第　3　部　第2章

ブロックチェーンの活用事例から見るその技術的側面

小林　直人

目　次

１．はじめに

ブロックチェーンは2008年のサトシ・ナカモトによるビットコインの論文から始まり、その後、暗号資産（仮想通貨）が知れわたるにつれ、その技術的性質に注目が集まるようになった。特に2015年頃からビジネス適用のための検討・検証が本格化したとされている［１］。2021年時点においても、技術と応用事例の両面において、多くのセミナーやシンポジウムが開催されている。

2016年時点で経済産業省は「ブロックチェーンは流通管理や土地の登記などへの応用が期待されており、潜在的な国内市場規模は67兆円になる」と予測した［２］。この頃からウェブ記事を始めとしてブロックチェーンに関する解説記事などが散見され始める。中には「世界を変える」と謳ったものもあった。そして、2021年現在、新型コロナウィルスによる経済変化の影響か、ビットコインの価値が乱高下して再び話題になる中、その基盤技術であるブロックチェーンは「世界を変える」ほどの存在には至っていないように思われる。この流れは、ブロックチェーンが注目を浴び始めてしばらくの間、ある意味でバズワード的な扱いをされた結果であり、さらに多くの技術者たちが検討や試行を重ねた過程であるとも言えるだろう。世界を変えると思えるほどの魅力がどのようなものであり、実際にどのようなことが実現できたのか。

本章では、ブロックチェーンの活用事例を挙げながら、その技術的側面について改めて見直す形で、その特徴や利用に適した場面などを整理していく。

２．ブロックチェーンの分類と構築プラットフォーム

本項では、ブロックチェーンの活用事例を踏まえながら、ブロックチェーンの分類について述べる。さらにスマートコントラクトとその構築のためのプラットフォームについてまとめる。

なお、ブロックチェーンの技術解説については、第１部と第２部を参考にして頂きたい。特に２．１「ブロックチェーンによる分散型台帳技術の解説」［３］での説明を前提として話を進めていく。なお解説［３］では、「台帳に取引情報を記録する」という表現を用いたが、実際の活用事例においては取引情報以外を記録する場合も多いため、本章では「データベースにデータを記録する」という表現を用いる。

2－1　パブリック型とコンソーシアム型

ブロックチェーンの活用事例を読み解くとき、特に気を付けなければいけないのが、ブロックチェーンには複数の型が存在するという点である。暗号資産の基盤技術に主として利用されるパブリック型ブロックチェーン、そして、複数企業間でデータの分散管理を行うためなどに利用されるコンソーシアム（共同事業体）型ブロックチェーンである[1]。後者はエンタープライズ型ブロックチェーンとも呼ばれる。パブリック型は自由参加型（非許可型）とも呼ばれ、管理者として参加するときに許可が不要で、誰でも管理者になることができる。対してコンソーシアム型は許可型とも呼ばれ、許可された者だけが管理者になることができる。分類方法については、文献により多少異なる場合がある。本章ではパブリック型とコンソーシアム型という分類名を用いる。

ここで改めて解説［3］を確認して頂きたい。「3.取引情報の分散管理」の説明において、「3－2 複数人で管理する場合（お互いに信頼できる場合）」に対応するのがコンソーシアム型、「3－3 複数人で管理する場合（お互いに信頼できない場合）」に対応するのがパブリック型である。

注意して欲しいのが、サトシ・ナカモトの画期的アイデアである「合意形成プロセスへの経済的インセンティブの導入」が行われているのはパブリック型だけである。コンソーシアム型も、チェインニングによる強固な改ざん耐性が実現されている。しかし、各ブロックの合意形成については、お互いに情報を交換しながら多数決的に合意していくという「平和的な」方法を取るため、マイニングの仕組みも一般的には用いられない。そのような点において、コンソーシアム型はパブリック型とは異なるものであり、ビットコインのような暗号資産の印象は切り離して考えた方が良いだろう。

しかし、ブロックチェーンの活用事例に関する記事の多くは、この分類を区別することなく説明している。これがブロックチェーンのあり方をややこしくしているのではないだろうか。

2－2　ブロックチェーンの活用事例とその型

ブロックチェーンの分類について説明するため、本章を執筆している時点での新しい活

1　多くの文献では、パブリック型、コンソーシアム型、そしてプライベート型の３つで分類している。プライベート型は１つの組織内でブロックチェーンを利用する許可型のものを指すが、本章では取り扱わない。

用事例を取り上げてみたい。Google ニュース検索を利用して「ブロックチェーン」というキーワードで検索してみると、2021 年 1 月 14 日付で、coindesk JAPAN による「中国・海南省、病院がブロックチェーンで請求書を発行――省内で初のケース」という記事［4］が表示される。以下、当記事を抜粋する。

