論　説

ブロックチェーンベースのスマートコントラクトにおける合意形成と契約理論

長谷川　貞之

〈目次〉

一　問題の所在

近年、スマートコントラクト（Smart Contract）という言葉が、各種のモノやサービス、情報などをインターネット上のネットワークを通じて取得したり、最適化することを内容とするシステムを示す用語として、様々な場面で使われている。自動販売機でいえば、通常、コンピュータ上のプログラムコードに「AならばX」という条件と結果が書き込まれ、Aが成就したとき自動的にXという処理がなされる。このとき、「AならばX」という合意自体は、法的にはスマートコントラクトとは別に当事者間で行われる。スマートコントラクトについては、今のところ明確な定義があるわけではなく、一般的に、コンピュータ上のプログラムコード（program code）により特定の条件の発生時に契約上の義務が自動的に履行されるように設計されている契約であるといわれる(1)。

現代社会におけるスマートコントラクトは、ブロックチェーンに搭載されて用いられることが多く(2)、現代の企業はブロックチェーン技術の採用に積極的である(3)。後述するように、ブロックチェーンは、ピア・ツー・ピア（P2P）のネットワークを通じて取引に参加する者同士をコンピュータで結びつけ、取引履歴の情報や記録をブロックごとに格納し、これをチェーン（鎖）のように直列に連結したデータベースである(4)。もとは暗号通貨であるビットコインを実現するための中核技術として開発され、二〇〇九年の運用が開始された技術である(5)。ビットコインの創始者であるサトシ・ナカモト（Satoshi Nakamoto）と名乗る人物によって投稿された論文には、第三者などの仲介機関を通さない直接的なオンライン取引を可能にする技術として、ブロックチェーンを用いたビットコインの仕組みが紹介されている(6)。

ピア・ツー・ピア（P2P）のネットワークを通じて行われる暗号通貨の取引では、取引履歴を台帳に記録し、その台帳に対して誰も恣意的に不正操作やハッキング、詐欺などが行えないようにしつつ、ネットワーク上で取引を管理できるようにする必要があった。そのための技術が分散型台帳としてのブロックチェーンである。

スマートコントラクトは、今日、このようなブロックチェーンを基盤としこれに搭載されて用いられるアプリケーションであり、特定の条件を満たすと契約を自動的に実行するコンピュータ上のプログラムコードである(7)。また、近頃では、スマートコントラクトがモノのインターネット（Internet of Things: IoT）と組み合わさり、デジタル経済を支えるデバイスとしても広く社会に浸透してきている(8)。ＩｏＴは、クラウドといったモジュール化可能な技術で構築されることが多いが、必要となる複数の機能をまとめてモジュール化して提供するのが、ＩｏＴプラットフォームである(9)。スマートコントラクトは、このＩｏＴプラットフォームに装備され、契約の自動化を促進させる役割も担っている。また、スマート・シティー構想の中では、ＩｏＴテクノロジーでインフラを管理し、環境に配慮しつつ経済発展を目指す社会の構築に向けた新テクノロジーとしての期待が高まっている。

スマートコントラクトという言葉が広く社会に普及し始めたのは、ブロックチェーン技術とスマートコントラクトとの融合が背景にある(10)。スマートコントラクトは、後述するように、契約の自動化または自己執行力を示す用語として古くからあったが、ブロックチェーンの登場により、ブロックチェーンを基盤としこれに搭載され、取引費用の削減、手続の迅速化、権利の譲渡または移転などの取引履歴の保存などの目的で広く用いられるようになった。いわば、ブロックチェーンのアプリケーションの一つが、いわゆるスマートコントラクトである。

ブロックチェーンは暗号通貨であるビットコインの中核技術であるが、この技術が今日知られるような広汎な用途

をもつ強力なテクノロジーとして誕生したということに気づいた者は、当時ほとんどいなかったといわれる。[11] 当初、ブロックチェーン技術は、これを用いることで、極めて低い費用で取引の信頼性を担保することが可能となり、電子取引システムとして機能することが期待されていた。[12] その後、信頼のおける第三者などの仲介機関を必要としないという先進性とその利点から、ブロックチェーン技術が俄かに注目を浴びるようになった。[13]

スマートコントラクトの基盤となるブロックチェーン技術には、ブロックの追加にあたり、ネットワーク参加者の各ノードによるコンセンサス・アルゴリズム（Consensus Algorithm）という合意形成が用いられており、不正や改ざんが困難で透明性が高いことや、中央の集権的な管理者や仲介者などの第三者が不要なため、取引費用の削減が期待できることなど、多くのメリットがある。この特性を利用し、ブロックチェーンのアプリケーションとしてスマートコントラクトを搭載することにより、契約内容をあらかじめプログラミングしておき、特定の条件が満たされると自動的に契約が実行される仕組みを作り出すことができる。スマートコントラクトでは、契約を意味する「コントラクト」という言葉が用いられているが、その実体はブロックチェーン上で展開されるコンピュータ上のプログラムコードである。[14]

新しいテクノロジーに依存する企業が増えるにつれて、現在では、スマートコントラクトをめぐる法律関係の明確化と規律の必要性が問われている。[15] また、その法的紛争の解決にも、新たな視点が求められている。[16] スマートコントラクトは、それ自体、契約といえるのかどうか。また、当事者間でコード化された一定の条件の解釈が事後的に争われたり、予期しないコードの破損やコード間の不整合、あるいは、システムやネットワークへの不法侵入（ハッキング）が生じたような場合、どのような紛争解決が導かれるのか、未知の部分が少なくない。申込みと承諾による意思

表示の合致（合意）を契約成立の基本的要件とする伝統的な契約理論からみれば、スマートコントラクトは機械思考の契約であり、これが果たして契約といえるのかどうか、より根本的な問題として問われることになる。[17]

スマートコントラクトに関する議論は、これまで技術的・経済的側面から議論されることが多かった。[18] しかし、社会におけるブロックチェーン技術、およびスマートコントラクトに対する注目度が高まるにつれて、これらの問題も法律上の主要な論点の一つとして取り上げられるようになってきた。[19] ブロックチェーン技術のもつ革新性とそれを基盤として利用されるスマートコントラクトは契約を取り巻く社会環境を大きく変える力をもっており、[20] 伝統的契約理論にとって重要な問題を提起するものである。[21]

スマートコントラクトめぐる契約上の問題をいち早く取り上げ、これを積極的に論じてきたのが、アメリカを中心とする諸外国の契約法である。アメリカにおけるスマートコントラクトに関する研究は、近年、極めて盛んである。[22] しかし、ブロックチェーン技術とスマートコントラクトとの関係、スマートコントラクトをめぐる契約上の効力や責任については未解決な問題や課題が少なくなく、議論はまだ始まったばかりである。[23]

本稿は、ブロックチェーン技術を基盤としこれに搭載されるスマートコントラクトについて、アメリカ契約法における議論を参考としながら、そのメカニズムを明らかにし、コードによって相互の合意を確保することの意味、コンセンサス・アルゴリズムによる合意形成と契約理論との関係を検討するものである。特定の法分野における既存の法的枠組みや規制を参照してスマートコントラクトの詳細な調査を行うことは、本稿の目的ではない。

本稿では、まず、スマートコントラクトの基盤となるブロックチェーン技術の先進性と特性、データ構造について分析する（二）。スマートコントラクトの抱える問題を法律的側面から解明するには、単にそれだけを取り上げて検

討するのではなく、スマートコントラクトの基盤となるブロックチェーン技術の基本的仕組み、その中で用いられるコンセンサス・アルゴリズムやコンピュータ上のプログラムコードといったシステム全体の構造を踏まえて行う必要がある。

次に、本稿は、ブロックチェーンに搭載されるスマートコントラクトについて、法律学の観点から、ブロックチェーン技術の特性を踏まえて、スマートコントラクトの意義、そのメリット、および問題点を整理する（三）。そのうえで、スマートコントラクトの活用が期待される主な適用場面を整理し、検討する（四）。

続いて、本稿では、ブロックチェーンベースのスマートコントラクトにおけるコンセンサス・アルゴリズムと複数主体間の合意形成および契約との関係を明らかにし、ネットワーク参加者によるコンセンサス・アルゴリズムは従来の伝統的な契約の基礎となる合意に準じて扱われることを指摘する（五）。

そして、最後に、ブロックチェーン技術およびスマートコントラクトの活用によってどのような未来が開かれようとしているのか、「分散型自律組織」（Decentralized Autonomous Organization: DAO）が創り出す世界についての展望を述べることにしたい（六）。

本稿で取り上げるテーマについては、まだ議論が始まったばかりで論点も明確ではない点が少なくない。法が社会の変容に的確に対応するには、まず、テクノロジーの進化がどのような社会の変化をもたらしているかを正しく理解しなければならない。そのうえで、そのような社会の変化が現在の法的枠組の中で処理できるかどうか、まず、この点を検討することが必要である。それにより、法が変革を迫られている問題点や課題が明らかになり、将来への対応が可能となるものと考える。

二　現代のスマートコントラクト

1　スマートコントラクトの現代的意義

スマートコントラクトは、前述したように、コンピュータプログラムにより特定の条件の発生時（if-then）に契約上の義務が自動的に履行されるようにプログラミングされている。その特徴は、コンピュータ上のプログラムコードを使用した契約の自動執行にある。当事者の一方が履行すべき範囲は、コンピュータ上のプログラムコードにおいて定められる。スマートコントラクトという用語のなかには、人間が恣意的な判断を下すことなく、アルゴリズムにより、またはネットワーク上のバーチャルな第三者（ＡＩや人工エージェントなど）を介して、契約が自動的に実行される場合も含まれる[24]。

このような特徴をもつスマートコントラクトは、契約の基本的要件である当事者間の合意や約束の相互交換を前提とするわけでなく、それ自体、コンピュータのプログラムコードにすぎないといった理解もありえよう。そのような観点からスマートコントラクトを性格づけるなら、スマートコントラクトは「電子コードにより表示されるプログラム」（programs represented by electronic code）[25]、あるいは、「コンピュータプロトコル」（computer protocol）[26]と呼ぶことができる。

ブロックチェーンが登場する以前にも、自動販売機などのようにスマートコントラクトといわれたものは存在した。古くは、古代ローマの属州であったアレキサンドリアにおいて、自動販売機の事例が見られる。当時、エジプトの寺院では、硬貨ドラクマが五枚投入されると、その重みでレバーが上に動いてバルブを開き、傾いた鍋に少量の聖水が

自動的に落ちてくる装置が開発されていたといわれる。[27] 現代に近いところでは、一七世紀のイギリスにおける図書の出版販売などにおいても自動販売機の事例が見られる。[28]

今日いうところのスマートコントラクトは、プログラムできる契約として、アメリカの法学者で暗号学者のニック・スザボ（Nick Szabo）が一九九〇年代に発表したスマートコントラクトに関する論文の中で登場し、その後広まって行った概念である。[29] スザボは、一例として、表示金額のお金を投入してボタンを押せば商品が出てくる自動販売機（vending machine）を取り上げ、特定の条件に合致すると契約が締結され、自動的に実行される契約をスマートコントラクトの概念を用いて説明した。

自動販売機の売買では、商品の内容や投入する金額は誰もが同じであり、時と場所で解釈が異なる余地はない。万が一お金を入れても商品が出てこないなどといった不具合があっても、返金ボタンでお金を取り戻すことができる仕組みとなっており、契約不履行のリスクも抑えられる。スザボによれば、スマートコントラクトは、「デジタル形式（digital form）で指定された一連の約束（a set of promises）で構成され、当事者がこれらの約束に基づいて実行する手順（protocols）を含む」ものである。[30]

自動販売機の仕組みは、法律上の観点からみると、非常に単純なものである。①あらかじめ契約条件を定義したうえで、②飲み物の代金を販売機に投入し購入したい飲み物のボタンを押すという条件を実行する、③自動販売機が対応した飲み物を出力するという契約を執行する、そして、④購入者は購入した飲み物を確認するという四つの段階を経ることで、プログラムされた契約が自動的に執行される。これは、「契約の事前定義→イベントの発生→契約の執行／価値の移転→決済」という一連の流れを全て自動化するものである。

