように生成者には一定の Augur トークンが支払われる仕組みを持っている。さらに、レース後の投票においても最終的な結論に至らない場合、チェーンがフォークすることも前提にした仕組みを持っている。そしてこの賭けのサービスを応用すると、保険機構も作れるのだ。「A さんが怪我を負うか」というトピックにに A さんがずっと「怪我を負う」賭け続け、A さん以外が「怪我を負わない」に賭け続けるとする。すると A さんが怪我を負った時、賭けに勝ったお金として保険金に当たる今まで「怪我を負う」に賭け続けた失ったトークンが戻ってくるのだ。この場合、怪我の認定について誰が行うかなどの曖昧な点が残されているが、原理としては行うことが出来る。このように、スマートコントラクトは単なる送金よりもフレキシブルなコードによって支配された非中央集権の世界を作ることの可能な技術なのだ。

3.5.3 solidity とチューリング完全

solidity は前述のスマートコントラクトを記述する言語である。そして、フレキシブルな世界実現のため、solidity はチューリング完全な言語となっている。例えば、貨幣のような価値を持つトークンの存在を前提としたスマートコントラクトには ERC20 という基準が存在するが、これについての記法について見てみる。これはこの ERC20 に沿っていれば、Ethereum ネットワーク上でトークンとしての役割を果たせると言えるものである。

ソースコード **3.4:** ERC20 を満たすために必要な関数とイベントの宣言文

```
function totalSupply() constant returns (uint256 totalSupply);
function balanceOf(address _owner) constant returns (uint256 balance);
```

```
function transfer(address _to, uint256 _value) returns (bool success);
function transferFrom(address _from, address _to, uint256 _value) returns (bool
    success);
function approve(address _spender, uint256 _value) returns (bool success);
function allowance(address _owner, address _spender) constant returns (uint256
    remaining);
event Transfer(address indexed _from, address indexed _to, uint256 _value);
event Approval(address indexed _owner, address indexed _spender, uint256 _value);
```

function totalSupply:当該トークンの供給量を取得する。

function balanceOf:指定した_owner アドレスの残高を取得する。

function transfer:呼び出し主のアドレスが所有するトークンから_value の量を_to のアドレスへ送金する。

function transferFrom:トークンを_from のアドレスから_to のアドレスへ_value の量を送る。このコントラクトの呼び出し主はトークンの管理者であり、_from アドレスは approve によって許可された範囲内での送金となる。

function approve:管理者のトークンのうち、_value までの値の分だけ_spender のアカウントから使うことを許されるように管理者が宣言する。

function allowance:指定した_owner は_spender アドレスに対してどれだけの量のトークンを支払うことを許可されているかを取得する。

event Transfer:トークンが送られた段階で発火し、_from から_to へ_value のトークンが移動したことを出力する。

event Approval:approve が呼ばれた際に発火し、承認情報を出力する。具体的には、_owner から_spender へ_value の量のトークンを流すことを承認したことを出力する。

以上が solidity の書き方である。また、solidity の関数にはセッター関数とゲッター関数の 2 種類が存在する。セッター関数は提出したトランザクションがブロックに入った時に実行されるもので、gas が必要となる。一方、ゲッター関数はその関数の実行コマンドを押した瞬間に実行され、結果が返ってくる。この処理にガスは必要ない。ブロックチェーン上の状態を変更するかしないかでこの 2 種類が存在し、ERC20 では transfer などが前者、totalSupply などが後者に分類される。そして書かれた solidity は solc と呼ばれるコンパイラによって EVM(Etherum Virtual Machine) が解釈可能なバイトコードへと変換され、スマートコントラクトとしてブロックチェーンネットワーク上へデプロイされる。以上がチューリング完全な言語である solidity の説明である。

3.5.4 μ Raiden

μ Raiden は Ethereum におけるオフチェーン技術の一つである。ビットコインのオフチェーンとは違い、これはスマートコントラクトによってオフチェーンを管理する。最初にトランザクションとしてのデポジットをスマートコントラクト上へ提出する。その後、ブロックチェーンとは無関係の通信によって最終的にこのコントラクトから払い戻されるトークン量を決める。最後に、その決まりに基づいてスマートコントラクト内の関数が呼び出され、払い戻しが行われる。μ Raiden はスマートコントラクトを使用しているので、よりフレキシブルにオフチェーン取引中の中間でトークンを引き出すこともできる。また、オフチェーンにデポジット

しているトークン量を増やすことも可能である。またペイメントチャネルと同様に、受け取り側が音信不通になった場合、一定のブロックが経過した後に残ったトークンを引き出せるようになっている。これは ERC20 に準拠した Ethereum ネットワーク上で動くトークンに対して全てで動くように設計されている。

3.6 まとめ

この章はブロックチェーン技術全般についての仕組みやその問題点、Bitcoin や Ethereum の特徴などについて述べた。途中ではトランザクションの処理の上限を緩和するための技術であるオフチェーン技術についても触れた。また、Ethereum は最初にブロックチェーンが実装された Bitcoin よりもフレキシブルな非中央集権のコードベースで動く世界を作れる可能性を秘めていることを述べた。

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)