中国南部の海南省にある公立病院「澄邁県（ちょうまいけん）人民病院」は 1 月 11 日、ブロックチェーンベースの請求書管理プラットフォームを使って、初めて患者に電子請求書を送信した。ブロックチェーンで請求書を発行、記録する同省で最初の病院となった。（中略）中国国内初のケースではないが、海南省は公共機関のオンライン行政プラットフォームにブロックチェーン技術を組み込む取り組みに成功した数少ない省の 1 つだ。（中略）「パイロットプロジェクトを推進することで、我々はブロックチェーンベースのプラットフォームを最適化し、多くの行政業務をブロックチェーンに移行していく。これにより政府機関は同じシステムを通じて情報を共有できるようになる」

ブロックチェーンの型は明記されていないが、これはコンソーシアム型のブロックチェーンの活用事例である。なお、この事例のように行政業務において民間（公営）企業とのデータ交換を安全に行うための仕組みで最も有名なのは、エストニアの X-Road であろう［5］。X-Road はエストニアという電子国家のバックボーンとなっているデータ交換のための基盤システムであり、2001 年から運用されている。政府や民間において異なる形でバラバラに動作しているデータベースをつなぐ役割を果たすことで、住民データの一元化を実現している。なお、2019 年に市川市も行政情報システムに X-Road を採用するということで話題となった［6］。この X-Road はブロックチェーン技術を採用していると紹介されることがあるが、これは正確ではない 2007 年、エストニアで大規模サイバー攻撃が発生し、これをきっかけとして「改ざん検知」の仕組みが 2008 年より試験的に開始された。この仕組みがブロックチェーンと類似点をもっていたために、後付け的に（その頃には世界的に話題となっていた）ブロックチェーンと名乗ったのだという［7］。この仕組みはデータを記録する仕組みを持っておらず、すなわちデータベースではないため、一般的なブロックチェーンとは異なるものである。

いずれにしても、海南省の事例は、政府機関や企業における業務を、不正などが起こらないよう安全に連携させることを目的としてコンソーシアム型ブロックチェーンを活用している。言い換えれば、組織間の「橋渡し」的にブロックチェーンを利用しているのである。

もう一つ活用事例を取り上げてみよう。同じく Google ニュース検索の結果を確認する

と、2021年1月18日付けで、日経産業新聞の「ブロックチェーンで融資　日立、みずほと物流情報基盤」という記事［８］が表示される。この記事も一部抜粋する。

日立製作所はみずほフィナンシャルグループ（FG）と共同で、ブロックチェーン（分散型台帳）技術を使って物流データを共有する実証実験を近く始める。荷主から物流業者、物流業者から運送業者への発注や納品、支払いに関する情報を一元管理する。発注時点で将来の売り上げ見合い（将来債権）に対してみずほ銀行が融資し、運送会社が配送前に資金を調達できるようにする。（中略）ブロックチェーンにより取引情報を正確に把握し、運送会社が物流会社から発注を受けた時点で将来発生する予定の債権をトークン化。物流会社の信用力をもとにみずほ銀行が融資することで、トークンを換金可能にする。

この事例についても利用されているのはコンソーシアム型のブロックチェーンであり、実装にあたって後述するHyperledger Fabricが利用されているという［９］。この事例のように、運送や貿易、サプライチェーンなどの、複数事業体が提携して行われる業務において、そのデータ管理にブロックチェーンを利用しようとする取組みは多い。なお、この記事には、「トークン」という暗号資産関連の用語[2]が登場しているが、これはみずほ銀行という金融機関がその価値を内々で担保している台帳上の数値といったものであり、パブリック型で実現されている暗号資産とは異なるものである。

他の検索結果を眺めてみても、その事例の多くはおそらくコンソーシアム型であろう。ここで取り上げた事例も含め、おそらく「データを分散しながらも一体となって管理することを目的している」といったものが多いと思われる。その名の通りコンソーシアム（共同事業体）に適したブロックチェーンなのである。一方、パブリック型の活用事例に関する記事を探すのは、困難であるとは言わないが、少しばかり工夫が必要かも知れない。

繰り返しになるが、コンソーシアム型ブロックチェーンは、ビットコインのような暗号資産の実現に必要不可欠な要素が導入されていない。また管理者として参加する場合にも許可が必要であり、その点で中央集権的な機関が存在していると言える。ビットコインの基盤技術としてブロックチェーンは誕生し、そのビットコインの目指すところは中央集権的な機関を必要としない通貨システムの実現であった。その意味でコンソーシアム型の利用方法は、パブリック型の目指すところと根本的に異なるのである。故にコンソーシアム

２　暗号資産においては「代用貨幣」の意味で利用され、既に存在する暗号資産のブロックチェーン上で新たに作られた暗号資産のことを指す。

型をブロックチェーンと呼んで良いのかという議論も見受けられる。そのため、コンソーシアム型のように､単に「分散して情報を管理する」仕組みを「分散型台帳技術」と呼び、ビットコインの基盤技術として利用されているパブリック型のブロックチェーンはその技術の一種であると区別されるようになってきている｡実際､日本銀行の広報活動サイト[10]においても、次のように区別している。