このように、スマートコントラクトは、プログラミングされたコードに基づき、コードが特定の条件の発生時（if-then）に契約上の義務を自己実行するようにプログラミングされている。これは、スザボが説いたようにデジタル形式で記載された一連の約束がスマートコントラクトということができる。(31)

2　ブロックチェーン技術とスマートコントラクトの融合

今日、スマートコントラクトは日常にあふれていて、前述の自動販売機の例のほかにも、様々なサービスにおいてスマートコントラクトが活用されている。なかでも、スマートコントラクトは、分散型台帳のテクノロジーであるブロックチェーン技術と融合し、これを基盤に活用されることが多い。

ブロックチェーンは、前述したように、地理的に分散したピア・ツー・ピア（P2P）のネットワークを通じて、ネットワーク参加者のノード（PCやサーバなど）によって管理される分散型台帳（Decentralige Ledger Technology: DLT）である。(32) ブロックチェーンには、ピア・ツー・ピア（P2P）のネットワークやアルゴリズムコンセンスなどの技術が集積しており、このブロックチェーン技術を基盤とし、これに搭載されて用いられるのがスマートコントラクトである。ブロックチェーンは、ネットワーク参加者のコンピュータによって共同で保持される台帳技術であり、単一の障害点といったものはない。記録を保持している個々のコンピュータがハッキングされるとか、オフラインになった場合でも、他のコンピュータはそれなしで続行が可能であり、複数のコピーを同期させておくためのソリューションを提供できる利便性をもっている。一方、ブロックチェーンに実装されるスマートコントラクトは、二当事者間の取引に限定されない。プログラムコードを通じて、複数の当事者間の取引を管理することも可能である。契約の

自動化を図るスマートコントラクトと分散型台帳のテクノロジーであるブロックチェーン技術には親和性があり、両者を融合させた点にスマートコントラクトの現代的意義がある[33]。このようなスマートコントラクトをここでは「ブロックチェーンベースのスマートコントラクト」（Blockchain-based Smart Contract）と呼ぶことにしたい。ブロックチェーンベースのスマートコントラクトは、ブロックチェーン技術と融合した新たなテクノロジーということができる。

3　基盤となるブロックチェーン技術のデータ構造

ブロックチェーンは、複数の取引履歴などの情報をデータとして記録したブロックを鎖（チェーン）のように直列に連結したデータベースである。ブロックチェーンでは、ピア・ツー・ピア（P2P）のネットワークを通じて取引が行われると、取引記録がネットワーク参加者全員に向けて発信される。ブロックチェーンの各ブロックには、直前のブロック内容を表すハッシュ（hash）値というデータが書き込まれている。ネットワークの参加者はマイナー（miner：採掘者）として、ブロック内の自由に変更できる領域に適当な数（nonce：ナンス）を書き込み、ナンスの変更とハッシュ計算を繰り返しながら、目的の条件を満たすハッシュ値を見つけるまでノード（PCやサーバなど）に計算を行わせる。この計算で目的の条件に合うハッシュ値を最初に発見した者が、新しい取引記録をブロックとして追加する権利を獲得する。通常、ノードは一台単独で取引記録を作成し、取引の公正を担保するために、新しい記録をネットワーク参加者の他のノードに公開する。他のノードは、公開されたデータ構造に誤りがないかを検査し、問題がなければこれを別の他のノードに送信する。最終的にすべてのノードで問題がないことが確認されると、これが新しいブ

ロックに取り込まれることになる。この検証プロセスを「プルーフ・オブ・ワーク」（Proof of Work: PoW）という。プルーフ・オブ・ワーク（PoW）は、生成されたブロックが有効と認められるのに必要な証明を提供するものである。ブロックチェーンでは、プルーフ・オブ・ワーク（PoW）により必要な計算を最初に成功させた者がそのデータを承認して、正しくブロックチェーンにつなぎ込む役割を担うとともに、新しくブロックを生成した者は報酬として一定量のビットコインなどの仮想通貨（暗号資産）を取得するものとし、検証プロセスにインセンティブが働くように設計されている。また、個々のブロックには、タイムスタンプと前のブロックへのリンクも含まれている。[34]

このように、ブロックチェーンは、ネットワーク参加者のノード（PCやサーバー）を通じて、同じデータを複数の場所に分散して管理することから、「分散型台帳」（distributed ledger）と呼ばれる。[35] ちなみに、分散型とは、それがP2Pによって非中央集権的に実行されることを意味するが、集権型（centralized）に対比される分散型には、ローカルな中心が数か所ある場合の「分散型」（decentralized）と、全員が同じ立場で互いに連絡しあっている「分散型」（distributed）とがあり、英語の文献ではこれらが区別されている。[36]

スマートコントラクトの当初の定義では、スマートコントラクトはデジタル手段で資産を管理することと関連づけられていた。今では、ブロックチェーン上で展開または実行できる契約上のプログラムをスマートコントラクトと理解し、ブロックチェーン上の分散アプリケーションと同義と考えられている。[37] スマートコントラクトは、ブロックチェーンを基盤としこれに搭載される場合、ブロックチェーンのもつ不変性と分散化の特性を獲得し、単に契約の自動化と自己執行力をもったプログラムコードではなく、契約の自律性と自己執行力を保証する潜在的に用途の広い汎用性をもったアプリケーションの地位をえたといえる。

三　ブロックチェーンベースのスマートコントラクトと契約

1　ブロックチェーンを基盤とするスマートコントラクト

ブロックチェーンを基盤とするスマートコントラクトは、ブロックチェーンに保存されたプログラムコードであり、特定の条件が満たされたときに契約が自動的に実行される。特定の条件は、コードに記述された「if ／ when ～ then …（～なら、…する）」式の形式がとられる。所定の条件を定義するには、参加者が当該契約に関するデータについてブロックチェーンでどのように表現されるかを決め、契約実行のためのフレームワークを決定する。そして、事前に定義した条件と合致した場合にだけイベントを実行するように、プログラミングがなされる。

スマートコントラクトが搭載されるブロックチェーンは、各取引における取引情報をブロックに集め、それをチェーン（鎖）のように時系列の順に、暗号技術を用いてつないでいる。一つのブロックには、取引ごとにそれぞれのアカウントの残高や属性情報などが記録され、保管されている。ネットワーク参加者の各ノードは同じデータを保持していることから、データの変更はノード間で合意がないと認められない仕組みとなっている。

以下、スマートコントラクトの基盤となるブロックチェーンの先進性と特性について、法律学の観点から検討を加えることにする。

2　ブロックチェーン技術の革新性と特性

(1)　分散型台帳としてのブロックチェーン

ブロックチェーン技術は、従来型の情報システムと比べると、ピア・ツー・ピア（P2P）のネットワークを介した分散的な仕組みで運用され、中央の集権的な管理者が存在しないこと、分散化システムにより仲介者が排除され、清算と決済が簡素化されるため、取引が高速化されるとともに、取引費用が削減されること、単一障害点がなく、それによりシステムがダウンしないことなどに特徴がある。従来の取引は、銀行など信頼を確立した中央集権的な機関が仲介し、管理することで行われてきた。取引が正当であることを確認するために、多くの組織と人間が関与し、関係する書類の照合などをすることによって、処理してきた。これに対し、ブロックチェーンでは、そうした管理主体の代わりに、ピア・ツー・ピア（P2P）で結ばれた参加者のコンピュータのネットワークが取引の正しさをチェックすることで行われる。それが、後述のプルーフ・オブ・ワーク（PoW）の検証プロセスである。

(2)　ブロックチェーン技術の革新性

ブロックチェーン技術が革新的といわれる理由は、次の二つある。一つは、コンピュータサイエンス上の古典問題といわれた「ビザンチン将軍問題」（Byzantine Generals Problem）の解決策を提示しえたこと、もう一つは、それによってインターネット上に「価値」を流通させられるようになったことが挙げられる[38]。

第一の「ビザンチン将軍問題」とは、すでに前稿でも紹介したが、分散型ネットワークにおいて参加者の故障したノードから誤った情報が発信された場合、あるいは、悪意あるノードから意図的に偽りの情報が送信された場合に、

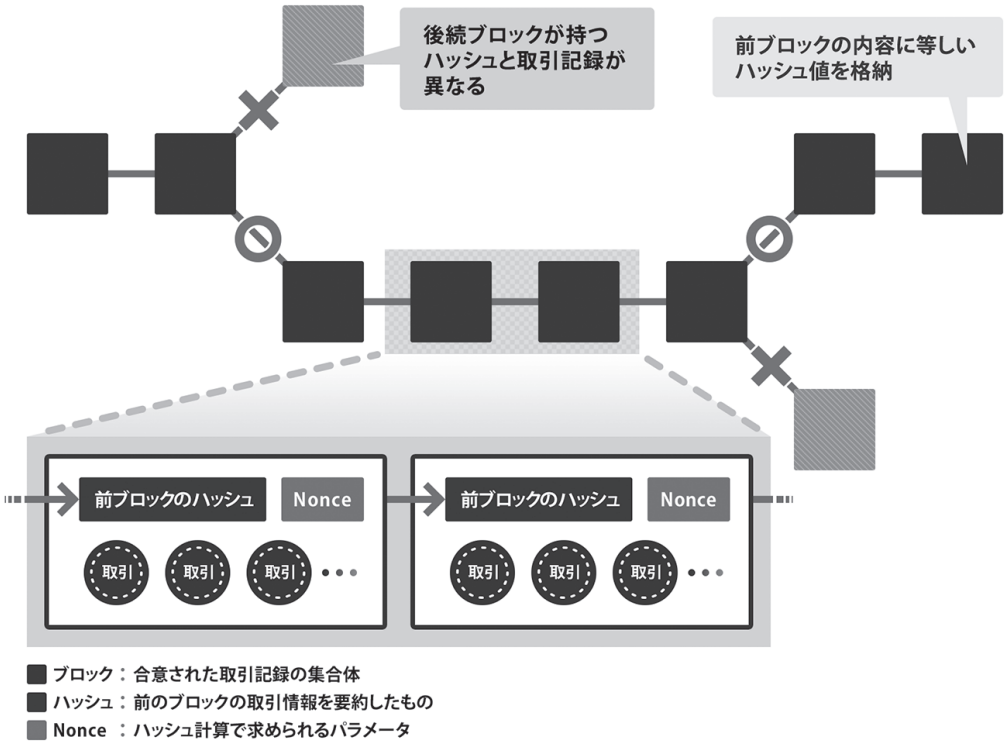
ネットワーク全体で正しい値を合意できるかという問題である。[39] 東ローマ帝国（ビザンチン帝国）の将軍らが戦場で抱えた問題に由来することから、この名が付けられた。[40]「ビザンチン障害耐性」（Byzantine Fault Tolerance: BFT）の問題と呼ばれることもある。

ビザンチン帝国の将軍たちがそれぞれ部隊を率いて敵を包囲している戦場において、各部隊はそれぞれ離れた場所におり、伝令を相互に送ることでしか連絡できないとした場合に、将軍たちの中に裏切り者がいても、誠実な将軍たちの判断を全員一致へと導く方法としては、裏切り者の将軍がN人のとき、誠実な将軍が2N＋1人以上であれば、誠実な将軍どうしの判断が一致させることができる。ランポートらは、この問題を耐性障害のある分散システムと利用者全体のコンセンサスの問題に置き換えることができるとし、間違った動作を行うコンピュータを裏切りの者の将軍、他の正常なコンピュータを誠実な将軍に見立てることで、複数の正常なコンピュータが同じ値をもつ方法やその条件を扱うことができるとした。

分散システムにおいてシステムが取引内容の改ざんや外部からの不正の攻撃により機能不全に陥った場合の問題については、今日、ランポートらの研究を踏まえて、ビザンチン障害耐性といった技術的な強みをもつことになった。ブロックチェーン技術は、この問題を確率的なコンセンサス・アルゴリズムによって解決することに成功し、その後の展開に新たな道を開くことになった。[41]

ブロックチェーンでは、前述したように、ナンスと呼ばれる適当な数値を用いて目的の条件を満たす数値（ハッシュ値）[42]をネットワーク参加者に計算させ、これを一番早く見つけた人を勝者とし、この者に報酬として一定量のビットコインなどの仮想通貨（暗号資産）を与えるとともに、新しい記録を他のネットワーク参加者に公開する。他

【図１】ブロックチェーンベースのスマートコントラクトと取引データ



（出典）　NTTDATA「ブロックチェーンの仕組み」
https://www.nttdata.com/jp/ja/services/blockchain/002/

のノードは、公開されたトランザクションに正しく署名がされているか、データ構造に誤りがないかを検査してから、問題がなければ他のノードにも伝搬させて、最終的に問題がないことが確認されると、これが新しいブロックに取り込まれることになる。[43] このような検証プロセスを経て、参加者間に合意があったものとするルールが採用されている。[44] この合意がコンセンサス・アルゴリズムである。プルーフ・オブ・ワーク（PoW）は、この検証プロセスにおいて生成されたブロックが有効と認められるのに必要な証明を提供するものである。

ブロックチェーンにおける各ブロックには、直前のブロック内容を表すハッシュ値というデータが書き込まれている。仮にデータを改ざんしようとしても、それによって導き出されるハッシュ値も異なり、それ以降のすべてのブロックのハッ

シュ値を変更することは極めて困難である。これに加えて、データの変更には、ブロックチェーンのネットワークに参加しているノードの過半数以上に対して同様の修正を実施しなければならない。各ノードの合意がとれないと、ブロックチェーンはフォークという形で分裂することになる[45]。ただ、フォークしたどちらの分岐も一方向の過去に向っており、どちらの分岐が切れるわけではない。元をたどればどちらの分岐も創設時のブロック（ジェネリックブロック）にたどりつく。自分が保有している資産はフォークしたどちらのチェーン上にも存在するから、失われることはない。保有資産を使うときに、どちらかのフォークで伸びたチェーンにブロックを積むかを検討することになる[46]。

第二の革新的理由としては、ブロックチェーン技術の出現により、インターネット上でビットコインなどの暗号通貨をはじめとする様々な価値を流通させることが可能となったことが挙げられる。分散型の台帳システムであるブロックチェーンでは、ピア・ツー・ピア（P2P）で結ばれた当事者間で第三者の仲介によることなく、あらゆる価値が自由に交換できるようになった[47]。こうした取引がブロックチェーンを基盤としてスマート化される場合には、トークンの流通性や兌換性が高まり、新しい経済が生まれる可能性がある[48]。例えば、ブロックチェーンで不動産をトークン化すると、今までは購入の契約や手続に司法書士などの専門職のサポートが必要であったが、ブロックチェーンを基盤としこれに搭載されるスマートコントラクトを利用することにより、自分一人でも不動産購入の契約が簡単にできることになる。

(3) ブロックチェーン技術のもつ特性

分散型台帳であるブロックチェーン技術の特性を整理してみると、ブロックチェーン技術は、①ピア・ツー・ピア（P2P）のネットワークで分散されたノードによってシステムを構成し、単一障害点を排除することによる高可用性、②トランザクションの履歴をハッシュ値で保持することによる改ざん耐性、③ノード間での自律的なデータ検証（コンセンサス・アルゴリズム）によるビザンチン障害耐性、そして、⑤真正な取引履歴の追跡可能性という強みをもっているといえる。[49]

① 高可用性

分散管理しているデータを各ノード間で常に共有しているため、一つのノードがダウンしても全体的なシステムダウンにはつながらない。

② 改ざん耐性

ブロックチェーン技術の仕組み自体がデータの改ざんを困難にさせる。

③ コンセンサス・アルゴリズムによるビザンチン障害耐性

各ノード間でデータの検証を自律的に行う仕組み（コンセンサス・アルゴリズム）によって、一部のノードが不正に利用されても、システム全体としては正常に作動する。

④ 追跡可能性

改ざんされていない真正な取引履歴のデータがネットワーク上のコンピュータに保存され、ネットワーク参加者の誰もがいつでも各自のノードを通じて同一のデータを閲覧し、確認することができる。

このようなブロックチェーンが提供する強みは、スマートコントラクトがブロックチェーンを基盤として利用される場合、これらの特性を標準装備として実装できる点にある[50]。ブロックチェーン技術の導入は、多くの場合、データの信頼性と透明性、追跡可能性の向上により、企業の信頼性を高めることにつながる。自律分散管理という特性をもつブロックチェーンは、これまでの集権的な社会や経済システムでは解決できなかった問題、例えば、企業間の横断的なシステムの構築、金銭以外の価値の流通、シェアリングエコノミーやモノのインターネット（IoT）などを解決できる可能性をもっている[51]。ブロックチェーンを基盤としこれにスマートコントラクトが搭載されるときには、両者が融合し、契約が人の手を介さず自動で執行され、不履行や不正のリスクが限りなく排除された効果をえることができるものと期待される[52]。ブロックチェーンベースのスマートコントラクトを用いた契約が多方面で普及するならば、後述するように規制やガバナンスについても今までとは違う捉え方が必要とされることになろう[53]。

3　ブロックチェーン技術が抱えるリスク

ブロックチェーン技術は、その特性の一つとして、外部からの不正な攻撃に対してビザンチン障害耐性といった技術的な強みをもっている。しかし、こうした耐性は絶対的なものではない[54]。例えば、ブロックチェーンにおける合意形成（コンセンサス・スルゴリズ）の手法であるプルーフ・オブ・ワーク（PoW）は、ネットワーク参加者のマイナーがブロックチェーンに新規のデータの塊（ブロック）を繋げる権利を競う計算による証明であるが[55]、ハッシュパワーの少ないチェーンでは期待通りにワークしないことが知られている[56]。そのような問題を回避するため、ブロックチェーンにおける合意形成のメカニズムには、仕事の量ではなく、保有するコイン（ネットワーク内でのトークン）の

量に応じて新規の追加ブロックが承認されるプルーフ・オブ・ステーク（Proof of Stake: PoS）という方式もある[57]。プルーフ・オブ・ステーク（PoS）は、後述するように、コインを多く保有していれば、それだけ高い確率でブロックを生成する権利が与えられる方法である。しかし、プルーフ・オブ・ステーク（PoS）で代替させるような場合であっても、既存のソフトウェアが正しく検証できないときは、ブロックチェーンはフォークという形で分裂することになる。フォークが起きた混乱の直後は、フォークで分かれたハッシュパワーが一時的に減少し、その分のセキュリティの強度が低下するため、外部からの攻撃に対して脆弱となる。

スマートコントラクトは、コンピュータプログラムに基づいて実行される契約の自動化であるので、コードのエラーや不具合、外部からのハッキングなどのシステミックリスクを引き起こす可能性がある。コードの脆弱性は、ピア・ツー・ピア（P2P）のネットワークで結びつけられているブロックチェーンベースのスマートコントラクトにあっては、そのコードで実行されるすべての取引に深刻な影響をもたらす恐れがある。

スマートコントラクトにおける契約上の紛争は、コンピュータ上のプログラムコードに関する不測の事態や契約条件の意味に関する意見の相違から生じることが多いが、コンピュータコードはそのような問題解決には対応していない。「合理的な配慮」（reasonable care）、「最善の努力」（best efforts）、「誠意」（good faith）などは、ありふれた解釈上の考慮要因ではあるが、コードで表現したり、コードに置き換えることは困難である。それをしようとすれば、多くの場合、複雑さが増すことになる。あらゆる事柄について交渉し、正確な条件でそれをコンピュータ上のプログラムコードに変換しようとすると、それに費やされる時間と労力が増え、契約費用が増加する。のみならず、コードの複雑さはバグの発生率も大幅に増加させることになる。

ところで、外部の第三者からの不正な攻撃に関しては、ブロックチェーンの改ざん耐性とその処理について問題を投げかけた事件として、「The DAO」事件がある。これは、二〇一六年四月、イーサリアムを用いて投資を行うThe DAOというベンチャーキャピタルファンドのプログラムコードがハッキングされ、約五二億円相当のイーサが盗取されたという事件である。ハッカー容疑者は、コードの契約条件に従ってイーサを引き出したにすぎず、不正はしていないと主張して争った。これに対し、イーサリアムの運営会社はハッキングされたコードを元に戻すために、「不正送金の取引自体を無効化する」といった決定をし、これを大多数の利用者が受け入れたことにより、事件は処理された[58]。しかし、ブロックチェーンには不変性があり、それが信頼の基礎である。修正されたコードを承認する大多数のユーザーの選択が優先されるべき理由は必ずしも明らかではない[59]。問題解決の選択肢としては、同じ価値の取引を逆に行うことで取引を実質的に元に戻すことは可能であった。大多数の利用者の判断は、失った資産の制御を取り戻したいという点で、明らかに利己的である。分割システムにおける責任の原理を探るべきであったとの見解もある[60]。この事件以後もかなりの数のユーザーが古いコードを使い続けたことから、イーサリアムには二つの並列したブロックチェーンが生まれた。ハードフォークで作成されたブロックチェーンはイーサリアム（ETH）して存続し、ハードフォークを拒否したブロックチェーンはイーサリアム・クラシック（ETC）としてメインのブロックチェーンから分離することになった[61]。

4　ブロックチェーンベースのスマートコントラクトと契約理論

(1)　プログラムコードを用いた合意

現代のスマートコントラクトは、ブロックチェーンを基盤としこれに搭載されることにより、ブロックチェーンのもつ不変性と分散化を獲得した。ブロックチェーンベースのスマートコントラクトは、単に契約の自動性と自己執行をもったプログラムコードではなく、潜在的に用途の広い可能性をもったアプリケーションである。ただ、スマートコントラクトがこのような汎用性を獲得するためには、前提としてプログラムコードが正確で完全に定義されたものである必要がある。そうでなければ、従来の契約よりも費用がかかり、効率が悪いということになる。

一般的に、ブロックチェーンベースのスマートコントラクトでは、「Xが発生した場合、Y個のトークンをアカウントAからアカウントBに送信する」というコードに基づき、契約上の義務が実行される形でプログラミングされている[62]。スマートコントラクトは、契約の成立および実行について可能な限り人的要素を排除し、契約の自動化と自己執行力を行わせるプログラムコードである。コードのプログラミングにあたっては、特定の契約条件ないし事項を定義し、それをコード化することから、人の入力と制御が必要となる。この点、ブロックチェーンベースのスマートコントラクトでは、そのコードは、ブロックチェーンに展開される前にオフチェーンで作成される。契約上の義務が履行されるためには、スマートコントラクトにおいて事前に契約条件を定める必要がある。事前の定義において相手方の存在を予定し、相手方がプログラムコードを受け入れ、これに追随することにより、契約の実行段階までには執行力のある契約の合意が形成されると考えられる[63]。取引の相手方は、契約が確実に実行されるという保証を通じて、契約上の利益を享受することになる。

契約上の義務は、契約当事者間において義務の源泉を構成する基本的な法的合意を必要とする。ほとんどの場合、契約当事者は契約をコードに翻訳する前に自然言語で交渉することになる。自然言語で適切に起草された契約の特定の側面（特定の条項や義務など）のみをコードを用いて自動化することになるが、コードを控えめに使用することでバグの数が制限され、基本的なエラーは法的合意に基づいてスマート条項の外で処理されることになる。

(2) オラクルによる契約事項の管理

ブロックチェーンベースのスマートコントラクトにおいて、アプリケーションとなるスマートコントラクトは、義務の発生源ではなく、特定の義務の履行を自動化するための技術的ツールである。ただ、法的な意味での契約ではないが、スマートコントラクトに法的な効果の発生を妨げるものは、何もない。法的拘束力をもつことを意図した合意はコンピュータのプログラムコードによって表示され、指示される。それでも、当事者の合意がコード全体で明示されることに、何の障害もない。自動化された契約履行のプロセスによって意思表示を行うことも、理論的には可能である。