また、これまで金融サービスが十分普及していなかった途上国や新興国でも、スマートフォンを利用した金融サービスが急速に広がる動きが進んでいます。さらに、分散型台帳技術（注１）やブロックチェーン（注２）といった技術も登場しています。

（注１）特定の帳簿管理主体を置く代わりに、複数の参加者が同じ帳簿を共有するかたちでの管理（分散型管理）を可能とする技術です。（注２）分散型台帳技術の一つで、改ざんを困難とする効果などを持っておりビットコインを支える技術です。

２－３　スマートコントラクトとその開発プラットフォーム

解説［３］で述べたように、ブロックチェーンの活用事例はスマートコントラクトを前提としている。前述した２つの活用事例も、記事中に明記はされていないものの、スマートコントラクトが導入されている。

スマートコントラクトは、一般的にコンピュータネットワーク上で自動的に契約処理を行う概念や機能を指す。ブロックチェーンに、プログラムの動作手順を記録できるようにし、そのプログラムを任意に実行できるような仕組みを導入することで、スマートコントラクトが実現される。このプログラムが実行されたとき、その結果もブロックチェーンに記録されていく。これにより、従来のサーバークライアント方式のように中央集権的な管理者がいない元で、任意のプログラムを実行し、その手順や出力結果が改ざんされていないことをすべての管理者で保証する環境が実現できるのである｡このような視点から､インターネットを情報の革命とするなら、ブロックチェーンは取引の革命と称することもある［１]。

より具体的に説明する。ブロックチェーンは複数の管理者の提供する複数のコンピュータにより成立している。そのすべてのコンピュータはネットワークを通じて接続され、同一のデータとプログラム（スマートコントラクト）が記録されたブロックチェーンを保持している。あるコンピュータが､あるプログラムを実行するように指示を受けた場合､ネットワークで接続された他のすべてのコンピュータにその指示を伝達し、そのプログラムを実行する。その指示は伝言ゲーム的にすべてのコンピュータに伝わるため、すべてのコンピュータが同じプログラムを実行する｡得られた実行結果をまとめてブロックとして扱い、

一定時間ごとに合意形成を行い、その結果をブロックチェーンに結合していく。「台帳への取引の記録」が「データとプログラムの記録」や「プログラムの実行」という汎用的な表現に変わる以外は概ね解説［3］での手順と同じである。

以上がスマートコントラクトの実現方法であるが、前述したようにスマートコントラクトとは「自動的に行われる契約処理」を意味する。この意味を正確に捉えるのであれば、上の説明において「あるプログラムを実行するように指示を受けた場合」とは、人手による指示でなく、何かしらの条件が見たされたときに「自動的に」実行されるもののみをスマートコントラクトと呼ぶということになる。

このことについて、前述した日立製作所の活用事例を例にして説明する。当該記事においては、一連の業務手順の中で「（業者の）信用度合いに応じて（銀行が）融資額や利率を決定」という処理が行われると説明されている。仮にこの処理が「自動的に」行われるとすれば、ブロックチェーンに記録されたプログラムが、人手を介さずにブロックチェーンに記録された「信用度合い」を確認し、融資額や利率を決定してブロックチェーンに記録する、という動作を行う。これは「自動的に行われる契約処理」であり、明確にスマートコントラクトと呼べるものであろう。しかし、もしこの処理が人手を介して行われる場合[3]、つまり、ブロックチェーンに記録された「信用度合い」を銀行員が確認し、融資額や利率を決定してブロックチェーンに記録する処理を行う、という形のものであれば、これは「自動的に行われる契約処理」ではない。ただし、実際は、後者のような仕組みであっても「スマートコントラクト」として呼称される場合があるため注意が必要である。

より具体的な用語として「分散型アプリケーション（Dapps : Decentralized applications）」がある。これは、ブロックチェーンに記録したデータに対して、同様にブロックチェーン上に記録されたプログラムで何かしらの処理を行う仕組みを指す。分散型とは、ブロックチェーンを保持しているすべてのコンピュータが同じプログラムを分散して実行することを意味している。

現在、スマートコントラクト（分散型アプリケーション）を開発するためのプラットフォームは複数存在する。ブロックチェーンを利用した情報システムの開発は、これらを用いて行われるのが一般的となっている。以下、パブリック型とコンソーシアム型それぞれの代表的な開発プラットフォームである。イーサリアムとHyperledger Fabricについて説明する。

3　なお、どちらの方法が採られているかは、記事からは明確にはわからない。

２－３－１ イーサリアム

イーサリアムは Ethereum Foundation が中心となって運営・開発がされているブロックチェーン開発プラットフォームである［11］。運用されているブロックチェーン自身をイーサリアムと呼ぶ場合もある。イーサリアムは、2021 年時点で、パブリック型のスマートコントラクト（分散型アプリケーション）開発の事実的標準といえるものである。