ただ、ブロックチェーンベースのスマートコントラクトにおいて、契約の履行がオフチェーンイベントを条件とする場合には、契約当事者はコードを信頼するだけでは足らず、オフチェーン情報にアクセスして、特定事項の発生を確認することになる。その役割を果たすのが、いわゆるオラクル（oracle）である。オラクルは、外部のデータソースに基づいてオフチェーンイベントの発生を確認するサービスプロバイダーである。スマートコントラクトを機能させるためには、スマートコントラクトのプログラムコードだけでなく、オラクルと契約の履行を確認するために使用

するデータも必要とされる。[64]

(3) ネットワーク参加者による合意形成

前述したように、ブロックチェーンのデータ構造は、取引履歴などを書き込んだブロックがハッシュ関数により前後関係をもつように配列され、チェーンのように結びつけられる。新たなブロックを追加するときは、直前のブロックのハッシュ値と追加されるブロックに含まれるデータの整合性を確認して承認する作業が行われる。この承認作業が、いわゆるプルーフ・オブ・ワーク（PoW）である。プルーフ・オブ・ワーク（PoW）は、作業を最も早く完了させた者をブロックチェーンにデータを書き込める代表者とする合意形成のアルゴリズムであり、ブロックチェーンにおいて不正が行われていないことを証明するものである。各ブロックに格納された取引履歴などのデータは、プルーフ・オブ・ワーク（PoW）によって担保されているとみることができる。[65]

このほか、データの整合性を確認して承認する作業としては、保有コイン（暗号資産）の残高によってブロックチェーンへの書き込み可能な代表者を決める方法がある。これが、前述のプルーフ・オブ・ステークス（PoS）である。プルーフ・オブ・ワーク（PoW）による検証作業は、膨大な時間とCPUパワーを必要とすること、悪意をもったマイナーがネットワークの半数以上を支配する場合には不正操作が可能になることが問題点として挙げられる。これに対し、プルーフ・オブ・ステークス（PoS）は、CPUの処理能力による影響を受けず、消費電力も比較的少なくて済むことから、プルーフ・オブ・ワーク（PoW）の代替案といわれる。ただ、プルーフ・オブ・ステークス（PoS）については、暗号資産の保有量が多い人ほどマイニングしやすいため、暗号通貨を貯め込む人が増え、結果

的にその流動性が下がる可能性などが指摘され、その暗号資産（仮想通貨）の保有量だけでなく保有期間なども考慮し、特定の個人や組織に権限が集中する事態を回避しようとする別のタイプも存在する。[66]

四　ブロックチェーンを基盤とするスマートコントラクトの実装

1　スマートコントラクトの代表的なアプリケーション

今日、スマートコントラクトは、ブロックチェーンベース技術と深く結びつき、ブロックチェーンに搭載されて用いられることが多いことは、前述した通である。現在、スマートコントラクトの基盤となるブロックチェーンのプラットフォームとしては、イーサリアム（Ethereum）、ハイパーレジャー・ファブリック（Hyperledger Fabric）、および、その他の独自開発の三種類がよく知られている。[67] イーサリアムとハイパーレジャー・ファブリックは、いずれもオープンソースソフトウェアのブロックチェーンを使ったアプリケーションを開発・運営するためのプラットフォームである。独自開発のプラットフォームとしては、コルダ（Corda）やリペル（Ripple）、ミジン（Mijin）、ハイパーレジャー・イロハ（Hyperledger Iroha）、ミヤビ（Miyabi）などがある。このうち、代表的なものの一つがイーサリアムである。イーサリアムは、分散型取引システムのアプリケーションを構築するためのプラットフォームを立ち上げ、ブロックチェーンにスマートコントラクトを搭載することにより、ピア・ツー・ピアのネットワーク上において自動的に契約を実行することができるシステムを提供している。[68]

2　実装の主な利用場面

ブロックチェーンは、ピア・ツー・ピア（P2P）のネットワークを介した分散型台帳技術である。ブロックチェーン技術が抱えるリスクには注意すべきで点もあるが、それでもブロックチェーンがもつ不変性や改ざん耐性、ビザンチン障害耐性、追跡可能性といった特性は、社会に信頼を与えるインセンティブとして極めて有用である。現代のスマートコントラクトは、このようなブロックチェーンを基盤として、これに搭載されることが多い。スマートコントラクトは、特定の条件が満たされた場合に契約を自動的に実行するプログラムコードであるが、ブロックチェーンを基盤としこれに搭載される場合には、ブロックチェーンプラットフォームに実装されたソフトウェアコードの形で存在し、ブロックチェーンのもつ不変性と分散化を獲得するとともに、契約の自律性と自己実行力を保証するものといえる。ブロックチェーンベースのスマートコントラクトは、単に契約の自動化と自己執行力をもったプログラムコードではなく、潜在的に用途の広い可能性をもったアプリケーションであるといえる。

当初、スマートコントラクトは、ビットコインなどの仮想通貨の技術の中核となるブロックチェーンを基盤としてプログラミングされ、自動送金や送金記録の保存を図る分散型データベースとして金融取引を中心に活用されてきた。最近では、金融取引以外の分野でも、ブロックチェーンをシステム基盤とするスマートコントラクトの利用が拡大しており、様々な分野で実用化が検討されている[69]。

例えば、不動産業界では、契約に至るまでの必要書類が多いことのほか、仲介者が多数介在することによる不透明さがある。こうした問題を解消するために、ブロックチェーンベースのスマートコントラクトによる不動産情報の記録や管理の簡易化が期待されている。ブロックチェーンにより改ざん防止や過去取引の追跡が可能になれば、安全性

と信頼性を客観的に高められる。また、取引を自動化し、ブロックチェーンで管理すれば、手続の効率化や管理費用の削減、契約書の改ざん防止と共有化などを図れることが期待できる。

また、宅配便の受け取りや民泊などといった新しいサービス分野では、鍵の管理や受け渡し、宅配ボックスの利用、民泊や自動車／自転車のシェアリングサービスなどで、ブロックチェーン技術を用いたスマートコントラクトの応用実験が始まっている。ここでの特徴は、モノのインターネット（IoT）との連携が試行されている点にある。例えば、宅配事業では、受取人が指定した、駅やコンビニのロッカーを使って荷物を受け渡す際に、正規の受取人だけが指定したロッカーのカギを開け、荷物を取り出せるシステムが導入されている。宅配業者が荷物を入れた記録や、カギの情報、受取人が取り出した記録などをブロックチェーンで管理すれば、改ざんもできず、確実に荷物をやり取りできる。加えて、伝票類も電子化できるため、配送業務の効率化や利便性も高められる。宅配業界では、不在時の再配達が人手不足と重なり大きな問題になっており、ブロックチェーンベースのスマートコントラクトはその解決策となりうることが期待されている。

このほか、企業ガバナンスにもスマートコントラクトの利用が検討されている。今日、企業や法人は、法的ルールや明文化された文書によって統治されているが、ブロックチェーンを用いると、組織はコードを用いてそのようなルールや手続の一部を実施できる。例えば、取締役の選任といった企業の活動は、もはや文書の送達や安全な電子代理サービスを必要としない。それらの管理はブロックチェーンを通じて行うことができる。利益の配当や損益の分配はスマートコントラクトを用いれば自動的になされるから、関連する支払いを管理する会計士や事務管理部門の従業員の必要性はなくなる。

ブロックチェーンに関する国内外動向調査をみると、金融取引以外で広がるブロックチェーンビジネスとしては、エネルギー・資源・鉱業、エンターテイメント&メディア、テクノロジー、ヘルスケア、サプライチェーン（消費財・小売・流通・運輸・物流）、官公庁・公的機関、自動車、重工業・産業機械、情報通信、不動産などの分野が挙げられる。[70]

ブロックチェーンビジネスの活用事例からみた新しい経済の見取り図としては、電力の産地価値証明、サプライチェーンのトレーサビリティ、二酸化炭素排出削減量の可視化とカーボン・オフセット、不動産の権利管理、学歴や資格の記録、記事の価値の可視化、ＩｏＴ機器のプログラム保証、人に紐づく履歴の管理、契約の自動化、契約書の共有・保管・電子契約、行政サービス利用手続のペーパーレス化、人と人との関係性の可視化などが挙げられる。[71]

3　実装における留意点

ブロックチェーン技術およびそれに搭載されるスマートコントラクトについては、実用化が試みられているもののいまだ完成されたものではなく、プログラムの誤りや欠陥（バグ）、データの改ざんが発生する可能性があるなど、改良すべき点がいくつか残されている。ピア・ツー・ピア（P2P）のネットワークを利用した分散システムが真に信頼できるものであるためには、取引内容の証明や取引量の正確性を担保し、支払いや決済のリスクが存在しないことを示す枠組みを構築する必要がある。この点は、ブロックチェーン技術を実装する際に、極めて重要な問題を提起する。

プログラムを作成する技術者には、何はさておき、バグのないコードの作成が求められる。ブロックチェーンに関

するリスクは、個々のブロックチェーンで採用されているアルゴリズムやブロックチェーンを管理する主体の有無によって異なる部分もあり、ガバナンスが適切に整備・運用されていることを証明することは容易ではない[72]。ブロックチェーン上で機能するスマートコントラクトなどのプログラムには、利用者が意図していない動作が記述されていないことを保証することが必要である[73]。また、複雑なコントラクトを書こうとすると、開発者が想定できなかった動きがバグとして混入することがあり、このような事態は避けなければならない。そのためには、より多くのテスト環境や検証装置を充実させて、効率よくバグのないコードを作成できる環境が必要となる[74]。

一方、利用者の側にも、ブロックチェーンがピア・ツー・ピア（P2P）のネットワークを介した分散型台帳技術であることを十分認識して、パスワードや情報の自己管理が求められる。パスワードを紛失したような場合、パスワードを再生成できる情報を別の装置によりバックアップするシステムの構築など、パスワードや情報の自己管理は必要不可欠である[75]。

ブロックチェーン技術が抱えるリスクには注意すべき点がいくつかあるが、それでもブロックチェーンがもつ不変性、改ざん耐性やビザンチン障害耐性、追跡可能性といった特性は社会に信頼を与えるインセンティブとして極めて有用であることを示している。ブロックチェーンをシステム基盤としてスマートコントラクトが実装される場合、これらの特性がスマートコントラクトにも標準機能として備わることになる。後述するように、ブロックチェーン技術とスマートコントラクトには、自律的な分散型共生社会を創設する原動力がある。スマートコントラクトの実装にあたっては、この点に留意する必要がある。

五　スマートコントラクトとコードによる規律

1　デジタル合意としてのスマートコントラクト

スマートコントラクトは、事前に定義された特定の条件が満たされた場合に契約を自動的に実行できるプログラムコードである。スマートコントラクトがブロックチェーンをシステム基盤としこれに搭載される場合には、ブロックチェーンプラットフォームに実装されたソフトウェアコードの形で存在する。スマートコントラクトでは、人間の関与を極力排除し、あらかじめコンピュータプログラムに埋め込まれた条件に従って契約は自動的に実行される。人が契約条項を読むといった義務や機会は著しく制限されており、従来の契約が要求する意思の合致などの基本的要件はスマートコントラクトには見られない(76)。スマートコントラクトのプログラムコードは、人の意思表示に代わる表現形式であるが、一方的なものであり、相手方の同意や承諾を前提とするものではない(77)。このような契約の基本的要件を欠くスマートコントラクトについては、契約を意味するコントラクトという名称が用いられるにしても、これを直ちに契約ということはできないという考え方もありえよう(78)。

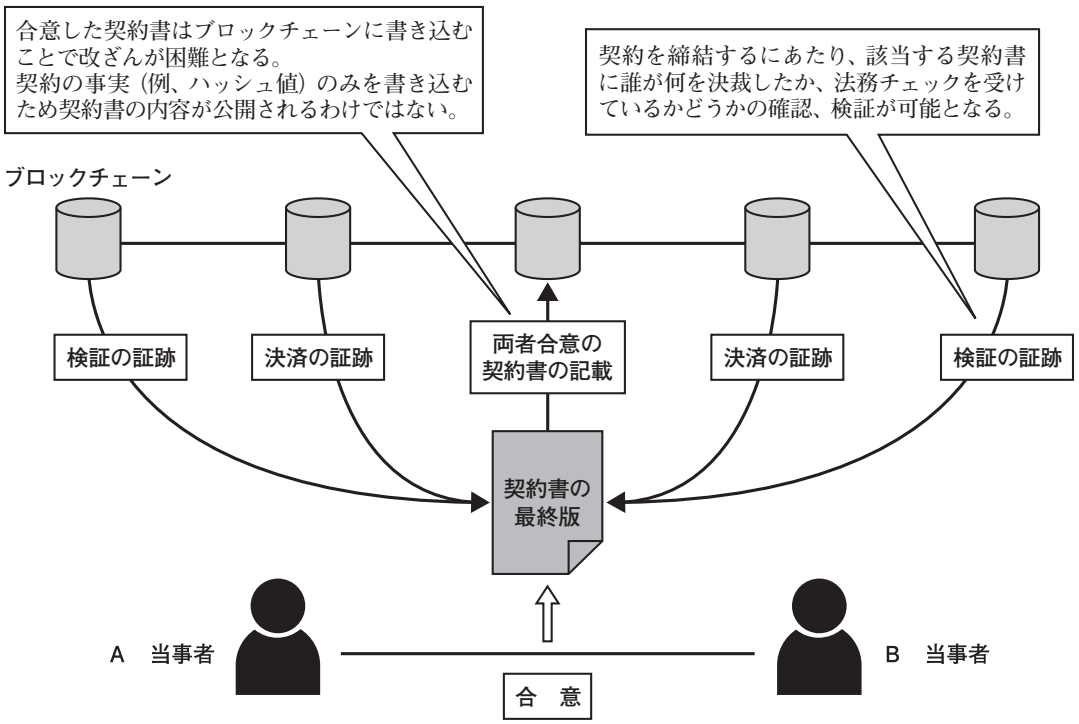
伝統的な契約理論は、契約の成立において人間の精神作用である意思的関与を必要とし、当事者の一方の申込とそれに対する相手方の承諾という相対立する意思表示の合致を要求した。意思の自律と私的自治が支配する伝統的な契約理論の下においては、合意は契約の成立にとって必要かつ不可欠な要件である。相手方が契約に寄せた信頼が重視され、契約上の義務に違反した場合には、損害賠償が課せられることになる。これに対し、スマートコントラクトは機械志向の契約であり、当事者の一方がインターネット上のプラットフォームに定めたコードをもって契約の条件を

提示し、他方の行為がコード化された特定の契約条件に合致すると、即時に契約上の義務が履行される。契約の成立と履行が自動化され、契約上の義務が即時に担保される仕組みが、スマートコントラクトである[79]。ここには、契約を構成する申込と承諾や当事者の合意といったものはない。それゆえ、スマートコントラクトについては、これを契約と評価することはできず、契約の概念それ自体に根本的な問題が投げかけられている[80]。

しかし、スマートコントラクトがブロックチェーンを基盤としこれに搭載して用いられる場合には、それに代わるべきものとして、コンセンサス・アルゴリズムというネットワーク参加者の全員による合意形成といった仕組みがブロックチェーンには盛り込まれている。これは軽視すべきではないように思われる。このような合意形成は、これを伝統的な契約理論でいう意思表示の合致という意味での契約と同様に考えることはできないが、契約締結に関する人の意思はコードによる契約の事前の定義の中に含まれており、また、コンセンサス・アルゴリズムという形で行われている。このような合意方法は信頼性の高いものであり、契約の実効性を実質的に担保するものである。そうであれば、これを「デジタル合意」（digital agreement）と評価し、従来の契約における合意と同様にあるいはそれに準じて扱うことは許されよう[81]。その意味で、ブロックチェーンベースのスマートコントラクトは、デジタル合意による契約を構築する契機をもっているといえる[82]。このような合意は、「デジタル形式で記載された一連の約束」（a set of promises, specified in digital form）ということができる[83]。

以上のように考えてみると、スマートコントラクトを、それ自体、契約当事者間における合意や約束の相互交換がないとか、紛争が生じた場合に人の判断を入れた柔軟な是正措置の余地がないといった形式的理由だけで、契約の拘束力を否定することは軽率である。ブロックチェーンベースのスマートコントラクトにあっては、プログラムコードに

【図２】契約の自動化、契約書の共有・保管



（出所）　正田正樹ほか『ブロックチェーンがひらく「あたらしい経済」』（幻冬舎、2020年）89頁を参考に作成（ただし一部修正）

よる契約の事前の定義を前提に、第三者の仲介を要することなく取引を効率化し、契約上の義務の履行を確保する点に主眼がある。[84] スマートコントラクトをブロックチェーンに搭載する場合には、単に契約が自動化され、執行されるだけでなく、契約書や契約に関する各種ドキュメントの保管・管理の効率化につながる。[85] 合意した契約は、これをブロックチェーンに書き込むことで改ざんを阻止するとともに、該当する契約書に誰が何を決裁したのか、法務チェックを受けているのかなどの確認、検証が可能である。契約のどの段階で、誰がどのような書類に承認したのかという記録が残されることから、責任の所在を明確にすることができる。[86] そのような観点からすると、伝統的な契約理論と必ずしも敵対する関係にあるというわけではない。むしろ、問題は、スマートコントラクトについて、その特徴ないし本質を踏まえて、まず、誰と誰との間にどのような契約が成立しているのか、当事者は何に合意

しているのかを明らかにすることが必要である[87]。重要なことは、ブロックチェーンベースのスマートコントラクトを伝統的な契約理論の中にどのように位置づけ、調和をもって運用して行くか、このことが求められるといえよう。

2　プログラムコードによる規律

これまで検討してきたように、スマートコントラクトは、特定の条件が満たされた場合に契約を自動的に実行するプログラムコードである。コードのプログラミングにあたっては、特定の契約条件ないし事項を定義し、それをコード化することから、人の入力と制御が必要となる。ほとんどの場合、自然言語で適切に起草された契約の特定の側面をコードを用いて自動化する。スマートコントラクトは、義務の発生源ではなく、特定の義務行為を自動化するための技術的なツールである。スマートコントラクトには法的効果の発生を妨げるものは何もない。法的効果をもつことを意図した当事者の合意は、コンピュータのプログラムコードによって表示され、指示される。理論的には、当事者の合意がコード全体で示されることに、何ら障害はない。当事者は、自動化された契約履行のプロセスによって意思表示を行うことも可能である。

スマートコントラクトを契約として用いるメリットとしては、コード化されたプログラムコードによる契約の実行により、契約費用を低減化し、契約締結を迅速に行うことが強調されがちであるが、次の点も見落とすことができない。まず、スマートコントラクトはコード化されたコンピュータプログラムであり、自然言語に固有のあいまいさから生じる不透明さに対処することができる。次に、スマートコントラクトにおいては、コンピュータプログラムが契約を自ら実行するため、契約条件が司法審査の対象とならないことを保証している。また、スマートコントラクトが

裁判所などの国家権力の介入を阻止し、外部からの不当な干渉を排除する点は、国家権力の個人の自治への従属を促進する要因をもっている。スマートコントラクトはこれをコード化されたコンピュータプログラムを用いて達成しようとするものであり、より効率的な方法で当事者の自律性を強化するものといえる。これに加えて、スマートコントラクトに携わる弁護士は、コードに実装する必要のある決まり文句（ボイラープレート条項）を特定してプログラミングすることにより、貴重な時間をより知的な仕事に集中させることが可能となる。

スマートコントラクトによる契約において、スマートコントラクトがブロックチェーンベースを基盤としこれに搭載されて利用される場合、スマートコントラクトは、単なる契約の自動化と自己執行力をもったプログラムコードではなく、ブロックチェーンプラットフォームに実装されたソフトウエアとして、ブロックチェーンのもつ不変性や改ざん耐性などの機能を標準装備し、運用されることになる。この点は、ブロックチェーンベースのスマートコントラクトの最大の強みといえる。

ただ、スマートコントラクトは、コンピュータプログラムに基づいて実行される契約であるので、コードのエラーやバグの発生、外部からのハッキングなどにより、システミックリスクを引き起こす可能性がある。このような場合でも、スマートコントラクトはこれを排除することはできず、契約は実行される。コードの脆弱性は、そのコードだけの問題ではなく、ピア・ツー・ピア（P2P）のネットワークで結びつけられているブロックチェーンベースのスマートコントラクトにあっては、そのコードで実行されるすべての取引に影響をもたらす可能性がある。当事者間に紛争が生じた場合には、紛争解決のために裁判所や弁護士などの第三者による司法支援は必要である。

また、契約の履行がオフチェーンイベントを条件とする場合には、当事者はコードを信頼するだけでは足らず、オ

フチェーン情報にアクセスして、特定事項の発生を確認する必要がある。その役割を果たすのがオラクルである。スマートコントラクトを機能させるためには、スマートコントラクトのプログラムコードだけでなく、オラクルと契約の履行を確認するために使用するデータも必要となる。

ブロックチェーンに搭載されて利用されるスマートコントラクトは、コードによる厳格かつ形式化されたルールを用いて人間の行為を形成し、制約する機能をもっている。この点において、法的合意のコードへの変換がみられる。問題は、コードは人間の行動に影響を与える規制手段として、果たして法や規則と並び立つものかどうかである。

一般に、法や規制は、人間が特定の仕方で行為するように行動を導くという目標をもって設けられる。ブロックチェーン技術やスマートコントラクトといった新しいテクノロジーも人間の行動に影響を与える同様の力をもっているが、法や規則とは異なり、人間がとるべき行動の方針を決定できる余地をほとんど残していない。スマートコントラクトによる契約の検討にあたっては、メリットのみならず、デメリットについてもこれを冷静に見つめ、コードによる規律への対応を同時に考える必要がある。

スマートコントラクトは、ブロックチェーンプラットフォームに実装されたソフトウェアコードの契約であり、コンピュータ上のプログラムコードをもって特定の条件の発生時に契約上の義務が自動的に履行されるように設計されている。ローレンス・レッシング教授は、一九九五年に『コード（CODE）』という書籍を出版し、その中で、技術的なコードがルールを作っていると指摘した[88]。法律ではなく、コードによって相互の意思を確保することは法的にどのような意味を有するのか、人はどこまでコードにより規律されるかという問題提起は、後述するように、ブロックチェーンベースのスマートコントラクトにおける契約概念を考えるとき、きわめて重要の意味をもつといえる[89]。

アメリカでは、スマートコントラクトの時代の変革をいち早く察知し、法律学者や弁護士、立法機関などは、ブロックチェーン技術を活用したスマートコントラクトに多くの関心と期待を寄せ、従来の契約法理との関係や理論的な問題点の把握、分散型台帳システムに基づく取引の管理やそのためのコンプライアンスガイドラインの策定などについて、検討の必要性が指摘されている[90]。そして、現在、こうした指摘を受けて、各州において検討が始められている[91]。

3　ネットワーク参加者のデジタル連帯責任

ブロックチェーンを基盤として実装されるスマートコントラクトにおいて契約当事者間にトラブルが発生した場合に、法ではなくコードという技術的な対応によって問題の解決を図ることは果たして可能なのであろうか[92]。機械志向の契約であるスマートコントラクトであっても、コード化された条件の解釈が事後的に問題となったり、システムにバグが生じたりするなどして、当事者間に利害の対立や損害が生じることがある。このような場合、当事者間の紛争はどのように解決されるのか、その責任はどのように考えられるかどうかである[93]。