イーサリアムは内部通貨として Ether が定められている。Ether は暗号資産として現実の通貨との取引もなされているほか、スマートコントラクトを利用する場合の手数料の支払いとしても用いられる。ブロックの合意形成はビットコインと同じプルーフオブワークにより行われる。イーサリアムのブロックチェーンには、世界中多くの管理者が参加している。彼らが提供するコンピュータによって、スマートコントラクトの実行とマイニングが行われることにより、パブリック型のブロックチェーンが成立している。イーサリアムのブロックチェーンには誰でもプログラムを記録（スマートコントラクトを登録）することができるが、利用するときに手数料を支払う必要がある。この手数料はプログラムの実行やデータ記録にかかる負荷が大きいほど高額となる。

なお、世界中のコンピュータが協力してプログラムの実行環境を提供していると捉えられるため、イーサリアムを「ワールドコンピュータ」と呼ぶこともある。

イーサリアムについてのより詳細な説明については、３．３「教育機関でのブロックチェーン技術の活用に関する現状と課題」［12］などを参照されたし。

２－３－２ Hyperledger Fabric

Hyperledger Fabric は、許可型ブロックチェーンの開発プラットフォーム（フレームワーク）である。Linux 財団の下で進められている分散型台帳技術に関するプロジェクトの１つであり［13］、オープンソースであることから、多くのコンソーシアム型ブロックチェーンで利用されている。

許可型のブロックチェーンの開発用で、イーサリアムと違い利用するのに手数料は必要しないが、コンピュータ資源は管理者となるそれぞれの企業が提供する必要がある。合意形成は PBFT（practical Byzantine Fault Tolerance）が用いられる。これは前述したように、お互いに情報を交換しあいながら多数決的に合意していくという「平和的な」方法である。詳しくは［14］などを参照されたし。

3．ブロックチェーンの特徴と利用に適した場面

ウェブ上のブロックチェーンの解説記事に目を通すと「データを分散管理できる」「中央集権的な管理者を必要としない情報システムが構築できる」「強い改ざん耐性を持つ」といった特徴が散見される。もちろんこれらは間違ってはいない。しかし、ブロックチェーンの活用方法を議論する上で重要なのは、「その仕組みをブロックチェーンで実現するとしたとき、既存技術で構築された同様のシステムと比較して、どのような長所があるのか」という点であり、言い換えれば「そのシステムを実現するために本当にブロックチェーンを使う必要があるのか」という点である。このような問題提起は、筆者が参加したブロックチェーンに関する勉強会やセミナーで耳にすることも多かった。

本項では、ブロックチェーンの特徴について、まず基本に立ち戻り、情報セキュリティの観点からまとめる。それを踏まえた上でブロックチェーンの利用に適した場面について整理し直してみる。

3－1　情報セキュリティの観点によるブロックチェーンの特徴

ISO/IEC27001（情報セキュリティマネジメントシステムに関する国際規格）では、情報システムのセキュリティについて「情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止、信頼性などの特性を維持することを含めることもある」と定めている。各要素の意味を表１に簡単にまとめる。

表１　情報セキュリティの７要素

機密性	第三者に情報を漏洩させないこと
完全性	情報や処理が正確（完全）であること
可用性	利用者が必要なときに利用可能な状態であること
真正性	偽造やなりすましでなく、主張するとおりのものであること
責任追跡性	誰の行動かを遡って追跡できること
否認防止	行動を後になって否認できないようにすること
信頼性	意図する行動と結果が矛盾なく一貫していること

ブロックチェーンについて、これらの観点から整理する。

まず機密性（第三者に情報を漏洩させないこと）については、パブリック型とコンソーシアム型で異なるが、いずれも機密性を高めるための仕組みを持っていない。特にパブリック型については解説［３］でも述べたように、そもそもブロックチェーンに記録するデー

タは公開されることが前提となっているため、機密性は一切持たないと言っても良い。この文脈においてブロックチェーンの特徴を表すのに適した言葉は「透明性」であり、機密性とは真逆の意味である。一方、コンソーシアム型においては、ブロックチェーンに記録されたデータをどのように公開するかというシステム全体の運用方法によるが、いずれにしてもブロックチェーンの導入によって機密性が高められるということはない。

完全性（情報や処理が正確であること）については、記録されたデータの改ざんを困難にすることができるという特徴により、完全性を高めることができる。これはブロックの記録をする際にチェイニングを行っていること、および同一のブロックチェーンを複数の管理者によって多重化して保持することで実現している。ただし、強い改ざん耐性だけを実現したいのであれば、後述するように既存の情報技術で十分に対応可能であり、ブロックチェーンを利用する必要はない。

可用性（利用者が必要なときに利用可能な状態であること）については、注意が必要である。ブロックチェーンの紹介記事には「ブロックチェーンは 24 時間 365 日ダウンすることなく稼働する」といった可用性の高さを謳うものも存在しているが、これは正確ではない。ブロックチェーンの可用性の高さは、多くのコンピュータで分散処理を行うことにより担保されているものである。パブリック型については、イーサリアムのような大規模なものであれば、無数のコンピュータで分散処理を行っているため、（スマートコントラクトのプログラム自体に不具合がない限り）非常に高い可用性を持つと言えるだろう。一方、多くのコンソーシアム型の活用事例では、少数のコンピュータでブロックチェーンが実現されており、必ずしもパブリック型のように可用性が高いとは言えない。さらに合意形成の処理において単一障害点が存在するといった報告もあり［15］［16］、ブロックチェーンを利用することで「24 時間 365 日ダウンすることがない」システムが必ずしも実現できるわけではないのである。

真正性、責任追跡性、否認防止については、いずれも強く保たれていると言える。これはブロックチェーンの基本的な情報記録方法が書き換えではなく追記による方法であること、前述したように強い改ざん耐性を持つこと、さらに電子署名による検証機能を持つことが理由である。もちろん解説［３］で述べたような「51% 攻撃」による改ざんは起こり得るため、絶対的なものではないことに注意する。最後の信頼性に関しては、スマートコントラクトのプログラム自体に依存するものであるため、本章では言及しない。

３－２　ブロックチェーンの利用に適した場面

前項で整理したように、ブロックチェーンを利用することで、情報セキュリティの基本

的な要素である「完全性」「真正性」「責任追跡性」「否認防止」を高く保つことができる。しかし、これらはチェインニングや電子署名（改ざんを困難にする）、および、追記による記録（ログを残すことに対応）といった技術によるものであるため、当然、既存の情報システムにおいても実現可能である。また、分散処理という特徴も、古くから行われているシステムの多重化［17］に相当する。

つまるところ、情報セキュリティの基本的な要素を満たすため「だけ」であれば、既存の情報システムの代わりにブロックチェーンを採用する意味はほとんどないと言って良い。ブロックチェーンの利用に適した場面は、その原点であるビットコインの目的に立ち戻ったもの、すなわち「中央集権が不在のシステムを実現したい場合」であり、雑な形で言い換えれば「遠隔地のコンピュータ同士で平等で安全なデータ管理を実現したい場合」である。また、イーサリアムやHyperledger Fabricのようなプラットフォーム上でのシステムを開発することで、製造コストを下げられるため、これを理由としてブロックチェーンを利用することもあり得るだろう。

以上を踏まえて、パブリック型とコンソーシアム型のブロックチェーンの利用に適した場面について整理していく。

パブリック型の利用方法は、独自のブロックチェーンを開発する方法とイーサリアムなどのプラットフォームを利用する方法に分けられる。前者は暗号資産の実現が最たる活用事例である。独自のブロックチェーンにより何らかの情報システムを実現するためには「経済的インセンティブの導入」が必須となる。つまり、そのシステムの管理者となりコンピュータ資源を提供した者に対して、仮想的なコインを提供するという仕組みが必要となるということである。そのコインに価値がなければ成立しないため、暗号資産以外の活用事例は見いだしにくいのではないだろうか[4]。

イーサリアムなどのプラットフォームを利用する場合は、経済的インセンティブの導入は必要ないが、代わりに利用料を支払う必要がある。イーサリアムを利用することで「サーバーを不要とした情報システムを構築できる」と謳われることもあるが、自前でサーバーを導入もしくはクラウドなどで利用する場合と比べて、運用コストが改善されるかどうかは、利用料として支払うEtherの価格によるので何とも言えない。

また、「中央集権が不在のシステムを実現したい」という視点で見ると、次のような状

4　ゲームを独自のブロックチェーン上のスマートコントラクトとして実現し、ゲーム内通貨を提供する仕組みであれば、エンタテイメント分野の活用事例として実現できなくはないだろうが、そのためにコンピュータ資源を提供する者を集めるのは難しいと思われる。

況が考えられる。

・複数の個人や組織からなる団体において、何かしらの永続的に管理したいデータが存在する
・かつ、その情報をなるべく広く透明性をもって公開したい
・かつ、その団体の中で中心的な管理者を決定できない

これは例えば、複数の大学が一体となって学習成果の証明書を発行するような場合に該当する。

ただし、イーサリアムのブロックチェーン上に大きなサイズのデータを記録しようとすると、前述したように、手数料を多く支払わなければならなくなる。そのため実際は、ブロックチェーンには重要なデータ（検証作業に必要なハッシュ値など）のみを記録し、その他に必要となるデータはブロックチェーンの外に記録するといった方法が用いられる。「外」というのは、何らかの形で準備した既存の情報システムのことである。当然、その情報システムを管理する者が必要となり、それは「中心的な管理者」に相違ない。それを決定できるのであれば、ブロックチェーンを利用せず、その管理者がすべてのデータを保持するという選択肢が生まれてしまう。つまり、上述した状況であっても、運用方法や組織間の信頼（対立）関係により、ブロックチェーンの利用が適しているかは十分な検討が必要となるのである。