この問題は、通常、損害賠償あるいは原状回復によって処理されることになると考えられる。損害賠償によるとした場合、その賠償は、履行利益の賠償でもなければ、利益の吐き出し的な損害の賠償でもなく、コードの破損やプログラム相互間の不整合が発生する前の元の状態に戻すことを目的とした信頼利益の賠償と考えられる[94]。ただ、仮にそうであるとしても、この損害を誰が、どのような方法で、いかに負担するのかということについては、さらに検討を要する。この問題は、これまであまり論じられることはなかったが、最近ではスマートコントラクトにおける紛争解

決処理として積極的に取り上げられ、議論が盛んである。[95]

損害賠償の方法による問題解決にあたっては、ネットワーク参加者が紛争解決のための基金を提供することが考えられる。[96] これは、各参加者が取引履歴の検証と認証にあたり一定額のトークン（仮想通貨など）を提供し、契約上の損害を補償するために使用するというものである。このような解決方法は、仮想通貨を失ったユーザーの救済のために使用されることから自動車保険に似ているともいわれるが、従来の合意による「契約上の連帯」（contractual solidarity）から「デジタル連帯」（digital solidality）への移行を示すものといえる。[97]

紛争の最終的な解決は、これまで裁判所の役割とされてきた。しかし、日々進展する新たなテクノロジーの下で、裁判者がスマートコントラクトに関する紛争の実態を正しく認識し、解明することは極めて難しい。この問題の解決策は、まだ議論が始まったばかりで明確ではない。現時点では、法律による規制を待つのではなく、プログラムコードの中に契約上の債務の履行に関する紛争や契約そのものを修正する機能を備えさせることが、スマートコントラクトの今後の課題であるといえよう。紛争解決機能を備えたスマートコントラクトは、従来の裁判所による伝統的な紛争解決に大きな影響を与えることになるものと思われる。

六　ブロックチェーンベースのスマートコントラクトが創り出すＤＡＯの世界

ブロックチェーン技術の開発とこれを基盤とするスマートコントラクトの活用によって、どのような未来が開かれようとしているのか。人は、元来、小さなコミュニティの中でお互いに助け合って暮らしを立てていた。コミュニ

ティ社会では、思想や趣味が一致する人たちが共通の価値を定め、これを保有する。お互いが共通認識できる形で価値の受け渡しを行い、特権的な管理者を作ることなく、自律できる社会であった。それが社会経済の発展に伴い友好的にまたは敵対的に統合され、組織化されることにより、現在のような社会の形となった[98]。現在の社会は、組織化と一緒にルール化も進み、複雑に階層化された社会である。これに対し、ブロックチェーン技術をシステム基盤とする分散型の社会は、ブロックチェーンプラットフォームに実装されるスマートコントラクトなどのソフトウエアコードをアプリケーションとして用いながら構築される「分散型自律組織」（Decentralized Autonomous Organization: DAO）が中核となる社会である[99]。ブロックチェーンは、取引履歴などのデータの保存と情報の管理を分散化するだけでなく、取引に関するネットワーク参加者全員の合意をコンセンサス・アルゴリズムにより形成させる機能を有しており、民主的で参加型の意思決定を伴う新しいガバナンスの開発にも役立ちうる。一方、スマートコントラクトは、特定の条件が満たされた場合に契約を自動的に実行するプログラムコードであるが、コードを通じて組織の運営や規律を設けることができる。ブロックチェーン技術の出現により、これと親和性のあるスマートコントラクトが融合し、新たな世界が創られようとしている[100]。

ＤＡＯが創り出す世界は、コンピュータプログラムを通じて、すべてがコードによって実行され、完全に透過的で自律した分割型の共生社会である[101]。分散システムが正しく運用されているかどうかは、ネットワーク利用者が相互に監視し、ルールから外れるものをチェックするという仕組みである[102]。ネットワークを通じた利用者間においては、文化基盤の再生として住民同士の交流を生み、シェアリングエコノミーやトークンなどを誘発する起爆剤となりうる要因をもっている。

ところで、ブロックチェーンベースの分散システムとそのアプリケーションであるスマートコントラクトのコードは、法的ルールを形成する機能を備えているため、現在の規制の枠組みである「法の支配」に取って代わりうるかどうか、「法律としてのコード」という問題を提起する。この問題については、近年、法学者の間でも関心が高まっている[103]。

一九九〇年代後半にレッシングが提唱した有名な方程式「コードは法律である」（code is law）は、今日、まったく新しい意味合いをもって理解されるようになっている。レッシングは、インターネットのアーキテクチャがインターネットを使用できる条件を設定し、それによってその空間で何が可能であるかを説いた。これに対し、この方程式を逆転させ、法律自体を成文化してコードとして定義できるとする考え方、すなわち「法律としてのコード」（code as law）が提唱されている[104]。

コードは、スマートコントラクトなどのブロックチェーンアプリケーションの動作を規制する際に、市場の原理、慣習、法律と密接に関連しており、これらと必然的に相互作用する。社会における規制のガバナンスは、法律のみならず、市場原理や慣習によって支えられ、また、コードによっても形成される。これらが相互に絡み合いながら、人々の間に信頼をもたらし、市場経済における商業関係を生み出し、人間関係を維持するうえでの共存するメカニズムを作り出す。ブロックチェーンベースのスマートコントラクトが法律に与える影響を検討するにあたっては、これらの規制モードを除外し、コードだけを取り上げて議論してもあまり意味はない。コードによる規律を考えるうえでは、コードを市場の原理、慣習、および法律と並ぶ社会的規範の一つに位置づけて検討することが求められる[105]。

法律としてのコードの問題については、コードによって最適化できる契約や取引に限定されるといった制限がある

ほか、コードのバグやハッキングの可能性は不可避である。当事者は、これらに起因して紛争が発生した場合のリスクの配分について、事前に検討しておく必要がある。契約の不履行や曖昧さなどをめぐって当事者間に紛争を生じた場合には、前述したように、別途、調停や仲裁、裁判所による紛争処理が必要となるなど、課題も多く残されている。[106]

七　結　語

本稿は、ブロックチェーン技術を基盤としこれに搭載されるスマートコントラクト（ブロックチェーンベースのスマートコントラクト）について、そのメカニズムを明らかにし、コードによって相互の合意を確保することの意味や、コンセンサス・アルゴリズムによる合意形成と契約との関係を検討したものである。スマートコントラクトは、契約成立の基礎を当事者間の合意や約束に求めるのではなく、プログラムコードに基づき、契約の締結および実行を自動化するものである。いわばコードによる機械志向の契約である。これを既存の法体系にどのように位置づけ、どのように取り込んで行くのか。これが、本稿の検討課題であった。本稿では、この検討課題に取り組むにあたり、スマートコントラクトの基盤となるブロックチェーンの特性を踏まえ、アルゴリズムやコードなどのコンピュータプログラムを含むシステム全体の構造、ブロックチェーンの仕組みなどを、法律学の観点から分析した。

本稿の検討によれば、スマートコントラクトの基盤となるブロックチェーンでは、ピア・ツー・ピア（P2P）のネットワーク参加者の検証を経て、有効な取引履歴として承認されたものがブロックがチェーンに追加される仕組み

となっている。これにより、取引履歴に関する情報などに不正がないかどうかが確認され、コンセンサス・アルゴリズムという形での合意形成が行われている。このような合意形成は、信頼性の高いものであり、契約の実効性を実質的に担保するものである。そうであれば、これを従来の契約における合意と同様にあるいはそれに準じて扱うことは許されるのではないかと考えられる。本稿では、これを「デジタル合意」と称し、ブロックチェーンベースのスマートコントラクトにおいても契約を形成する要因をもっていることを指摘した。スマートコントラクトによる契約の法律構成を考えるうえでは、コードに対する参加者全員の同意という理論構成が有用であり、コードのエラーやバグ、第三者によるハッキング、契約の意味内容や解釈について紛争が生じた場合の責任についても、デジタル合意を基礎に、参加者全員にデジタル連帯責任を追及して行くことが可能であるように思われる。

ブロックチェーンの技術は、本稿でも指摘したように革新的技術であり、社会を変容させる可能性を秘めている。このブロックチェーン技術、およびこれと融合したスマートコントラクトを用いることによって、人は自らの手を介することなく契約を自動的に執行することが可能となり、不履行や不正のリスクが限りなく排除された世界を創り出すことができる。現代のスマートコントラクトは、このブロックチェーン技術と結び付くことにより、既存の流通システムや法体系を大きく変容させる力をえたといえる。その様相は様々であるが、共有化されたデータの保存や管理、利用などにとどまらず、既存の産業や社会構造に対する変革をもたらし、自律した分散型の共生社会の到来を予感させるものがある。

（1）　長谷川貞之「スマートコントラクトによる契約と伝統的契約理論」日本法学八六巻二＝三号（二〇二〇年）三九頁。

（2）　ビットバンク株式会社＆『ブロックチェーンの衝撃』編集委員会『ブロックチェーンの衝撃』（日経ＰＢ社、二〇一六年）二〇八頁以下。Scott A. McKinney et al., *Smart Contract, Blockchain, and the Next Frontier of Transactional Law*, 13 Wash. J. L. Tech. & Arts. 313, 340 ff. (2018)。

（3）　アマゾン（Amazon）やウォルマート（Walmart）などの大企業は、ブロックチェーンベースのスマートコントラクトに大きく依存している。Alex Murray et al., *Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance*, [2019] Academy of Management Perspectives 36-42.

（4）　ブロックチェーン技術につき、赤羽善治・愛敬真生『ブロックチェーン仕組みと理論［増補改訂版］』（リックテレコム、二〇一九年）三六頁以下、コンセンサス・ベイス株式会社『ブロックチェーンのしくみと開発がこれ一冊でしっかりわかる教科書』（技術評論社、二〇一九年）一〇頁以下、森川夢佑斗『これからのブロックチェーンビジネス』（ＭｄＮ、二〇一八年）一二頁以下、ビットバンク株式会社ほか・前掲注（2）二頁以下、リテシュ・モディ／花村直親ほか訳『Solidityプログラミング：ブロックチェーン・スマートコントラクト開発入門』（講談社、二〇一九年）二頁以下、山崎重一郎ほか『ブロックチェーン技術概論：理論と実践』（講談社、二〇二一年）など。欧語文献として、JAMES A. COX AND MARK W. RAUSMUSSEN (EDS.), BLOCKCHAIN FOR BUSINESS LAWYERS, Science & Technology Law 2019, pp. 1 ff.; MICHELE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE, Cambridge University Press 2019, pp. 1 ff.; KEVIN WERBACH, TTHE BLOCKCHAIN AND THE NEW ARCHITECHTURE OF TRUST, MIT Press 2018, pp. 71 ff. のほか、Thibault Schrepel, *Collision by Blockchain and Smart Contract*, 33 Harv. J. L. & Tech. 117 (219); Giasella Finochiano & Chantal Bomprezzi, *A Legal Analysis of the Uses of Blockchain Technology for the Formation of Smart Legal Contracts*, 19 Media Law 20 (220); Mckinney, *supra* note 2, at 313; Philip Peach, *The Governance of Blockchain Financial Networks*, 80 M. L. R. 1073 (2017); IMRAN BASHIR, MASTERING BLOCKCHAIN SECOND EDITION, Packet 2018. pp. 9 ff. など。

（5）　ビットバンク株式会社ほか・前掲注（2）二六五頁。

(6) PwCあらた有限責任監査法人［編］『ブロックチェーンをビジネスで活用する：新規事業の創出とガバナンス・関連制度』（中央経済社、二〇二一年）一一三頁。

(7) Jared Arcari, *Decoding Smart Contracts: Technology, Legitimacy, & Legislative Uniformity*, 24 Fordham J. Corp. & Fin. L. 363 (2019); Blaise Carron and Valentin Botteron, *How Smart can a Contract be ?*, in BLOCKCHAINS, SMART CONTRACTS, DECENTRALISIDE AUTOMOUS ORGANISATIONS AND THE LAW, edited by DANIEL KRAUS et al. Elger 2018, pp. 101 ff.; Valentina Gatteschi et al., *Technology of Smart Contracts*, in THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORMS, edited by LARRY A. DIMATTIO, et al., Cambridge University Press 2020, pp. 37 ff. など。