一方、コンソーシアム型について、「遠隔地のコンピュータ同士で平等で安全なデータ管理を実現したい場合」という視点で考えてみる。これは２－２で述べたような同業他社や関連企業からなる共同事業体で協力してデータ管理を行う場合に相当する。ただし、注意しなければならないのは、パブリック型と同様、その共同事業体の中に「データ管理を任せることのできる組織」が存在する場合は、従来のサーバークライアント方式を利用することでも実現はできるという点である。

以上、ブロックチェーンの利用に適した場面について整理したが、いずれも否定的な表現が多くなってしまっている。ただ、これはブロックチェーンという言葉が、ある意味でバズワード的に、大げさな（もしくは間違っている）謳い文句と共に広まってしまったことに対して、「従来方式と比較する形での検討が必要である」という当然の視点から整理したためである。しかし、大げさな謳い文句と共に広まったこと自体は、その技術の魅力を伝えることに繋がるため、必ずしも悪いことではないだろう。実際、筆者が参加したセミナーにおいても、「ブロックチェーンの話題が経営陣にまで広がった結果、初めて同業

他社の研究者たちと協力して勉強会などを行う機会が得られた」といった話を聞くことがあった。

それ以外にも、筆者が参加したセミナーや講演会では、実践的研究に携わる方々の話を聞くことができた。その中でも特にコンソーシアム型（エンタープライズ型）の活用について印象に残っているお二人の意見を引用することで、ここまでのまとめとしたい。

今日ご紹介したようなコンソーシアム型の事例は、当初のブロックチェーンのコンセプトにインスパイアされて、長年放置されてきた業界横断的な課題を解決していこうという取り組みであり、これ自体は当初のブロックチェーンの浮き沈みとはもう関係なく、今後も進んでいくのではないのかと考えています。[5]

ブロックチェーンはまだまだ黎明期。エンタープライズ型ブロックチェーンの本質は、”共有されるミドルウェア”。複数の法人・組織間で、データやプロセスを共有することで、既存の業務を変革する。ビジネス価値のあるユースケース設計やガバナンスモデルのチャレンジ。適材適所：どの基盤を使うべきかは、ユースケースによって異なる。世界的には、実用化は着々と進みつつある。[6]

４．様々な活用事例

本項ではブロックチェーンの様々な活用事例について、これまでの内容を踏まえながらまとめていく。なお活用事例については、筆者が参加した勉強会やセミナーで取り上げられたものを主に取り上げており、網羅的に整理したものではないことをご了承頂きたい。

４－１　暗号資産（仮想通貨）

ビットコインを始めとした、様々な暗号資産が投資的に取引されているということは改

5　情報処理学会 第 81 回全国大会（2019 年 3 月 16 日開催）「ブロックチェーンによるイノベーションの展望と課題 ―デジタルプラクティスライブ―」におけるパネル討論での近藤真史氏（（株）日本取引所グループ 総合企画部 フィンテック推進室）の発言。同内容を記録した文献［18］より引用。

6　情報処理学会 連続セミナー 2020「ブロックチェーンの社会実装とそのインパクト」（2020 年 11 月 20 日開催）における吉濱佐知子氏（日本アイ・ビー・エム株式会社 東京基礎研究所シニア・テクニカル・スタッフ・メンバー，FSS & Blockchain 担当部長）の講演スライド資料より引用。

めて述べる必要はないだろう。暗号資産の大半は、独自のパブリック型ブロックチェーンで運用されているが、リップル［19］のようにコンソーシアム型（許可型）で運用されているものもある。

特異な事例として、国家が暗号資産（仮想通貨）を発行したベネズエラが有名であろう。2018年２月、ベネズエラは原油により裏付けされるとした世界初の仮想通貨「ペトロ」の発行を発表した。当時ベネズエラ政府は「石油による裏付けとブロックチェーン技術の利用により、ペトロは信頼できる仮想通貨である」とアピールした［20］。なお、2021年時点でほぼ破綻している状態であるという［21］。

４－２　ブロックチェーンゲーム

ブロックチェーンを利用したゲーム、通称「ブロックチェーンゲーム」は、ブロックチェーンの活用事例として、興味深い位置づけにある。広く注目を浴びるきっかけとなったのは、2017年にサービスを開始したCryptoKitties［22］である。CryptoKittiesは、イーサリアム上のスマートコントラクトとして開発され、猫のキャラクターを集めて育成する単純なゲームである。しかし、その猫のキャラクターをEtherによって売買できる仕組みを設けていた。その結果、大人気となり、BBCやニューヨーク・タイムズをはじめとする世界中のメディアが取り上げた。人気絶頂期には20万ドル（約2100万円）以上で取引されたという［23］。現在も様々なブロックチェーンゲームのサービスが提供されている[7]。

４－３　取引履歴やデータの真正性証明

ブロックチェーンの活用事例として、エバーレッジャー社のダイヤモンド取引履歴は、度々話題として挙げられる。その内容について2017年の東洋経済の記事［25］から引用する。

英ベンチャー企業のエバーレッジャー社は、ダイヤモンドの鑑定書や取引履歴をブロックチェーン上でデータ化して取引できるようにし、そのデータについて警察や保険会社も参照できるビジネスモデルを構築した。これによって、横行していた鑑定書偽造や保険金詐欺をなくすといった社会的問題を解決しながら、安心して取引できる流通プラットフォームを作ることに成功している。

7　通常のゲームと異なり、現金的な価値を持つ暗号資産で取引を行うため、ゲームの設計によっては賭博罪や景品表示法に違反する可能性があるという指摘もある［24］。

データの透明性や真正性などを確保するためにブロックチェーンを導入した活用事例と言えるだろう。同様の活用事例として美術品の所有権や展示の履歴をブロックチェーンに記録し、証明書を発行するという事例もある［26］。また、大学などの成績評価、学位の記録の管理に利用することもできる。この詳細については３．３「教育機関でのブロックチェーン技術の活用に関する現状と課題」［12］を参考にされたし。

また、公文書管理にブロックチェーンを利用するという話は定期的に話題となり、実証実験も行われている。確かに透明性や真正性の確保という意味において適してはいるが、当然のことながら、ブロックチェーンに記録するより前の段階で、現実に存在する公文書そのものに対して不正が行われた場合は無力である。このような「現実に存在するモノの情報と、ブロックチェーン上のデータの結びつき」の問題は、特にスマートコントラクトとしての活用を考えるにあたり、まず検討しなければならないことである。前述した東洋経済の記事［25］に掲載された次の事例について考えてみる。

例を挙げれば、カーシェアリング。カーシェアを使いたいとき、スマートフォン(スマホ)のアプリで注文すれば、瞬時にスマートコントラクトが契約を自動執行し、代金が決済され、利用者ニーズにぴったり合った車が自動走行して目の前に止まり、ドアが開く、といった日が来るかもしれない。

このようなことが実現されるかどうか定かではない。しかし、すぐに思いつくのは「届いた自動車が壊れていたらどうするか」といった問題である。どの時点で故障したのかは利用者に判断できないため、何かしらの物理センサーなどを自動車に搭載して、機械的に判断しなければならない。しかし、仮にセンサーも壊れていて、誤った情報をブロックチェーンに記録してしまった場合、どうすれば良いのだろうか。

暗号資産や成績証明書のように、現実に存在するモノと結びついていない対象は、コンピュータ上のデータとして閉じた形で処理を完結できる。しかし、ダイヤモンドや美術品のような現実に存在するモノについての情報をブロックチェーンに記録するときは、多くの場合、人手によって検証しながら行う必要がある。その「現実的な手順」に誤りが生じて、それをブロックチェーンに記録してしまった場合、ブロックチェーンの仕組み上、それを修正するのは容易ではない。また、誤りによって取引が破綻してしまうような場合に備えるため、仲介者の存在が必要となるだろう。現実に存在するモノを扱った活用事例については、このような点に注意して読み解く必要がある。

４－４　コンソーシアム型の活用事例

２－１で例示したように、コンソーシアム型ブロックチェーンを利用し、複数事業者間でデータを分散しながらも一体となって管理することを目的する活用事例は、今後増えてくるだろう。サプライチェーン［27］や貿易業務［28］の事例などは、実践的な検証も行われており、実用化が期待される対象である。

５．まとめ

本章では、ブロックチェーンの活用事例を挙げながら、その技術的側面についてまとめてきた。決して丁寧にまとめたと言えるものではないが、ブロックチェーンの活用事例を読み解くときのヒントとなれば幸いである。

参考文献

［１］吉濱佐知子 , 町田武夫 , " ブロックチェーン技術と IBM の取り組み ", https://www.ibm.com/downloads/cas/ 9GVNPQLP ProVISION No.91, 日本 IBM, 2017.

［２］日本経済新聞 2016 年 4 月 29 日号 , " 仮想通貨で使う「ブロックチェーン」、国内潜在市場 67 兆円」".

［３］小林直人、宮田大輔 , " ブロックチェーンによる分散型台帳技術の解説 ," 国府台経済研究 第 31 巻第 2 号 , 2021.

［４］David Pan（山口晶子訳）," 中国・海南省、病院がブロックチェーンで請求書を発行――省内で初のケース ", coindesk JAPAN 2021 年 1 月 16 日(2021 年 1 月 22 日閲覧).

［５］"e-estonia toolkit" https://e-estonia.com/e-estonia-toolkit/（2021 年 1 月 22 日閲覧）.