(8) IoTの進展について、総務省編『IoT・ビッグデータ・AI：ネットワークとデータが創造する新たな価値』〈情報通信白書平成二八年版〉（発売・全国官報販売協同組合、二〇一六年）八〇頁以下。IoTに関する国内外の取組みについて、総務省編・前掲書一一一頁以下。スマートコントラクトとIoTとの関係につき、IoT産業技術研究会『未来IT図解これからのIoTビジネス』（MdN、二〇一八年）一一頁以下、高橋郁夫ほか編著『デジタル法務の実務Q&A』（日本加除出版、二〇一八年）一二三頁以下、福岡真之介編『IoT・AIの法律と戦略』（商事法務、二〇一七年）一頁以下、八子知礼編著『IoTの基本・仕組み・重要事項が全部わかる教科書』（SB Creative、二〇一七年）一頁以下、IoT検定ユーザー教育推進ワーキンググループ『図解戦力IoTのしくみと技術がこれ一冊でしっかりわかる教科書』（技術評論社、二〇二〇年）一二〇頁以下、DIAMONDハーバード・ビジネス・レビュー編集部編『IoTの衝撃』（ダイヤモンド社、二〇一六年）一〇頁以下など。欧語文献では、Iran Giuffrida et al., *A Legal Perspective on the Trial and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies will Affect the Law*, 68 Case W. Res. L. Rev. 747 (2018); Anthony J. Bellia, *Contracting with Electronic Agents*, 50 Emory L. J. 1047 (2001) など。

(9) 八子編著・前掲注(8)四一頁以下、IoT産業技術研究会・前掲注(8)五七頁以下、一一四頁。

(10) Arcari *supra* note 5, at 365; Schrepel, *supra* note 4, at 142; Finochiaro & Bomprezzi, *supra* note 4, at113; Mckinney et

al, *supra* note 2, at 317. ブロックチェーンの出現後は、各種のプラットフォームを介してブロックチェーンに搭載されて、分散型取引データの記録台帳の役割も果たすようになった。Dickson C. Chin, *Smart Code and Smart Contracts*, in BLOCKCHAIN FOR BUSINESS LAWYERS, edited by JAMES A. COX and MARK W. RAWSMUSSEN, Science & Technology Law 2018. pp. 87 ff. & 90-112.

(11) ビットバンク株式会社ほか・前掲注(2)二六五頁。

(12) 分散型台帳のブロックチェーンにおける支払手段の仕組みとして始まった暗号資産は、今日、日本国内でも、大手量販店のほか、飲食店や美容室、ホテル、オンラインショッピングモールなどで、徐々に広まりつつある。ＰｗＣあらた有限責任監督法人［編］・前掲書四頁。ちなみに、近時の金融商品取引法の改正により、それまでセキュリティ・トークンと呼ばれていたものが金融商品取引法において明記され、暗号資産の範囲から除かれたことで、資金決済法ではなく、金融商品取引法によって規制されることになった。詳細は、ＰｗＣあらた有限責任監督法人［編］・前掲注(6)五四頁以下。

(13) ビットバンク株式会社ほか・前掲注(2)一四七頁。

(14) 長谷川・前掲注(1)五二頁。

(15) 福岡編・前掲注(8)二一頁以下。

(16) 長谷川・前掲注(1)四〇頁。詳しくは、Fahrshad Ghodoosi, *Digital Solidarity: Contracting in the Age of Smart Contracts*, 29 ff., at https://ssrn.com/abstract=3449674 (2019).

(17) Ghodoosi, *supra* note 16, at 17 ff.; Daniel Markovits, *Contract and Collaboration*, 113 Yale L. J. 1417, 1419 (2003). わが国でも同様の指摘がなされている。増島雅和「スマートコントラクトの法的側面について」翁百合ほか編著『ブロックチェーンの未来』（日本経済新聞社、二〇一七年）二〇七頁以下、二一三頁［増島雅和］、小出篤「分散台帳技術と法制度」ジュリスト一五二九号（二〇一九年）二一頁以下、二六―二七頁。

(18) わが国では、ブロックチェーン技術との関連で、技術的側面からスマートコントラクトが取り上げられることが多かった。加藤長門ほか『スマートコントラクト開発』（マイナビ、二〇一九年）二頁以下、コンセンサス・ベイス株式会社『ブロック

チェーンのしくみと開発がこれ一冊でしっかりわかる教科書』（技術評論社、二〇一九年）一七三頁以下、森川夢佑斗『これからのブロックチェーンビジネス』（ＭｄＮ、二〇一八年）三〇頁以下、鳥谷部昭寛ほか『スマートコントラクト本格入門』（技術評論社、二〇一七年）六八頁以下、赤羽喜治「分散台帳技術とは何か」ジュリスト一五二九号（二〇一九年）一四頁以下、翁ほか編著・前掲注(11)一五四頁、一九七頁以下［柳川範之］、二〇七頁以下［増島雅和］、ビットバンク株式会社＆『ブロックチェーンの衝撃』編集委員会・前掲注(2)一八頁、二五二頁以下など。なお、柳川範之「ブロックチェーン技術にはどのような応用可能性があるのか」翁ほか編著・前掲注(17)一四五頁以下、一六三頁参照。

(19) Arcari, *supra* note 7, at 370-372; Jonathan G. Rohr, *Smart Contracts and Traditional Contract Law, Or: The Law of the Vending Machine*, 67 Clev. St. L. Rev. 71, 73-74 (2019); Sarah Templin. *Blocked-Chain: The Application of the Unauthorized Practice of Law to Smart Contracts*, 32 Georg. J. Legal Ethics 958-962 (2019); Mark Verstraete, *The Stakes of Smart Contracs*, 50 Loy. U. Chi. L. J. 743, 746-757, 778-780 (2019); Maren Woebbeking, *The Impact of Smart Contracts on Traditional Concepts of Contract law*, 10 J. Intell. Prop. Infa. Tech. & Elec. Con. L. 105, 106 (2019) など。わが国では、増島・前掲注(18)二〇七頁以下、同「ブロックチェーン技術を用いたスマートコントラクトの検討」ＮＢＬ一〇九三号（二〇一七年）二八頁以下、小出・前掲注(17)二一頁以下、倉橋雄作「スマートコントラクトの法的分析と実務対応」ＮＢＬ一一二五号（二〇一八年）八六頁、木下信行「スマートコントラクトについて」ＮＢＬ一一一〇号（二〇一七年）四頁、木村真生子「ＡＩと契約」弥永真生・宍戸常寿編『ロボット・ＡＩと法』（有斐閣、二〇一八年）一三一頁以下、森剛敏＝上田綾乃「ブロックチェーン技術におけるスマートコントラクトの可能性と課題」金融財政事情六八巻七号（二〇一七年）三〇頁以下、橘大地「スマートコントラクト時代における裁判以外の紛争解決可能性」ビジネス法務一八巻九号（二〇一八年）九二頁以下、小塚壮一郎「スマートコントラクトとＣＩＳＧ」ジュリ一五六九号（二〇二一年）一四頁以下など。

(20) スマートコントラクトが従来の伝統的な契約理論に取って代わられる可能性を有するとの指摘もある。Adam Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, 21 Stan. Tech. L. Rev. 198, 221-222 (2019).

(21) Templin, *supra* note 19, at 958-962; Verstraete, *supra* note 19, at 746-757, 778-780; Arcari, *supra* note 7, at 365-366,

370-372; Rohr, *supra* note 19, at 3-74; Woebbeking, *supra* note 19, at 106など

(22)　文献などの紹介も含めて，詳細は，長谷川・前掲注(1)五九頁以下。

(23)　長谷川・前掲注(1)四〇―四一頁。

(24)　ビットバンク株式会社ほか・前掲注(2)一八頁。

(25)　Arcari, *supra* note 7, at 370.

(26)　Woebbeking, *supra* note 19, at 106.

(27)　Alexander Savelyev, *Contract Law 2.0 ≪SMART≫ Contracts as the Beginning of the End of Classic Contract Law*, National Research University Higher School of Economics WP BRP71/LAW/2016, 8; 自動型水機の考案につき，KERRT SEGRAVE,VENDING MACHINES: AN AMERICAN SOCIAL HISTORY, McFarland, 2002, p.3.

(28)　Sati Agnikhotram & Antonios Kouroutaki, *Doctrinal Challenges for the Legality of Smart Contarcts: Lex Cryptographia or a New, 'Smart' Way to Contract?*, 19 J. High Tech. L. 300, 312 (2019).

(29)　長谷川・前掲注(1)四四頁。スザボの著作として，Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, Extropy (1996), available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html; ID., Smart Contracts: *Formalizing and Securing Relationships on Public Networks,* Monday 2 (9), Article 1 (1997), abailable at https://doi.org/10.5210/fm.v2i9.548など。スザボの人物像を含めて，詳しくは，Rory Unsworth, *Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for "Self-excuting" Contracts*, in LEGAL TECH, SMART CONTRACTS AND BLOCKCHAIN, edited by MARCELO CORRALES et al., Springer 2019, 17 ff.; Nathan Reiff, *Who is Nick Szabo, and Is he Satoshi Nakamoto*, INVESTOPEDIA, Apr. 12, 2018, available at https://www.investopedia.com/news/who-nick-szabo-and-he-satoshi-nakamoto/.

(30)　前掲注(18)および後掲注(65)参照。

(31) Morgan N. Temte, *Blockchain Challenges Traditional Contract law: Just How Smart Are Smart Contracts?*, 19 Wyo. L. Rev. 87, 94 (2019)

(32) A. Walch, *The Path of the Blockchain Lexion (and the Law)*, 36 Rev. Banking & Fin. L. 713 (2016). ビットコインとその中核技術であるブロックチェーンとの関係につき、畠山久志編著『仮想通貨法の仕組みと実務』(日本加除出版、二〇一八年)六一頁、PwCあらた有限責任監査法人[編]『仮想通貨の会計・税務・監査』(中央経済社、二〇一八年)二頁以下など。

(33) Kelvin F.k. Low and Eliza Mik, *Pause the Blockchain Legal Revolution* (2019), p. 25, available at SSRN: https://ssrn.com/abstract=3439918; Arcari, *supra* note 5, at 367; Temte, *supra* note 31, at 94; Rohr, *supra* note 19, at 79; Mckinney et al., *supra* note 2, at 313; Schrepel, *supra* note 4, at 142; Templin, *supra* note 19, at 957, Finocchiaro & Bomprezzi, *supra* note 4, at 113など。

(34) Jean Bacon et al., *Blockchain Demystified: A Legal and Legal Introduction to Distributed and Centralized Ledgers*, 25 Rich. J. L. & Tech. 1 (2019). 正田正樹ほか『ブロックチェーンがひらく「あたらしい経済」』(幻冬舎、二〇二〇年)一六九頁、一七二頁。

(35) 小出篤「『分散型台帳』の法的問題・序論―『ブロックチェーン』を契機として」江頭憲治郎先生古稀記念『企業法の進路』(有斐閣、二〇一七年)八二七頁以下、赤羽・前掲注(18)一四頁以下。

(36) この点の指摘につき、野口悠紀雄『ブロックチェーン革命[新版]』〈日経ビジネス文庫〉(日経BP社、二〇二〇年)二九五頁参照。

(37) R. Maull et al., *Distributed Ledger Technology: Applications and Implications*, 26 Strategic Change 481, 483 (2017). 野口・前掲注(36)一四―一五頁。

(38) ビットバンク株式会社ほか・前掲注(2)二五頁。

(39) 長谷川・前掲注(1)三七頁以下、六四頁、一〇三頁注(41)。詳しくは、佐藤一郎「コラム『ビザンチン将軍問題』とは何か」NII Today六九号(二〇一五年)八頁以下。

(40) Leslie Lamport et al., *The Byzantine problems*. https://doi.org/10.1145/357172.357176

(41) 野口・前掲注(36)五三―五四頁。

(42) ハッシュ値は、これから記録しようとする新たなブロックの内容をもとに、ハッシュ関数を使った計算で導き出される。マイナーは、ブロック内の自由に変更できる領域に適当な数（ナンス）を書き込み、ナンスの変更とハッシュ計算を繰り返しながら、ある難易度の条件を満たすハッシュ値を見つけるまでノードに計算を行わせる。正田ほか・前掲注(34)一六九頁。

(43) 正田ほか・前掲注(34)一六九頁。

(44) 正田ほか・前掲注(42)一七二頁。

(45) 正田ほか・前掲注(42)二〇四頁。

(46) 正田ほか・前掲注(42)二〇八頁。

(47) ビットバンク株式会社ほか・前掲注(2)二六頁。

(48) 正田ほか・前掲注(34)一〇七頁。

(49) ＰｗＣあらた有限責任監督法人［編］・前掲注(6)一二一頁。

(50) ＰｗＣあらた有限責任監督法人［編］・前掲注(6)一二三頁。

(51) ＰｗＣあらた有限責任監督法人［編］・前掲注(6)一二三頁以下、正田ほか・前掲注(42)一〇七頁以下

(52) ビットバンク株式会社ほか・前掲注(2)一四七頁。

(53) ビットバンク株式会社ほか・前掲注(2)七三頁。

(54) ＰｗＣあらた有限責任監督法人［編］・前掲注(6)一二一頁。

(55) もっとも、ブロックチェーンの検証プロセスにおけるマイニングは必要な時間と費用を用することから特定のノードに集中しており、多数派のルールが不利に扱われる可能性がある。そうであれば、ブロックチェーンのコンセンサス・アルゴリズムは、粗雑な民主主義といわねばならない。Low and Mik, *supra* note 33, at 6.