［６］杉田悟 ,"「DX 先進都市」を目指す市川市、エストニア電子政府のデータ連携技術「X-Road」を採用 ", https://it.impress.co.jp/articles/-/18058 IT Leaders 2019 年 6 月 12 日 , インプレス（2021 年 1 月 22 日閲覧）.

［７］小島 健志 , 孫 泰蔵 ," ブロックチェーン、AI で先を行くエストニアで見つけた つまらなくない未来 ," ダイヤモンド社 ,2018.

［８］日経産業新聞 2021 年 1 月 18 日 , " ブロックチェーンで融資　日立、みずほと物流情報基盤 ".

［９］清宮信志 ," 日立とみずほ、ブロックチェーンで物流の輪配送代金を早期資金化 ,"https://www.watch.impress.co.jp/docs/news/1298321.html Impress Watch 2021 年 1 月 5 日 , インプレス（2021 年 1 月 22 日閲覧）.

[10] 日本銀行 公表資料・広報活動 ,"FinTech（フィンテック）とは何ですか？ ," https://www.boj.or.jp/announcements/education/oshiete/kess/i25.htm/（2021 年 1 月 22 日閲覧）.

[11] Ethereum Project, https://ethereum.org/en/.

[12] 長尾雄行 , " 教育目的でのブロックチェーンの応用 ," 国府台経済研究 第 31 巻第 2 号 , 2021.

[13] Hyperledger https://wiki.hyperledger.org/ .

[14] Aram Mine," コンソーシアム型ブロックチェーンで使用できる合意形成アルゴリズム「PBFT」," Blockchain Biz 2017 年 10 月 13 日 , https://gaiax-blockchain.com/pbft（2021 年 1 月 22 日閲覧）.

[15] 河田雄次 , " 分散型台帳技術にかかる基礎実験 ", 日本銀行決済機構局 FinTech センター 第 3 回 FinTech フォーラム , 2017 年 2 月 27 日 , https://www.boj.or.jp/announcements/release_2017/data/rel170227a5.pdf（2021 年 1 月 22 日閲覧）.

[16] 安達仁 , " ここがつらいよ、Hyperledger Fabric の商用適用 ", Blockchain GIG # 4 発表資料 2019 年 9 月 4 日 , https://www.slideshare.net/nttdata-tech/hyperledgerfabric-production-release-blockchainig 4 （2021 年 1 月 22 日閲覧）

[17] 干場一彦 ," 可用性を高める「サーバー多重化」", 日経クロステック 2008.02.26, https://xtech.nikkei.com/it/article/COLUMN/20080218/294034/（2021 年 1 月 22 日閲覧）

[18] " ブロックチェーンによるイノベーションの展望と課題 ", デジタルプラクティス Vol.10 No.3, 情報処理学会 , 2019.

[19] Colin Harper, "What Is XRP, and How Is It Related to Ripple?," coindesk.com 2020/12/12, https://www.coindesk.com/what-is-ripple-what-is-xrp（2021 年 1 月 22 日閲覧）

[20] 坂口安紀 ," 新興国発イノベーション 第 7 回 破綻経済と仮想通貨（ベネズエラ）," 日本貿易振興機構アジア経済研究所 2020 年 7 月 , https://www.ide.go.jp/Japanese/IDEsquare/Column/ISQ000011.html（2021 年 1 月 22 日閲覧）

[21] 毎日新聞 2021 年 1 月 3 日 " ベネズエラ仮想通貨「ペトロ」低迷　市民利用せず　独裁政権の資金調達不発 ".

[22] CryptoKitties, https://www.cryptokitties.co/

[23] Christine Kim, Shuai Hao（山口晶子訳）" イーサリアムについて知っておくべき 5 つのこと ," coindesk 2020 年 8 月 9 日 , https://www.coindeskjapan.com/73929/（2021

年１月22日閲覧）
［24］斎藤創 ," ブロックチェーンゲームと日本法 ," So & Sato Law Offices Articles 2018年10月４日 , https://innovationlaw.jp/blockchain-games-under-japanese-laws/（2021年１月22日閲覧）
［25］翁百合 ,"「ブロックチェーン」は世界をこう一変させる　仮想通貨の技術が国境を越えて駆け巡る時代 ," 東洋経済オンライン 2017年１月11日 , https://toyokeizai.net/articles/-/152506（2021年１月22日閲覧）
［26］" ブロックチェーンで美術品の所有権証明　東大発ベンチャーの技術、SBI のオークションで採用 " ITmedia News, 2019年04月09日 , https://www.itmedia.co.jp/news/articles/1904/09/news095.html（2021年１月22日閲覧）
［27］"IBM Blockchain Supply Chain ソリューション ", https://www.ibm.com/jp-ja/blockchain/industries/supply-chain（2021年１月22日閲覧）
［28］金子雄介 , 田村浩気 , 河合伸浩 , 田中俊太郎 , 岡知博 , " 貿易実務のブロックチェーン利用、実践と課題 ", デジタルプラクティス　Vol.10 No.3, 情報処理学会 , 2019.