(56) 正田ほか・前掲注(34)二〇五頁。

(57) 正田ほか・前掲注(34)一二〇四―一二〇五頁。このほか、ブロックチェーンにおける合意形成のメカニズムには、PoWとPoSを組み合わせたプルーフ・オブ・アクティビティという方式もある。これは、マイナーが生成したブロックはそのままでは仕えず、参加者からランダムに選ばれた人たちの署名を経て初めて有効となる。詳しくは、ビットバンク株式会社ほか・前掲注(2)一六六頁以下、ドン・タスコット、アレックス・タスコット／高橋璃子・訳『ブロックチェーン・レボリューション―ビットコインを支える技術はどのようにビジネスと経済、そして世界を変えるのか』（ダイヤモンド社、二〇一六年）四一―四二頁。

(58) The DAO 事件の概要については、Virginia Valenzuela, *The History of the DAO* (Feb. 1, 2022), available at https://editorial.superrare.com/2021/11/17/the-history-of-the-dao/; Quinn DuPont, *Experiments in Algorithmic Governance: A History and Ethnography of "The DAO," a Failed Decentralized Autonomous Organization*, in BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAIN, AND GLOBAL GVERNANCE edited by MALCOLM CAMPBELL-VERDUYN (Routledge 2017) pp. 157 ff.; Osman Gazi Güçlütürk, *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts* (Aug. 1, 2018), available at https://ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562; Latia Metjahic, *Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organization*, 39 Cardozo L. Rev. 1533 (2018) などに詳しい。なお、併せて、K.F.K. Low and E.G.S. *Teo, Bitcoins and Other Cryptocurrencies as Property?*, 9 L.I.T. 235 (2017); Kolber, *supra* note 20, 198ff. 参照。

(59) Low & Mik, *supra* note 33, at 8.

(60) Peder Østbye, *Exploring DAO Members' Individual Liability* (Feb. 28, 2022), available at https://ssrn.com/abstract=4045799.

(61) Low & Mik, *supra* note 33, at 23.

(62) V. Buterin, *Ethereum* (White Paper): *A Next Generation Smart Contract and Decentralized Application Platform* (2015), available at https://github.com/ethereum/wiki/wiki/White-Paper.

(63) Gabriel Jacard, *Smart Contracts and the Role of Law*, 22 (2017), available at https://ssrn.com/abstract=3099885.

(64) Low and Mik, *supra* note 33, at 29.

(65) 唐澤光彦「ブロックチェーンの基礎知識と合意形成アルゴリズム」（二〇一八年）一頁以下。https://dcross.impress.co.jp/docs/column/column20180725-01/000730-3.html。赤羽＝愛敬・前掲注(4)一三四頁。

(66) 唐沢・前掲注(65)三頁、赤羽＝愛敬・前掲注(4)一三一頁。

(67) 赤羽＝愛敬・前掲注(4)一一九頁以下。

(68) リテシュ・モディ／花山直親ほか訳『Solidity プログラミング：ブロックチェーン・スマートコントラクト開発入門』（講談社、二〇一九年）一二〇頁、五一頁以下、クリス・ダネン／ウイリング訳『Ethereum＋Solidity 入門』（インプレス、二〇一九年）一一五頁以下。

(69) 鳥谷部・前掲注(18)八三頁以下、Smart Contracts Alliance, Smart Contracts: 12 Cases for Business & Beyond, Chamber of Digital Commerce (2016) は一二の応用例を図解入りで解説している。

(70) PwCあらた有限責任監査法人［編］・前掲注(6)二八頁以下。

(71) 正田ほか・前掲注(34)五一頁以下。

(72) PwCあらた有限責任監査法人［編］・前掲注(6)一三八頁。

(73) 正田ほか・前掲注(34)一一六頁。

(74) 正田ほか・前掲注(34)一一六頁。

(75) 正田ほか・前掲注(34)一一五頁。

(76) Stuart D. Levi and Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATIONS (2018), available at https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

(77) Harry Surden, *Computable Contract*, 46 U.C. DAVIS L. REV. 629, 656 (2016).

(78) Kolber, *supra* note 20, at 220; Bellia, *supra* note 8, at 1065.

(79) Bellia, *supra* note 8, at 1058-1059.

(80) この議論の詳細は，長谷川・前掲注(1)五八頁。

(81) Temte, *supra* note 31, at 94; Agnikhotram & kouroutaki, *supra* note 28, at 301-302; Peach, *supra* note 4, at 3; Templin, *supra* note 19, at 959など。

(82) 長谷川・前掲注(1)五八頁。

(83) Szabo, *supra* note 28 (*Formalizing and Securing Relationships on Publicnetworks*), First Monday 2, No. 9.

(84) Karen Yeung, *Regulation by Blockchain: the Emerging Battle for SupremacyBetween the Codes of Law and Code as Law*, 82 M.L.R. 207, 220, 224 (2019); Larry A. DiMatteo et al., *Smart Contracts and Contract Law*, in THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORM, edited by LARRY A. DIMATTEO et al., Cambridge University press 2020, at 4.

(85) Yeung, *supra* note 84, at 236, 239; Gatteschi et al., *supra* note 7, at 53; Matteo et al., *supra* note 84, at 4 et seq., 10.

(86) タスコット，タスコット／高橋訳・前掲注(57)二二六頁。

(87) 正田ほか。前掲注(34)八八頁。

(88) ローレンス・レッシグ／山形浩生・柏木亮二［訳］『Code: インターネットの合法・違法・プライバシー』（翔泳社，二〇〇一年）三頁以下，七七頁以下。

(89) Yeung, *supra* note 84, at 209, 215-216, 219-220; Savelyev, *supra* note 27, at 14. 詳しくは，後注(103)―(106)参照。

(90) 新たなテクノロジーに対する法的規制の必要性と法律家の役割につき，Frank A. Pasquale and Glyn Cashwell, *Four Futures of Legal Automation*, 63 UCLA. L. Rev. Discource 26 (2015).

(91) 詳しくは，長谷川・前掲注(1)六八―六九頁，Arcari, *supra* note 7, at 365-366.

(92)　前稿で簡単に検討した。長谷川・前掲注(1)一九四頁。なお、小出・前掲注(17)二一頁以下、一二六頁参照。近時のアメリカ法の動向につき、ANDREA STAZI, SMART CONTRACTS AND COMPARATIVE LAW: A WESTERN PERSPECTIVE, Springer 2021, 75 ff.; A. Papantoniou, *Smart Contracts in the New Era of Contract Law*, 1 Digital L. J. 1, 4 ff. (2020), available at https://ssrn.com/abstract=3950988; G. Finocchiaro and C. Bomprezzi, *supra*. note 4. at 115-117.　概括的にいえば、学説は、スマートコントラクトには従来の伝統的な契約と同等の法的効力を有すると考えるなど、スマートコントラクトを過大に評価する傾向にある。この背景には、スマートコントラクトでは特定の条件を満たせばコンピュータのプログラムコードで自動的に処理されることを当事者が合意していたとする当事者の意図が尊重されているように思われる。この点につき、H. Surden, *Computable contracts*, 46 (2) UC Davis L. Rev. 629 (2012) ; J. Stark, *Making Sense of Blockchain Smart Contracts*, CoinDesk (2016). www.coindesk.com/making-sense-smart-contracts など参照。スマートコントラクトによる契約の自動化と自己執行力といった利点は、従来の伝統的な契約への依存を縮小させるものであるが、強制力を契約の本質と理解する限り、従来の契約と根本的な違いはないといえる。

(93)　議論の現況につき、Chodoosi, *supra* note 16, at 29ff.; Amy J. Schmitz and Colin Rule, *Online Dispute Resolution for Smart Contracts*, 2019 J. Disp. Resol. 103, 110ff. (2019) など。

(94)　Lon Luvois Fuller & William R. Perdue, *Reliance Interest in Contract Damages: 1*, 46 Yale L. J. 52, 87 (1936).

(95)　Ghodoosi, *supra* note 16, at 46.

(96)　Ghodoosi, *supra* note 16, at 32.

(97)　Ghodoosi, *supra* note 16, at 47.

(98)　正田ほか・前掲注(34)一四二頁。

(99)　野口・前掲注(36)二六六―二六七頁。

(100)　Garcia Rolo, António, *Challenges in the Legal Qualification of Decentralised Autonomous Organisations (DAOs): The Rise of the Crypto-Partnership?* (2018), available at https://ssrn.com/abstract=3417900; Wulf A. Kaal, *Decentralized*

Autonomous Organizations – Internal Governance and External Legal Design (2020), available at https://ssrn.com/abstract=3652481; Peder Østbye, *Exploring DAO Members' Individual Liability* (2022), available at https://ssrn.com/abstract=4045799など。

(101) 正田ほか・前掲注(34)一四二頁以下。

(102) ビックバン株式会社ほか・前掲注(2)六五―六六頁。

(103) Minni Zou, *Code, and other Laws of Blockchain*, 40 (3) Oxford J. Legal Stud. 645 (2020) ; Florian Möslein, *Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions* (May 1, 2018), available at https://ssrn.com/abstract=3174823.

(104) 多くの文献があるが、Primavera De Filippi & Aaron Wright の BLOCKCHAIN AND THE LAW: THE RULE OF CODE (Harvard University Press , 2018) ; 同書の翻訳として、『ブロックチェーンと法：「暗号の法」（レックス・クリプトグラフィカ）がもたらすコードの支配』プリマヴェラ・デ・フィリッピ、アーロン・ライト／片桐直人編訳（弘文堂、二〇二〇年）と Kevin Werbach の BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (MT Press, 2018) ; 同書の翻訳として、『ブロックチェーンの技術と革新：ブロックチェーンが変える信頼の世界』ケビン・ワーバック／山崎裕貴訳（ニュートンプレス、二〇二一年）は、非常に思慮深い専門書である。どちらも「法としてのコード」を共通のテーマとして取り上げ、分散型ブロックチェーンネットワークが独自のルールを備えた規制のアーキテクチャとみなしうるとしている。両書の分析につき、Zou, *supra* note 103, at 647 ff.

(105) Karen E. C. Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law*, 3 Engaging Science, Technology, and Society 1 (2017).

(106) Levi and Lipton, *supra* note 76, at "Governing Law and Venue".